Investigating Advances in the Acquisition of Secure Systems Based on Open Architecture , Open Source Software, and Software Product Lines

Grant #N00244-10-1-0077

Walt Scacchi and Thomas A. Alspaugh
Institute for Software Research
University of California, Irvine
Irvine, CA 92697-3455 USA
{wscacchi, alspaugh}@ics.uci.edu

Final Report
November 2011

Executive Summary

In 2007-08, we began an investigation of problems, issues, and opportunities that arise during the acquisition of software systems that rely on open architectures and open source software. The current effort funded for 2010-2011 seeks to continue and build on the results in this area, while refining its focus to center on the essential constraints and tradeoffs we have identified for software-intensive systems with open architecture (OA) and continuously evolving open source software (OSS) elements. The U.S. Air Force, Army, and Navy have all committed to an open technology development strategy that encourages the acquisition of software systems whose requirements include the development or composition of an OA for such systems, and the use of OSS systems, components, or development processes when appropriate. Our goal is to further develop and document foundations for emerging policy and guidance for acquiring software systems that require OA and that incorporate OSS elements.

The research described in this final report focuses on continuing investigation and refinement of techniques for reducing the acquisition costs of complex software systems. Over the past three years, we have investigated, demonstrated and refined techniques and tools that articulate interaction between system requirements and software architecture that can increase or decrease the cost of software system acquisition. We have developed software architecture modeling techniques, notational schemes, and formal logic that can be incorporated into automated tools that allow for the construction of open architecture systems using proprietary and open source software components. Such capabilities allow for increase choice and flexibility for how best to satisfy system requirements through alternative software architectures that can accommodate different components and system configurations. Such capabilities help reduce system acquisition costs. In the proposed effort, we continue these investigations by incorporating *reusable software product line (SPL) techniques* within OA systems composed from proprietary and open source software (OSS) components subject to different intellectual property rights licenses, and where *software components are subject to different security requirements.* The combination of SPLs and OSS components within secure OA systems represents a significant opportunity for reducing the acquisition costs of software-intensive systems by the DoD and other government agencies.

This report documents and describes the findings and results that we have produced as a result of our research into the area of the acquisition of software systems that rely on OA, OSS and SPLs. In particular, it includes four research papers that have been refereed, reviewed, presented, and published in national and international research conferences, symposia, and workshops.

The first of these papers [Scacchi and Alspaugh 2011] was originally presented at the 2011 Acquisition Research Symposium in May 2011. Three other refereed research papers were also produced, two included at international research conferences [Alspaugh, Asuncion and Scacchi 2011, Scacchi 2011b], one of which received a **Best Paper** award [Scacchi 2011b], and a preliminary study at an international research workshop [Scacchi 2011a] held for the first time on games and software engineering, at the *33rd International Conference on Software Engineering* (May 2011). All four of these research publications are included in this report.

Finally, our efforts addressing OSS modding, computer games, and game-based virtual worlds [Scacchi 2011a,b] were leveraged in a related study [Scacchi, Brown, and Nies 2011] sponsored by the Center for the Edge at the Naval Postgraduate School, where we applied these methods to explore and demonstrate the ability to rapidly prototype SPL-based OA systems for military command and control (C2) systems.

Table of Contents

Executive Summary.....2
Research Description.....5
Advances in the Acquisition of Secure Systems Based on Open Architectures.....18
Presenting Software License Conflicts through Argumentation.....36
Modding as an Open Source Approach to Extending Computer Game Systems.....42
Modding as a Basis for Developing Game Systems.....56

Research Description

In this research effort, we investigated the incorporation of reusable software product line (SPL) techniques within open architecture (OA) systems composed from proprietary and open source software (OSS) components subject to different intellectual property rights licenses, and where software components are subject to different security requirements. The combination of SPLs and OSS components within *secure OA systems* represents a significant opportunity for reducing the acquisition costs of software-intensive systems by the DoD and other government agencies. This effort builds on both our prior acquisition research, and related acquisition research efforts at the PEO IWS [Guertin and Clements 2010] and Software Engineering Institute (SEI) [Bergey and Jones 2010] that address SPLs, as well as SEI efforts addressing OSS [Hissam, *et al.* 2010].

OSS is an integrated web of people, processes, and organizations, including project teams operating as virtual organizations [Scacchi 2007, 2009]. There is a basic need to understand how to identify an optimal mix of OSS within OA systems as products, production processes, practices, community activities, and multi-project (or multi-organization) software ecosystem. However, the relationship among OA, OSS, requirements, and acquisition is poorly understood [cf. Scacchi 2009, Naegle and Petross 2007]. Subsequently, in 2007-08, we began by examining how different OSS licenses can encumber software systems with OA, which therefore give rise to new requirements for how best to acquire software-intensive systems with OA and OSS elements [Scacchi and Alspaugh 2008]. As a result of our most recent efforts [Scacchi, Alspaugh, and Asuncion 2010] we have been able to demonstrate that for enterprise information systems, which are widespread throughout DoD and the U.S. government, it is both possible and feasible to develop systems that incorporate best-of-breed software components, whether proprietary or OSS, in ways that can reduce the initial and sustaining acquisition costs of such systems. Doing so however requires automated tools for explicitly modeling the architecture of the OA system during its development and evolution, along with modeling the annotating the architecture with software component licenses. Our results thus demonstrate a major technological advance in the acquisition and development of OA systems, as a breakthrough in negotiating and simplifying software license analyses

throughout the contracting activities.

Two lines of inquiry follow from our accomplishments described above and in detail elsewhere [Alspaugh, Asuncion, and Scacchi 2009a,b,c, Scacchi, Alspaugh, and Asuncion 2010]. One is how our results might shed light on software systems whose architectures articulate a *software product line*, while the other is how our approach might be extended to also address the semantic modeling and analysis of *software system security requirements.*

Software Product Lines and OA Systems research problem:

Organizing and developing software product lines (SPLs) relies on the development and use of explicit software architectures [Bosch 2001, Clements and Northrop 2003]. However, the architecture of a SPL is not necessarily an OA — there is no requirement for it to be so. Thus, we are interested in discussing what happens when SPLs may conform to an OA, which is a concern we shared with others [Guertin and Clements 2010]. In particular, our interest here is to consider an OA system that incorporates heterogeneously licensed SPL components. Three considerations come to mind. First, If the SPL is subject to a single homogeneous software license, which may often be the case when a single vendor or government contractor has developed the SPL, then the license may act to reinforce a vendor lock-in situation with its customers. One of the motivating factors for OA is the desire to avoid such lock-in, whether or not the SPL components have open or standards-compliant APIs. Second, if an OA system employs a reference architecture much like we have in the design-time architecture depicted in Figure 1, which is then instantiated into a specific software product configuration, as suggested in the build-time architecture shown in Figure 2, then such a reference or design-time architecture as we have presented it here effectively defines a SPL consisting of possible different system instantiations composed from similar components instances (e.g., different but equivalent Web browsers, word processors, email, calendaring applications, relational database management systems). Third, if the SPL is based on an OA that integrates software components from multiple vendors or OSS components that are subject to heterogeneous licenses, then we have the situation analogous to what we have presented in our previous work [Alspaugh, Asuncion, and Scacchi 2009a,b,c, Scacchi, Alspaugh, and Asuncion 2010]. This leads us to conclude that SPL

concepts are compatible with OA systems that are composed from heterogeneously licensed components. Consequently, in this effort, we sought *to systematically investigate, model, and analyze how this might work in both (a) enterprise information systems, and (b) command-and-control or related weapons systems, if/when they incorporate OSS and non-OSS components subject to different security licenses.* Our goal was to demonstrate what is possible and feasible, as well as how feasible alternatives facilitate cost reduction opportunities in system acquisition efforts.

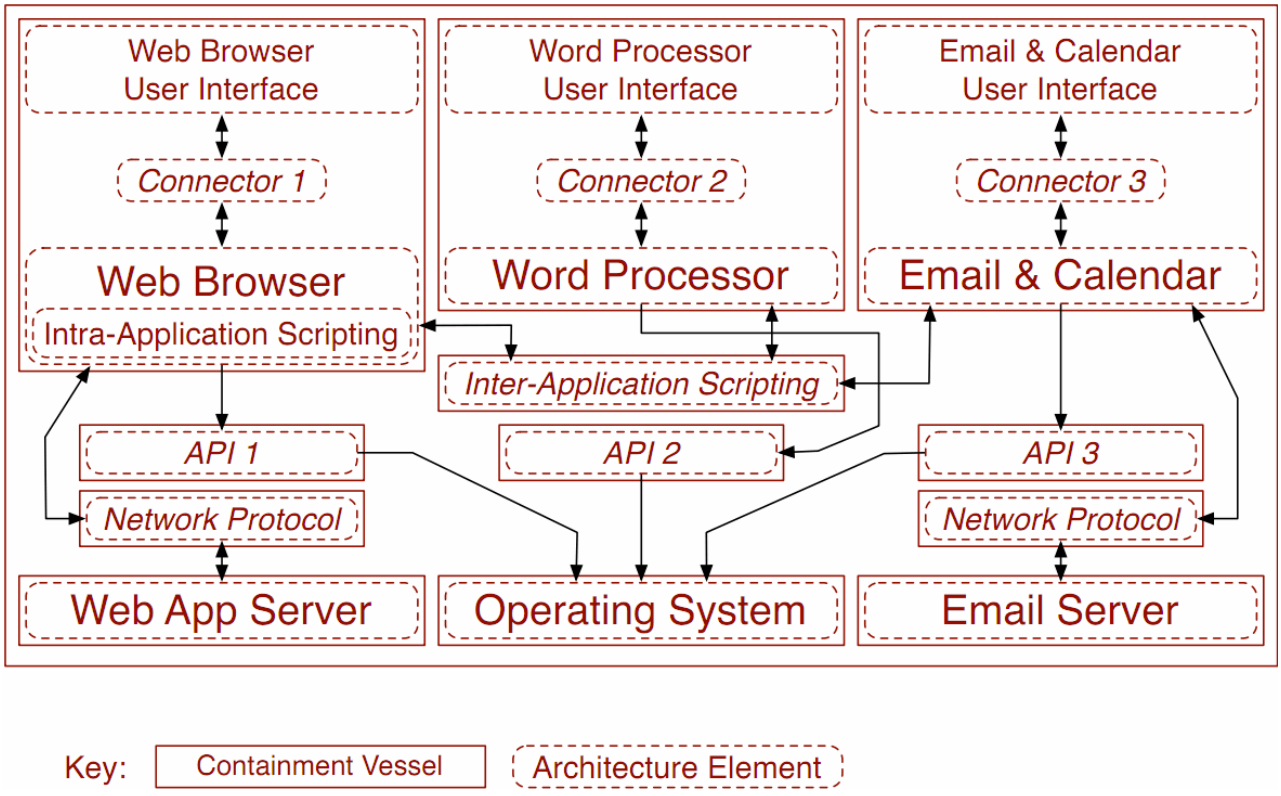

Figure 1. A design-time reference architecture or SPL for a secure enterprise information system consisting of a Web browser, word processor, email and calendaring applications, hosted on a network of servers and host operating system, each within its own secure "confinement vessel" as a virtual machine [Scacchi and Alspaugh 2011].

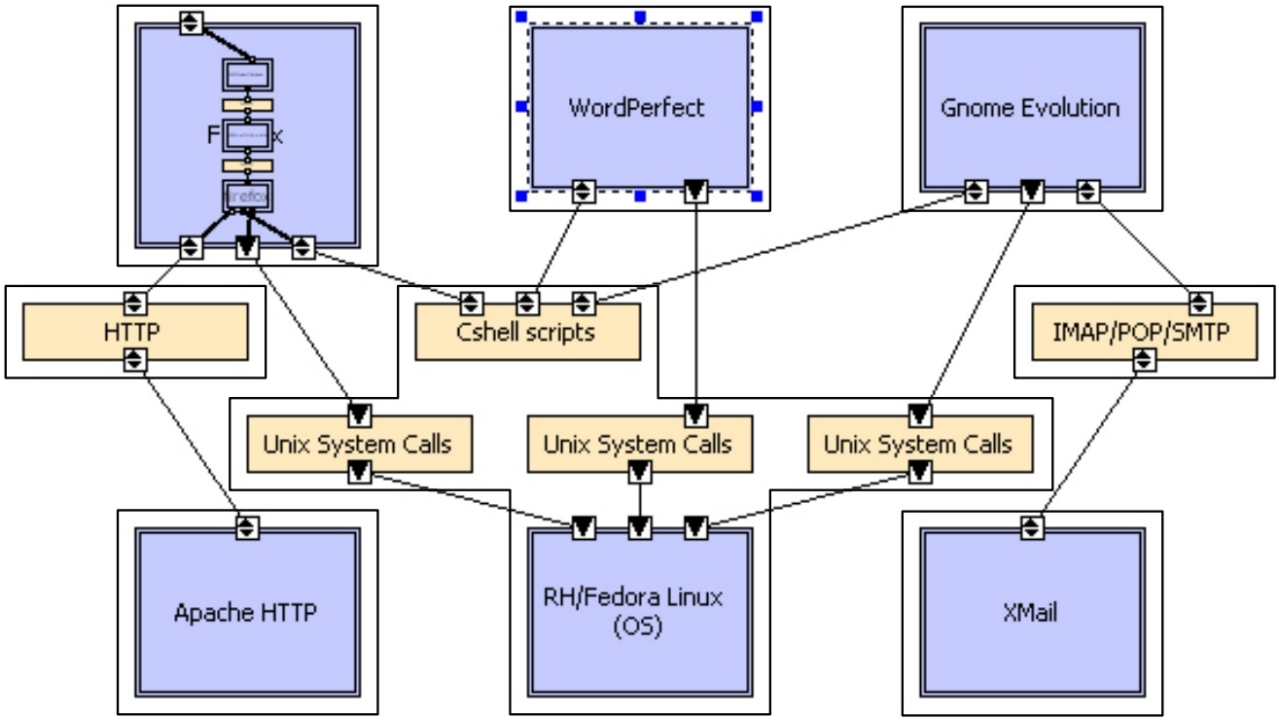

Figure 2. A build-time OA instance for a secure enterprise information system consisting of a Web browser, word processor, email and calendaring applications, hosted on a network of servers and host operating system, using a mixed security confinement configuration [Scacchi and Alspaugh 2011].

Software component security within OA systems research problem:

As already noted in our previous work [Alspaugh, Asuncion, and Scacchi 2009a,b,c, Scacchi, Alspaugh, and Asuncion 2010], software component licenses represent a collection of rights and obligations for what can or cannot be done with a licensed software component. Licenses thus denote non- functional requirements that apply to a software systems or system components as intellectual property (IP) during their development and deployment. But rights and obligations are not limited to concerns or constraints applicable only to software as IP. Instead, they can be written in ways that stipulate non-functional requirements of different kinds. Consider, for example, that desired or necessary software system security properties can also be expressed as rights and obligations addressing system confidentiality, integrity,

accountability, system availability, and assurance [Breaux and Anton, 2005, 2008].

Traditionally, developing robust specifications for non-functional software system security properties in natural language often produces specifications that are ambiguous, misleading, inconsistent across system components, and lacking sufficient details [Yau and Chen 2006]. Using a semantic model to formally specify the rights and obligations required for a software system or component to be secure [Breaux and Anton, 2005, 2008, Yau and Chen 2006] means that it may be possible to develop both a "security architecture" notation and model specification that associates given security rights and obligations across a software system, or system of systems. Similarly, it suggests the possibility of developing computational tools or interactive architecture development environments that can be used to specify, model, and analyze a software system's security architecture at different times in its development — design-time, build- time, and run-time.

The approach we have been developing for the past few years for modeling and analyzing software system license architectures for OA systems [Alspaugh, Asuncion, and Scacchi 2009a,b,c, Scacchi and Alspaugh 2008, Scacchi, Alspaugh, and Asuncion 2010], can be extended to also address OA systems with heterogeneous "software security license" rights and obligations. Furthermore, the idea of common or *reusable software security licenses* may be analogous to the reusable security requirements templates proposed by Firesmith [2004] at the SEI. Consequently, such *an exploration and extension of the semantic software license modeling, meta-modeling, and computational analysis tools to also support secure OA systems* was the next stage of our research studies, which we recently demonstrated and described [Scacchi and Alspaugh 2011].

To help motivate our approach to realizing the results presented in this final report, we provide some background on emerging issues in the acquisition of software-intensive systems that require OA and encourage or embrace the utilization of OSS, such as rapid, distributed evolution to meet immediate warfighter needs and its interplay with validation and system management. Next, we describe the body of this research effort. This covers the problem, issues, opportunities, and approach for acquisition research we identify. Following this, we

describe our prospects for longer-term acquisition-related research.

Background

Across the three military services within the DoD, OA means different things and is seen as the basis for realizing different kinds of outcomes [Scacchi and Alspaugh 2008]. Thus, it is unclear whether the acquisition of a software system that is required to incorporate an OA, as well as utilize OSS technology and development processes [Wheeler 2007], for one military service will realize the same kinds of benefits anticipated for OA-based systems by another service. Somehow, DoD acquisition program managers must make sense of or reconcile such differences in expectations and outcomes from OA strategies in each service and across DoD. Yet there is little explicit guidance or reliance on systematic empirical studies for how best to develop, deploy, and sustain complex software-intensive military systems in the different OA and OSS presentations and documents that have so far been disseminated [Starrett 2007, Weathersby 2007, Wheeler 2007], though [Hissam, *et al*. 2010] does mark a progressive effort to change this.

It is becoming clear that verification and validation (V&V) is a crucial activity for OSS in OA. Two key benefits of OSS are its reliability and its openness to rapid, agile evolution in response to changing needs. Following Scacchi and Alspaugh [2008], we envision that warfighters will be not only users of OSS but also as contributing “developers” or “modders” [Scacchi 2011a, 2011b] to it, as they know what is needed "right now" to give them the edge over their opponents and are best placed to translate that quickly into new system capabilities. However, it is still important that OSS/OA systems be reliable and remain open. The benefit of having a new feature to respond to a current threat is reduced if the change causes a needed existing feature to stop working, or in the worst case causes the system to fail unexpectedly. With development activities extended out close to "the tip of the spear" it is also necessary to extend V&V out to the same developers and their quick-response development. Not only do they need to be able to quickly validate the changes they have made, they also need to be able to do quick, highly automated regression testing to identify any existing functions that the new changes have interfered with. At the same time, DoD needs a structure for managing the evolution of OSS and OA systems at higher levels, to deal

with the decisions of which "spear-tip" changes to fold into the system for larger groups of users, and when, and to resolve the inevitable conflicts that will arise as different groups of developers take the system in different, sometimes conflicting directions. In addition, verification must confirm that the changed system remains open, as well as correct. V&V must be done quickly and convincingly at these broader levels as well, and will be important in supporting decisions about which modifications to disseminate when. The recent work Berzins [2008] presented shows one approach that applies a high degree of automation to make regression testing more efficient and manageable in response to modifications.

The V&V issues surface a key issue for OA, as for any architecture: how to choose and evolve a specific OA in order to support effective, efficient V&V. Architectural structure is typically used to modularize V&V, so that it can be made more manageable with a "divide and conquer" approach. With the increased importance and frequency of V&V in OSS and OA systems, verifiability becomes a key quality for OA. Ensuring that the architecture is open may be only a first step; the OA's support of verifiability may be necessary for it to be of practical value, and for the OA system to achieve its goals.

Subsequently, this leads us to consider the following questions: what is the problem for acquisition research into secure OA systems that incorporate SPLs and OSS? What issues or research questions for acquisition research follow from such a problem? What research approach can best explore the opportunities for acquisition research built from related research efforts in OSS and SPLs and software architectural analysis that can also inform future acquisition cost reduction practices? We now turn to briefly elaborate these questions in turn through the remainder of this research report overview.

Problem for Acquisition Research

OA seems to imply software system architectures incorporating OSS components and open application program interfaces (APIs), while also conforming to open standards. But not all software system architectures incorporating OSS components, open APIs, and open standards will produce OA [cf. Scacchi and Alspaugh 2008], since OA depends on: (a) how/why OSS and open APIs are located within the system architecture, (b) how OSS and open APIs are implemented, embedded, or interconnected, (c) whether the copyright licenses

assigned to different OSS components encumber all/part of a software system's architecture into which they are integrated. Similarly, (d) alternative architectural configurations and APIs for a given system may or may not produce an OA at design-time, build-time, or release and run-time [Alspauch, Asuncion, Scacchi 2009a,b, 2010]. Subsequently, we believe this can lead to situations in which if program acquisition stipulates a software-intensive system with an OA and OSS, and the architectural design of a system constrains system requirements (i.e., what requirements can be satisfied by a given system architecture, or given system requirements what architecture is implied), then the resulting software system may or may not embody an OA.

Given the goal of realizing secure OA systems, together with the use of evolving OSS components, SPLs, and open APIs, *how should program acquisition, system requirements, software V&V, open architectures, and post-deployment system support be aligned to achieve this goal?* As such, this is a core research problem we seek to investigate in order to identify principles, best practices, and knowledge for how best to insure the success of the OA strategy when OSS and open APIs are required or otherwise employed. Without such knowledge, program acquisition managers and PEOs are unlikely to acquire software-intensive systems that will result in an OA that is clean, robust and transparent. This may frustrate the ability of program managers or PEOs to realize faster, better, and cheaper software acquisition, development, and post-deployment support.

Issues for Acquisition Research

Based on current research into the acquisition of OA systems with OSS components [Scacchi and Alspaugh 2008, Alspaugh, Asuncion, and Scacchi 2009a,b,c, Scacchi, Alspaugh, and Asuncion 2010], this research project also sought to explore the following kinds of research questions: How does the interaction of requirements and architectures for OA systems incorporating OSS components facilitate or inhibit acquisition practices over time? What are the best available ways and means for continuously verifying and validating the functionality, correctness, openness and security of OA when OSS components and SPLs are employed? How do OA systems evolve over time when incorporating continuously improving OSS components? How can use of continuously evolving OSS in OA be combined with the need

to verify and validate critical systems security requirements and to manage their evolution? How do reliability and predictability trade-off against the cost and flexibility of an OA system when incorporating OSS components? How should OA software systems be developed and deployed to support warfighter modification in the field or participation in post-deployment system support, when OSS components are employed?

Opportunities and Approach

Overall, our efforts developed in this research project and described in this report sought to articulate the acquisition research problem with respect to the issues identified above in order to determine what types or kinds of answers can be realized through this investigation. Subsequently, our efforts focused on the following four activities:

- Investigating the interactions between software system acquisition guidelines, software system requirements, requirements for OSS, and consequences of alternative software system architectures that incorporate different mixes of OSS components, SPLs with open APIs and open standards [Scacchi and Alspaugh 2008, Alspaugh, Asuncion, and Scacchi 2009a,b,c, Scacchi, Alspaugh, and Asuncion 2010]. This entails exploring the balance between development, verification, and validation of property and security rights, as well as contractual obligations within continuously improving OSS system elements while managing the evolution of OA systems at design-time, build-time, and release and run-time.
- Developing and refining the formal foundations for establishing acquisition guidelines for use by program managers seeking to provide software-intensive systems in cost reducing ways that rely on development and deployment of secure OA systems using OSS and SPL technology and processes [Alspaugh, Asuncion, and Scacchi 2009b].
- Developing concepts for the design of a comprehensive automated system that can support acquisition of OA systems so as to determine their conformance to acquisition guidelines/policies, contracts, and related license management issues [Alspaugh, Asuncion, and Scacchi 2009c, Asuncion 2009].
- Documenting and presenting final results [Scacchi and Alspaugh 2011] at the *8th*

Annual Acquisition Research Conference, in Monterey, CA as well as related research venues and publications, where we can elicit the strongest critical feedback on our research efforts and results.

Inter-project research coordination

We believe we are extremely well positioned to leverage our current research work and results [Scacchi and Alspaugh 2008, Alspaugh, Asuncion, and Scacchi 2009a,b,c, Scacchi, Alspaugh, and Asuncion 2010] with the effort described here. We continued to build on our recent research efforts in OSS [Scacchi 2007, 2011a,b] and software requirements-architecture interactions [Asuncion 2009, Scacchi and Alspaugh 2008, Scacchi 2009], as well as our track record in prior acquisition research studies. Similarly, we find current related research supported by the DoD addressing related issues in OSS [Hissam, *et al*. 2010] also influences our proposed effort. In addition, our effort build from and contribute to research on software system acquisition within the DoD, whether focusing on SPLs [Guertin and Clements 2010, Bergey and Jones 2010], or how to improve software system acquisition through workforce upgrades and government-industry teaming [Heil 2010]. We thus believe our complementary research places us at an extraordinary advantage to conduct the proposed study that addresses a major strategic acquisition goal of the DoD and the three military services [Starrett 2007, Weathersby 2007, Wheeler 2007].

Prospects for longer-term Acquisition-related research

Each of the military services has committed to orienting their major system acquisition programs around the adoption of an OA strategy that in turn embraces and encourages the adoption, development, use, and evolution of OSS. Thus, it would seem there is a significant need for sustained research that investigates the interplay and inter-relationships between (a) current/emerging guidelines for the acquisition of software-intensive systems within the DoD community (including contract management and software development issues), and (b) how software systems that employ an OA incorporating OSS products and production processes are essential to improving the effectiveness of future, software-intensive program acquisition efforts. Consequently, we have focused our research project, and the results appearing in this

final report to continue to lay new foundations for long-term acquisition-related research in support of the Acquisition Research Program based at the Naval Postgraduate School.

References

Alspaugh, T.A, Asuncion, H., and Scacchi, W. (2009a). Software Licenses, Open Source Components, and Open Architectures, *Proc. 6th Annual Acquisition Research Symposium*, NPS-AM-09-026, Naval Postgraduate School Monterey, CA, May.

Alspaugh, T.A, Asuncion, H., and Scacchi, W. (2009b). Intellectual Property Rights Requirements for Heterogeneously Licensed Systems, in in *Proc. 17th International Conference on Requirements Engineering (RE09*), Atlanta, GA, 24-33, September.

Alspaugh, T.A, Asuncion, H., and Scacchi, W. (2009c). Analyzing Software Licenses in Open Architecture Software Systems, *Proc. Workshop on Emerging Trends in FLOSS Research and Development, Intern. Conf. Software Engineering*, Vancouver, Canada, May.

Alspaugh, T., Asuncion, H. and Scacchi, W. (2011). Presenting Software License Conflicts through Argumentation, *Proc. 22Nd Intern. Conf. Software Engineering and Knowledge Engineering* (SEKE2011), Miami, FL, July 2011.

Asuncion, H. (2009). *Architecture Centric Traceability for Stakeholders (ACTS)*. Doctoral Dissertation, Information and Computer Science, University of California, Irvine, Irvine, CA, Summer.

Bergey, J., & Jones, L. (2010). Exploring acquisition strategies for adopting a software product line approach. Proc. 7th Annual Acquisition Research Symposium. Vol. 1, 111-122, Naval Postgraduate School, Monterey, CA.

Berzins, V. (2008). Which Unchanged Components to Retest after a Technology Upgrade, *Proc. 5th Annual Acquisition Research Symposium*, NPS-AM08031, NPS, Monterey, CA, May.

Bosch, J. (2000). *Design and Use of Software Architectures: Adopting and Evolving a Product-Line Approach*. Addison-Wesley Professional, New York.

Breaux, T.D. and Anton, A.I. (2005). Analyzing goal semantics for rights, permissions, and obligations. In *Proc. 13th IEEE International Conference on Requirements Engineering (RE'05)*, 177–188.

Breaux, T.D. and Anton, A.I. (2008). Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, 34(1), 5–20.

Clements, P. and Northrop, L. (2003). *Software Product Lines: Practices and Patterns*. Addison-Wesley Professional, New York.

Firesmith, D. (2004). Specifying reusable security requirements. *Journal of Object Technology*, 3(1), 61-75, Jan-Feb.

Guertin, N. and Clements, P. (2010). Comparing Acquisition Strategies: Open Architecture versus Product Lines, Vol. 1, 78-90, *Proc. 7th Annual Acquisition Research Symposium*, Naval Postgraduate School, Monterey, CA.

Heil, J. (2010). Enabling Software Acquisition Improvement: Government and Industry Software Development Team Acquisition Model, Vol. 1, 203-218, *Proc. 7th Annual Acquisition Research Symposium*, Naval Postgraduate School, Monterey, CA.

Hissam, S., Weinstock, C.B., and Bass, L. (2010). *On Open and Collaborative Software Development in the DoD*, Vol. 1, 219-235, *Proc. 7th Annual Acquisition Research Symposium*, Naval Postgraduate School, Monterey, CA.

Naegle, B. and Petross, D. (2008). Software Architecture: Managing Design for Achieving Warfighter Capability, *Proc. 5th Annual Acquisition Research Symposium*, NPS-AM-07-104, Naval Postgraduate School, Monterey, CA, May.

Scacchi, W., (2007). Free/Open Source Software Development: Recent Research Results and Methods, in M. Zelkowitz (Ed.), *Advances in Computers*, 69, 243-295, 2007.

Scacchi, W., (2009). Understanding Requirements for Open Source Software, in K, Lyytinen, P. Loucopoulos, J. Mylopoulos, and W. Robinson (eds.), *Design Requirements Engineering: A TenYear Perspective*, LNBIP 14, Springer Verlag, 467-494, 2009.

Scacchi, W. (2011a). Modding as a Basis for Developing Game Systems, *Proc. 1St Workshop Games and Software Engineering* (GAS'11), 33rd Intern. Conf. Software Engineering, Waikiki, Honolulu, HI, May 2011.

Scacchi, W., (2011b). Modding as an Open Source Approach to Extending Computer Game

Systems, in S. Hissam, B. Russo, M.G. de Mendonca Neto, and F. Kan (Eds.), *Open Source Systems: Grounding Research, Proc. 7Th IFIP Intern. Conf. Open Source Systems*, 62-74, IFIP ACIT 365, (Best Paper award), Salvador, Brazil, October 2011.

Scacchi, W. and Alspaugh, T., (2008). Emerging Issues in the Acquisition of Open Source Software within the U.S. Department of Defense, *Proc. 5th Annual Acquisition Research Symposium*, NPS-AM-08-036, Naval Postgraduate School, Monterey, CA, May.

Scacchi, W., and Alspaugh, T. (2011). Advances in the Acquisition of Secure Systems Based on Open Architectures, *Proc. 8Th Annual Acquisition Research Symposium*, Monterey, CA, May 2011.

Scacchi, W., Alspaugh, T., and Asuncion, H., (2010). The Challenge of Heterogeneously Licensed Systems in Open Architecture Software Ecosystems, *Proc. 7th Annual Acquisition Research Symposium*, Vol. 1, 91-110, Naval Postgraduate School, Monterey, CA, May.

Scacchi, W., Brown, C., and Nies, K. (2011). *Investigating the Use of Computer Games and Virtual Worlds for Decentralized Command and Control*, Final Report on Grant #N00244-10-1-0064 from the Center for the Edge, Naval Postgraduate School, Monterey, CA

Starrett, E. (2007). Software Acquisition in the Army, *Crosstalk: The Journal of Defense Software Engineering*, 48, May, http://stsc.hill.af.mil/crosstalk.

Weathersby, J.M., (2007). Open Source Software and the Long Road to Sustainability within the U.S. DoD IT System, *The DoD Software Tech News*, 10(2), 20-23, June.

Wheeler, D.A., (2007). Open Source Software (OSS) in U.S. Government Acquisitions, *The DoD Software Tech News*, 10(2), 7-13, June.

Yau, S.S. and Chen, Z. (2006). A framework for specifying and managing security requirements in collaborative systems. In *Proc. Third International Conference on Autonomic and Trusted Computing (ATC 2006)*, 500–510.

Advances in the Acquisition of Secure Systems Based on Open Architectures

Walt Scacchi and Thomas A. Alspaugh
Institute for Software Research
University of California, Irvine
Irvine, CA 92697-3455 USA
wscacchi@ics.uci.edu, thomas.alspaugh@acm.org

Abstract
The role of software acquisition ecosystems in the development and evolution of secure open architecture systems has received insufficient consideration. Such systems are composed of software components subject to different security requirements in an architecture in which evolution can occur by evolving existing components or by replacing them. But this may result in possible security requirements conflicts and organizational liability for failure to fulfill security obligations. We have developed an approach for understanding and modeling software security requirements as "security licenses", as well as for analyzing conflicts among groups of such licenses in realistic system contexts and for guiding the acquisition, integration, or development of systems with open source components in such an environment. Consequently, this paper reports on our efforts to extend our existing approach to specifying and analyzing software intellectual property licenses to now address software security licenses that can be associated with secure OA systems.

Biographies

Walt Scacchi is a senior research scientist and research faculty member at the Institute for Software Research, University of California, Irvine. He received a Ph.D. in Information and Computer Science from UC Irvine in 1981. From 1981-1998, he was on the faculty at the University of Southern California. In 1999, he joined the Institute for Software Research at UC Irvine. He has published more than 150 research papers, and has directed 45 externally funded research projects. In 2007, he served as General Chair of the 3rd. IFIP International Conference on Open Source Systems (OSS2007), Limerick, IE. In 2010, he chaired the Workshop on the Future of Research in Free and Open Source Software, Newport Beach, CA, for the Computing Community Consortium and the National Science Foundation. He also serves as Co-Chair of the Software Engineering in Practice (SEIP) Track at the 33rd International Conference on Software Engineering, 21-28 May 2011, Honolulu, HI.

Thomas Alspaugh is adjunct professor of Computer Science at Georgetown University, and visiting researcher at the Institute for Software Research at UC Irvine. His research interests are in software engineering and software requirements. Before completing his Ph.D., he worked as a software developer, team lead, and manager in industry, and as a computer scientist at the Naval Research Laboratory on the Software Cost Reduction project, also known as the A-7E project.

1 Introduction

A substantial number of development organizations are adopting a strategy in which a software-intensive system is developed with an open architecture (OA) [20], whose components may be open source software (OSS) or proprietary with open application programming interfaces (APIs). Such systems evolve not only through the evolution of their individual components, but also through replacement of one component by another, possibly from a different producer or under a different license. With this approach to software system acquisition, the system development organization becomes an integrator of components largely produced elsewhere that are interconnected through open APIs as necessary to achieve the desired result.

An OA development process arises in a software acquisition ecosystem in which the integrator is influenced from one direction by the goals, interfaces, license choices, and release cycles of the component producers, and in another direction by the needs of its consumers. As a result the software components are reused more widely, and the resulting OA systems can achieve reuse benefits such as reduced costs, increased reliability, and potentially increased agility in evolving to meet changing needs.

An emerging challenge is to realize the benefits of this approach when the individual components are subject to different security requirements. This may arise due either to how a component's external interfaces are specified and defended, or to how system components are interconnected and configured in ways that can or cannot defend the composed system from security vulnerabilities and external exploits. Ideally, any software element in a system composed from components from different producers can have its security capabilities specified, analyzed, and implemented at system architectural design-time, build-time, or at deployment run-time. Such capability-based security in simplest form specifies what types, value ranges, and values of data, or control signals (e.g., program invocations, procedure or method calls), can be input, output, or handed off to a software plug-in or external (helper) application, from a software component or composed system.

When designing a secure OA system, decisions and trade-offs must be made as to what level of security is required, as well as what kinds of threats to security must be addressed. The universe of possible security threats is continually emerging and the cost/effort of defending against them ongoing. Similarly, anticipating all possible security vulnerabilities or threats is impractical (or impossible). Further, though it may be desirable that all systems be secure, different systems need different levels of security, which may come at ever greater cost or inconvenience to accommodate. Strategic systems may need the greatest security possible, while other systems may require much less rigorous security mechanisms. Thus, finding an affordable, scalable, and testable means for specifying the security requirements of software components, or OA systems composed with components with different security requirements, is the goal of our research.

The most basic form of security requirements that can be asserted and tested are those associated with virtual machines. Virtual machines (VM) abstract away the actual functional or processing capabilities of the computational systems on which they operate, and instead provide a limited functionality computing surround (or "sandbox"). VM can isolate a given component or system other software applications, utilities, repositories, or external/remote control data access (input or output). The capabilities for a VM (e.g., an explicit, pre-defined list of approved operating system commands or programs that can write data or access a repository) can be specified as testable conditions that can be assigned to users or programs authorized to operate within the VM. The VM technique is now widely employed through software "hypervisors" (e.g., IBM VM/370, VMware, VirtualBox, Parallels Desktop for Mac) that isolate software applications and operating system from the underlying system platform or hardware. Such VM act like "containment vessels" through which it is possible to specify barriers to entry (and exit) of data and control via security capabilities that restrict other programs. These capabilities thus specify what rights or obligations may be, or may not be, available for access or update to data or control information. Thus architectural design-time decisions pertaining to specifying the security rights or obligations for the overall system or its components

are done by specification of VM that contain the composed system or its components. These rights or obligations can be specified as pre-conditions on input data or control signals, or post-conditions on output data or control signals.

The problem of specifying the build-time and run-time security requirements of OA systems is different from that at design-time. In determining how to specify the software build sequence, security requirements are manifest as capabilities that may be specific to explicitly declared versions of designated programs. For example, if an OA system at design-time specifies a "Web browser" as one of its components, at build-time a particular Web browser (Mozilla Firefox or Internet Explorer) must then be specified, as must its baseline version (e.g., Firefox 4.0 or Internet Explorer 9.0). However, if the resulting run-time version of the OA system must instead employ a locally available Web browser (e.g., Firefox 3.6.1 or Internet Explorer 8.0 Service Pack 2), then the OA system integrators may either need to produce multiple run-time versions for deployment, or else build the OA system using either (a) an earlier version of the necessary component (e.g., Firefox 3.5 or Internet Explorer 7.0) that is "upward compatible" with newer browser versions; (b) a stub or abstract program interface that allows for a later designated compatible component version to be installed/used at run-time; or else (c) create different run-time version alternatives (i.e., variants) of the target OA systems that may or not be "backward compatible" with the legacy system component versions available in the deployment run-time environment. The need to specify build-time and run-time components by hierarchical versions numbers like Firefox 3.6.16.144 (and possibly timestamps of their creation or local installation) arises since evolutionary version updates often include security patches that close known vulnerabilities or prevent known exploits. As indicated in the Related Research section below, security attacks often rely on system entry through known vulnerabilities that are present in earlier versions of software components that have not been updated to newer versions that don't have the same vulnerabilities.

As we have been able to address an analogous problem of how to specify and analyze the intellectual property rights and obligations of the licenses of software components, our efforts now focus on the challenge of how to specify and analyze software components and composed system security rights and obligations using a new information structure we call a "security license." The actual form of such a security license is still to be finalized, but at this point, we believe it is appropriate to begin to develop candidate forms or types of security licenses for further research and development, especially for security license forms that can be easily formalized, readily applied to large-scale OA systems, as well as be automatically analyzed or tested in ways we have already established [4,5]. This is another goal of our research here.

Next, the challenge of specifying secure software systems composed from secure or insecure components is inevitably entwined with the software ecosystems that arise for secure OA systems. We find that an OA software acquisition ecosystem involves organizations and individuals producing and consuming components, and supply paths from producer to consumer; but also

- the OA of the system(s) in question, and how best to secure it,
- the open interfaces provided by the components, and how to specify their security requirements,
- the degree of coupling in the evolution of related components that can be assessed in terms of how security rights and obligations may change, and
- the rights and obligations resulting from the security licenses under which various components are released, that propagate from producers to consumers.

An example software acquisition ecosystem producing and integrating secure software components or secure systems is portrayed in Figure 1.

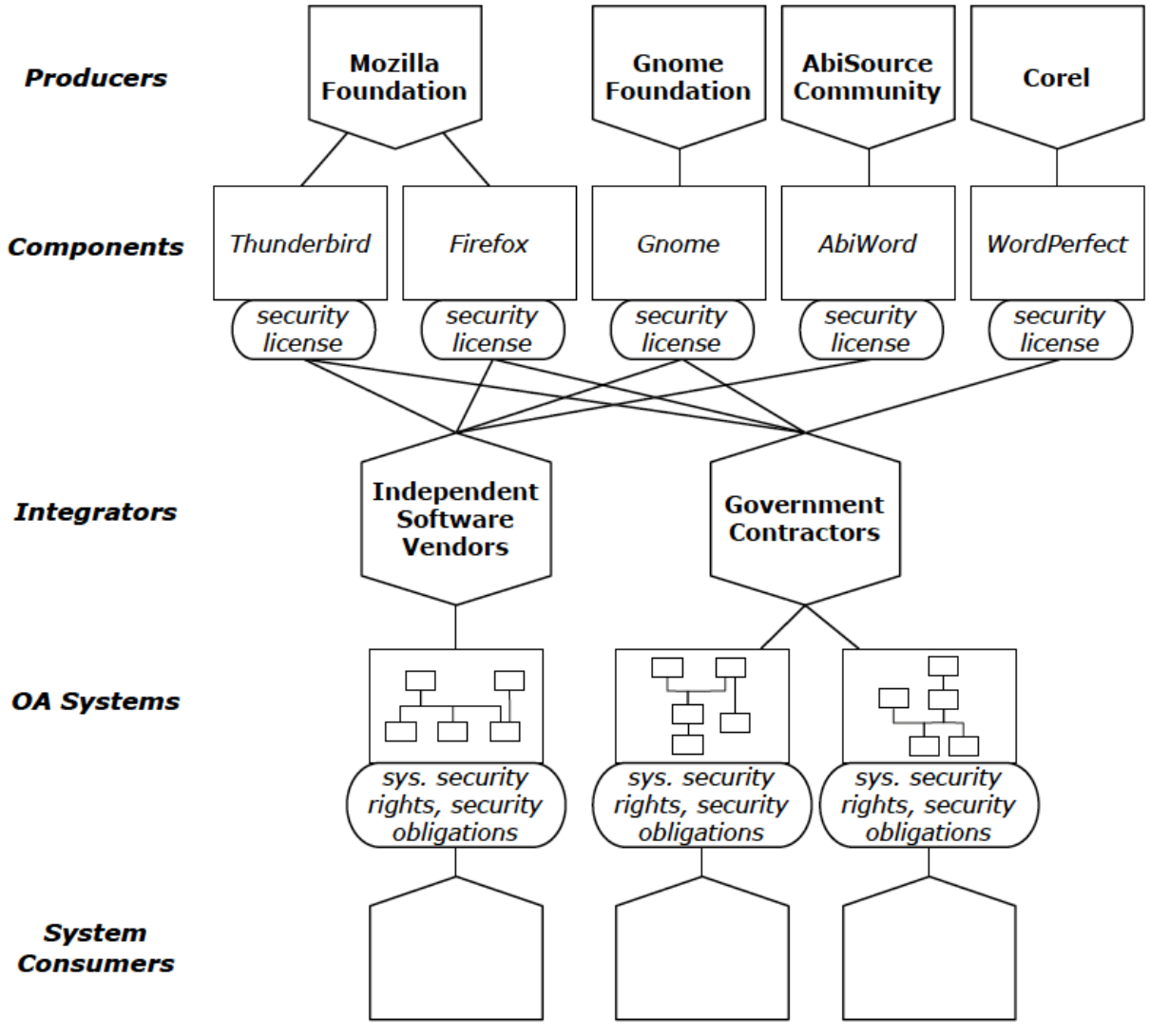

Figure 1: An example of a software acquisition ecosystem in which secure OA systems may be developed

In order to most effectively use an OA approach in developing and evolving a system, it is essential to consider this OA ecosystem. An OA system draws on components from proprietary vendors and open source projects. Its architecture is made possible by the existing general ecosystem of producers, from which the initial components are chosen. The choice of a specific OA begins a specialized software ecosystem involving components that meet (or can be shimmed to meet) the open interfaces used in the architecture. We do not claim this is the best or the only way to reuse components or produce secure OA systems, but it is an ever more widespread way. In this paper we build on previous work on heterogeneously-licensed systems [15, 22, 2] by examining how OA development affects and is affected by software ecosystems, and the role of security licenses for components included within OA software ecosystems.

In the remainder of this paper, we survey some related work (Section 2), define and examine characteristics of open architectures with or without secure software elements (Section 3), define and examine characteristics for how secure OA systems evolve (Section 4), introduce a structure for security licenses (Section 5), outline security license architectures (Section 6), and sketch our approach for security license analysis (Section 7). We then close with a discussion addressing how our software license and analysis scheme relates to software products lines (Section 8), before stating our conclusions (Section 9).

2 Related Work

Software systems, whether operating as standalone components, or as elements within large system compositions are continuously being subjected to security attacks. These attacks seek to slip through software vulnerabilities known to the attackers but perhaps not by the system integrators or consumers. These attacks often seek to access, manipulate, or remotely affect the data values or control signals that a component or composed system processes for nefarious purposes, or seek to congest or over-saturate networked services. Recent high profile security attacks like *Stuxnet* [11] reveal that security attacks may be very well planned and employ a bundle of attack vectors and social engineering tactics in order for the attack to reach strategic systems that are mostly isolated and walled off from public computer networks. The Stuxnet attack entered through software system interfaces at either the component, application subsystem, or base operating system level (e.g., via removable thumb drive storage devices), and their goal was to go outside or beneath their entry context. However, all of the Stuxnet attacks on the targeted software system could be blocked or prevented through security capabilities associated with the open software interfaces that would (a) limit access or evolutionary update rights lacking proper authorization, as well as (b) "sandboxing" (i.e., isolating) and holding up any evolutionary updates (the attacks) prior to their installation and run-time deployment. Furthermore, as the Stuxnet attack involved the use of corrupted certificates of trust from approved authorities as false credentials that allowed evolutionary system updates to go forward, it seems clear that additional preventions are needed that are external to, and prior to, their installation and run-time deployment. In our case, that means we need to specify and analyze software security requirements and evolutionary update capabilities at architectural design-time and system integration built-time, and then reconcile those with the run-time system composition. It also calls for the need to maintain the design-time, build-time, and run-time system compositions in repositories remote from system installations, and in possibly redundant locations that can be encrypted, randomized, fragmented and dispersed (e.g., via Torrents or "onion routing") then cross-checked and independently verified prior to run-time deployment in a high security system application.

As already noted, both software intellectual property licenses, and security licenses represent a collection of rights and obligations for what can or cannot be done with a licensed software component. Licenses thus denote non-functional requirements that apply to a software systems or system components as intellectual property (IP) or security requirements (i.e., capabilities) during their development and deployment. But rights and obligations are not limited to concerns or constraints applicable only to software as IP. Instead, they can be written in ways that stipulate non-functional requirements of different kinds. Consider, for example, that desired or necessary software system security properties can also be expressed as rights and obligations addressing system confidentiality, integrity, accountability, system availability, and assurance [8, 9]. Traditionally, developing robust specifications for non-functional software system security properties in natural language often produces specifications that are ambiguous, misleading, inconsistent across system components, and lacking sufficient details [23]. Using a semantic model to formally specify the rights and obligations required for a software system or component to be secure [8, 9, 23] means that it may be possible to develop both a "security architecture" notation and model specification that associates given security rights and obligations across a software system, or system of systems. Similarly, it suggests the possibility of developing computational tools or interactive architecture development environments that can be used to specify, model, and analyze a software system's security architecture at different times in its development — design-time, build-time, and run-time. The approach we have been developing for the past few years for modeling and analyzing software system IP license architectures for OA systems [3, 4, 5, 22], may therefore be extendable to also being able to address OA systems with heterogeneous "software security license" rights and obligations. Furthermore, the idea of common or reusable software security licenses may be analogous to the reusable security requirements templates proposed by Firesmith [13] at the Software Engineering Institute. But such an exploration and extension of the semantic software license

modeling, meta-modeling, and computational analysis tools to also support software system security can be recognized as a promising next stage of our research studies.

3 Secure Open Architecture Composition

Open architecture (OA) software is a customization technique introduced by Oreizy [20] that enables third parties to modify a software system through its exposed architecture, evolving the system by replacing its components. Increasingly more software-intensive systems are developed using an OA strategy, not only with open source software (OSS) components but also proprietary components with open APIs. Similarly, these components may or not have their own security requirements that must be satisfied during their build-time integration or run-time deployment, such as registering the software component for automatic update and installation of new software versions that patch recently discovered security vulnerabilities or prevent invocation of known exploits. Using this approach can lower development costs and increase reliability and function, as well as adaptively evolve software security [22]. Composing a system with heterogeneously secured components, however, increases the likelihood of conflicts, liabilities, and no-rights stemming from incompatible security requirements. Thus, in our work we define a secure OA system as *a software system consisting of components that are either open source or proprietary with open API, whose overall system rights at a minimum allow its use and redistribution, in full or in part such that they do not introduce new security vulnerabilities at the system architectural level*.

It may appear that using a system architecture that incorporate secure OSS and proprietary components, and uses open APIs, will result in a secure OA system. But not all such architectures will produce a secure OA, since the (possibly empty) set of available license rights for an OA system depends on: (a) how and why secure or insecure components and open APIs are located within the system architecture, (b) how components and open APIs are implemented, embedded, or interconnected, and (c) the degree to which the IP and security licenses of different OSS components encumber all or part of a software system's architecture into which they are integrated [22, 1].

The following kinds of software elements appearing in common software architectures can affect whether the resulting systems are open or closed [6].

Software source code components—These can be either (a) standalone programs, (b) libraries, frameworks, or middleware, (c) inter-application script code such as C shell scripts, (d) intra-application script code, as for creating Rich Internet Applications using domain-specific languages such as XUL for the Firefox Web browser [12] or "mashups" [19]. whose source code is available and they can be rebuilt, or (e) similar script code that can either install and invoke externally developed plug-in software components, or invoke external application (helper) components. Each may have its own distinct IP/security requirements.

Executable components—These components are in binary form, and the source code may not be open for access, review, modification, or possible redistribution [21]. If proprietary, they often cannot be redistributed, and so such components will be present in the design-and run-time architectures but not in the distribution-time architecture.

Software services—An appropriate software service can replace a source code or executable component.

Application programming interfaces/APIs—Availability of externally visible and accessible APIs is the minimum requirement for an "open system" [18].

Software connectors—Software whose intended purpose is to provide a standard or reusable way of communication through common interfaces, e.g. High Level Architecture [17], CORBA, MS .NET, Enterprise Java Beans, and GNU Lesser General Public License (LGPL) libraries. Connectors can also limit the propagation of IP license obligations or provide additional security capabilities.

Methods of connection—These include linking as part of a configured subsystem, dynamic linking, and client-server connections. Methods of connection affect license obligation propagation, with different

methods affecting different licenses.

Configured system or subsystem architectures—These are software systems that are used as atomic components of a larger system, and whose internal architecture may comprise components with different licenses, affecting the overall system license and its security requirements. To minimize license interaction, a configured system or sub-architecture may be surrounded by what we term a *license firewall,* namely a layer of dynamic links, client-server connections, license shims, or other connectors that block the propagation of reciprocal obligations.

Figure 2 shows a high-level run-time view of a composed OA system whose reference architectural design in Figure 3 includes all the kinds of software elements listed above. This reference architecture has been instantiated in a build-time configuration in Figure 4 that in turn could be realized in alternative run-time configurations in Figures 5, 6, 7 with different security capabilities.The configured systems consist of software components such as a Mozilla Web browser, Gnome Evolution email client, and AbiWord word processor (similar to MS Word), all running on a RedHat Fedora Linux operating system accessing file, print, and other remote networked servers such as an Apache Web server. Components are interconnected through a set of software connectors that bridge the interfaces of components and combine the provided functionality into the system's services. However, note how the run-time software architecture does not pre-determine how security capabilities will be assigned and distributed across different variants of the run-time composition.

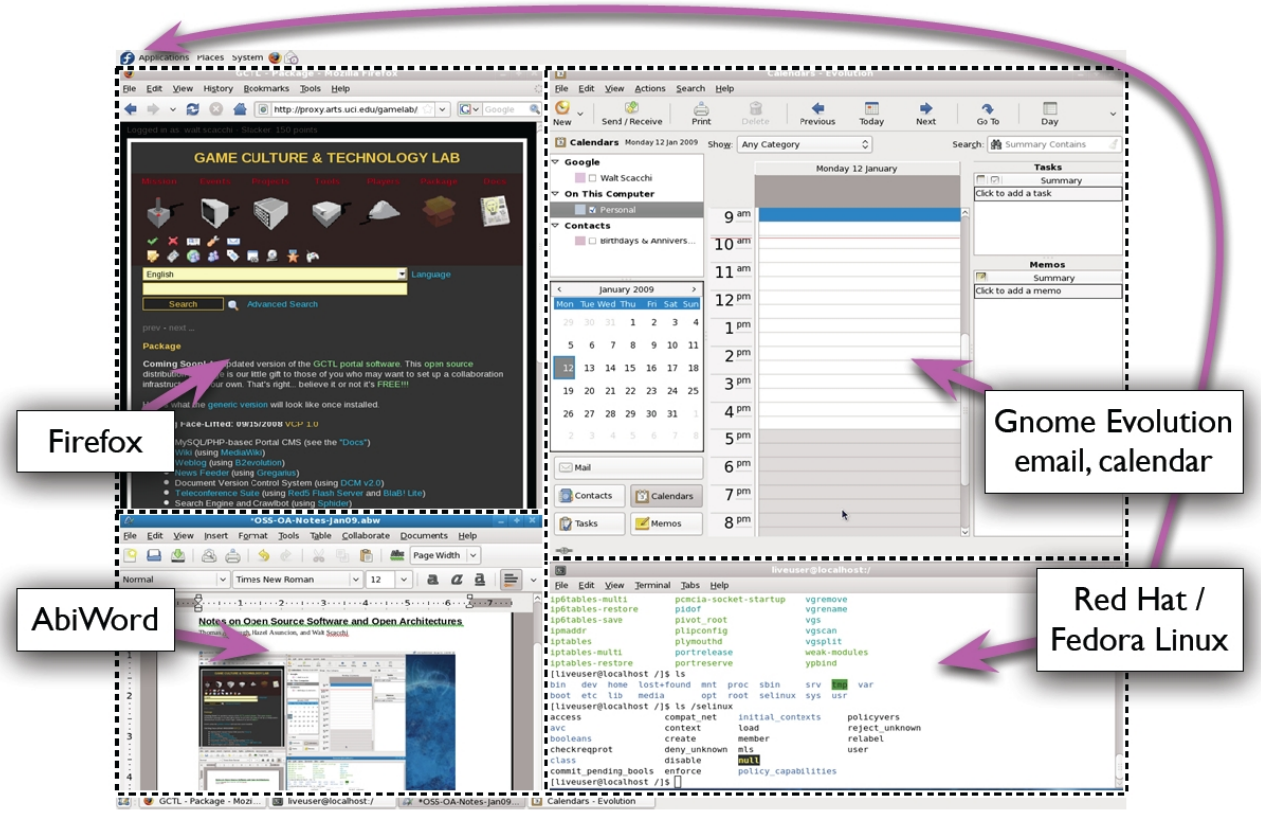

Figure 2: An example composite OA system potentially subject to different IP and security licenses

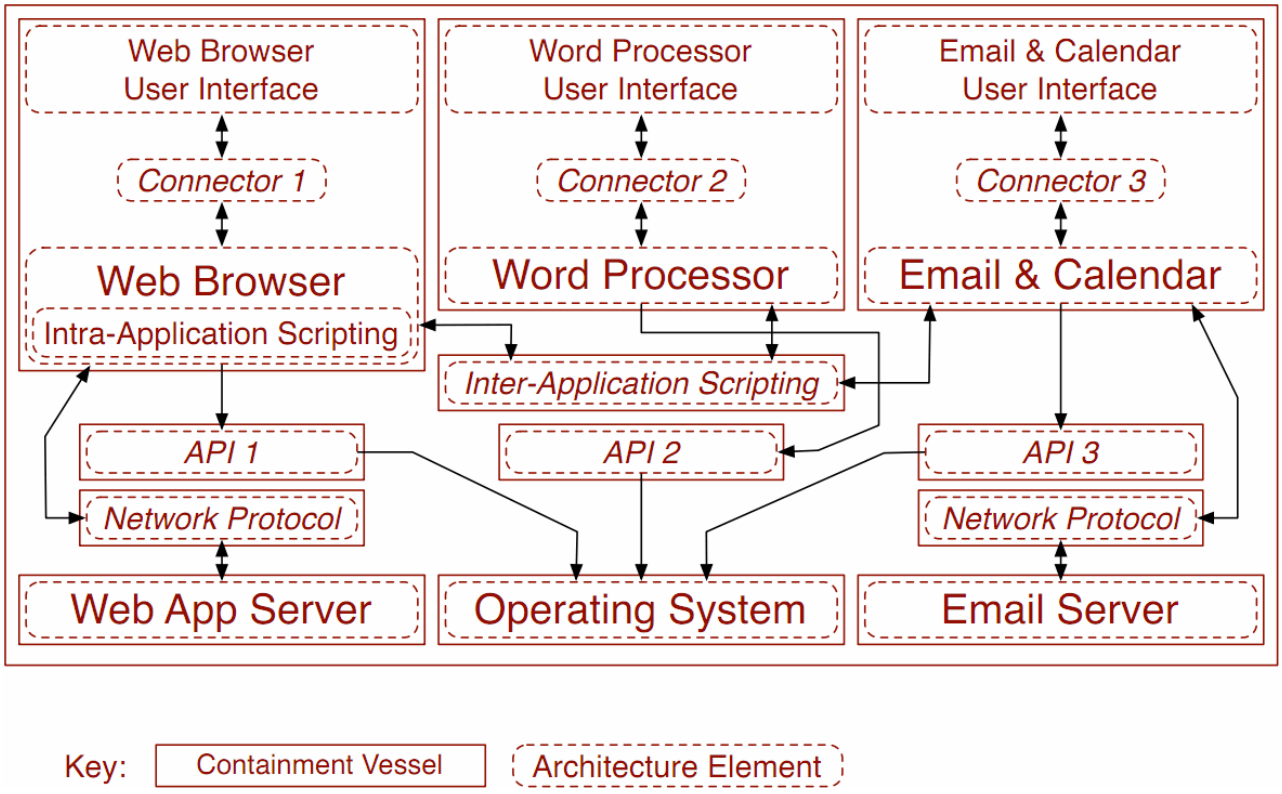

Figure 3: The design-time architecture of the system in Figure 2 that specifies a required security containment vessel scheme.

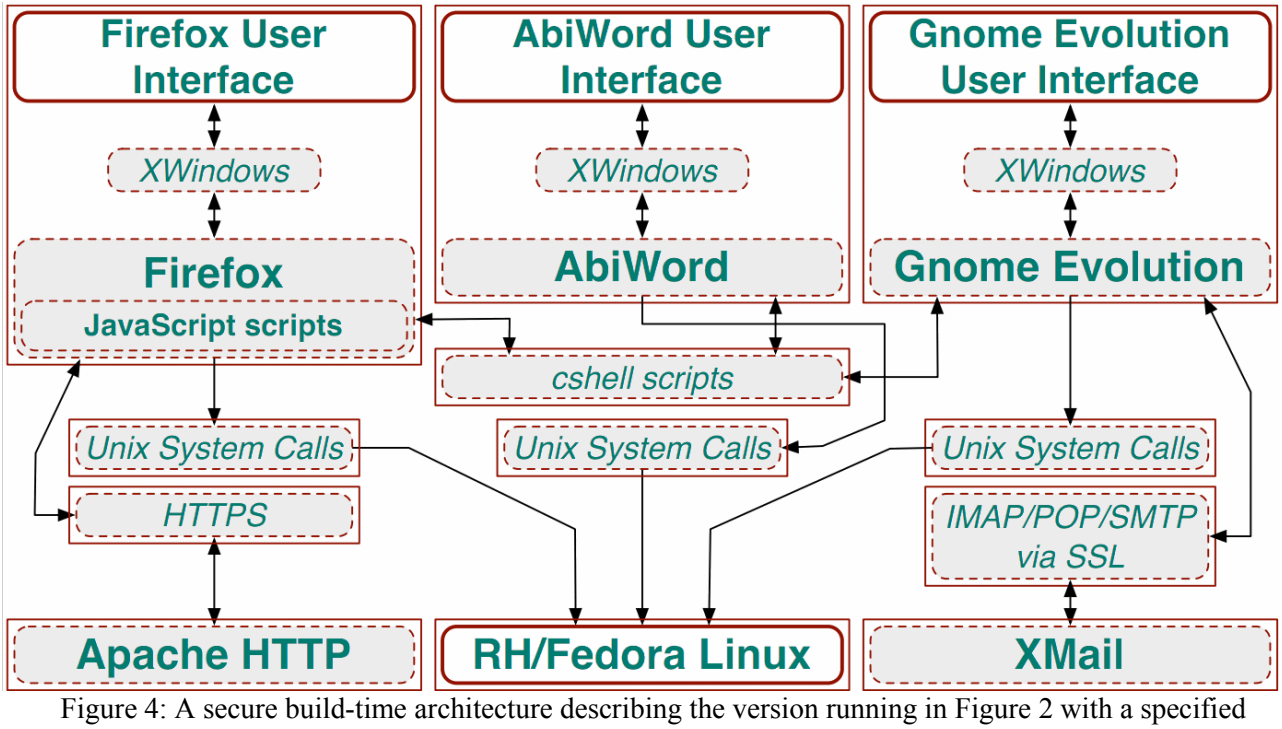

Figure 4: A secure build-time architecture describing the version running in Figure 2 with a specified security containment vessel scheme.

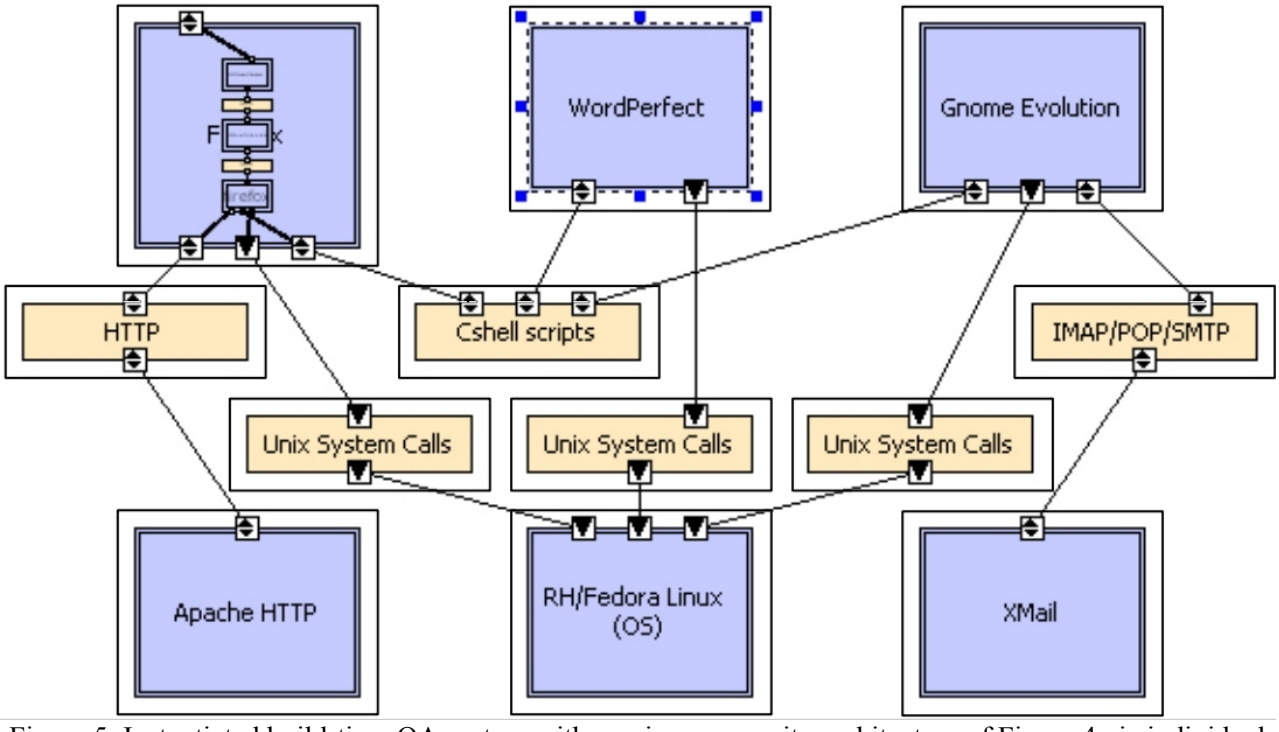

Figure 5: Instantiated build-time OA system with maximum security architecture of Figure 4 via individual security containment vessels for each system element.

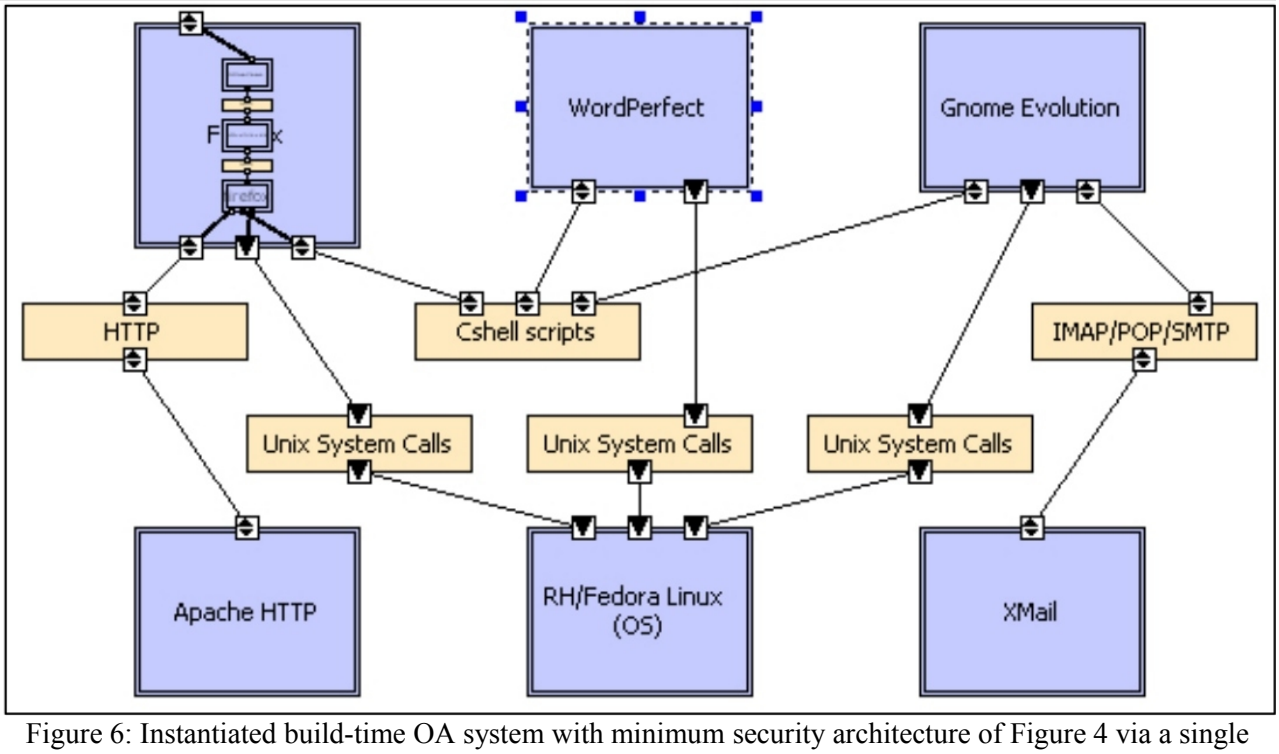

Figure 6: Instantiated build-time OA system with minimum security architecture of Figure 4 via a single overall security containment vessel for the complete system using a common software hypervisor.

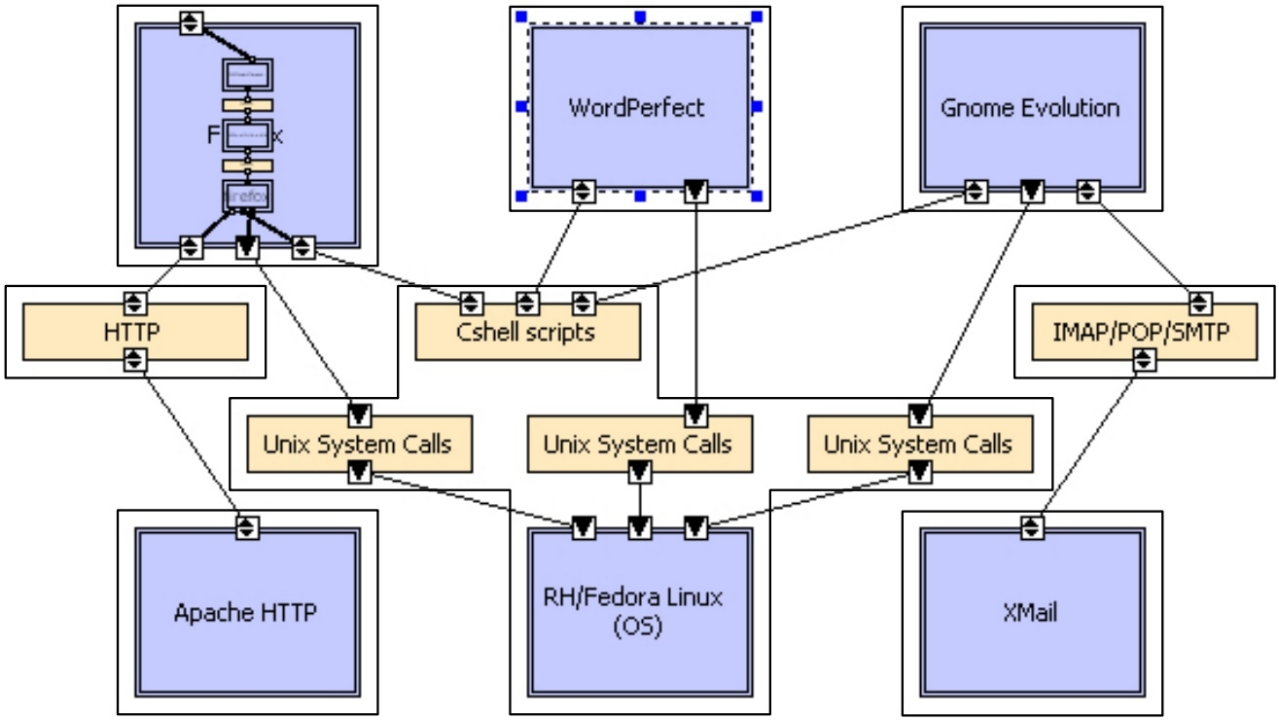

Figure 7: Instantiated build-time OA system with mixed security architecture of Figure 4 via security containment vessels for some groupings of system elements.

4 OA System Evolution

An OA system can evolve by a number of distinct mechanisms, some of which are common to all systems but others of which are a result of heterogeneous IP and security licenses in a single system.

By component evolution— One or more components can evolve, altering the overall system's characteristics (for example, upgrading and replacing the Firefox Web browser from version 3.5 to 3.6 which may update existing software functionality while also patching recent security vulnerabilities).

By component replacement— One or more components may be replaced by others with different behaviors but the same interface, or with a different interface and the addition of shim code to make it match (for example, replacing the AbiWord word processor with either Open Office or MS Word, depending on which is considered the least vulnerable to security attack.).

By architecture evolution— The OA can evolve, using the same components but in a different configuration, altering the system's characteristics. For example, as discussed in Section 3, changing the configuration in which a component is connected can change how its IP or security license affects the rights and obligations for the overall system. This could arise when replacing email and word processing applications with web services like Google Mail and Google Docs, which we might assume may be more secure since the Google services (operating in a cloud environment) may not be easily accessed or penetrated by a security attack.

By component license evolution— The license under which a component is available may change, as for example when the license for the Mozilla core components was changed from the Mozilla Public License (MPL) to the current Mozilla Disjunctive Tri-License; or the component may be made available under a new version of the same license, as for example when the GNU General Public License (GPL) version 3 was released. Similarly, the security license for a component may be changed by its producers, or the security license for a composed system changed by its integrators, in order to prevent or deter recently discovered security vulnerabilities or exploits before an evolutionary version update (or patch) can be made available.

By a change to the desired rights or acceptable obligations— The OA system's integrator or consumers may desire additional IP or security license rights (for example the right to sublicense in addition to the right to distribute), or no longer desire specific rights; or the set of license obligations they find acceptable may change. In either case the OA system evolves, whether by changing components, evolving the architecture, or other means, to provide the desired rights within the scope of the acceptable obligations. For example, they may no longer be willing or able to provide the source code for components that have known vulnerabilities that have not been patched and eliminated.

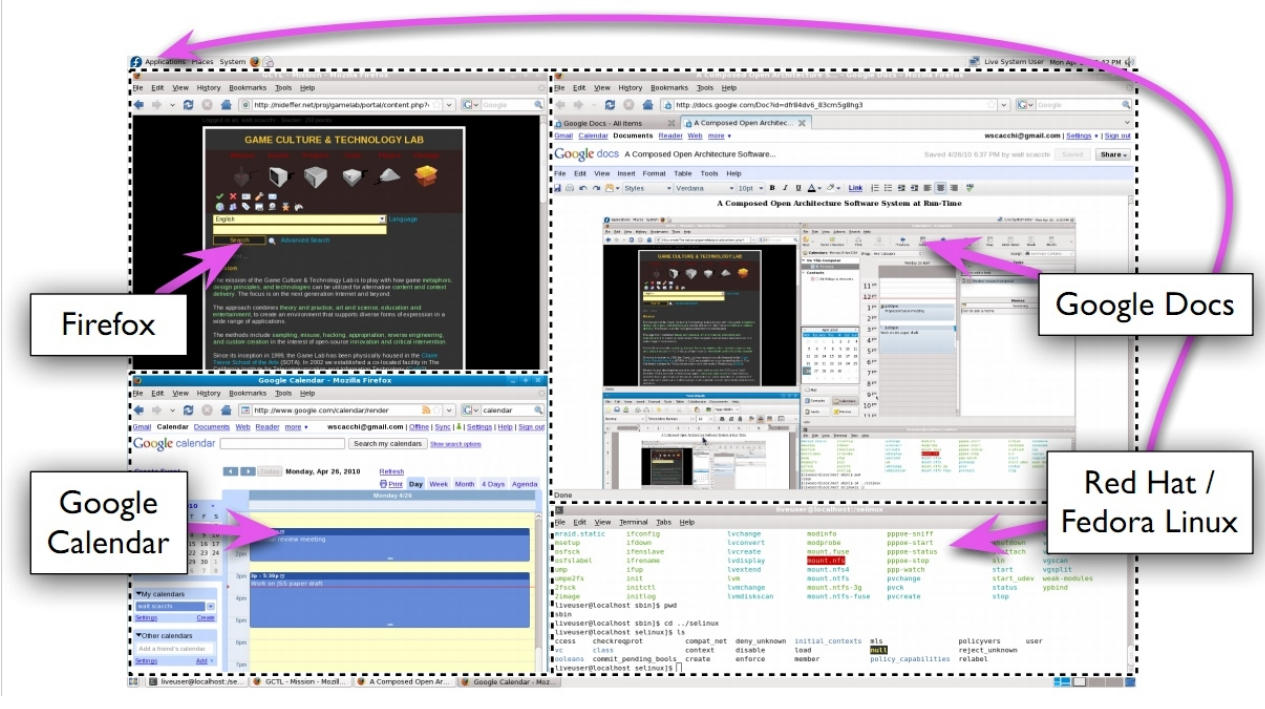

Figure 8: A second instantiation at run-time (Firefox, Google Docs and Calendar operating within different Firefox run-time sessions, Fedora) of the OA system in Figures 2, 3, and 4 as an evolutionary alternative system version, which in turn requires an alternative security containment scheme.

The interdependence of integrators and producers results in a co-evolution of software within an OA ecosystem. Closely-coupled components from different producers must evolve in parallel in order for each to provide its services, as evolution in one will typically require a matching evolution in the other. Producers may manage their evolution with a loose coordination among releases, for example as between the Gnome and Mozilla organizations. Each release of a producer component create a tension through the ecosystem relationships with consumers and their releases of OA systems using those components, as integrators accommodate the choices of available, supported components with their own goals and needs. As discussed in our previous work [2], license rights and obligations are manifested at each component's interface, then mediated through the system's OA to entail the rights and corresponding obligations for the system as a whole. As a result, integrators must frequently re-evaluate an OA system's IP/security rights and obligations. In contrast to homogeneously-licensed systems, license change across versions is a characteristic of OA ecosystems, and architects of OA systems require tool support for managing the ongoing licensing changes.

We propose that such support must have several characteristics.

- It must rest on a license structure of rights and obligations (Section 5), focusing on obligations that are enactable and testable.
- It must take account of the distinctions between the design-time, build-time, and distribution-time

architectures (Sections 3, 5, 6) and the rights and obligations that come into play for each of them.

- It must distinguish the architectural constructs significant for software licenses, and embody their effects on rights and obligations (Section 3).
- It must define license architectures (Section 6).
- It must provide an automated environment for creating and managing license architectures. We are developing a prototype that manages a license architecture as a view of its system architecture [2].
- Finally, it must automate calculations on system rights and obligations so that they may be done easily and frequently, whenever any of the factors affecting rights and obligations may have changed (Section 7).

5 Security Licenses

Licenses typically impose obligations that must be met in order for the licensee to realize the assigned rights. Common IP/copyright license obligations include the obligation to publish at no cost any source code you modify (MPL) or the reciprocal obligation to publish all source code included at build-time or statically linked (GPL). The obligations may conflict, as when a GPL'd component's reciprocal obligation to publish source code of other components is combined with a proprietary component's license prohibition of publishing its source code. In this case, no rights may be available for the system as a whole, not even the right of use, because the two obligations cannot simultaneously be met and thus neither component can be used as part of the system. Security capabilities can similarly be expressed and bound to the data values and control signals that are visible in component interfaces, or through component connectors.

Some typical security rights and obligations might be:

- The right to read data in containment vessel T.
- The obligation for a specific component to have been vetted for the capability to read and update data in containment vessel T.
- The obligation for a user to verify his/her authority to see containment vessel T, by password or other specified authentication process.
- The right to replace specified component C with some other component.
- The right to add or update specified component D in a specified configuration.
- The right to add, update, or remove a security mechanism.

The basic relationship between software IP/security license rights and obligations can be summarized as follows: if the specified obligations are met, then the corresponding rights are granted. For example, if you publish your modified source code and sub-licensed derived works under MPL, then you get all the MPL rights for both the original and the modified code. Similarly, software security requirements are specified as security obligations that when met, allow designated users or other software programs to access, modify, and redistribute data and control information to designated repositories or remote services. However, license details are complex, subtle, and difficult to comprehend and track—it is easy to become confused or make mistakes. The challenge is multiplied when dealing with configured system architectures that compose a large number of components with heterogeneous IP/security licenses, so that the need for legal counsel begins to seem inevitable [21, 14].

We have developed an approach for expressing software licenses of different types (intellectual property and security requirements) that is more formal and less ambiguous than natural language, and that allows us to calculate and identify conflicts arising from the rights and obligations of two or more component's licenses. Our approach is based on Hohfeld's classic group of eight fundamental jural relations [16], of which we use right, duty, no-right, and privilege. We start with a tuple <actor, operation, action, object> for expressing a right or obligation. The actor is the "licensee" for all the licenses we have examined. The operation is one of the following: "may", "must", "must not", or "need not", with "may" and "need not" expressing rights and "must" and "must not" expressing obligations. The action is a verb or verb phrase describing what may, must, must not, or need not be done, with the object completing the description. A license may be expressed as a set of rights, with each right associated with zero or more obligations that must be fulfilled in order to enjoy that right. Figure 9 shows the meta-model with which we express licenses.

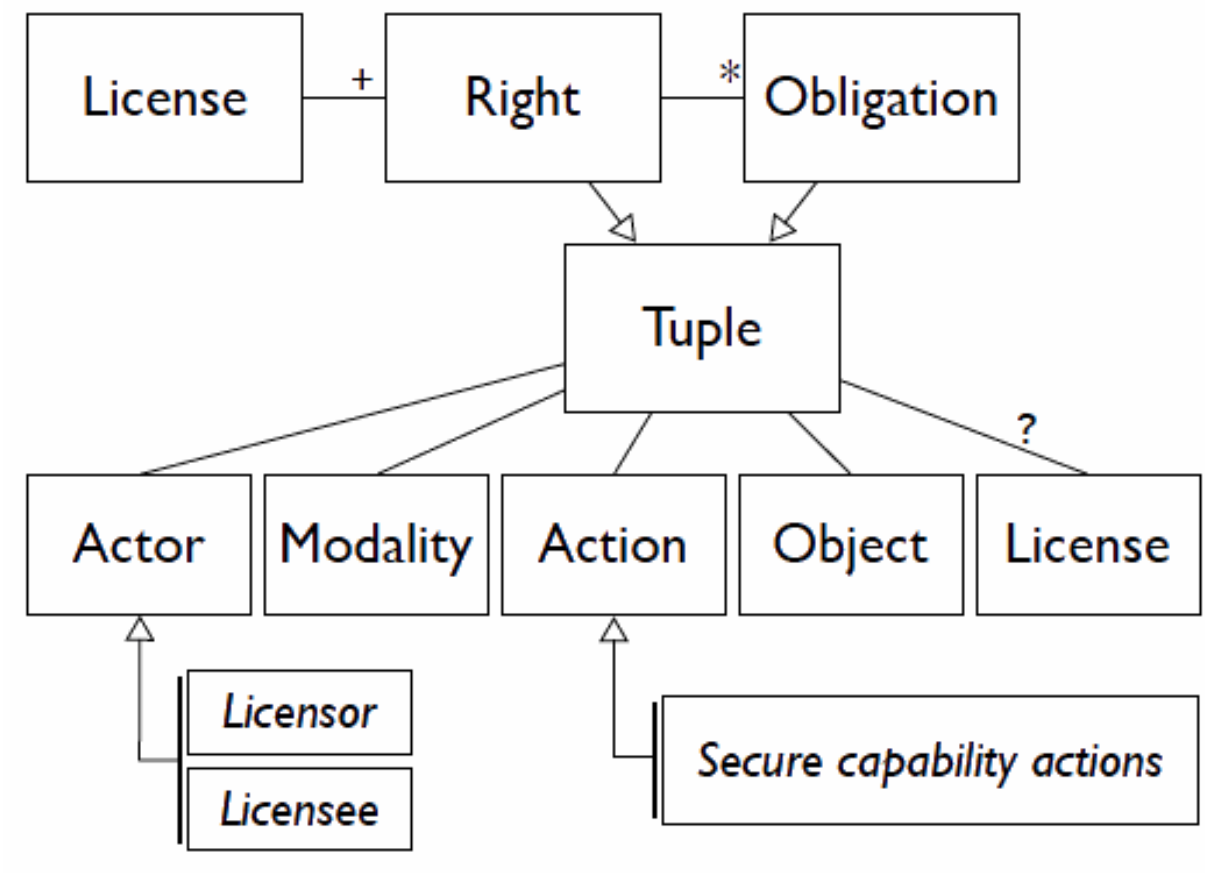

Figure 9: Security license meta-model

Designers of secure systems have developed a number heuristics to guide architectural design in order to satisfy overall system security requirements, while avoiding conflicts among interacting security mechanisms or defenses. However, even using design heuristics (and there are many), keeping track of security rights and obligations across components that are interconnected in complex OAs quickly becomes too cumbersome. Automated support is needed to manage the complexity of multi-component system compositions where different security requirements must be addressed through different security capabilities.

6 Security License Architectures

Our security license model forms a basis for effective reasoning about licenses in the context of actual systems, and calculating the resulting rights and obligations. In order to do so, we need a certain amount of information about the system's configuration at design-time, build-time, and run-time deployment. The needed information comprises the license architecture, an abstraction of the system architecture:

1. the set of components of the system (for example, see Figure 2) for the current system configuration, as well as subsequently for system evolution update versions (as seen in Figure 8);
2. the relation mapping each component to its security requirements (specified and analyzed at design-time, as exemplified in Figure 3) or capabilities (specified and analyzed at build-time in Figure 4 and run-time across alternatives shown in Figure 5, 6, and 7);
3. the connections between components and the security requirements or capabilities of each connector passing data or control signals to/from it; and
4. possibly other information, such as information to detect or prevent IP and security requirements conflicts, which is as yet undetermined.

With this information and definitions of the licenses involved, we believe it is possible to automatically calculate rights and obligations for individual components or for the entire system, as well as guide/assess system design and evolution, using an automated environment of the kind that we have previously demonstrated [2, 3, 4, 5].

7 Security License Analysis

Given a specification of a software system's architecture, we can associate security license attributes with the system's components, connectors, and sub-system architectures, resulting in a license architecture for the system, and calculate the security rights and obligations for the system's configuration. Due to the complexity of license architecture analysis, and the need to re-analyze every time a component evolves, a component's security license changes, a component is substituted, or the system architecture changes, OA integrators really need an automated license architecture analysis environment. We have developed a prototype of such an environment for analogous calculations for software copyright licenses [3, 5], and are extending this approach to security licenses.

7.1 Security obligation conflicts

A security obligation can conflict with another obligation, a related right for the same or nearby components, or with the set of available security rights, by requiring a right that has not been granted. For instance, consider two connected components C and D with security obligations

> (O1) The obligation for component C to have been vetted for the capability to read and update data in containment vessel T.
>
> (O2) The obligation for all components connected to specified component D to grant it the capability to read and update data in containment vessel T.

If C has not been vetted, then these two obligations conflict. This possible conflict must be taken into

consideration in different ways at different development times:

- at design time, ensuring that it will be possible to vet C;
- at build time, ensuring that the specific implementation of C has been vetted successfully; and
- possibly at run time as well, confirming that C is certified to have been vetted, or (if C is dynamically connected at run time) vetting C before trusting this connection to it.

The second obligation may also conflict with the set of available security rights, for example if D is connected to component E for which the security right

(R1) The right to read and update data in containment vessel T using component E

is not available.

The absence of such conflicts does not mean, of course, that the system is secure. But the presence of conflicts reliably indicates that it is not secure.

7.2 Rights and obligations calculations

The rights available for the entire system (the right to read and update data in containment vessel T, the right to replace components with other components, the right to update component security licenses, etc.) are calculated as the intersection of the sets of security rights available for each component of the system. If a conflict is found involving the obligations and rights of interacting components, it is possible for the system architect to consider an alternative scheme, e.g. using one or more connectors along the paths between the components that act as a security firewall. This means that the architecture and the automated environment together can determine what OA design best meets the problem at hand with available software components. Components with conflicting security licenses do not need to be arbitrarily excluded, but instead may expand the range of possible architectural alternatives if the architect seeks such flexibility and choice.

8 Discussion

Our approach to specifying and analyzing the security requirements for a complex OA system is based on the use of a security license. As noted, a security license is a new kind of information structure whose purpose is to declare operational capabilities that express the obligations and rights of users or program to access, manipulate, control, update, or evolve data, control signals, and accessible software system elements. Our proposed security license is influenced by IP licenses that are employed to specify property control and declared copyright freedoms/restrictions, such as those for OSS components subject to licenses like the GPLv2, MPL, LGPL, or others. These IP licenses as information structures often pre-exist to facilitate their widespread use, dissemination, and common interpretation. Further, the choice of which IP license to choose or assign to a software component results from a trade-off analysis typically performed by the components producers, rather than the system integrators or consumers, as a way to protect or propagate the obligations and rights to use, evolve, and redistribute the updated component's open source code.

The security licenses we propose may or not necessarily exist prior to their specification and assignment to a given OA system. Similarly, we may anticipate or expect that generic security licenses will emerge and be assigned by software component producers, as they have for OSS components, though no such security licenses from producers yet exist. However, one follow-on goal we seek to address is whether and how best to specify security licenses for different types of software elements or components so that it becomes possible to semi-automatically specify the security license for a given component or composed OA system through the reuse and instantiation of security requirement templates. This idea is somewhat similar to the license templates and taxonomy that is employed by the Creative Commons for non-software intellectual property like online art or new media content (cf. http://creativecommons.org/licenses/). In this regard, it may be possible to develop a technique and supporting computational environment whereby system

integrators or consumers can conveniently specify the security requirements they seek (e.g. fill out online security requirements forms), while the environment interprets these specifications to generate operational security capabilities that can be guard the entry and exit of data or control information from the appropriate containment vessel that encapsulates the corresponding system element. Consequently, this is a topic for further study and investigation.

Next, one might wonder why it is not simply desirable to have maximum system security under all circumstances. When considering the alternative run-time system composition variants shown in Figures 5, 6, and 7, it appears there may be trade-offs in one layout of security capabilities over another. For example, the layout in Figure 5 maximizes security by encapsulating each system element within its own containment vessel. This in turn requires a VM technology of a kind different from that commonly available (e.g., like VMware), and instead requires a new lightweight VM technology that can provide security capabilities (e.g., create, read, update authorizations) for potentially small-scale software elements (e.g., Cshell inter-application integration or run-time scripts). Similarly, the different security containment layouts may affect system performance, ease of evolutionary update, and associated level of security administration. But these again all represent trade-offs in the desire to achieve affordable, practical, and evermore robust and testable secure software component/system capabilities build-time and run-time. Thus, we take the position that it is better to provide the ability to specify and analyze the security requirements of different software elements at design-time, as well as specify and analyze the security capabilities at build-time and run-time, rather than the current practice that does not account for system architecture nor license architecture, and is thus inherently vulnerable to attacks that can otherwise be prevented or detected.

One other topic that follows from our approach to semantically modeling and analyzing OA systems that are subject to software security licenses. More specifically, how our approach and emerging results might shed light on software systems whose architectures articulate a software product line.
Accordingly, organizing and developing software product lines (SPLs) relies on the development and use of explicit software architectures [7, 10]. However, the architecture of a secure SPL is not necessarily a secure OA — there is no requirement for it to be so. Thus, we are interested in discussing what happens when SPLs may conform to a secure OA, and to an OA that may be composed from secure SPL components. Three considerations come to mind.

First, if the SPL is subject to a single homogeneous security software license, which may often be the case when a single vendor or government contractor has developed the SPL, then the security license may act to reinforce a vendor lock-in situation with its customers. One of the motivating factors for OA is the desire to avoid such lock-in, whether or not the SPL components have open or standards-compliant APIs.

Second, if an OA system employs a reference architecture much like we have in the design-time architecture depicted in Figure 3, which is then instantiated into a specific software product configuration, as suggested in the build-time architecture shown in Figure 4), then such a reference or design-time architecture as we have presented it here effectively defines a SPL consisting of possible different system instantiations composed from similar components instances (e.g., different but equivalent Web browsers, word processors, email, calendaring applications, relational database management systems).

Third, if the SPL is based on an OA that integrates software components from multiple vendors or OSS components that are subject to heterogeneous security licenses (i.e., those that may possible conflict with one another), then we have the situation analogous to what we have presented in this paper. So secure SPL concepts are compatible with secure OA systems that are composed from heterogeneously security licensed components.

9 Conclusion

This paper introduces the concept and initial scheme for systematically specifying and analyzing the security requirements for complex open architecture systems. We argue that such requirements should be expressed as operational capabilities that can be collected and sequenced within a new information structure we call a security license. Such a license expresses security in terms of capabilities that provide users or programs obligations and rights for how they may access data or control information, as well as how the may update or evolve system elements. These security license rights and obligations thus play a key role in

how and why an OA system evolves in its ecosystem of software component producers, system integrators and consumers.

We note that changes to the license obligations and rights, whether for control of intellectual property or software security, across versions of components is a characteristic of OA systems whose components are subject to different security requirements or other license restrictions. A structure for modeling software licenses and automated support for calculating its rights and obligations are needed in order to manage an OA system's evolution in the context of its ecosystem.

We have outlined an approach for achieving these and sketched how they further the goal of reusing components in developing software-intensive systems. Much more work remains to be done, but we believe this approach turns a vexing problem into one for which workable, as well as robust formal, solutions can be obtained.

Acknowledgments

This research is supported by grant #N00244-10-1-0038 and #N00244-10-1-077 from the Acquisition Research Program at the Naval Postgraduate School, and by grant #0808783 from the U.S. National Science Foundation. No review, approval, nor endorsement implied.

References

[1] T. A. Alspaugh and A. I. Anton. Scenario support for effective requirements. *Information and Software Technology*, 50(3):198–220, Feb. 2008.

[2] T. A. Alspaugh, H. U. Asuncion, and W. Scacchi. Analyzing software licenses in open architecture software systems. In *2nd International Workshop on Emerging Trends in FLOSS Research and Development* (FLOSS), May 2009.

[3] T. A. Alspaugh, H. U. Asuncion, and W. Scacchi. Intellectual property rights requirements for heterogeneously-licensed systems. In *17th IEEE International Requirements Engineering Conference* (RE'09), pages 24–33, Aug. 31–Sept. 4 2009.

[4] T. A. Alspaugh, H. U. Asuncion, and W. Scacchi. The Challenge of Heterogeneously Licensed Systems in Open Architecture Software Ecosystems, In *Proc. 7th Acquisition Research Symposium*, May 2010.

[5] T. A. Alspaugh, W. Scacchi, and H. U. Asuncion. Software licenses in context: The challenge of heterogeneously-licensed systems. *Journal of the Association for Information Systems,* 11(11):730–755, Nov. 2010.

[6] L. Bass, P. Clements, and R. Kazman. *Software Architecture in Practice*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2003.

[7] J. Bosch. *Design and Use of Software Architectures: Adopting and Evolving a Product-Line Approach*. Addison-Wesley, 2000.

[8] T. D. Breaux and A. I. Anton. Analyzing goal semantics for rights, permissions, and obligations. In RE '05: *Proceedings of the 13th IEEE International Conference on Requirements Engineering*, pages 177–188, 2005.

[9] T. D. Breaux and A. I. Anton. Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, 34(1):5–20, 2008.

[10] P. Clements and L. Northrop. *Software Product Lines: Practices and Patterns*. Addison-Wesley Professional, 2001.

[11] N. Falliere, L. O Murchu, and E. Chien. *W32.Stuxnet dossier, Version 1.4,* February 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[12] K. Feldt. *Programming Firefox: Building Rich Internet Applications with XU*L. O'Reilly Media, Inc., 2007.

[13] D. Firesmith. Specifying reusable security requirements. *Journal of Object Technology*, 3(1):61– 75, Jan.–Feb. 2004.

[14] R. Fontana, B. M. Kuhn, E. Moglen, M. Norwood, D. B. Ravicher, K. Sandler, J. Vasile, and A. Williamson. *A Legal Issues Primer for Open Source and Free Software Projects*. Software Freedom Law Center, 2008.

[15] D. M. German and A. E. Hassan. License integration patterns: Dealing with licenses mis-matches in component-based development. In *28th International Conference on Software Engineering* (ICSE '09), May 2009.

[16] W. N. Hohfeld. Some fundamental legal conceptions as applied in judicial reasoning. *Yale Law Journal*, 23(1):16–59, Nov. 1913.

[17] F. Kuhl, R. Weatherly, and J. Dahmann. *Creating computer simulation systems: an introduction to the high level architecture*. Prentice Hall, 1999.

[18] B. C. Meyers and P. Oberndorf. *Managing Software Acquisition: Open Systems and COTS Products*. Addison-Wesley Professional, 2001.

[19] L. Nelson and E. F. Churchill. Repurposing: Techniques for reuse and integration of interactive systems. In *International Conference on Information Reuse and Integration* (IRI-08), page 490, 2006.

[20] P. Oreizy. *Open Architecture Software: A Flexible Approach to Decentralized Software Evolution*. PhD thesis, University of California, Irvine, 2000.

[21] L. Rosen. *Open Source Licensing: Software Freedom and Intellectual Property Law*. Prentice Hall, 2005.

[22] W. Scacchi and T. A. Alspaugh. Emerging issues in the acquisition of open source software within the U.S. Department of Defense. In *5th Annual Acquisition Research Symposium*, May 2008.

[23] S. S. Yau and Z. Chen. A framework for specifying and managing security requirements in collaborative systems. In *Third International Conference on Autonomic and Trusted Computing* (ATC 2006), pages 500–510, 2006.

Presenting Software License Conflicts through Argumentation

Thomas A. Alspaugh
Computer Science Dept.
Georgetown University
Washington, DC, USA
thomas.alspaugh@acm.org

Hazeline U. Asuncion
Computing and Software Systems
University of Washington, Bothell
Bothell, Washington, USA
hazeline@u.washington.edu

Walt Scacchi
Institute for Software Research
University of California, Irvine
Irvine, California, USA
wscacchi@ics.uci.edu

***Abstract*—Heterogeneously-licensed systems pose new challenges to architects and designers seeking to develop systems with appropriate intellectual property rights and obligations. In the extreme case, license conflicts may prevent a system's legal use. Our previous work showed that rights, obligations, and conflicts can be calculated. But architects benefit from fuller information than simply (for example) a list of conflicts. In this work we demonstrate an approach for presenting intellectual property results in terms of arguments supporting them. The network of argumentation provides not only an explanation of each conclusion, but also a guide to the tradeoffs available in choosing among design alternatives with different licensing results. The approach has been integrated into the ArchStudio software architecture environment. We present an illustrative example of its use.**

I. Introduction

An increasing number of development organizations are adopting a strategy in which software-intensive systems are composed of *heterogeneously licensed* (HtL) components, with different components governed by different software licenses. The components are either open source software (OSS) or proprietary software with open application programming interfaces (APIs), and are combined in an open architecture (OA) in which components with comparable interfaces can be substituted for each other [10]. Under this strategy the development organization becomes an integrator of components largely produced elsewhere, interconnected to achieve the desired result.

The resulting OA systems can achieve reuse benefits such as reduced costs, increased reliability, and potentially increased agility in evolving to meet changing needs. But rather than a single proprietary license as when acquired from a proprietary vendor, or a single OSS license as in uniformly-licensed OSS projects, the resulting system typically has no recognized single software license. Instead it has, strictly speaking, a *virtual license* [2] composed of each component's rights and obligations for that component under its governing license. The rights available for the system as a whole are the intersection of the rights sets for each component. In some cases the licenses may produce conflicting obligations and this intersection is empty, leaving a system that cannot legally be used, distributed, or modified. An emerging challenge is to realize the reuse benefits of HtL systems while managing virtual licenses to ensure that the desired system rights are available for an acceptable set of obligations.

In our previous work (summarized in Section IV) we described and implemented a novel approach for calculating conflicting obligations, unavailable rights, and virtual licenses in an architectural design context. Calculation is necessary because the number of entailments in a typical HtL system is large, the system's architecture is constantly evolving, its design-, distribution-, and run-time architectures are often distinct, component licenses evolve and components are relicensed, and the consequences of infringement can be substantial. Therefore identifying conflicts and virtual licenses through calculation is a substantial boon. But we soon realized that *explaining* them was of even greater value.

We present an approach in which arguments are used to explain the results of right and obligation calculations. The calculations proceed by elaborating a directed acyclic graph (dag) of inferences among rights to obligations for entities in the system architecture. In this work we reimplemented the software that performs the calculations so that the dag is retained in its entirety as the primary calculation product, containing within it the obligation conflicts, unavailable rights, and virtual license for the system under analysis. Then an explanation for a specific result corresponds to the traversal of a path through the dag, starting at the result in question and continuing until the question has been answered.

- *Conflicting obligations:* the traversal branches for each obligation to show the desired rights, license provisions, and architectural entities from which that obligation is produced, and at the root of the traversal shows in what ways the obligations conflict.
- *Unavailable rights:* for each such right, a traversal identifies the exclusive copyright right that subsumes the right in question, the architectural entity to which the right pertains, and why no right in the entity's license grants the right in question.
- *Virtual license:* traversals show the chains of inference by which each right and obligation is entailed by the system architecture, the stated license for each component, and the desired rights for the system as a whole.

The dag calculation algorithm follows the steps of legal

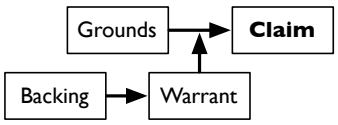

Fig. 1. A *claim*, supported by *grounds*, their pertinence to the claim justified by a *warrant*, whose validity is supported by *backing* (diagram after [14])

reasoning (formalized to support automation) by which an informed analyst would reason out the results. Thus the traversals follow inference paths that follow (in more detail) the paths by which an analyst reasons out the same conclusions.

II. Related Work

The most influential approach for structuring legal arguments is that of Toulmin, who classified the parts of arguments into claims, grounds, warrants, backing, qualifiers, and rebuttals, in a recursive structure with a diagrammatic notation outlined in Figure 1 [14]. His approach has spread beyond the area of legal arguments and is used in general rhetoric and computer science. Toulmin divides arguments into

1) *claims* asserted to be true;
2) for each claim whose truth is disputed, one or more *grounds* supporting it;
3) if it is disputed whether a claim's grounds suffice for it, then a *warrant* stating why the grounds entail the claim;
4) if the warrant is disputed, then *backing* supporting it.

If a ground or backing is disputed, then it is made the claim of a lower-level argument constructed in its support. The recursion of arguments continues as long as grounds or backings are in dispute, or until the original claim is abandoned. (Qualifiers and rebuttals address the degree of strength of arguments, and are not used in the present work.)

Hohfeld sought a theory by which to resolve the imprecise terminology and ambiguous classifications he found in use for legal relationships. In a seminal article published in 1913 and cited to the present day, he set forth a system of eight jural relations intended to express and classify all legal relationships between people. The first four regulate ordinary actions and are *right* ("may"), *no-right* ("cannot"), *duty* ("must"), and *privilege* ("need not"). Each relation has an *opposite* relation whose sense is its opposite, and a *correlative* relation whose sense is its complement. We use Hohfeld's first four jural relations as the basis of our representation of the enactable, testable provisions of software licenses (Section IV).

There has been much work on analysis of laws in AI over the past few decades. A widely-cited example is Sergot et al.'s re-expression of the British Nationality Act as a Prolog program; the resulting program applied the Act to any person's situation and characteristics to determine nationality [12].

A number of researchers have used argumentation to guide decision making, notably Haley et al. who propose an approach for using satisfaction arguments to evaluate and guide evolution of security requirements [7]. Decision choices for which no convincing argument is found are set aside in favor of choices for which stronger arguments have been identified.

III. Licensing Background

A. Intellectual Property (IP)

An individual can own a tangible thing, and have property rights in it such as the rights to use it, improve it, sell it or give it away, or prevent others from doing so, subject to some statutory restrictions. Similarly, an individual can own *intellectual property* (IP) of various types, and have specific property rights in the intangible intellectual property, such as the rights to copy, use, change, distribute, or prevent others from doing so, again subject to some statutory restrictions.

Software licenses are primarily concerned with copyrights Copyright is defined by Title 17 of the U.S. Code and by similar law in many other countries. It grants exclusive rights to the author of an original work in any tangible means of expression, namely the rights to

- reproduce the copyrighted work;
- distribute copies;
- prepare derivative works;
- distribute copies of derivative works; and
- (for certain kinds of work) perform or display it.

Because the rights are exclusive, an author can prevent others from exercising them, except as allowed by "fair use", or can grant others any or all of the rights or any part of them; one of the functions of a software license is to grant such rights, and define the conditions under which they are granted.

B. Software Licenses

Traditional proprietary licenses allow a company to retain control of software it produces, and restrict the access and rights that outsiders can have. OSS licenses, on the other hand, encourage sharing and reuse of software, and grant access and as many rights as possible.

Academic OSS licenses such as the Berkeley Software Distribution (BSD) license, the Apache Software License, and perl's Artistic License [1] grant nearly all rights and impose few obligations. Typical academic license obligations are simply to not remove the copyright and license notices.

Reciprocal OSS licenses impose an obligation that distributed modifications of reciprocally-licensed software be freely licensed under the same license. Examples are the Lesser General Public License (LGPL), Mozilla Public License (MPL), and Common Public License [1].

Some reciprocal licenses additionally require that software combined with the licensed software (for various definitions of "combined") also be freely licensed under the same license. We term such licenses *propagating*; they are also known as *strong copyleft* licenses. Examples are the General Public License versions 2 and 3 (GPLv2, GPLv3) [1].

Some OSS is *multiply-licensed*, or distributed under two or more licenses. The MySQL database software is distributed either under GPLv2 for OSS projects or a proprietary license for commercial projects. The Mozilla Disjunctive Tri-License licenses the core Mozilla components under any of three licenses (MPL, GPL, or LGPL).

C. Licenses and Software Architectures

Certain classes of architectural features affect the application and propagation of license provisions. The most common such features are listed below. A software architecture is composed of components, each of which is a "locus of computation and state" in a system, and connectors which link them and mediate interactions between them.

Software source code components—These can be

- standalone programs,
- libraries, frameworks, or middleware,
- inter-application script code such as C shell scripts, or
- intra-application script code, to creating Rich Internet Applications using domain-specific languages like XUL for the Firefox Web browser [6] or "mashups"[9].

The distinguishing characteristic of a source code component is that its source code is available and it can be modified and rebuilt. Each may have its own explicit license, though often script code connecting programs and data flows has no stated license unless the script is substantial or proprietary.

Executable components—These components are in binary form, with source code not available for access, review, modification, or possible redistribution [11]. If proprietary, they often cannot be redistributed, and so such components will be present in the design- and run-time architectures but not in the distribution-time architecture.

Software services—An appropriate software service can replace a source code or executable component.

APIs—These are not and cannot be licensed, but connections through APIs can be used to limit the propagation of some license obligations.

Software connectors—These are software elements providing a standard or reusable way of communication through common interfaces, such as High Level Architecture, CORBA, or Enterprise Java Beans. Connectors can also limit the propagation of some license obligations.

Methods of composition—These include linking as part of a configured subsystem, dynamic linking, and client-server connections. Methods of composition affect license obligation propagation, with different methods affecting different licenses. How and to what extent this occurs have not been resolved in court or in practice [5], [13].

Configured system or subsystem architectures—These are software systems used as atomic components of a larger system. Their internal architecture may contain subcomponents under several licenses, which may affect the rights and obligations for the configured (sub)system and the overall system containing it. To minimize license interaction, a configured system or subsystem architecture may be surrounded by what we term a *license firewall* [2], namely a layer of dynamic links, client-server connections, license shims, or other connectors that block the propagation of obligations.

D. Heuristics for Designing HtL Systems

HtL system designers have developed heuristics to guide architectural design while avoiding some license conflicts.

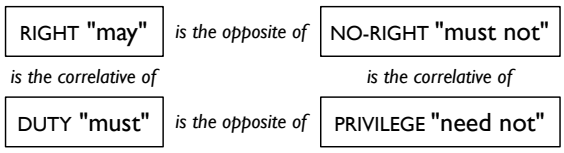

Fig. 2. Hohfeld's four basic relations

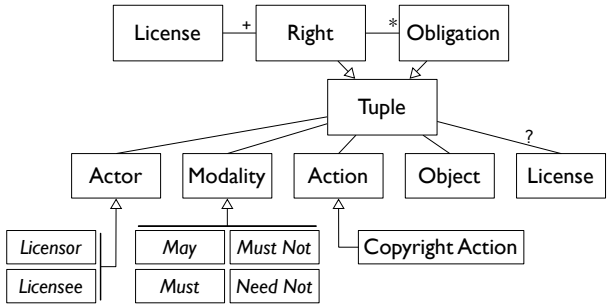

Fig. 3. Metamodel for software licenses

First, it is possible to use a reciprocally-licensed component through a license firewall that limits the scope of reciprocal obligations for specific licenses (depending on how the license provisions are interpreted). Rather than connecting conflicting components directly through static build-time links, the connection is made through a dynamic link, client-server protocol, license shim, or run-time plug-in.

A second approach used by a number of large organizations is to avoid using any components with reciprocal licenses.

Even using design heuristics such as these, keeping track of license rights and obligations across components that are interconnected in complex OAs quickly becomes cumbersome. Organizations wishing to follow a "best-of-breed" component selection policy, without regard to component licenses, face even steeper challenges. Automated support is needed to manage this multi-component, multi-license complexity.

IV. License Rights and Obligations

In our previous work [2] we developed an approach for expressing software licenses that is more formal and less ambiguous than natural language, and that allows us to calculate rights and obligations for an HtL system and identify conflicts arising from the rights and obligations of two or more component's licenses. Our approach is based on Hohfeld's eight fundamental jural relations [8], of which we use *right* ("may"), *duty* ("must"), *no-right* ("must not"), and *privilege* ("need not") (Figure 2). Each relation has a *correlative* relation, which in our context relates an obligation to its necessary right:

- if actor A must perform action X, then A requires the correlative right to perform it, expressed as "A may X";
- if actor A must not perform action X, then A requires the correlative right to not perform it, "A need not X".

We express rights and obligations as tuples (Figure 3):

<actor, modality, action, object, license>

The actor is either the "Licensee" or in a few cases "Licensor" for all the enactable, testable provisions of the licenses

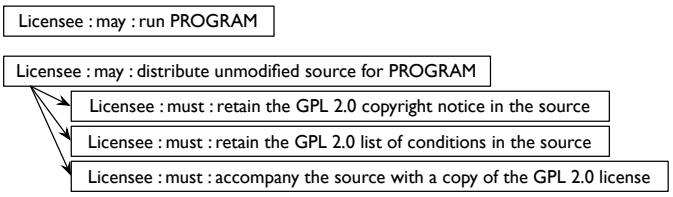

Fig. 4. Some tuples for the GPLv2 license

we have examined [3]. The modality is "may" or "need not" for a right and "must" or "must not" for an obligation. The action is a verb phrase acting on an object, describing what may, need not, must, or must not be done. The object is a module of the system or a related artifact such as a source file, the original version, documentation, and so forth. Typically a license right applies to any of a class of objects distributed under the license, such as any binary file or any modified source file; and the right's obligations will apply to the same object or a related object, such as the right's object's sources or the right's object's originals. For this reason we term rights and obligations as expressed in a license *abstract*, in contrast to a *concrete* right or obligation for one specific entity. Some actions are parameterized by a license as well.

Because copyright rights are exclusive to the copyright holder and licensees, the actions in copyright rights are distinguished from other actions; rights with those actions are only available through the object's license. Rights formed from all other actions are freely and immediately available, unless the object's license obligations restrict them.

A license is expressed as a set of rights, each right associated with zero or more obligations that must be fulfilled be granted it, and possibly a set of overall obligations that must be fulfilled for the license as a whole. Figure 4 sketches two rights from GPL version 2.0 (GPLv2), the first with no obligations and the second with three corresponding obligations.

The details of the license specification approach are described in our earlier work [2], [3].

V. Applying Licenses to Software

A. Calculating the Inference Dag

In order to obtain a particular desired right *r* for a specific module or other entity *e*, in other words a desired *concrete right*, one of two cases must hold:

1) *r* is *not* subsumed by any of the five copyright rights, and does not conflict with any general obligation of *r*'s license *L*. In this case *r* is freely available.
2) *r is* subsumed by an abstract right *R* of the license, with *e* likewise subsumed by *R*'s object. In this case all *R*'s obligations $O_1, O_2, \ldots, O_n$ must be fulfilled, with their objects replaced by whatever function of *e* they signify, in order for *r* to be granted. These could be *e* itself, all sources of *e*, the original version of *e*, and so forth. *n* may be zero, in which case *L* immediately grants *r*.

Figure 5 illustrates one step of the application of a license to obtain a desired concrete right *r*. In the license of *r*'s object

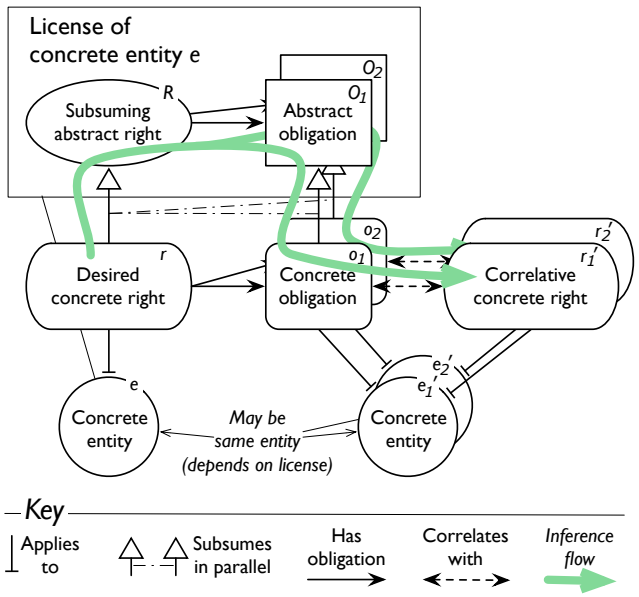

Fig. 5. A step in a rights/obligations inference

e, we search for an abstract right *R* subsuming *r*. The figure shows two obligations O_1 and O_2 of *R*, which we apply to *r*'s object *e* in order to obtain *r*'s concrete obligations o_1 and o_2. Depending on what kind of object O_1 has, o_1 could apply to *e* itself, in which case $e = e'_1$, or to an entity related to *e*, or (if *L* is a propagating license) to another module linked or otherwise connected to *e*. Finally, in order to fulfill o_1 we must have o_1's correlative right r'_1. The same considerations apply for O_2, of course. The heavy arrow shows the flow of inference from desired concrete right through to required concrete obligations and correlative rights.

If r'_1 (r'_2) is immediately available, its branch of the inference is complete. If not, the process recurses from r'_1 (r'_2).

The license rights and obligations for an entire system are calculated by repeating this process for every module of the system. If all modules are under the same license, analogous rights and obligations obtain for every module. If the system is heterogeneously-licensed, however, the calculation is much more varied, and if some of the modules are propagationally licensed then a right for one of those modules can produce obligations for other modules of the system. Such an architecture can easily result in license conflicts, as for example when a license propagates the obligation to be sublicensed under the same license to a proprietary component whose license forbids sublicensing. In such a case, the calculation will fail to produce a simultaneously satisfiable collection of obligations, and no rights will be available for the system as a whole.

Figure 6 shows in Toulmin form a portion of an example inference that produces a conflict, involving a component `e1` obtained under GPLv2 and modified, linked to a component `e2` obtained under the proprietary Corel Transactional License (CTL) [1]. The architectural connection between `e1` and `e2` is one that is interpreted for this inference as propagating

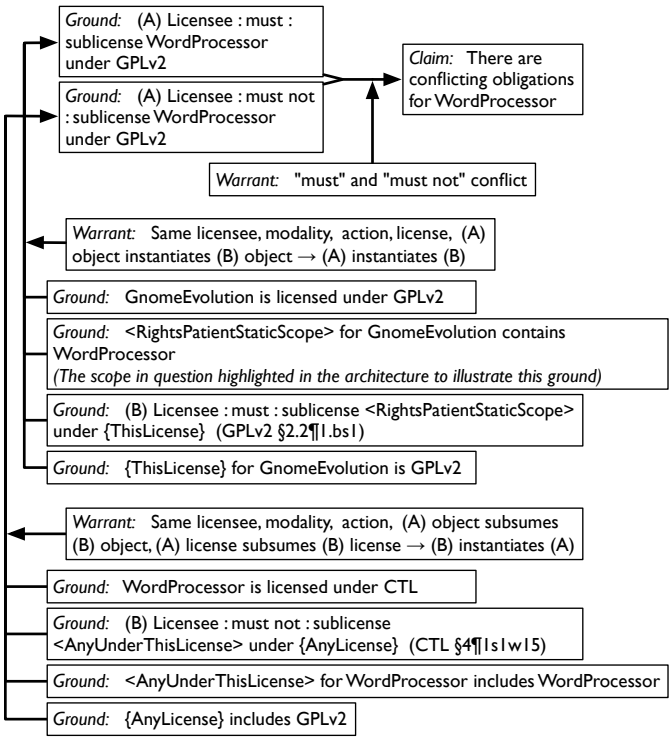

Fig. 6. Toulmin-structured arguments supporting (and explaining) a typical conflict between obligations for a GPLv2 and a proprietary component

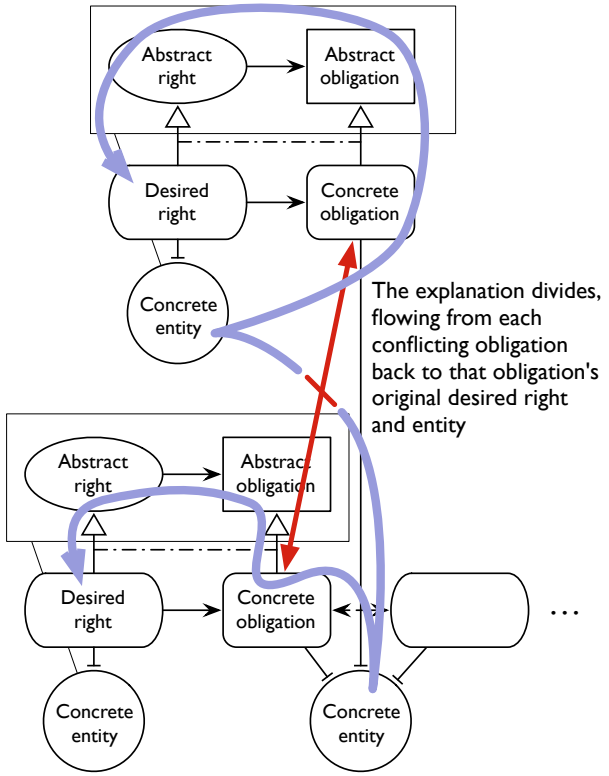

Fig. 7. Divided explanation flow for a conflict between two obligations

GPLv2 obligations, such as a static link. The right to distribute copies of the containing system is desired. In our prototype implementation (Figure 8) these arguments are presented in outline form, with the claim as the root of the outline and its grounds and warrant as its subheads, to be expanded as desired if further explanation is needed. A typical use would be:

1) Why does the WordProcessor component need to be sublicensed under GPLv2?
2) It is in the static-linked scope of the GnomeEvolution component; that component is annotated with the GPLv2 license; and GPLv2 obligates sublicensing under GPLv2 (GPLv2 §2.2¶1.bs1).
3) Why can't the WordProcessor component be sublicensed under GPLv2?
4) The WordProcessor component in the architecture has been annotated with the CTL license, and CTL forbids sublicensing under any license (CTL §4¶1s1w15).

B. Explanation by Argumentation

Figure 7 shows the two explanation flows for a conflict between obligations. Each flow begins at the conflict and explains how one half of the conflicting pair came to be. The connection between the pair is straightforward, as they are identical except for their modalities which are always "must" for one and "must not" for the other.

The flow and the required explanations are analogous for a right-obligation conflict, with the right and obligation again identical except for their modalities, which are always opposites, either "may" and "must not" or "must" and "need not".

After examining the kinds of information that are available in the vicinity of a problem (a conflict or unavailable right), we realized the inferences leading up to it provide the clearest insight into what the problem signifies and why it is present.

- The chains of inference leading up to the problem constitute precisely the portion of the calculation relevant to the problem. No other parts of the calculation—or of the applications of license provisions, determined by the architecture and its annotations, that the calculation identifies—affect whether the problem is present or not.
- The inferences place the problem in the context of licenses, components and their annotations, and architectural configuration — the context in which a designer using the tool is already working.
- Each chain of inference, followed in reverse, provides an unfolding explanation for the problem's presence, which an analyst can explore as far as is helpful in providing understanding and insight.

Each step of a chain of inference is a point at which it can be broken—by replacing a component with one differently licensed, replacing one or more connectors to firewall off a propagating obligation, replacing a build-time component with one provided by users at run time, or other design decisions.

C. Automation

The license metamodel, calculation, and an assortment of license interpretations are implemented in a Java package. The

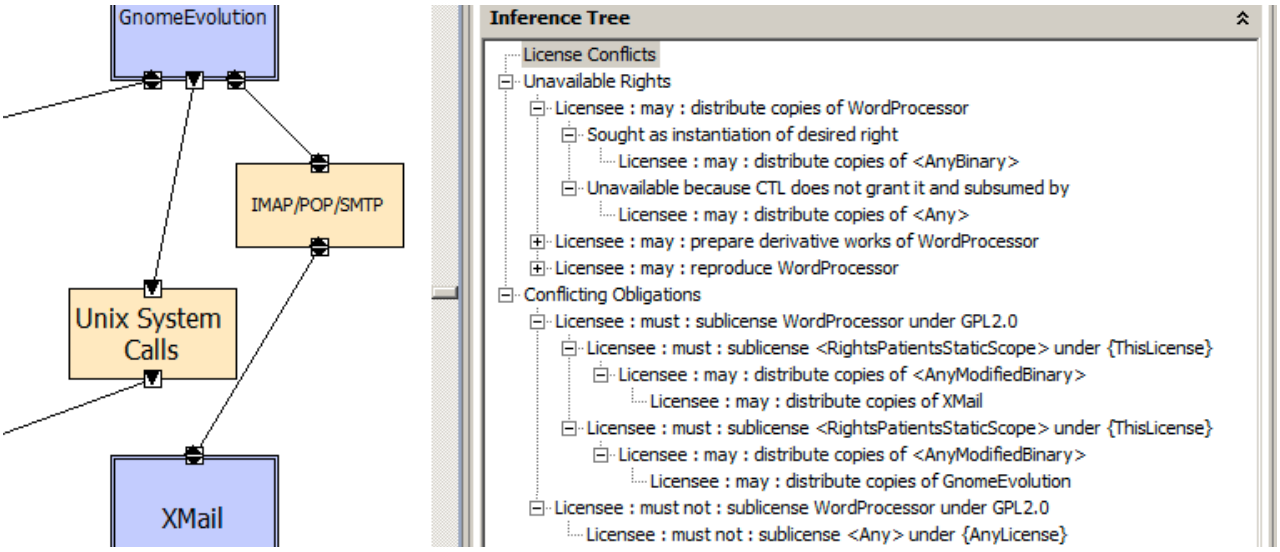

Fig. 8. Prototype explanation results for a CTL-GPL2.0 conflict: (at top) unavailable rights (partially collapsed), (middle) two conflicting obligations.

calculation builds the entire dag, which is then available for presentation in whatever ways are desired. Each abstract right and obligation in a license interpretation has its provenance in the license or interpretation for use in explanations. The package supports the addition and use of new interpretations.

The package is connected into the system design context by its integration into an ArchStudio 4 plugin [4]. The plugin maps features of software architectures onto the license architecture abstraction needed for the virtual license calculation and displays results in the context of the architecture.

The argument grounds drawn from the texts of licenses are implemented through URLs hyperlinking into our collection of software licenses tagged for reference with §-¶-sentence-word numbers [1]. Each URL cites the sentence or phrase from which a right or obligation arises. Word-level `id`s allow references to, for example, #S2.2p1.bs1w11 for the phrase beginning at word 11 of that sentence.

VI. Conclusion

HtL system design and development provide important benefits but impose new demands difficult to meet using only manual methods and human insight. Our approach for supporting HtL development and acquisition automates the calculation of HtL system virtual licenses. We have integrated it into a software architecture tool so it can be applied at the point in the development process when the necessary information is available and the relevant design decisions are made. A key benefit it provides is the automated calculation of license conflicts, desired but unavailable rights, and virtual licenses. But explaining them is of even greater value.

We present a novel approach that presents each conflict in the form of structured arguments showing why each conflict exists and (by implication) points of attack for eliminating it. These arguments provide an informative presentation that brings together all the available information in a compact, evocative form that is easier to interpret, act on, and verify.

Acknowledgments

This research supported by grant #0808783 from the U.S. National Science Foundation, and grant #N00244-10-1-0077 from the Acquisition Research Program at the Naval Postgraduate School. No review, approval, or endorsement is implied.

The authors thank the anonymous reviewers of earlier versions of this paper for their insightful suggestions.

References

[1] T. A. Alspaugh. OSS (and other) licenses, §/¶/sentence/word-numbered. http://www.thomasalspaugh.org/pub/osl-sps/.

[2] T. A. Alspaugh, H. U. Asuncion, and W. Scacchi. Intellectual property rights requirements for heterogeneously-licensed systems. In *17th Int. Requirements Engineering Conference (RE'09)*, pages 24–33, 2009.

[3] T. A. Alspaugh, W. Scacchi, and H. U. Asuncion. Software licenses in context: The challenge of heterogeneously-licensed systems. *Journal of the Association for Information Systems*, 11(11):730–755, Nov. 2010.

[4] E. Dashofy, H. Asuncion, S. Hendrickson, et al. Archstudio 4: An architecture-based meta-modeling environment. In *28th Int. Conference on Software Engineering, Companion Volume*, pages 67–68, 2007.

[5] L. Determann. Dangerous liasons—software combinations as derivative works? *Berkeley Technology Law Journal*, 21(4), 2006.

[6] K. Feldt. *Programming Firefox: Building Rich Internet Applications with XUL*. O'Reilly Media, Inc., 2007.

[7] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh. Security requirements engineering: A framework for representation and analysis. *IEEE Transactions on Software Engineering*, 34(1):133–153, 2008.

[8] W. N. Hohfeld. Some fundamental legal conceptions as applied in judicial reasoning. *Yale Law Journal*, 23(1):16–59, 1913.

[9] L. Nelson and E. F. Churchill. Repurposing: Techniques for reuse and integration of interactive systems. In *International Conference on Information Reuse and Integration (IRI-08)*, page 490, 2006.

[10] P. Oreizy. *Open Architecture Software: A Flexible Approach to Decentralized Software Evolution*. PhD thesis, Univ. of Calif., Irvine, 2000.

[11] L. Rosen. *Open Source Licensing: Software Freedom and Intellectual Property Law*. Prentice Hall, 2005.

[12] M. J. Sergot, F. Sadri, et al. The British Nationality Act as a logic program. *Communications of the ACM*, 29(5):370–386, May 1986.

[13] M. L. Stoltz. The penguin paradox: How the scope of derivative works in copyright affects the effectiveness of the GNU GPL. *Boston University Law Review*, 85(5):1439–1477, 2005.

[14] S. Toulmin, R. Rieke, and A. Janik. *An introduction to reasoning*. Macmillan, 1984.

Modding as an Open Source Approach to Extending Computer Game Systems

Walt Scacchi
Institute for Software Research
and
Center for Computer Games and Virtual Worlds
University of California, Irvine
wscacchi@ics.uci.edu

Abstract. This paper examines what is known so far about the role of open source software development within the world of game mods and modding practices. Game modding has become a leading method for developing games by customizing or creating OSS extensions to game software in general, and to proprietary closed source software games in particular. What, why, and how OSS and CSS come together within an application system is the subject for this study. The research method is observational and qualitative, so as to highlight current practices and issues that can be associated with software engineering and game studies foundations. Numerous examples of different game mods and modding practices are identified throughout.

1. Introduction

User modified computer games, hereafter *game mods*, are a leading form of user-led innovation in game design and game play experience. But modded games are not standalone systems, as they require the user to have an originally acquired or licensed copy of the unmodded game software.

Modding, the practice and process of developing game mods, is an approach to end-user game software engineering [4] that establishes both social and technical knowledge for how to innovate by resting control over game design from their original developers. At least four types of game mods can be observed: user interface customization; game conversions; machinima; and hacking closed game systems. Each supports different kinds of open source software (OSS) extension to the base game or game run-time environment. Game modding tools and support environments that support the creation of such extensions also merit attention. Furthermore, OSS game extensions are commonly applied to either proprietary, closed source software (CSS) games, or to OSS games, but generally more so to CSS games. Why this is so also merits attention. Subsequently, we conceive of game mods as covering customizations, tailorings, remixes, or reconfigurations of game embodiments, whether in the form of game content, software, or hardware denoting our space of interest.

The most direct way to become a game mod developer (a game *modder*) is through self-tutoring and self-organizing practices. Modding is a form of learning – learning how to mod, learning to be a game developer, learning to become a game content/software developer, learning computer game science outside or inside an academic setting, and more [5,20]. Modding is also a practice for learning how to work with others, especially on large, complex games/mods. Mod team efforts may also self organize around emergent software development project leaders or "want to be" (W.T.B.) leaders, as seen for example in the *Planeshift* (http://www.planeshift.it/) OSS massively multiplayer online role-playing game (MMORPG) development and modding project [20].

Game mods, modding practices, and modders are in many ways quite similar to their counterparts in the world of OSS development, even though they often seemingly isolated to those unaware of game software development. Modding is increasingly a part of mainstream technology development culture and practice, and especially so for games, but also for hardware-centered activities like automobile or personal computer customization. Modders are players of the games they reconfigure, just as OSS developers are also users of the systems they develop. There is no systematic distinction between developers and users in these communities, other than there are many users/players that may contribute little beyond their usage, word of mouth they share with others, and their demand for more such systems. At OSS portals like SourceForge.net, the domain of "Games" is the second most popular project category with nearly 42K active projects, or 20% of all projects[1]. These projects develop either OSS-based games, game engines, or game development tools/SDKs, and all of the top 50 projects have each logged more than 1M downloads. So the intersection of games and OSS covers a substantial socio-technical plane, as game modding and traditional OSS development are participatory, user-led modes of system development that rely on continual replenishment of new participants joining and migrating through project efforts, as well as new additions or modifications of content, functionality and end-user experience [19,20,21]. Modding and OSS projects are in many ways experiments to prototype alternative visions of what innovative systems might be in the near future, and so both are widely embraced and practiced primarily as a means for learning about new technologies, new system capabilities, new working relationships with potentially unfamiliar teammates from other cultures, and more [cf. 21].

Consequently, game modding appears to be (a) emerging as a leading method for developing or customizing game software; (b) primarily reliant of the development and use of OSS extensions the ways and means for game modding; and (c) overlapping a large community of OSS projects that develop computer game software and tools that has had comparatively little study. As such, the research questions that follow then are

[1] See http://www.sourceforge.net/softwaremap/index.php, accessed 15 April 2011. The number one category of projects is for "Development" with more than 65K OSS projects, out of 210K projects. So OSS Development and OSS Games together represent half of the projects currently hosted on SourceForge.

why do these conditions exist, how have they emerged, and how are they put into practice in different game modding efforts.

This paper seeks to examine what is known so far about game mods and modding practices. The research method in this study is observational and qualitative. It seeks to snapshot and highlight current practices that can be associated with software engineering and game studies, as well as how these practice may be applied in CSS versus OSS game modding. Numerous examples of different game mods and modding practices are identified throughout to help establish an empirically grounded baseline of observations, from which further studies can build or refute. Furthermore, the four types of game mods and modding practices identified in this paper have been employed first-hand in game development projects led or produced by the author. Such observation can subsequently serve as a basis for further empirical study and technology development that ties together computer games, OSSD, software engineering, and game studies [19,20,21,22].

2. Related Research

Two domains of research inform the study here: software extension within the field of software engineering, and modding as cultural practice within game studies. Each is addressed in turn.

2.1 Software Extension

Game mods embody different techniques and mechanisms for software extension. However, the description of game mods and modding is often absent of its logical roots or connections back to software engineering. As suggested, mods are extensions to existing game software systems, so it is appropriate to review what we already know about software extensions and extensibility.

Parnas [15] provides an early notion of software extension as an expression of modular software design. Accordingly, modular systems are those whose components can be added, removed, or updated while satisfying the original system functional requirements. Such concepts in turn were integrated into software architectural design language descriptions and configuration management tools [14]. But reliance on explicit software architecture descriptions is not readily found in either conventional game or mod development. Hentonnen and colleagues [8] examine how software plug-ins support architectural extension, while Leveque, et al. [11] investigate how extension mechanisms like views and model-based systems support extension, also at the architectural level. Last, the modern Web architecture is itself designed according to principles of extensibility through open APIs, migration across software versions, network data content/hypertext transfer protocols, and representational state transfer [6]. Mod-friendly networked multi-player games often take advantage of these capabilities.

Elsewhere, Batory and associates [3] describe how domain-specific languages (for scripting) and software product lines support software extension, and now such techniques are used in games that are open for modding. Next, OSS development as a complementary approach to software engineering, relies on OSS code and associated online artifacts that are open for extension through modification and redistribution of their source representations [21]. Finally, other techniques to extend the functionality or operation of an existing CSS system may include unauthorized modifications that might go beyond what the end-user license agreement might allow, and so appear to fall outside of what software engineering might anticipate or encourage. These include extensions via hacking methods like code injection or hooking, whose purpose is to gain/redirect control of normal program flow through overloading or intercepting system function calls, or provide a hidden layer of interpretation, which allow for "man in the middle" interventions. So software extensions and extensibility is a foundational concept in software engineering, as well as foundational to the development of game mods. However, the logical connections and common/uncommon legacy of game modding, OSS development, and software engineering remain under specified, which this paper begins to address.

2.2 Modding as Cultural Practice

Game modding is a practice for user content creation that creates/networks not only game mods but game modders. Within anthropological, behavioral, and sociological studies of computer game play, modding has been studied as an emerging cultural practice that mediates both game play and player interaction with other players (including the game's developers). In some early studies, modding has been designated as a form of "playbour" whereby player actions to create game extensions for use by other players is observed as a form of unpaid (or underpaid) labor that primarily benefits the financial and property interests of game development corporations or hegemonic publishers [10,16,26].

Game modding also modifies or transforms game play experience, since what is play and what is experience(d) are culturally situated. Examples of this may include single player games being modded into multi-player games. So the experience of single player versus the game environment is transformed into other situations including player versus player, multi-player group play, or team versus team play. Similarly, the modding of games to enable experiences other than expected game play, like using a modded game for storytelling or film-making experiences is also a practice of growing interest, with the emergence of a distinguishable community of gamer-filmmakers who produce *machinima* (described later) as either a literary medium, or an art form [9,12,13].

Other studies have observed that user/modders also benefit from modding as a way to achieve a sense of creative ownership and meaning in the modded games they share and play with others [17,19,20,23], and that game mods and modding practices

become central elements in what constitutes play with and through games [24]. Finally, as already observed, OSS project portals like SourceForge host thousands of OSS game development projects that develop and deploy role-playing games (4.3K projects), simulation-based games (2.6K), board games (2.3K), side-scrolling/arcade games (2K), turn-taking strategy games (1.7K), multi-user dungeons or text-based adventure/virtual worlds (1.6K), first-person shooters (1.6K), MMORPG (0.6K) and more. So development of OSS games and related game development tools can be recognized as a central element in the cultural world of computer games and game development, as well as the world of OSS development [19,20,21].

3. Four Types of Game Mods

At least four types of game mods are realized through OSS development practices. These include (i) user interface customizations and agents, (ii) game conversions, (iii) machinima, and (iv) hacking closed source game systems. Each is examined in turned, and each is facilitated (or prohibited) according to its copyright license.

3.1 User Interface Customizations and Agents

User interfaces to games embody the practice and experience of interfacing users (game players) to both the game system and the play experience designed by the game's developers. Game developers act to constrain and govern what users can do, and what kinds of experience they can realize. Some users in turn seek to achieve a form of competitive advantage during game play by modding the user interface software for their game, when so enabled by game developers. These mods acquire or reveal additional information that users believe will help their play performance and experience. User interface add-ons subsequently act as the medium through which game development studios support game product customization, which is a strategy for increasing end-user satisfaction and thus the likelihood of product success [4].

Three kinds of user interface customizations can be observed. First and most common, is the player's ability to select, attire or accessorize a *player's in-game identity*. Second, is for players to customize *the color palette and representational framing borders* of the their game display within the human-computer interface, much like what can also be done with Web browsers (e.g, Firefox 4 “personas” and “themes”) and other end-user software applications. Third, are *user interface add-on modules* that modify the player's in-game information management dashboard, but do not modify the underlying game play rules or functions. These add-ons provide additional information about game play state that may enhance the game play experience, as well as increasing a player's sense of immersion or omniscience within the game world through perceptual expansion. This in turn enables awareness of game events not visible in the player's pre-existing in-game view. Furthermore, some add-on facilities (e.g., those available with the proprietary *World of Warcraft*

MMORPG, scripted in the LUA language) accommodate the creation of automated agent scripts that can read/parse data streamed to the UI within an existing or other add-on dashboard component, and then provide some additional value-added play experience, such as sending out messages or status reports to other players automatically. Such add-on agents thus modify or reconfigure the end-user play experience, rather than the core functionality or play mechanics available to all other of the game's players. Consequently, the first two kinds of customizations result from meta-data selections within parametric system functions, while the third represents a traditional kind of user-created modular extension; one that does not affect the pre-existing game's functional requirements, nor one included in the operational source code base during subsequent system builds or releases, unless they do alter the software's requirements (e.g., by introducing a new security vulnerability or exploit that must be subsequently prevented).

3.2 Game Conversions

Game conversion mods are perhaps the most common form of game mods. Most such conversions are partial, in that they add or modify: (a) in-game characters including user-controlled character appearance or capabilities, opponent bots, cheat bots, and non-player characters; (b) play objects like weapons, potions, spells, and other resources; (c) play levels, zones, maps, terrains, or landscapes; (d) game rules; or (e) play mechanics. Some more ambitious modders go as far as to accomplish (f) total conversions that create entirely new games from existing games of a kind not easily determined from the originalgame. For example, one of the most widely distributed and played total game conversions is the *Counter-Strike* (CS) mod of the *Half-Life* (HL) first-person action game from Valve Software. As the success of the CS mod gave rise to millions of players preferring to play the mod over the original HL game, then other modders began to access the CS mod to further convert in part or full, to the point that Valve Software modified its game development and distribution business model to embrace game modding as part of the game play experience that is available to players who acquire a licensed copy of the HL product family. Valve has since marketed a number of CS variants that have sold over 10M copies as of 2008, thus denoting the most successful game conversion mod, as well as the most lucrative in terms of subsequent retail sales derived from a game mod.

Another example is found in games converted to serve a purpose other than entertainment, such as the development and use of games for science, technology, and engineering applications. For instance, the *FabLab* game [22] is a conversion of the *Unreal Tournament 2007* retail game, from a first-person shooter to a simulator for training semiconductor manufacturing technicians in diagnosing and treating potentially hazardous materials spills in a cleanroom environment. This conversion is not readily anticipated by knowledge of the Unreal games or underlying game engine, though it maintains operational compatibility with the Unreal game itself. So

game conversions can re-purpose the look, feel, and intent of a game across application domains, while maintaining a common software product line [cf. 3].

Finally, it is common practice that the underlying game engine has one set of license terms and conditions to protect original work (e.g., no redistribution), while game mod can have a different set of terms and conditions as a derived work (e.g., redistribution allowed only for a game mod, but not for sale). In this regard, software licenses embody the business model that the game development studio or publisher seeks to embrace, rather than just a set of property rights and constraints. For example, in *Aion*, an MMORPG from South Korean game studio NCSoft, no user created mods or user interface add-ons are allowed. Attempting to incorporate such changes would conflict with its EULA and subsequently put such user-modders at risk of losing their access to networked *Aion* multi-player game play. In contrast, the MMORPG *World of Warcraft* allows for UI customization mods and add-ons only, but no other game conversions, no reverse engineering of the game engine, and no activity intended to bypass WoW's encryption mechanisms. And, in one more variation, for games like *Unreal Tournament*, *Half-Life*, *NeverWinterNights*, *Civilization* and many others, the EULAs encourage modding and the free redistribution of mods without fee to others who must have a licensed copy of the proprietary CSS game, but not allowing reverse engineering or redistribution of the CSS game engine required to run the OSS mods. This restriction in turns helps game companies realize the benefit of increased game sales by players who want to play with known mods, rather than with the un-modded game as sold at retail. Mods thus help improve games software sales, revenue, and profits for the game development studio, publisher, and retailer, as well as enable new modes of game play, learning, and skill development for game modders.

3.3 Machinima

Machinima can be viewed as the product of modding efforts that intend to modify the visual replay of game usage sessions. Machinima employ computer games as their creative media, such that these new media are mobilized for some other purpose (e.g., creating online cinema or interactive art exhibition). Machinima focuses attention to playing and replaying a game for the purpose of story telling, movie making, or retelling of daunting or high efficiency game play/usage experience [12,13]. Machinima is a form of modding the experience of playing a specific game, by recording its visual play session history, so as to achieve some other ends beyond the enjoyment (or frustration) of game play. These play-session histories can then be further modded via video editing or remixing with other media (e.g., adding music) to better enable cinematic storytelling or creative performance documentation. Machinima is a kind of play/usage history process re-enactment [cf. 18] whose purpose may be documentary (replaying what the player saw or experienced during a play session) or cinematic (creatively steering a play session so as to manifest observable play process enactments that can be edited and remixed off-line to

visually tell a story). Machinima mods are thus a kind of extension of game software use experience that is not bound to the architecture of the underlying game software system, except for how the game facilitates a user's ability to structure and manipulate emergent game play to realize a desired play process enactment history.

3.4 Hacking Closed Game Systems

Hacking a closed game system is a practice whose purpose oftentimes seems to be in direct challenge to the authority of commercial game developers that represent large, global corporate interests. Hacking proprietary game software is often focused not so much on how to improve competitive advantage in multi-player game play, but instead is focused on expanding the range of experiences that users may encounter through use of alternative technologies [7,20]. For example, Huang's [7] study instructs readers in the practice of "reverse engineering" as a hacking strategy to understand both how a game platform was designed and how it operates in fine detail. This in turn enables reconfiguration of new innovative modifications or original platform designs, such as installing and running a Linux operating system (instead of Microsoft's proprietary CSS offering). While many game developers seek to protect their intellectual property (IP) from reverse engineering through end-user license agreements (EULAs) whose terms attempt to prohibit such action under threat of legal action, reverse engineering is not legally prohibited. Consequently, the practice of modding closed game consoles/systems is often less focused on enabling players to achieve competitive advantage when playing retail computer games, but instead may encourage those few so inclined for how to understand and ultimately create computing innovations through reverse engineering or other modifications.

Closed game system modding is a style of software extension by game modders who are willing to forego the "protections" and quality assurances that closed game system developers provide, in order to experience the liberty, skill, knowledge acquisition, conceptual appropriation ("pwned"), and potential to innovate, that mastery of reverse engineering affords. Consequently, players/modders who are willing to take responsibility for their actions (and not seek to defraud game producers due to false product warranty claims or copyright infringement), can enjoy the freedom to learn how their gaming systems work in intimate detail and to potentially learn about game system innovation through discovery and reinvention with the support of others like-minded [cf. 20]. Proprietary game development studios may sometimes allow for such mod-based infringement of their games. For example, the team of modders behind the hacking and conversion of the single-player CSS game, *Grand Theft Auto*, have produced an OSS (now GPL'd) game mod using code injection and hooking cheating methods to realize a networked multi-player variant called *Multi Theft Auto,* that Rockstar Games has chosen not to prosecute for potential EULA violation, but instead to embrace as GTA fan culture [25]. Nonetheless, large corporate interests may assert that their IP rights allow them to install CSS rootkits that collect potentially private

information, or that prevent the reactivation of previously available OSS (e.g., the Linux Kernel on the Sony PS3 game console[2]) that game system hackers seek to undo.

Finally, games are one of the most commonly modified types of proprietary CSS that are transformed into "pirated games" that are "illegally downloaded." Such game modding practice is focused on engaging a kind of meta-game that involves hacking into and modding game IP from closed to (more) open. Game piracy has thus become recognized as a collective, decentralized and placeless endeavor (i.e., not a physical organization) that relies on torrent servers as its underground distribution venue for pirated game software. As recent surveys of torrent-based downloads reveals, in 2008 the top 10 pirated games represented about 9M downloads, while in 2009 the top 5 pirated games represent more than 13M downloads, and in 2010 the top 5 pirated games approached 20M, all suggesting a substantial growth in interest in and access to such modded game products[3]. Thus, we should not be surprised by the recent efforts of game system hackers that continue to demonstrate the vulnerabilities of different hardware and software-based techniques to encrypt and secure closed game systems from would be crackers. However, it is also very instructive to learn from these exploits how difficult it is to engineer truly secure software systems, whether such systems are games or some other type of application or package.

4. Game Modding Software Tools and Support

Games are most often modded with tools providing access to unencrypted representations of game software or game platform. Such a representation is accessed and extended via a domain-specific (scripting) language. While it might seem the case that game vendors would seek to discourage users from acquiring such tools, a widespread contrary pattern is observed.

Game system developers are increasingly offering software tools for modifying the games they create or distribute, as a way to increase game sales and market share. Game/domain-specific Software Development Kits (SDKs) provided to users by game development studios represent a contemporary business strategy for engaging users to help lead product innovation from outside the studio. Once Id Software, maker of the *DOOM* and *Quake* game software product line, and also Epic Games, maker of the *Unreal* software game product line, started to provide prospective game players/modders with software tools that would allow them to edit game content, play mechanics, rules, or other functionality, other competing game development studios were pressured to make similar offerings or face a possible competitive disadvantage in the marketplace. However, the CSS versions of these tools do not provide access to the underlying source code that embodies the proprietary game

[2] For details, see http://en.wikipedia.org/wiki/George_Hotz#Hacking_the_PlayStation_3 .

[3] For 2008, see http://torrentfreak.com/top-10-most-pirated-games-of-2008-081204/
For 2009, http://torrentfreak.com/the-most-pirated-games-of-2009-091227/
For 2010, http://torrentfreak.com/call-of-duty-black-ops-most-pirated-game-of-2010-101228/

engine—a large software program infrastructure that coordinates computer graphics, user interface controls, networking, game audio, access to middleware libraries for game physics, and so forth. But the complexity and capabilities of such a tool suite mean that any one person, or better said, any game development or modding team, can now access modding tools or SDKs to build commercial quality CSS games through OSS extensions. But mastering these tools appears to be an undertaking likely to be only of interest to highly committed game developers who are self-supported or self-organized.

In contrast to game modding platforms provided by game development studios, there are also alternatives provided by the end-user community. One approach can be seen with facilities provided in meta-mods like *Garry's Mod* or the *AMX Mod X* mod-making package. Modders can use these packages to construct a variety of plug-ins that provide for development of in-game contraptions as game UI agents or user created art works, or to otherwise create comic books, program game conversions, and produce other kinds of user created content. But both packages require that you own a licensed CSS game like *Counter-Strike: Source*, *Half-Life2* or *Day of Defeat: Source* from Valve Software.

A different approach to end-user game development platforms can be found arising from OSS games and game engines. The *DOOM* and *Quake* games and game engines were released as free software subject to the GPL, once they were seen by Id Software as having reached the end of their retail product cycle. Thousands of games/engines, as already observed, have been developed and released for download. Some started from the OSS that was previously the CSS platform of the original games. However, the content assets (e.g., in-game artwork) for many of these CSS-then-OSS games are not covered by the GPL, and so user-developers must still acquire a licensed copy of the original CSS game if its content is to be reused in some way[4]. Nonetheless, some variants of the user-created GPL'd games now feature their own content that is limited/protected by Creative Commons licenses.

5. Opportunities and Constraints for Modding

Game modding demonstrates the practical value of software extension as a user-friendly approach to customizing software. Such software can extend games open to modding into diverse product lines that flourish through reliance on domain-specific game scripting languages, and integrated SDKs. Modding also demonstrates the success of end-users learning how to extend software to create custom user interface add-ons, system conversions, replayable system usage videos, as well as to discover security vulnerabilities. Game modding therefore represents a viable form of end-user engineering of complex software that may be transferable to other domains.

[4] For example, see http://assault.cubers.net/docs/license.html, accessed 13 April 2011.

Modding is a form of OSS-enabled collaboration. It is collaboration at a distance where the collaborators, including the game developers and game users, are distant in space and time from each other, yet they can interact in an open but implicitly coordinated manner through software extensions. Comparatively little explicit coordination arises, except when CSS game developers seek to embrace and encourage the creation of OSS game mods that rely on the proprietary CSS game engine (and also SDK), as a way to grow market share and mid share for the proprietary engine as a viable strategy to entry into the game industry.

However, mods are vulnerable to evolutionary system version updates that can break the functionality or interface on which the mod depends. This can be viewed as the result of inadequate software system design practice, such that existing system modularization did not adequately account for software extensions that end-users seek, or else the original developer wanted to explicitly prohibit end-users from making modifications that transform game play mechanics/rules or unintentionally allow for modification or misappropriation of copy protected code or media assets.

Last, one the key constraints on game modding in particular, and software extension in general, are the rights and obligations that are expressed in the original software EULA. Mods tend to be licensed using OSS or freeware licenses that allow for access, study, modification, and redistribution, rather than using free software licenses (e.g., GPLv2 or GPLv3). Software extensions that might be subject to a reciprocal GPL style license require that the base/original software system incorporate an explicit software architectural design that requires the propagation of reciprocal rights across an open interface, except through an LGPL software shim [1]. Otherwise, the scope of effectiveness and copyright protections of either free or non-free software (or related media assets) cannot be readily determined, and thus may be subject to copyright infringement or licenses non-compliance allegations. They may also be treated as social transgressions within a community of modders whose perceived ownership of the game mods demands respect and honor of a virtual license that may or may not be legally valid [2]. As the OSS community has long recognized, software rights and freedoms are expressed through IP licenses that insure whether or not a person has the right to access, study, modify, and redistribute the modified software, as long as the obligation to include a free software license is included that restates these rights in unalterable form, is included with the OSS code and its modified distributions.

6. Conclusions

Modding is emerging as a viable approach for mixing proprietary CSS systems with OSS extensions. The result is modded systems that provide the benefits of OSSD to developers of proprietary CSS systems, and to end-users who want additional functionality of their own creation, or from others they trust and seek to interact with through game play.

In contrast, modding is not so good for protecting software and media/content copyrights. Modding tests the limits of software/IP copyright practices. Some modders want to self-determine what copy/modding rights they have or not, and sometimes they act in ways that treat non-free software and related media as if it were free software. Who owns what, and which copy rights or obligations apply to that which is modded, are core socio-technical issues when engaging in modding.

This study helps to demonstrate that game modding is becoming a leading method for developing or customizing game software, whether based on proprietary CSS or OSS game systems. OSS-based software extensions are the leading ways and means for modding game-based user interfaces, converting games from one style/genre to another, for recording game play sessions for cinematic production and replay, and for hacking closed source game systems. Finally, the development of computer game software and tools itself represents a large community of OSS projects that has had comparatively little study, and thus merits further attention as its own cultural world as well as one for OSS development. This last consideration may be important as other empirical studies of OSS development that rely on data from SourceForge will increasingly include OSS game projects within large project samples. This study has therefore begun to address why and how these conditions have they emerged, and how are they put into practice in different game modding efforts. Future study should also consider whether and how modding might be applied and adopted in other application domains where CSS can be extended through OSS mods.

7. Acknowledgments

The research described in this paper has been supported by grants #0808783 and #1041918 from the National Science Foundation, and grant #N00244-10-1-0077 from the Naval Postgraduate School. No review, approval or endorsement implied. The anonymous reviewers also provided helpful suggestions for improving this paper.

8. References

1. Alspaugh, T.A., Asuncion, H.A., Scacchi, W. Intellectual Property Rights Requirements for Heterogeneously Licensed Systems, in *Proc. 17th. Intern. Conf. Requirements Engineering (RE09*), Atlanta, GA, 24-33, September 2009.
2. Alspaugh, T.A., Scacchi, W., Asuncion, H.A. Software Licenses in Context: The Challenge of Heterogeneously Licensed Systems, *J. Assoc. Information Systems*, 11(11), 730-755, November 2010.
3. Batory, D., Johnson, C., MacDonald, B., von Heeder, D., Achieving extensibility through product lines and domain specific languages: a case study, *ACM Trans. Software Engineering and Methodology*, 11(2), 191-214, 2002.
4. Burnett, M., Cook, C., Rothermel, G., End-User Software Engineering, *Communications ACM*, 47(9), 53-58, 2004.

5. El-Nasr, M.S., Smith, B.K., Learning Through Game Modding, *ACM Computers in Entertainment*, 4(1). Article 3B.
6. Fielding, R.T., Taylor, R.N., Principled Design of the Modern Web Architecture, *ACM Trans. Internet Technology*, 2(2), 115–150, 2002.
7. Huang, A., *Hacking the Xbox: An Introduction to Reverse Engineering,* No Starch Press, San Francisco, CA.2003.
8. Henttonen, K., Matinlassi, M., Niemela, E., Kanstren, T., Integrability and Extensibility Evaluation in Software Architectural Models—A case study, *The Open Software Engineering Journal,* 1(1), 1-20. 2007.
9. Kelland, M. From Game Mod to Low-Budget Film: The Evolution of Machinima, in H. Lowood and M. Nitsche (Eds.), *The Machinima Reader*, 23-36, MIT Press, Cambridge, MA, 2011.
10. Kücklich, Precarious playbour: Modders and the digital games industry, *Fiberculture*, issue 5, 2005. http://journal.fibreculture.org/issue5/kucklich.html, accessed 13 April 2011.
11. Leveque, T., Estublier, J., Vega, G., Extensibility and Modularity for Model-Driven Engineering Environments, *16th IEEE Conf. On Engineering Computer-Based Systems* (ECBS 2009), 305-314, 2009.
12. Lowood, H. and Nitsche, M. (Eds.), *The Machinima Reader*, MIT Press, Cambridge, MA, 2011.
13. Marino, P. *3D Game-Based Filmmaking: The Art of Machinima*. Paraglyph Press, Scottsdale, AZ, 2004.
14. Narayanaswamy, K., Scacchi, W. Maintaining Evolving Configurations of Large Software Systems, *IEEE Trans. Software Engineering*, SE-13(3), 324-334, 1987.
15. Parnas, D.L. Designing Software for Ease of Extension and Contraction, *IEEE Trans. Software Engineering*, SE-5(2), 128-138, 1979.
16. Postigo, H. Of mods and modders: Chasing down the value of fan–based digital game modifications, *Games and Culture*, 2(4), 300–313, 2007.
17. Postigo, H. Video Game Appropriation through Modifications: Attitudes Concerning Intellectual Property among Modders and Fans. *Convergence*, 14(1), 59-74, 2008.
18. Scacchi, W. Modeling, Integrating, and Enacting Complex Organizational Processes, in K. Carley, L. Gasser, and M. Prietula (Eds.), *Simulating Organizations: Computational Models of Institutions and Groups*, 153-168, MIT Press, 1998.
19. Scacchi, W. Understanding the Requirements for Developing Open Source Software, *IEE Proceedings—Software Engineering,* 149(1), 24-39, February 2002. Revised version in K, Lyytinen, P. Loucopoulos, J. Mylopoulos, and W. Robinson (Eds.), *Design Requirements Engineering: A Ten-Year Perspective*, LNBIP 14, Springer-Verlag, 467-494, 2009.

20. Scacchi, W., Free/Open Source Software Development Practices in the Game Community, *IEEE Software*, 21(1), 59-67, January/February 2004.
21. Scacchi, W. Free/Open Source Software Development: Recent Research Results and Emerging Opportunities, *Proc. European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering,* Dubrovnik, Croatia, 459-468, September 2007.
22. Scacchi, W. Game-Based Virtual Worlds as Decentralized Virtual Activity Systems, in W.S. Bainbridge (Ed.), *Online Worlds: Convergence of the Real and the Virtual*, Springer, New York, 225-236, 2010.
23. Sotamaa, O. When the Game Is Not Enough: Motivations and Practices Among Computer Game Modding Culture, *Games and Culture*, 5(3), 239-255, 2010.
24. Taylor, T.L., The Assemblage of Play, *Games and Culture*, 4(4), 331-339, 2009.
25. Wen, H., Multi Theft Auto: Hacking Multi-Player Into Grand Theft Auto With Open Source, *OSDir*, 25 May 2005, http://osdir.com/Article4775.phtml. Also see http://www.mtavc.com/ and http://en.wikipedia.org/wiki/Multi_Theft_Auto. All accessed 1 June 2011.
26. Yee, N., The Labor of Fun: How Video Games Blur the Boundaries of Work and Play, *Games and Culture*, 1(1), 68-71, 2006.

Modding as a Basis for Developing Game Systems

Walt Scacchi
Institute for Software Research
University of California, Irvine
Irvine, CA 92697-3455 USA
wscacchi@ics.uci.edu

ABSTRACT

This paper seeks to briefly examine what is known so far about game mods and modding practices. Game modding has become a leading method for developing games by customizing extensions to game software. The research method in this study is observational and qualitative, so as to highlight current practices and issues that can be associated with software engineering foundations. Numerous examples of different game mods and modding practices are identified throughout.

Categories and Subject Descriptors

D.2 [Software Engineering]: s*oftware development, software architecture, design methodology*

General Terms

Design, Human Factors.

Keywords

Computer games, software extension, game modding

Revised version appears in *Games And Software Engineering, GAS'11*, May, 2011, Waikiki, Honolulu, HI, USA. Copyright 2011 ACM 978-1-4503-0578-5/11/05…$10.00.

1. INTRODUCTION

User modified computer games, hereafter *game mods*, are a leading form of user-led innovation in game design and game play experience. But modded games are not new, clean-sheet standalone systems, as they require the user to have an originally acquired or authorized copy of the unmodded game.

Modding, the practice and process of developing game mods, is typically a "Do It Yourself" (DIY) approach to end-user game software engineering [2] that can establish both social and technical knowledge for how to innovate by resting control over game design from their original developers. At least four types of game mods can be observed: user interface customization; game conversions; machinima; and hacking closed game systems. Each enables different kinds of extension to the base game or game run-time environment. Game modding tools and support environments that support the creation of such extensions also merit attention. Subsequently, we conceive of game mods as covering customizations, tailorings, and remixes—that is, *software extensions*—of game embodiments, whether in the form of game content, software, or hardware denoting our space of interest.

The most direct way to become a game modder is through self-tutoring and self-organizing practices. Modding is a form of learning – learning how to mod, learning to be a game developer, learning to become a game content/software developer, learning computer game science outside or inside an academic setting, and more [3,13]. Modding is also a practice for learning how to work with others, especially on large, complex games/mods. Mod team efforts may also self organize around emergent software development project leaders or "want to be" (W.T.B.) leaders, as seen for example in the *Planeshift* open source MMOG development/modding project [13].

Game mods, modding practices, and modders are in many ways quite similar to their counterparts in the world of free/open source software development (FOSSD). Modding is to games, like FOSSD is to software — they are increasingly becoming a part of mainstream technology development culture and practice. Modders are players of the games they construct, just like FOSS developers are also users of the systems they develop. There is no systematic distinction between developers and users in these communities, other than there are users/players that may contribute little beyond their usage, word of mouth they share with others, and their demand for more such systems. At FOSSD portals like SourceForge.com, as of January 2011, indicates the domain of "games" appears as the third most popular project category with over 23K active projects. These projects develop either FOSS-based games, game engines, or game tools/SDKs, and all of the top 50 projects each have logged more than 1M downloads. So the intersection of games and FOSS covers a substantial social and technological plane, as both modding and FOSS development are participatory, user-led modes of system development that rely on continual replenishment of new participants joining and migrating through project efforts, as well as new additions or modifications of content, functionality and end-user experience [12,13,14]. Modding and FOSSD projects are in many ways experiments to prototype alternative visions of what innovative systems might be in the near future, and so both are widely embraced and practiced primarily as a means for learning about new technologies, new system capabilities, new working relationships with potentially unfamiliar teammates from other cultures, and more [cf. 14].

Consequently, game modding can be recognized as a leading method for developing or customizing game software. And software extensions are the leading ways and means for game modding.

This paper seeks to briefly examine what is known so far about game mods and modding practices. The research method in this study is observational and qualitative, so as to highlight current practices and issues that can be associated with software engineering foundations. Numerous examples of different game mods and modding practices are identified throughout to help distinguish empirically grounded observation from conjecture. All of the types of game mods and modding practices identified in this paper have been employed first-hand by game development projects led or produced by the author. Such observation can subsequently has served as a basis for further empirical study and technology development that ties together computer games and software engineering [12,13,14].

2. SOFTWARE EXTENSION

Game mods embody different techniques and mechanisms for software extension. However, the description of game mods and modding is often absent of its logical roots or connections back to software engineering. As suggested, mods are extensions to existing game software systems, so it is appropriate to review what we already know about software extensions and extensibility.

Parnas [10] provides an early notion of software extension as an expression of modular software design. Accordingly, modular systems are those whose components can be added, removed, or updated while satisfying the core system functional requirements. Such concepts in turn were integrated into software architectural design language descriptions and configuration management tools [7]. But reliance on software architecture descriptions is not readily found in either conventional game or mod development. Hentonnen and colleagues [6] examine how software plug-ins support architectural extension, while Leveque, et al. [8] investigate how extension mechanisms like views and model-based systems support extension also at the architectural level. Last, the modern Web architecture is itself designed according to principles of extensibility through open interfaces, migration across software versions, network data content/hypertext transfer protocols, and representational state transfer [4]. Mod-friendly networked multi-player games appear to take advantage of these capabilities. Elsewhere, Batory and associates [1] describe how domain-specific (scripting) languages and software product lines provide support software extension, and it now seems clear that such techniques are commonly used in games that are open for modding. Finally, FOSSD has become another approach to extensible software engineering in practice [14].

So software extensions and extensibility is a foundational concept in software engineering, and thus to no surprise, also foundational to the development of game mods. However, the logical connections and common/uncommon legacy remain under specified, which this paper seeks to address and update.

3. FOUR TYPES OF GAME MODS

Four types of game mods can be readily identified: user interface customizations, game conversions, machinima, and hacking closed game systems. Each is described in turn.

3.1 User interface customizations

User interfaces to games embody the practice and experience of interfacing users (game players) to the game system and play experience designed by game developers. Game developers act to constrain and govern what users can do, and what kinds of experience they can realize. Some users in turn seek to achieve some competitive advantage during game play by modding the user interface software for their game, when so enabled by game developers, to acquire or reveal additional information that the users believe will help their play performance and experience. User interface add-ons subsequently act as the

medium through which game development studios support game product customization as a strategy for increasing the likelihood of product success through end-user satisfaction [2].

Three kinds of user interface customizations can be observed. First and most common, is the player's ability to select, attire or accessorize a *player's in-game identity*. Second, is for players to customize *the color palette and representational framing borders* of the their game display within the human-computer interface, much like what can also be done with Web browsers and other end-user software applications. Third, are *user interface add-on modules* that modify the player's in-game information management dashboard that do not modify game play rules or functions. These add-ons provide additional information about game play or game state that may enhance the game play experience, as well as increasing a player's sense of immersion or omniscience within the game world through sensory or perceptual expansion. This in turn enables awareness of game events not visible in the player's current in-game view. Consequently, the first two kinds of customizations result from meta-data selections within parametric system functions, while the third represents a traditional kind of modular extension that does not affect the pre-existing game's functional requirements.

3.2 Game conversions

Game conversion mods are perhaps the most common form of game mods. Most such conversions are partial, in that they add or modify (a) in-game characters including user-controlled character appearance or capabilities, opponent bots, cheat bots, and non-player characters, (b) play objects like weapons, potions, spells, and other resources, (c) play levels, zones, maps, terrains, or landscapes, (d) game rules, or (e) play mechanics. Some more ambitious modders go as far as to accomplish (f) total conversions that create entirely new games from existing games of a kind that are not easily determined from the originating game. For example, one of the most widely distributed and played total game conversions is the *Counter-Strike* (CS) mod of the *Half-Life* (HL) first-person action game from Valve Software. As the success of the CS mod gave rise to millions of players preferring to play the mod over the original HL game, then other modders began to access the CS mod to further convert in part or full. Valve Software subsequently modified its game development and distribution business model to embrace game modding as part of the game play experience that is available to players who acquire a licensed copy of the HL product family. Valve has since marketed a number of CS variants that have sold over 10M copies as of 2008, thus denoting the most successful game conversion mod, as well as the most lucrative in terms of subsequent retail sales derived from a game mod.

Another example is found in games converted to serve a purpose other than entertainment, such as the development and use of games for science, technology, and engineering applications. For instance, the *FabLab* game [15] is a conversion of the *Unreal Tournament 2007* retail game, from a first-person action shooter to a simulator for training semiconductor manufacturing technicians in diagnosing and treating potentially hazardous materials spills in a cleanroom environment. However, this conversion is not readily anticipated by knowledge of the Unreal games or underlying game engine, though it maintains operational compatibility with the Unreal game itself. So game conversions can repurpose the look, feel, and intent of a game across application domains, while maintaining a common software product line [cf. 1].

Finally, it is common practice that the underlying game engine has one set of license terms and

conditions to protect original work (e.g., no redistribution), while game mod can have a different set of terms and conditions as a derived work (e.g., redistribution allowed only for a game mod, but not for sale). In this regard, software licenses embody the business model that the game development studio or publisher seeks to embrace, rather than just a set of property rights and constraints. For example, in *Aion*, an MMOG from South Korean game studio NCSoft, no user created mods or user interface add-ons are allowed. Attempting to incorporate such changes would therefore conflict with its end-user license agreements (EULA) and subsequently put such user-modders at risk of losing their access to networked *Aion* multi-player game play. In contrast, the MMOG *World of Warcraft* allows for UI customization mods and add-ons only, but no other game conversions, no reverse engineering game engine, and no activity intended to bypass WoW's encryption mechanisms. And, in one more variation, for games like *Unreal Tournament*, *Half-Life*, *NeverWinterNights*, *Civilization* and many others, the EULAs encourage modding and the free redistribution of mods without fee to others who must have a licensed game copy, but no reverse engineering or redistribution of the game engine required to run the mods. This restriction in turns helps game companies realize the benefit of increased game sales by players who want to play with known mods, rather than with the unmodded game as sold at retail. Mods thus help improve game software sales, revenue, and profits for the game development studio, publisher, and retailer

3.3 Machinima

Machinima can be viewed as the product of modding efforts that intend to modify the visual replay of game usage sessions. Machinima employ computer games as their creative media, such that these new media are mobilized for some other purpose (e.g., creating online cinema or interactive art exhibition). Machinima focuses attention to playing and replaying a game for the purpose of story telling, movie making, or retelling of daunting or high efficiency game play/usage experience [9]. Machinima is a form of modding the experience of playing a specific game through a recording of its visual play session history so as to achieve some other ends beyond the enjoyment (or frustration) of game play. These play-session histories can then be further modded via video editing or remixing with other media (e.g., audio recordings) to better enable cinematic storytelling or creative performance documentation. Machinima is thus a kind of play/usage history process re-enactment [cf. 11] whose purpose may be documentary (replaying what the player saw or experienced during a play session) or cinematic (creatively steering a play session so as to manifest observable play process enactments that can be edited and remixed off-line to visually tell a story). Machinima mods are thus a kind of extension that is not bound to the architecture of the underlying game system, except for how the game facilitates a user's ability to structure and manipulate emergent game play to realize a desired play process enactment history.

3.4 Hacking closed game systems

Hacking a closed game system is a practice whose purpose oftentimes seems to be in direct challenge to the authority of commercial game developers that represent large, global corporate interests. Hacking proprietary game software is often focused not so much on how to improve competitive advantage in multi-player game play, but instead is focused on expanding the range of experiences that users may encounter through use of alternative technologies [5,13]. For example, Huang's [5] study instructs readers in the practice of "reverse engineering" as a strategy to understand both how a game platform was designed and how it operates in fine detail, as a basis for developing new innovative modifications or

original platform designs, such as installing and running a Linux open source operating system (instead of Microsoft's proprietary closed source offering). While many game developers seek to protect their intellectual property (IP) from reverse engineering through EULA whose terms attempt to prohibit such action under threat of legal action, reverse engineering is not legally prohibited nor discouraged by the Courts. Consequently, the practice of modding closed game systems is often less focused on enabling players to achieve competitive advantage when playing retail computer games, but instead may encourage those few so inclined for how to understand and ultimately create computing innovations through reverse engineering or other DIY game system modifications. Closed game system modding is thus a style of software extension by game modders who are willing to fore go the "protections" and quality assurances that closed game system developers provide, in order to experience the liberty, skill and knowledge acquisition, as well as potential to innovate, that mastery of reverse engineering affords. Consequently, players/modders who are willing to take responsibility for their actions (and not seek to defraud game developers or publishers due to false product failure warranty claims or copyright infringement), can enjoy the freedom to learn how their gaming systems work in intimate detail and to potentially learn about game system innovation through discovery and reinvention with the support of others like-minded [cf. 13].

Finally, games are one of the most commonly modified types of software that are transformed into "pirated games" that are "illegally downloaded." Such game modding practice is focused on engaging a kind of meta-game that involves modding game IP from closed to (more) open. Game piracy has thus become recognized as a collective, decentralized and placeless endeavor (i.e., not a physical organization) that relies on torrent servers as its underground distribution venue for pirated game software. As recent surveys of torrent-based downloads reveals, in 2008 the top 10 pirated games represented about 9M downloads, while in 2009 the top 5 pirated games represent more than 13M downloads, and in 2010 the top 5 pirated games approached 20M, all suggesting a substantial growth in interest in and access to such modded game products. Thus, we should not be surprised by the recent efforts by game system hackers that continue to demonstrate the vulnerabilities of different hardware and software-based techniques to encrypt and secure closed game systems from would be hackers. However, it is also very instructive to learn from these exploits how difficult it is to engineer truly secure software systems, whether such systems are games or some other type of application or package.

4. GAME MODDING SOFTWARE TOOLS AND SUPPORT

Games are most often modded with tools that provide access to an unencrypted representation of the game software or game platform. Such a representation is accessed and extended via a domain-specific (scripting) language. While it might seem the case that game vendors would seek to discourage users from acquiring such tools, we observe a widespread contrary pattern.

Game system developers are increasingly offering software tools for modifying the games they create or distribute, as a way to increase game sales and market share. Game/domain-specific Software Development Kits (SDKs) provided to users by game development studios represent a contemporary business strategy for engaging users to help lead product innovation from outside the studio. Once id Software, maker of the *DOOM* and *Quake* game software product line, and also Epic Games, maker of the *Unreal* software game product line, started to provide prospective game players/modders with software tools that would allow them to edit game content, play mechanics, rules, or other functionality, other competing game development studios were pressured to make similar offerings or

face a possible competitive disadvantage in the marketplace. However, these tools do not provide access to the underlying source code that embodies the proprietary game engine—a large software program infrastructure that coordinates computer graphics, user interface controls, networking, game audio, access to middleware libraries for game physics, and so forth. But the complexity and capabilities of such a tool suite mean that any one, or better said, any game development or modding team, can now access modding tools or SDKs to build commercial quality games. But mastering these tools appears to be a significant undertaking likely to be only of interest to highly committed, would-be game developers who are self-supported or self-organized.

In contrast to game modding platforms provided by game development studios, there are also alternatives provided by the end-user community. One approach can be seen with facilities provided in *Garry's Mod* mod-making package that you can use to construct a variety of fanciful contraptions as user created art works, or to create comic books, program game conversions, and produce other kinds of user created content. But this package requires that you own a licensed game like *Counter-Strike: Source*, *Half-Life2* or *Day of Defeat: Source* from Valve Software.

A different approach to end-user game development platforms can be found arising from free/open source software games and game engines. The *DOOM* and *Quake* games and game engines were released as free software subject to the GPL, once they were seen by id Software as having reached the end of their retail product cycle. Hundreds of games/engines have been developed and released for download starting from the free/open source software that was the platform of the original games. However, the content assets for many of these games (e.g., in-game artwork) are not covered by the GPL, and so user-developers must still acquire a licensed copy of the original game if its content is to be reused in some way. Nonetheless, some variants of the user-created GPL'd games now feature their own content that is limited/protected by Creative Commons licenses.

5. OPPORTUNITIES FOR MODDING AND SOFTWARE ENGINEERING

Game modding demonstrates the practical value of software extension as a user-friendly approach to custom software. Such software can extend games open to modding into diverse product lines that flourish through reliance on domain-specific game scripting languages, and integrated software development kits. Modding also demonstrates the success of end-users learning how to extend software to create custom user interface add-ons, system conversions, replayable system usage documentaries and movies, as well as to discover security vulnerabilities. Game modding therefore represents a viable form of end-user engineering of complex software that may be transferable to other domains.

6. ACKNOWLEDGMENTS

The research described in this paper has been supported by grants #0808783 and #1041918 from the U.S. National Science Foundation, grants #N00244-10-1-0064 and #N00244-10-1-0077 from the Acquisition Research Program at the Naval Postgraduate School. No review, approval, or endorsement implied.

7. REFERENCES

[1] Batory., D., Johnson, C., MacDonald, B., von Heeder, D., Achieving extensibility through product lines and domain specific languages: a case study, *ACM Trans. Software Engineering and Methodology*, 11(2), 191-214, 2002.

[2] Burnett, M., Cook, C., Rothermel, G., End-User Software Engineering, *Communications ACM*, 47(9), 53-58, 2004.

[3] El-Nasr, M.S., Smith, B.K., Learning Through Game Modding, *ACM Computers in Entertainment*, 4(1). Article 3B.

[4] Fielding, R.T., Taylor, R.N., Principled Design of the Modern Web Architecture, *ACM Trans. Internet Technology*, 2(2), 115–150, 2002.

[5] Huang, A., *Hacking the Xbox: An Introduction to Reverse Engineering,* No Starch Press, San Francisco, CA.2003.

[6] Henttonen, K., Matinlassi, M., Niemela, E., Kanstren, T., Integrability and Extensibility Evaluation in Software Architectural Models—A case study, *The Open Software Engineering Journal,* 1(1), 1-20. 2007.

[7] Narayanaswamy, K., Scacchi, W. Maintaining Evolving Configurations of Large Software Systems, *IEEE Trans. Software Engineering*, SE-13(3), 324-334, 1987.

[8] Leveque, T., Estublier, J., Vega, G., Extensibility and Modularity for Model-Driven Engineering Environments, *16th IEEE Conf. On Engineering Computer-Based Systems* (ECBS 2009), 305-314, 2009.

[9] Marino, P. *3D Game-Based Filmmaking: The Art of Machinima*. Paraglyph Press, Scottsdale, AZ, 2004.

[10] Parnas, D.L. Designing Software for Ease of Extension and Contraction, *IEEE Trans. Software Engineering*, SE-5(2), 128-138, 1979.

[11] Scacchi, W., Modeling, Integrating, and Enacting Complex Organizational Processes, in K. Carley, L. Gasser, and M. Prietula (Eds.), *Simulating Organizations: Computational Models of Institutions and Groups*, 153-168, MIT Press, 1998.

[12] Scacchi, W., Understanding the Requirements for Developing Open Source Software, *IEE Proceedings—Software Engineering,* 149(1), 24-39, February 2002. Revised version in K, Lyytinen, P. Loucopoulos, J. Mylopoulos, and W. Robinson (Eds.), *Design Requirements Engineering: A Ten-Year Perspective*, LNBIP 14, Springer-Verlag, 467-494, 2009.

[13] Scacchi, W., Free/Open Source Software Development Practices in the Game Community, *IEEE Software*, 21(1), 59-67, January/February 2004.

[14] Scacchi, W. Free/Open Source Software Development: Recent Research Results and Emerging Opportunities, *Proc. European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering, Dubrovnik, Croatia, 459-468, September 2007.*

[15] Scacchi, W. Game-Based Virtual Worlds as Decentralized Virtual Activity Systems, in W.S. Bainbridge (Ed.), *Online Worlds: Convergence of the Real and the Virtual*, Springer, New York, 225-236, 2010.