Computer Systems Research

Ardalan Amiri Sani

Computer systems research

Finding the "right way" to build systems

What does it take?

- Systems programming
 - Programming (i.e., hacking) the OS kernel, hypervisor, core system services, drivers, etc.

What does it take?

• Systems programming

- Programming (i.e., hacking) the OS kernel, hypervisor, core system services, drivers, etc.
- Countless hours
 - Often a bug can take days or weeks to fix

Then why should you do it?

• Acquire valuable expertise

Then why should you do it?

- Acquire valuable expertise
- Experience the satisfaction of fixing a bug, and even better, make a difficult system work

Then why should you do it?

- Acquire valuable expertise
- Experience the satisfaction of fixing a bug, and even better, make a difficult system work
- The Turtles Project from OSDI'10
 - The authors did it simply because someone told them it can't be done
 - Now their code is integrated in Linux kernel

• Zongheng Ma



- Zongheng Ma
 - First author on our HotMobile'17 paper
 - Second author on our recent ASPLOS'18 paper

• Zhihao (Zephyr) Yao



• Zhihao (Zephyr) Yao

• First author on our recent ASPLOS'18 paper

Sugar: secure GPU acceleration for web browsers

- WebGL allows web apps to perform hardware accelerated 3D rendering using the power GPU
- Unfortunately, WebGL raises a lot of security concerns

An attack through WebGL

| | 🗅 WebGL WEBGL_dra x |
|------|---|
| | ← → C ③ 127.0.0.1:8000/376951/webgl-draw-buffers.html |
| | |
| = >_ | This test verifies the functionality of the WEBGL_draw_buffers extension, if it is available. |
| | On success, you will see a series of "PASS" messages, followed by "TEST COMPLETE". |
| | |
| | the structure struct |
| | *. tenos itiva |
| | |
| | on a stetirp tatev a styliphilist s.e. h[]sit≥tn totrevel a store by shit stateno Th. nee a opra sativia on a stretting tatev a styliphilist s.e. h[]sit≥tn totrevel a store totre store a store and store a store totre store a sto |
| | on a stetirp tetav a a wirpihilisi s |
| | un a metrip tervia e vuptini si sie niisuraten touravenatisia pisinia ustenoite, melejopra jaluvia e |
| | on a stettip terzy a stylphilist state inibiation to invested a state of the tasteno The more other with a son a stetting later a stylphilist stelling as |
| | on a stetup tarky a sturpubli st 3 ste heleture noti tved p ts intseton atal sturi ste nivda pi ts (In |
| Į | , d s trift zr ateprive. Noti tved p triftseton stal sthrift, ite nivda pi ts (Th |
| | ; a s is int 29 acebi tve. Hotrivia p is intered star star it. The prival pris ; int |
| A | i a s isThi 31 ateprive. Therefive a p isThiseton atel sthrifting in the nivation is in the start sthrifting a sisThi 32 ateorive in perivation is Thiseton area sthrifting and start start sthrifting a start |
| | ; a s isThi 33'ateprive. Notriva p isThiseton and sunlinke nivab pris ; IN ; a s isThi 34'ateprive. Notriva p isThiseton and sunlinke nivab pris ; Th |
| a, | <i a="" e="" hriaon<br="" hrist.="" i="" irs="" irzustath="" n="" nrep="" onebativora="" ot="" p="" s="" seta="" si="" sihr="" sti="" toxteta="" virp="">si sihr virp a si nrev i si si i hriaon</i> |
| | st sum vup a «hristike n toxieta p is suf air svata in skyl on etalivpra levol mep tr. a sti 'hriaon si sihi 'vip a «hristike n tovieta p is suf air svata in skyl on etaliona a of of ot of the tr. a skyl (hriaon |
| | zi strum kurp a «hristike" ni tostete pitisisete tirevistis thi sisti ometativpra iciotince itrsia isti. "hri eon za zakri viero a "hristike" ni tostete Φi isizere urevisterni sisti ometativpra iciotince itrsia isti. "hri son za afkri viero a "hristike" ni tostete Φi isizere urevisterni sisti ometativpra iciotince itrsia isti. "hri son |
| | st sthriving a shristike in tokteta pitissata trisvisisih siyi on eta tuppi se otimepitis a isti ihriaon st shristike in tokteta pitissus tircvisisih siyi on stattupra relotince itraalisti ihriaon |
| | . ? το την αυτό τον βηδά: . c în tonte : The i : set a travat a the s : J'on crait wora re of nep tra . B sat i ? hr a sat si sint our a : |
| | 25 This is a private note. This is a private note. This is a private note. This is a pri 26 This is a private note. This is a private note. This is a private note. This is a pri |
| | 24 This is a private note. This is a private note. This is a private note. This is a pri |
| | 22. This is a private note. This is a private note. This is a private note. This is a pri 23. This is a private note. This is a private note. This is a private note. This is a pri |
| | 21 This is a private note. This is a private note. This is a private note. This is a pri |
| | pote This is a pri |

What is the problem?



How we solved it



How we solved it



Sugar in practice!



Summary

- Systems research is difficult but awesome
- If you like the challenge and you think you can do well at systems programming, send me an email!
 - ardalan@uci.edu