THE RISE OF MULTI-FACTOR AUTHENTICATION

A PRESENTATION BY GEOFFREY TUCKER
INTRODUCTION

1. What is wrong with passwords?
2. How are passwords being compromised?
3. How can we improve our security beyond passwords?
4. What is in store for the future of online security?
THE PROBLEM WITH PASSWORDS

• Passwords are rarely ever changed

• Most people prefer short, easy-to-remember passwords

• People tend to re-use their password(s) across multiple applications

• Answers to security questions could be revealed through online profiles
THE SOLUTION: PASSWORD MANAGERS! ...RIGHT?

• Easy way to remember large numbers of complex, secure passwords
• Safer than using one password for all websites
• The user must still remember a secure master password
• Exposes the user to a single point of failure
HOW ARE PASSWORDS BEING COMPROMISED?

• Password guessing
• Brute-force / dictionary attack
• Keystroke logging
• Phishing, pharming
• Shared computers
• Man in the middle
HOW CAN WE IMPROVE OUR SECURITY?
MULTI-FACTOR AUTHENTICATION

**KNOWLEDGE FACTORS**
Things only the user knows

**INHERENCE FACTORS**
Things only the user is

**POSSESSION FACTORS**
Things only the user has
KNOWLEDGE FACTORS
THINGS ONLY THE USER KNOWS

• Passwords
• Secret questions
• Personal identification numbers (PIN)
INHERENCE FACTORS
THINGS ONLY THE USER IS

- Fingerprints
- Voiceprints
- Iris scan
POSSESSION FACTORS
THINGS ONLY THE USER HAS

• Mobile phones
• Connected tokens
• Disconnected tokens
POSSESSION FACTORS

MOBILE PHONES

• SMS one-time password
• Smartphone push
POSSESSION FACTORS

CONNECTED TOKENS

• Magnetic stripe cards
• Contact smart cards
• Contactless smart cards
POSSESSION FACTORS

DISCONNECTED TOKENS

• Sequence-based
• Time-based
• Challenge-Response
THE FUTURE OF ONLINE SECURITY

• Two or three-factor authentication on all critical accounts
• Password managers become increasingly common
• Magnetic stripe cards will eventually be replaced by smart cards
• Hackers and researchers will continue to push the boundaries
THANK YOU

... any questions?