CyberSecurity Challenges

Guest Lecture
Current Challenges in Cyberinfrastructure
Rensselaer Polytechnic Institute (RPI) Guest Lecture

Von Welch
April 9, 2011
About me

• Applied researcher in cybersecurity for scientific computing.
• Designed, developed and operated new security paradigms to support bleeding edge distributed scientific cyberinfrastructure (CI).
• Authored two RFCS and several dozen peer-reviewed papers.
This presentation

- Survey of challenges in cybersecurity on the Internet
- Certainly not comprehensive
  - Other topics: SCADA, medical devices, self-driving cars, etc.
- All opinions are mine.
- All the images aren’t mine.
The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

"Security is the process of maintaining an acceptable level of perceived risk." - Richard Bejtlick

"measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack"

http://www.merriam-webster.com/dictionary/cybersecurity

Cybersecurity – My version

The art and science of managing the risks from malicious entities to a computer system supporting an organization’s mission.
What shapes cybersecurity?
Starts with technology.

For example, Internet early 90’s was all about technology.

(There was a time commercial use of the Internet was a hot debate.)
Then follows how people use, misuse and pay for the technology.

It has been proven over and over that no amount of “it’s not secure enough” trumps economics or human behavior.
The third piece of the environment is laws and policies.

The difference between what is possible and permissible is the difference between techies using it and the general population.
The three areas feed into each other and changes in one will drive changes in the other.

The more intermixed a problem, the more difficult it is.

Here be dragons.
Some observations

• What’s possibly technically >> what’s done technically in practice.
• Economics is currently the biggest influence.
• Human behavior and technology are close seconds.
• Policy and Legal is growing.
Three phases of cybersecurity

• Prevention
• Detection
• Recovery

• Don’t think you will prevent all attacks or detect them before they do harm.
• How do you balance your resources across the three?
On to some challenges...
Authentication

• Who are you?

• As opposed to Authorization – what are you allowed to do?

• Today this is mainly passwords
• Can also be smart cards, biometrics, etc.
Passwords

“Security geeks aren’t interested in making passwords work because everyone knows that they’re insecure, and all the real action is in PKI smart cards single sign-on identity-based encryption biometrics federated identity OpenID.”

(Strike thoughts in original text.)
Passwords

• Here to stay for a good while.
• Lots of rules of thumb….
  • Writing passwords down is bad?
  • How often should you change your password?
  • Is your password more likely to be guessed or sniffed?
• Is a good password on my computer good on my smart phone?
Passwords…

• Passwords are secret, so they are hard to research.

• Ironically, best data is coming from exposed password data bases.

• For some good reading, see Cormac Herley’s work.
  https://research.microsoft.com/en-us/people/cormac/
Other authentication issues

• Alice and Bob never actually talk, their computers do.
• More and more we are authenticating password managers, applications, web browsers, security tokens, smart phones, etc.
• How do we manage when there are dozens of “you”?
Other authentication issues

• Federated identity, Facebook Connect, OpenId, Oauth….

• Everybody wants you to trust them
• No one wants to trust someone else

• Economics is driving it?
PKIs

- Cybersecurity gets run over by economics
- When users can’t judge trustworthiness, they go with cheapest...
PKI – next generation?

• Is there a better model?
  • Tie to DNS with Dane?
  • Distributed verification with Perspectives/Convergence?
  • Make everything public with Sovereign Keys?
• Very complicated mix of economics, usability and security.
Software Assurance (SwA)

• Economics means time-to-market will win over security in almost all cases.
  • We’re lucky when it works, much less works securely.
• Unless legal kicks in and brings liability for bad software, we need to drive cost of security software down so it works with economics
Software Assurance

• What can technology do?
  • Improve software development
  • Improve SwA tools and techniques
  • Make them easy to use so developers use and benefit from them.

• Or other words, make them cheaper.
Systems Assurance

• Harder problems are systems-level: integration, deployment
• What exactly does each component provide and assume? What are the gaps/misassumptions when it all gets put together?
• When it fails, how do you fix it?
Security Metrics

- Will deploying X make me more secure?
- Is it worth $N to do so?
- Am I more secure today than yesterday?

https://xkcd.com/538/
Security Metrics

- Long history of struggle in this space.
- I think it has to take threats into accounts: Changes in the world more important than changes I make.
- For example, Anonymous/Lulzsec/hackivism changed the game (at least for a while) more than any technology.
Privacy/Anonymity

• A very serious issue in some parts of the world.
• Increased computing power and access to multiple data sets is breaking down anonymity and privacy protocols.
  • Not to mention economic incentives.
• Integration with real world devices like cell phones adds to the challenge.
Data access for research

- Accessing data for cybersecurity research is a challenge
- Due to privacy – need consent, hard to gather timely information
- Due to danger – Malware
- Honeypots in various forms address this
- Need framework for research – technical, ethical, legal
“Cyberwar” and “Cybercrime”
“Cyberwar” and “Cybercrime”

- And “cyberespionage”, “cyberterrorism”, “on-line piracy”…
- The different in terminology here matters.
  - Military vs law enforcement vs corporate…
- Big policy debate right now and the choice of words will shape it.
Attackers vs Defenders

- Right now, attackers have the advantage.
  - Even the best security companies get hacked.
- I think this has always been true on the Internet.
- Changing this will require technical, legal and economic changes.
  - Attribution, punishment, etc.
Attribution

• Who just attacked me?
  • Botnet?
  • Hacked system? (or a string of them)
  • Malware?
  • Some dynamic IP?
  • A hacker using their own computer?

• Uncertainty in attribution is a big problem with cyberdeterrence.
Law Enforcement Access

- Encrypting communications, data-at-rest, etc. is good for security.
- Make LE’s job harder.
- Requiring backdoors has huge economic, privacy and security impacts.
- One person’s LE is another person’s evil government.
Intrusion Detection

- Is getting harder…
- Encryption hampers network IDS
- Higher and higher volume
- Self-modifying viruses and other attacks
When things go wrong?

• Never assume your cybersecurity won’t be broken.
• How could we handle a foundational technology being broken?

After RSA Breach, Are SecurID Tokens in Jeopardy?

By Jeremy Kirk, IDG News

The intrusion by hackers of security giant RSA, a unit of EMC, has left customers and analysts wondering if it is still safe to use millions of the one-time passcode tokens used to log into enterprise IT systems.

http://www.pcworld.com/businesscenter/article/222559/after_rsa_breach_are_securid_tokens_in_jeopardy.html
Dealing with Failure

- Depending on the context:
  - Containment
  - Recovery
- Asking users what to do is doomed.
Further Reading

- Real world security engineering: Bruce Schneier, Peter Gutmann, Ross Anderson, Cormac Herley, IEEE Security and Privacy
- Legal issues with data access for cybersecurity research: Aaron Burstein (UCB), Erin Kenneally (CAIDA)
Summary

- Cybersecurity depend on a confluence of technical, economics, human behavior and legal influences.
- Tough challenges are at the intersection of the above.
Thank you

• Von Welch
  vwelch@indiana.edu