



Network Security: Now and the Future - be prepared for unknown

Chun-Jen (James) Chung

Arizona State University

Agenda

- The World of Security Now
- 1990s Security vs Early 2000s vs Late 2000s
- Attacks, Vulnerabilities and Defenses
- Now and in the Future
- What Works and What Doesn't?
- What Will Happen?
- How to prepare for network security job?

What is Security Today?

- Fighting hackers?
- Protecting networks?
- Fixing vulnerabilities?
- Selling “boxes”? 😊
- Managing risk?
- Securing information?





- Q: Why Start Security From 1990s?
- A: Before 90s, There Was Security (Of Course!), But **No Security Industry!**

Trends: 1990s

- **Explosive global malware: Blaster, Slammer, ILoveYou**
- **Server exploits: IIS is a kind of Swiss cheese**
- **Hacking for fun and fame...mostly: system penetrations, DDoS “for fun”**
- **Buffer overflows everywhere**
- Think about it! - we call it “*good old days!*” 😊

Trends: Early 2000s

- Small circulation **commercial malware**, spyware (but lots of it!)
- **Bots: “*industrial revolution*” in hacking ([video](#))**
 - **Google “How to Steal a Botnet and What Can Happen When You Do ” ([video](#))**
- **Web and “[Web 2.0](#)”**
 - **[Top 10 Web 2.0 attacks](#)**
- Rapid growth of **client-side attacks**
- **Hacking for money: Phishing, Spam, [DDoS for ransom](#), etc.**

Trends: Late 2000s - Future

- **Mobile malware? Cell/mobile phones, PDAs, other connected devices**
- **New Technologies: VOIP, “Web 2.0”, Tor, etc**
- **More application and web application hacking:** more stuff moves to the web
- **Attackers focus more on data, less on infrastructure**
- **Semantic Attacks?**
 - <http://www.bloomberg.com@www.badguy.com>
 - WWW.BL00MBERG.COM
- **Cloud Computing and Security**
 - **Virtualization security**
 - **New Internet Infrastructure (GENI)**
 - **CSE591 (started from Spring 2011) Virtualization and Cloud Computing**
 - **CSE548 Advanced Network Security**

Attackers of Today

- Phisher
- Other ID Thief
- Bot Herder (for rental bots)
- Spammer (on Owned boxes)
- Malicious Hacker

Attackers of Tomorrow

- Software engineer?
- VOIP or SMS Spammer?
- What is the application?
- Google? Cloud providers?
- More mobile...

Someone we don't know about:

- Find 5 ways to make money with computers **or mobile devices, illegally**

Don't forget cyberwar

- Georgia Takes a Beating in the Cyberwar With Russia ([link](#))

Vulnerability of Today

- Good Old Buffer Overflow, Format String, etc
- Other Browser Bugs
- Client Software Holes
- [SQL Injection](#)
- Cross-site scripting (XSS) and Cross-site request forgery (CSRF)

**SANS Top 20 (www.sans.org/top20) and
OWASP Top 10 (www.owasp.org/)**

Vulnerability of Tomorrow

- **More web exploitation: vulnerabilities and “inherent” web weaknesses (HTTP, etc)**
- **Fun with web services, “XML vulnerabilities”**
- **Business logic weaknesses: application does X when it should do Y**
 - These “vulnerabilities” are really hard to find!
- **New Bug Types: Maybe, Maybe Not ...**
- **Weak security infrastructure (Cloud, etc.)**

More Places to Look ...

New Technologies - **New Security Implications**

- VOIP (MITM, ARP spoof, DoS, buffer-overflow, etc...)
- Virtualization and cloud computing
- More “secure hardware” (TPM)
- GSM and more “wireless everything”
- “Social networking” and other “Web 2.0” stuff
- “Intelligent” networks, e.g., Software Defined Network (SDN) security

Defenses of Today

- Anti-virus / anti-spyware
- Firewalls and “firewalling” network gear
- Network intrusion detection
- Network intrusion prevention and UTM (unified threat management)
- NAC (cisco network admittance control) and NAP (microsoft network access protection)
- Host (mostly server) intrusion prevention
- Vulnerability scanners
- Encryption
- Multi-factor authentication
- User awareness
- System hardening and patch management

Do These Really Work?

Defenses of Tomorrow

Best prediction: **more of the same!**

- More encryption (including *bad!*) *everywhere*
- Secure coding? Code analysis tools?
- XML firewalls?
- VOIP defenses?
- HIPS with full behavior blocking and “hive intelligence”?
- Auditing Everything? Logs, Logs, Logs!
- Mobile anti-malware?
- Monitoring (Data Provenance), high speed Internet Security (10 Gig Ethernet, petabyte core network, etc.)
- Smart Grids? Smart home? Smart (intelligent) transportation systems?

“Security Laws” of Today (US)

- [Sarbanes – Oxley](#), [GLBA](#), etc
- [HIPAA](#), [FISMA](#)
- [PCI DSS](#)
- [ISO27001](#), [ITIL](#), [COBIT](#), etc
- Standards: [CVSS](#), [CEE](#), [OVAL](#), etc

Trend: control assurance, audit, proof of “due diligence”, documentation, processes (such as incident response), breach disclosure, *privacy*

Wishful Thinking?

A few things we NEED in security future! And probably won't get for a while

- Security **metrics**
 - Measure “badness”, security effectiveness and efficiency, security process strength
- Defenses ready for the “unknown unknowns”
 - Well, can I *dream for a second?*
- Smarter IT **users?**

Security Purchasing: Today and Next

Why People **Buy Security**?

- Cause everybody else does 😊
- To prevent *this from happening ... AGAIN!!!*
- Due to a law or a regulatory mandate
- Cause there is value in this ... but how do you know (*you don't!*)?

Final Thoughts

- Security is here not because of “TCP/IP” or Mr. Bill G. It is here because of **humans** 😊
- New technologies -> new attacks -> new defenses: **endless cycle**
- **Go small, go convenient, go portability, go wireless, go social networks, go high bandwidth, go smarter (dummier), go dynamic, and go with it (attack).**