Cyber Security

How to Avoid Being the Next Headline

Michael S. Kirkpatrick, Ph.D.
Department of Computer Science

JAMES MADISON UNIVERSITY®

Two-step plan

- Fire all your workers
- Destroy all your computers

Success is still not guaranteed

Verizon DBIR* findings

- End-point security is weak
  - *Dominant threats are hacking (81%) and malware (69%)*
- Organized crime targeting easy victims
  - *79% were targets of opportunity*
- Discovery is not obvious
  - *92% discovered by third party*
- Attacks are **fast**
  - *85% attack to compromise in* ***minutes or seconds***

*2012 Data Breach Investigations Report, Verizon RISK Team

No rules, no silver bullet

Image source: CERT, with unknown attribution

End-point security

- No platform is safe
  - *Malware for Macs, Linux and VMs, too*
  - *Cross-platform exploits (Java, Flash, browser-based)*
- Threats emerge faster than defenses
  - *60,000 new malware examples found* ***per day***
- Absolute safety is impossible

A tale of two hacks

Unpatched vulnerability

HBGary
Detecting Tomorrow's Threats Today

CEO password

http://www.hbgaryfederal.com

Password database:

- MD5 protected
- passwords

Unpatched vulnerability

Source: arstechnica.com

A tale of two hacks

Password reset link

Temporary password

What's your mother's maiden name?

Billing address and last 4 digits of your CC number?

I "fo pa

I forgot the answer that I made up.

Pa rd re nk

iCloud

Source: slate.com

Lessons learned

- Strong, **unique** passwords (min. 16 chars)
  - *Use a password manager (KeePass, Sxipper)*
  - *Better: use public key encryption*
- Patch and update software
- Use multi-factor authentication
- Complexity == vulnerability
- Use full-disk encryption, not remote wipe
  - *Windows BitLocker, OS X FileVault, TrueCrypt*

Lessons learned

- Email is **not** secure
  - *Links are inherently dangerous*
  - ***Never*** *click on links in emails*
  - ***Never*** *send sensitive data over email*
- Practice healthy skepticism
  - *If you didn't go looking for it, don't install it*

Technical guidelines

- All passwords should be hashed and salted
  - *Use SHA-256 or bcrypt, not MD5 or SHA-1*
  - *Free online classes at https://www.coursera.org/*
- Use secure coding practices
  - http://www.cert.org/secure-coding/
- Use network-based and host-based intrusion detection systems (Snort, Tripwire)

One last observation

Security failures follow incentive failures

The good news

- Defenses exist
  - *97% stopped by simple or intermediate controls (firewalls, changing default passwords, IDS, anti-virus, auto-updates)*
- Best practices are...best practices
  - *96% were not PCI DSS compliant*
- You are probably not being targeted by the really tough attacks
  - *79% were targets of opportunity*