Cybersecurity for Individuals

Eric Jacksch, CPP, CISM, CISSP

June 10, 2015

OPCUG

Disclaimer

- This presentation focuses on common threats faced by individuals
- Information is provided on an as-is basis without any warranty or liability
- All opinions expressed are mine alone

Tonight…

- Selected cybersecurity threats
- Cyber self-defence
- Q&A

Threat categories

- Automated scanning
- Internet surveillance
- Opportunistic attacks
- Targeted attacks
- Natural disasters and accidents

Automated scanning

- Goals
  - Research
  - Identify vulnerable systems for later exploitation

Automated scanning

- Vectors
  - Automated scans and probes
  - HTTP, HTTPS, SSH, SMTP, SIP

Automated scanning

- Actors
- Researchers
- Hackers

Automated scanning

- Assessment
  - Minimal impact unless home firewall is vulnerable or port-forwarding is used

Opportunistic attacks

- Goals
  - Steal credentials
  - Serve botnets
  - Extortion

Opportunistic attacks

- Vectors
  - Malicious email attachments
  - Email links to phishing sites for credential theft
  - Email links to hostile web sites that exploit browser and plugin vulnerabilities
  - Malicious web sites that exploit a browser and plugin vulnerabilities

Opportunistic attacks

- Actors
  - Hackers
  - Organized crime

Opportunistic attacks

- Assessment
  - Significant risk to individuals, especially those who do not regularly apply security patches and who engage in high-risk online behaviour

Internet surveillance

- Goals
  - Data for targeted advertising
  - Widespread metadata collection
  - Full content data collection
  - Access to stored data

Internet surveillance

- Vectors
- Cookies
- Website activity
- Search history collection
- Backbone data collection
- Court orders and agreements with providers
- Hacking ISPs and telecom providers

Internet surveillance

- Actors
- Advertising networks
- Governments

Internet surveillance

- Assessment
  - Significant privacy risk to individuals
  - Corporations generally use data for advertising only
  - Western governments are generally only targeting criminals and terrorists, but that could change…

Targeted attacks

- Goals
  - Persistent, long-term access to networks, computers, and data
  - Compromise and install implants for future use

Targeted attacks

- Vectors
  - Malicious email with zero-day exploits
  - Spear-phishing to hostile websites with zero-day exploits
  - Web session redirection and session hijacking

Targeted attacks

- Actors
  - Organized crime
  - Competitors
  - Governments

Targeted attacks

- Assessment
  - Most home users are not targets
  - Some may be targeted to gain access to their employer's assets

Natural disasters and accidents

- Consequences
  - Loss of availability (temporary or permanent)
  - Data destruction

Natural disasters and accidents

- Vectors
  - Natural disasters (fire, flood, storms, earth movement)
  - Power spikes, sags, brownouts, blackouts
  - Accidents at and around the keyboard
  - Equipment failure

Disasters and accidents

- Assessment
- Moderate risk
- Increases over time, especially with regard to hardware failures

Cyber self-defence for individuals

- Baseline security
- Enhanced security
- Cloud services
- Mobile devices

Baseline security

- Backups
- Internet behaviour
- Password discipline
- Patching
- Firewall
- Antivirus
- Separate computers for work and family members

Enhanced security

- UTM/NGFW
- VPN
- Network separation (especially work and family)

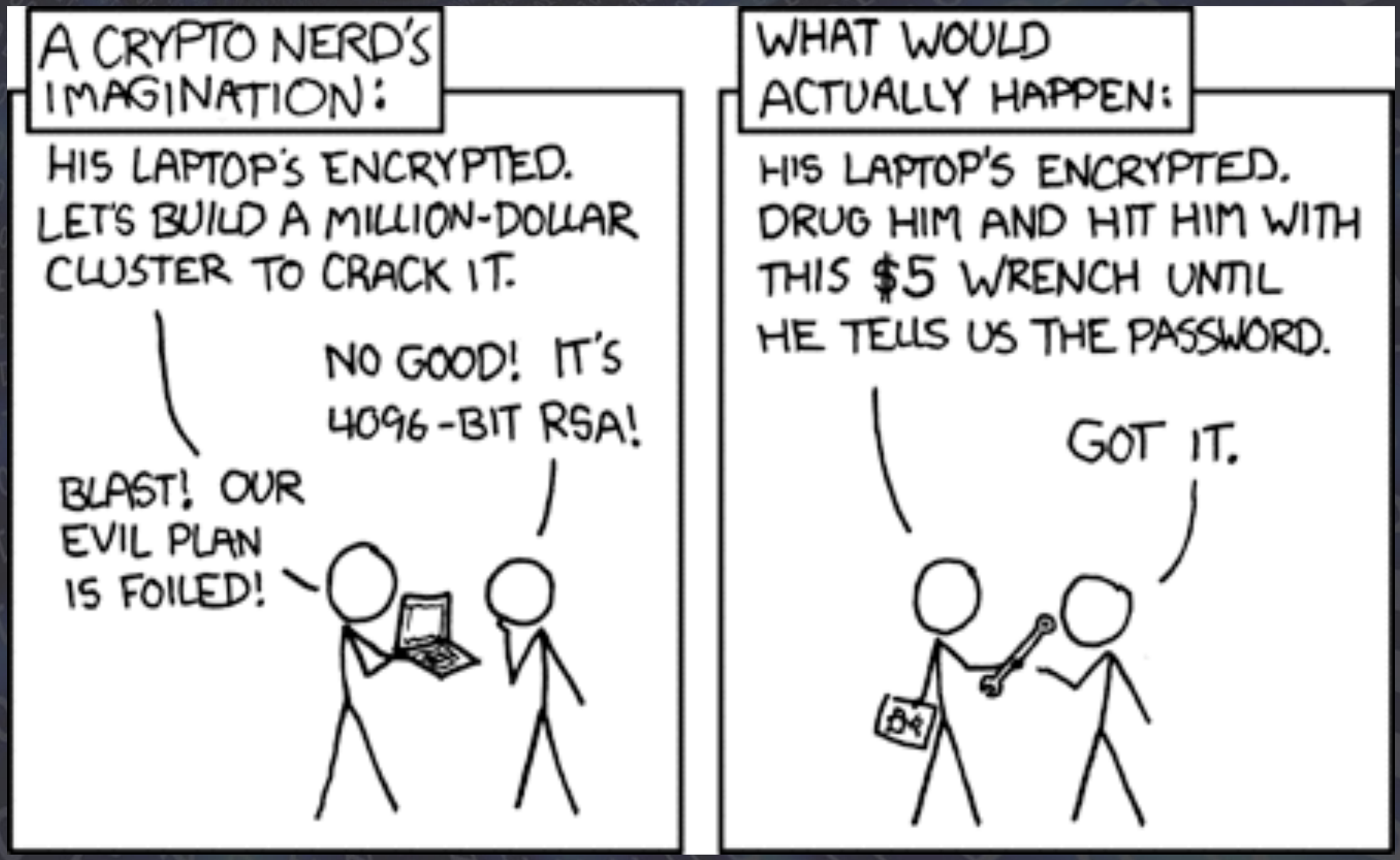
Cloud services

- Choosing a provider
  - Reputation and financial stability
  - Security and privacy policies
  - Legal jurisdictions and related issues
- Some data doesn’t belong in the cloud
- Use discretion on social media sites

Mobile devices

- Full disk/device encryption
- Password/PIN
- Consider border search implications
- Dedicated computer for travel?

xkcd on security



Questions?

eric@jacksch.com
https://securityshelf.com