Introduction to Cybersecurity and Hacking

Andrew Sanford | BYU

Welcome!

To the workshop, BYU, and Utah!

About Me

- Concurrently getting BS and MS of IS, emphasis in PhD Prep.
  - Other coursework in cybersecurity
- Certifications
  - CompTIA Security+
  - ACE Certified Forensics Examiner
- Internships at:
  - EY (formerly Ernst & Young)
  - RiskRecon
- Academic research
  - Recent Wells Fargo account fraud *(accepted for publication)*
  - Ezubao Ponzi Scheme *(in progress)*
  - Adapting cybersecurity principles to accounting fraud prevention/detection *(in progress)*

Overview

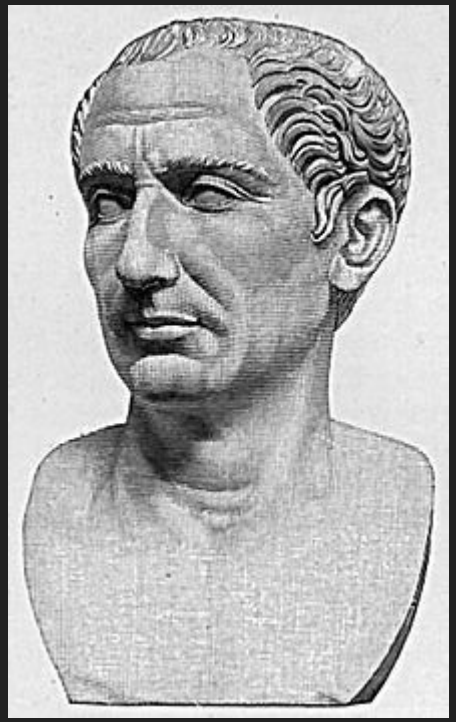
- Workshop Objective: Learn the basics of security and know where you can learn more

- Cryptography
- Attacker Types
- Major Threats and Mitigation Techniques
  - Physical
  - Social Engineering
  - Digital
- Current Events & the Future
- Kali Linux

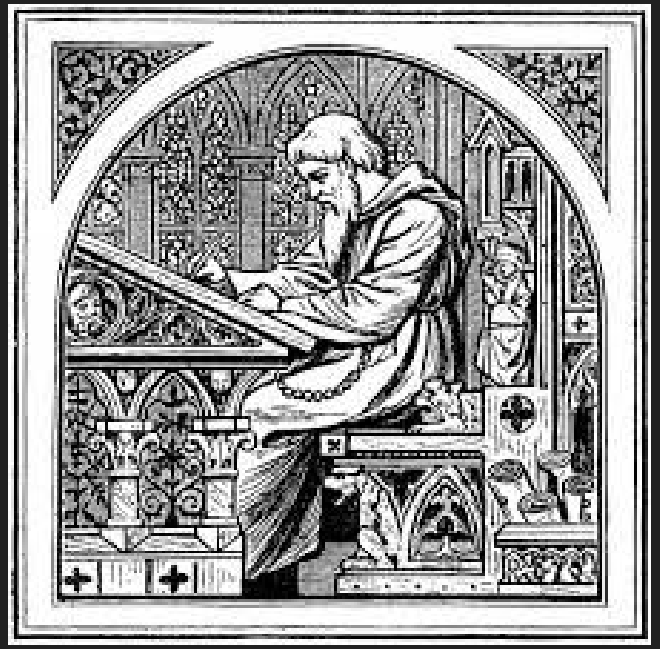
****Do not use what you learn without appropriate and prior authorization****

Cryptography

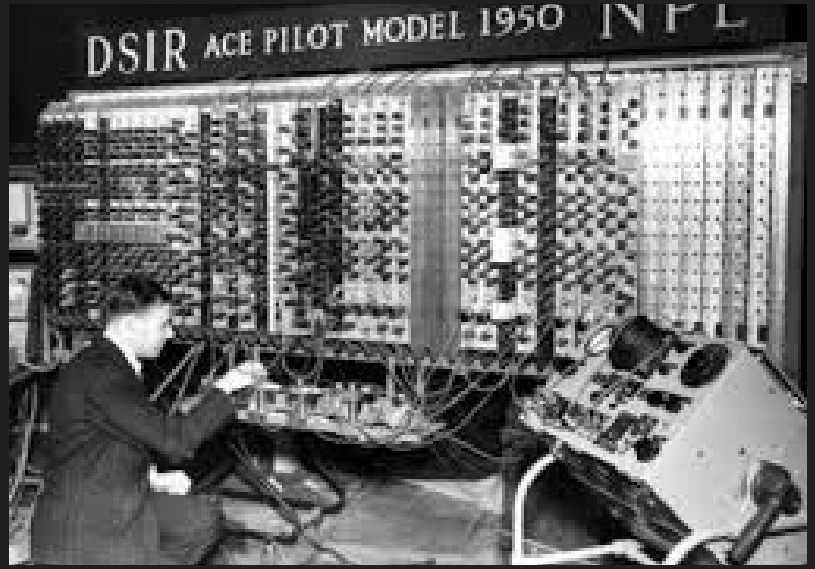
Early Encryption - Caesar Cipher



Early Decryption - Arabs and Christian Monks

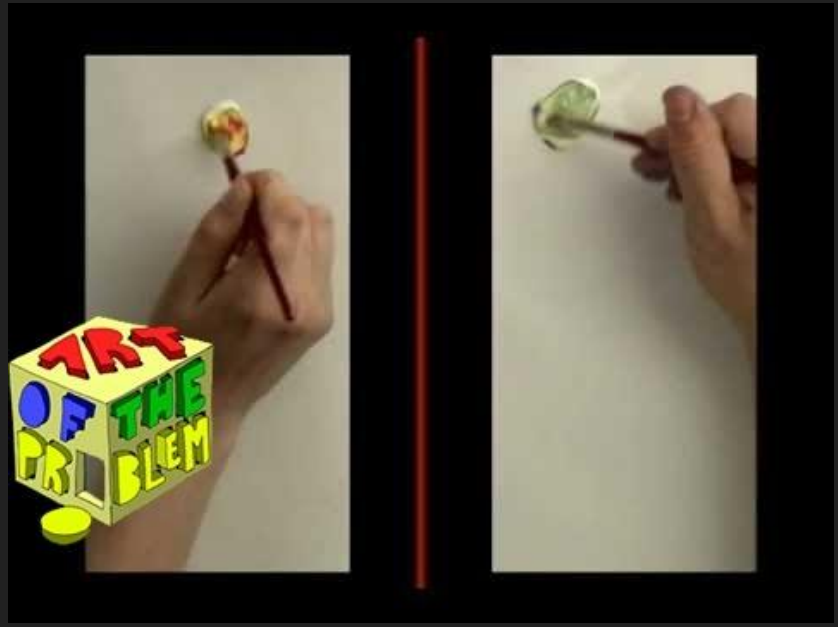


Electromechanical - WWII & Enigma



Modern Cryptography

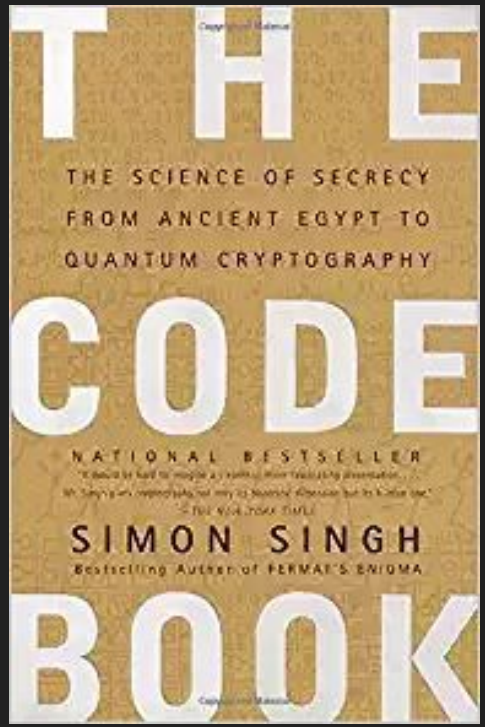
- Complex mathematical algorithms
- 2 Main Types:
  - Symmetric
    - AES
  - Asymmetric
    - Diffie-Hellman Key Exchange
    - RSA
  - The internet uses both



- Crytpo is a cat-and-mouse game, with encryption winning at the moment
  - And for the foreseeable future, even with quantum computing

Additional Learning

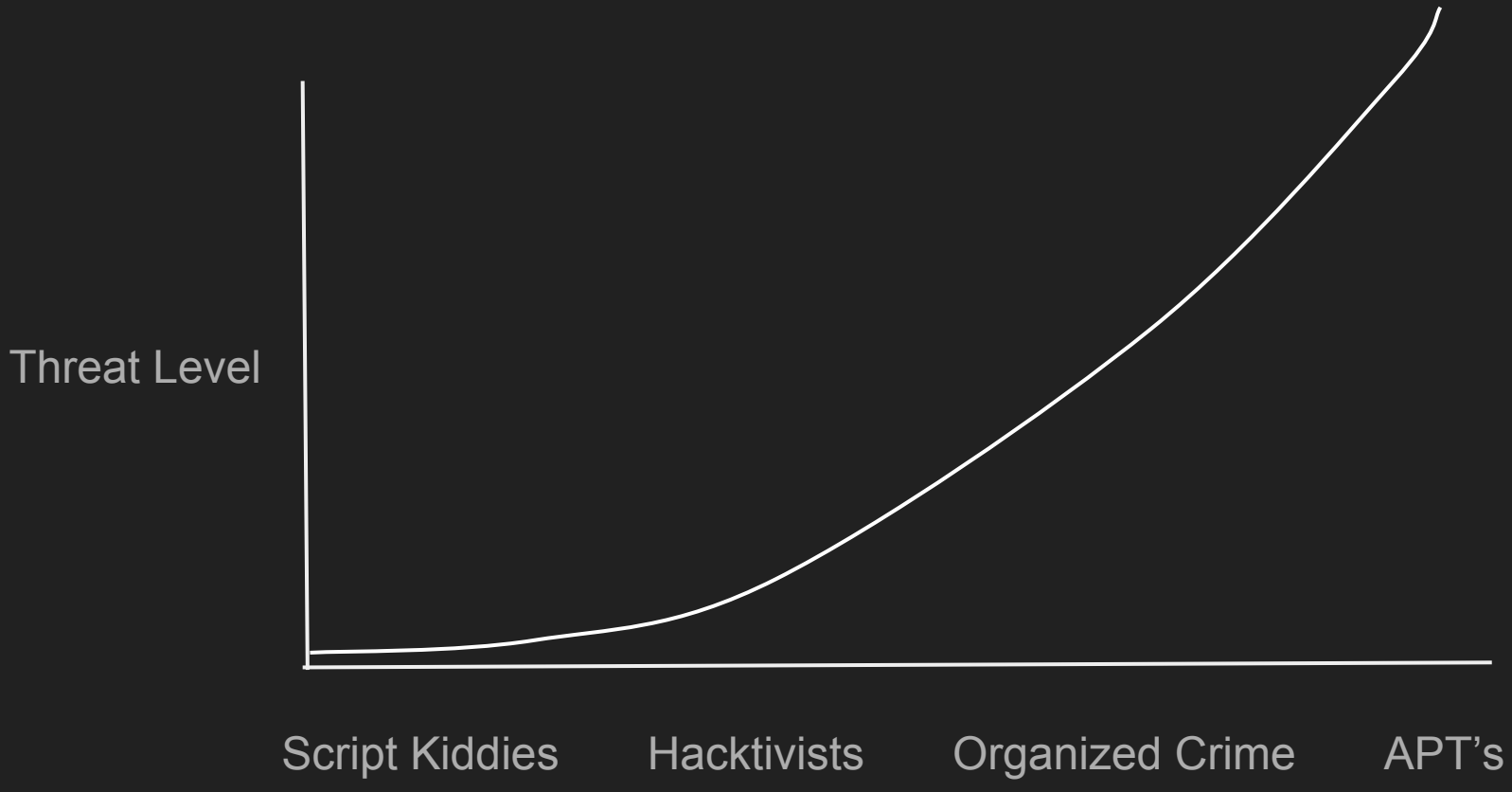
KHANACADEMY



Attacker Types

1. Script Kiddies
2. Hacktavists
3. Organized Crime
4. Advanced Persistent Threats (APT’s), i.e. nation-states

Attacker Types



Major Threats and Mitigation Techniques

- Physical
- Social Engineering
- Digital

Major Threats | Physical

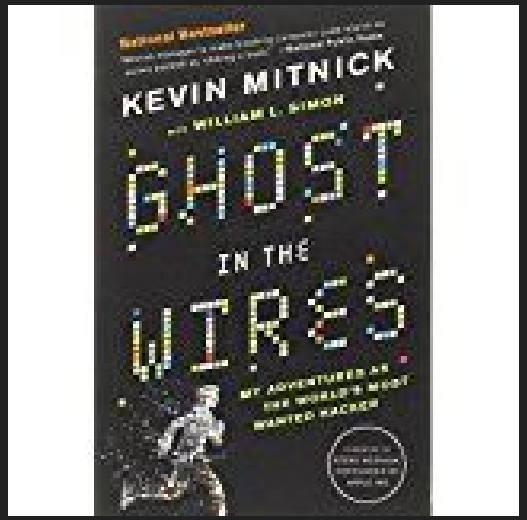
Major Threats | Social Engineering

- Manipulates underlying trust
- Exploits what’s most often the weakest link in security (i.e., the people)
- Can be extremely effective
  - Best hackers exploit this more than technological vulnerabilities
- SET on Kali Linux

Major Threats | Social Engineering

Major Threats | Social Engineering

- Kevin Mitnick



Major Threats | Digital

- Passwords
- Phishing*
- WiFi
  - Public
  - Personal/Home
- Outdated Software

**Also falls under social engineering*

Major Threats | Digital - Passwords

- Avg. # of Attempts to Break Password = *(Character Set ^ length)/2*
  - This assumes the password has to be randomly guessed

- Passwords can be cracked much quicker utilizing password lists:
  - Known passwords
  - Biographical
- Cracking Passwords:
  - Hashcat
  - John the Ripper
  - PRTK
- Test your password(s):
  - https://dl.dropboxusercontent.com/u/209/zxcvbn/test/index.html

Major Threats | Digital - Making Strong Passwords

- Random v. Pseudorandom
- Good Password Characteristics
  - Random passphrases (min. 6 words)
    - EFF Long Word List / Diceware
  - Password manager
    - LastPass
    - 1Password
    - *Both more secure and more convenient*

Major Threats | Digital - Phishing

- Attempts to get sensitive data by tricking a person into:
  - “Logging in” to a fake login portal
  - Download malware
  - Etc.
- SET, which is on Kali Linux, lets you do this

Major Threats | Digital - WiFi (Public)

- WiFi Sniffing
  - Wireshark
  - Fiddler (can decrypt HTTPS traffic)
- MITM Attacks
- Fake hotspots

Major Threats | Digital - WiFi (Personal/Home)

- Use strong password/passphrase
- Use best encryption algorithm (WPA2)

Major Threats | Digital - Outdated Software

- Patch your software

Current Events & The Future

- Apple v. FBI
- Governments
  - Cyberweapons (e.g., Stuxnet)
  - Mass surveillance
  - Whistleblowers (e.g., Edward Snowden)
  - Shadow Brokers NSA exploit dump
- Privacy v. Security (it’s not)

Government Regulation

- Bruce Schneier

Hacking | Penetration Testing Lifecycle

1. Reconnaissance
2. Scanning
3. Exploitation
4. Maintaining Access
5. Reporting

Hacking w/ Kali Linux

Image Credit: Kali.org

Kali Linux Tutorial Textbook

- Hacking with Kali Linux (by James Broad and Andrew Binder)
  - Available on Google Books or possibly your university's library

Learn More

- http://andrewnsanford.com/cybersecurity/security.html
  - Habits & Resources section

Q&A