John McKittrick: There's no way that a high school punk can put a dime into a telephone and break into our system! He's got to be working with somebody else. He's got to be!

Wigan: He does fit the profile perfectly. He's intelligent, an underachiever, alienated from his parents, has few friends. A classic case for recruitment by the Soviets.

– War Games, 1983
Security Threats

Anti-Patterns for Security Threats

- Assuming unsophisticated attacks
- Ignoring operational environment changes
- Ignoring threats from equipment owner

Security Threats:

- What is the motivation for attacking you?
- How sophisticated are the attackers?
  - Are they likely to have access to tool support?
- What’s your operational environment?
  - How can they compromise the CIA properties in your particular system?
StuxNet Embedded Controller Attack

- Specifically designed to attack embedded controllers
  - Spread malware via USB stick
    - Network isolation doesn’t stop this
  - Infect Siemens Step7 Windows controller management software
  - Step7 then infects Siemens PLCs
    - Monitors Profibus (embedded network)
    - Over-rev of centrifuge controllers for uranium enrichment

How StuxNet Worked

1. Infection
   Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. Search
   Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. Update
   If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. Compromise
   The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities - software weaknesses that haven’t been identified by security experts.

5. Control
   In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. Deceive and Destroy
   Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.

Motivation: Why Attack Someone?

- **Nation-State attacks**
  - Political, economic goals
  - Surveillance

- **Criminals**
  - It’s about the $$$
    - Ransomware
    - Denial of service
  - ICS access as a service
    - Sell access to Bad Guys

- **Just for the LoLs**
  - Fame, publicity, notoriety
  - Revenge

[Diagram showing countries and their associated threat types]

Example Attacker Threat Levels

- **Casual abuser**
  - Tries default password, “1234”, etc.

- **Script Kiddie**
  - Uses tools created by others

- **Organized group (criminal, hactivist)**
  - Sophisticated, clever attacks, broken crypto
  - Willing to spend weeks/months on an attack

- **Nation-State**
  - Advanced persistent threat (waiting for an opportunity)
  - Can exploit unpublished vulnerabilities, marginal crypto
  - Willing to spend years on an attack

- **Owner**
  - Can reverse engineer system to recover secrets
  - *Should assume attacker can find out any secrets from a unit they buy*
System Owner Can Be An Attacker

DirecTV Piracy
(Circa 2001)

Power Glitching
Smart Card Pirate Board

DirecTV attacks hacked smart cards
Electronic warfare for the private sector
25 Jan 2001 at 19:26

Satellite television behemoth DirecTV struck a decisive blow against signal pirates Sunday night, when it transmitted a carefully-crafted electronic signal from its orbiting satellites and destroyed thousands of hacked smart cards, which for the last four years allowed pirates to gain free access to hundreds of channels of programming. According to sources in the satellite TV underground, the vast majority of illicitly reprogrammed DirecTV access cards, which once had a street value of several hundred dollars each, were wiped out on what hackers are calling "Black Sunday."

https://goo.gl/6CXaUm

Power Glitching
Black Sunday Security
Fuse Bypass Card
Operational Environment

- **How exposed are you to attack?**
  - Is your equipment directly on the Internet?
  - Is your wireless network unencrypted?
  - Can anyone buy and reverse engineer your equipment?

- **Network connections?**
  - Ethernet, embedded networks, discrete I/O, user interface

- **Data upload/download?**
  - Firmware or configuration file updates?
  - On-line updates, or do they require manual access to equipment?

- **Trusted Personnel?**
  - Do only trusted personnel have access to equipment?
  - Are employees incentivized to attack your system (e.g., due to time pressure)?
  - Is security seen as important, or something that gets in the way?
Embedded Internet Attack Vectors

**Internet connectivity**
- If it’s on the Internet, it is being attacked 24x7
- Firewalls are often bypassed or porous

**Wireless connectivity**
- “Short range” wireless can be attacked from afar

---

**Davis Besse Nuclear Power Plant**

*Event:* Aug 20, 2003 Slammer worm infects plant

*Impact:* Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC)

*Specifics:* Worm started at contractors site
- Worm jumped from corporate to plant network and found an unpatched server
- Patch had been available for 6 months

**Lessons learned:**
- Secure remote (trusted) access channels
- Ensure Defense-in-depth strategies with appropriate procurement requirements
- Critical patches need to be applied

---

**Range of over 1 km**

http://www.tomsguide.com/us/how-to-bluesniper-pt1,review-408.html

---

© 2017 Philip Koopman
**Data Integrity** – data not altered
- Publish both data and digest of data
- Receiver checks digest against message
- If digest does not match, it is corrupted

**Digest techniques:**
- Checksum/CRC: **insecure** – accidental only
- Message Authentication Code: symmetric key hash (shared key)
- Secure Digital Signature: asymmetric key signature (public+private key pair)

**Authentication:** you know who computed the digest
- Identity implicit in which key was used. MAC can be forged by receiver.
- PKI provides identity, revocation, non-repudiation
- Non-repudiation: signer can’t say “that wasn’t me” if PKI info is archived
Confidentiality

- **Secrecy**
  - Data can’t be understood by others
  - Data can only be read by those who know the decryption key

- **Secrecy via encryption**
  - Symmetric encryption (shared key)
    - Need to trust receiver with secret key
  - Asymmetric encryption (public + private key pair)
    - Only need to trust PKI to establish identity

- **Privacy**
  - Activity can’t be associated with an individual
  - Encryption might only be a part of this
    - For example, encryption does not hide who is communicating

https://goo.gl/1YVuWB
LG Smart TV Privacy Issue, Nov 2013

- LG TVs support “Smart Ads” by monitoring your viewing habits
  - Turned off viewing data collection (on by default)
  - But, TV still sent viewing information back to LG servers anyway
  - AND, snooped file names on a USB flash drive and sent them in too

- LG Initial Response: “… as you accepted the Terms and Conditions on your TV, your concerns would be best directed to the retailer.”

- Do you think Netflix Streaming monitors your viewing habits?
  - What happens with that info?

https://goo.gl/v9BZRH
Services are available when desired

- **Denial of Service**: attacker hits system with requests to drain resources
  - Overload CPU
  - Fill up memory with incompleted transactions
  - Drain battery on portable system

- **Distributed Denial of Service (DDoS)**:
  - Coordinated attack from many different IP addresses
  - Often accomplished using a BotNet (multiple “Bot” Zombie machines)

**Feature activation**

- Malicious ability to turn on unpaid features on a pay-per-function system
- Vendor ability to turn off features on cloned or counterfeit system

http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=15944&view=map

Attack on China.cn name servers
Best Practices for Threat Assessment

- Determine what parts of CIA you care about
  - Is secrecy really necessary? Privacy?
  - Integrity usually matters a lot
  - Does availability matter if shutdown is safe?

- Assume strong threats
  - Tool support for sophisticated attacks
  - Over time, system might be networked
  - Equipment owner might attack system
    - To recover manufacturer “secrets”
    - To subvert a particular system

- Pitfalls
  - Assuming naïve, un-motivated attackers
  - Incorrectly emphasizing secrecy (encryption)