Prof. Philip Koopman

Carnegie Mellon University

Electrical & Computer ENGINEERING

Security Threats

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

Carnegie Mellon University

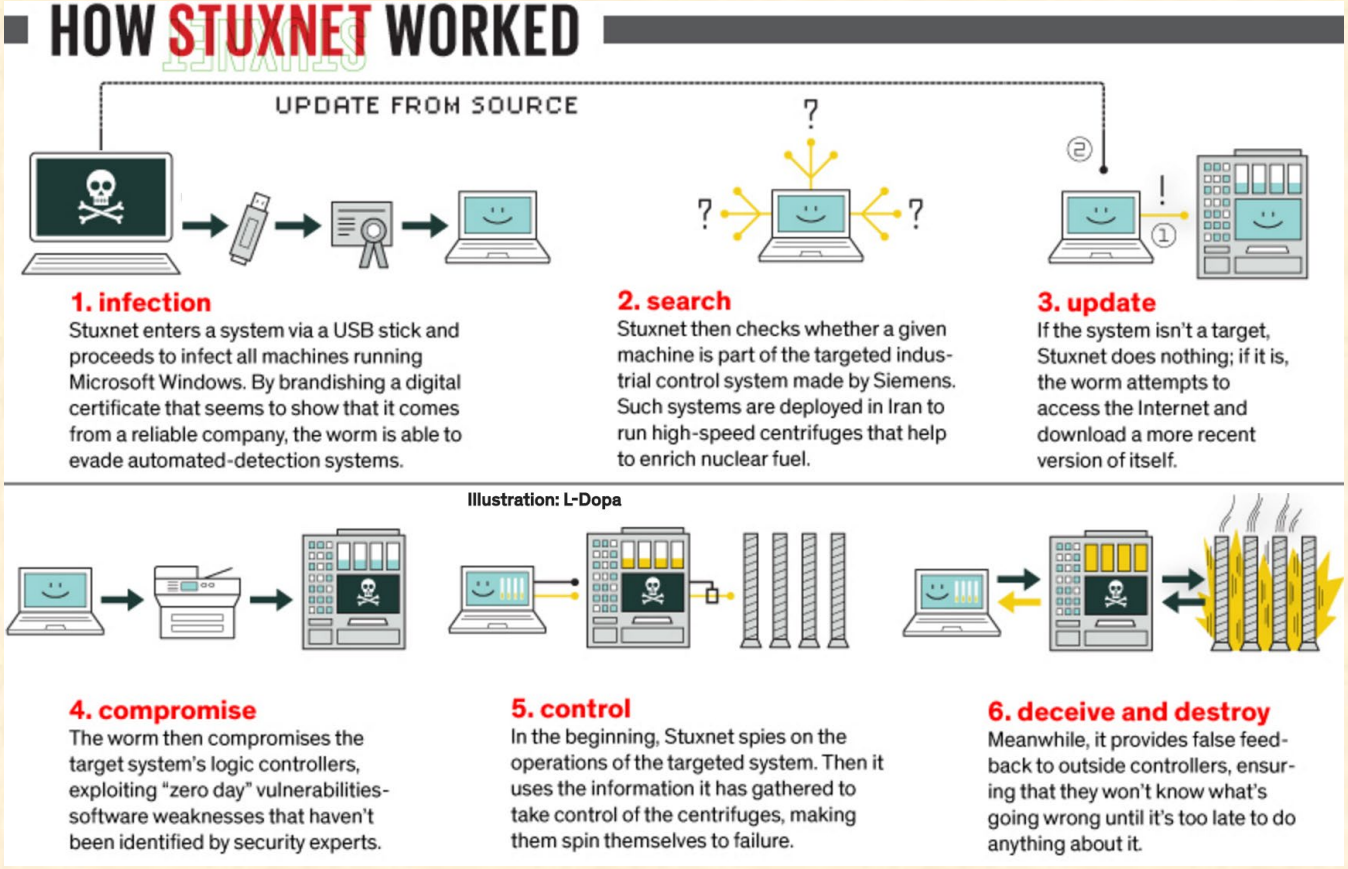
- Anti-Patterns for Security Threats
  - Assuming unsophisticated attacks
  - Ignoring operational environment changes
  - Ignoring threats from equipment owner

- 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? {Confidentiality, Integrity, Availability}

StuxNet Embedded Controller Attack

Carnegie Mellon University

- 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

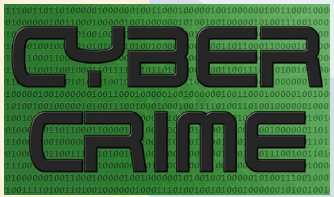


http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Motivation: Why Attack Someone?

Carnegie Mellon University

- **Nation-State attacks**
  - Political, economic goals
  - Surveillance
- **Criminals**
  - It's about the $$$
    - Ransomware
    - Denial of service
  - Attacks as a service
- **Just for the LoLs**
  - Fame, publicity, notoriety
  - Revenge



RUSSIA
TARGETS: Electricity, manufacturing, mining, oil and gas, railway
DEMONSTRATED CAPABILITY: Penetrate ICS operator IT and OT networks
PRIMARY OBJECTIVES: Geopolitically driven disruption and destruction of infrastructure
RISK: Likely to conduct disruptive or destructive attacks outside U.S., likely to target U.S. ICS operators, unlikely to cause disruption or destruction against U.S. operators

NORTH KOREA
TARGETS: Light rail and electricity
DEMONSTRATED CAPABILITY: Penetrate ICS operator IT networks
PRIMARY OBJECTIVES: Retaliatory strikes against national adversaries
RISK: Likely to conduct disruptive or destructive attacks outside U.S., possible disruptive or destructive attacks against U.S. ICS operators

IRAN
TARGETS: Electricity, water and dam
DEMONSTRATED CAPABILITY: Penetrate ICS operator IT and OT networks
PRIMARY OBJECTIVES: Retaliatory strikes against national adversaries, establish persistent access as contingency for future conflict
RISK: Likely to target U.S. ICS operators, unlikely to cause disruption or destruction

CHINA
TARGETS: Manufacturing, electricity, light rail, oil and gas, water and dam
DEMONSTRATED CAPABILITY: Penetrate ICS operator IT and OT networks
PRIMARY OBJECTIVES: Traditional espionage, support of national economic interests through intellectual property theft, establish persistent access as contingency for future conflict
RISK: Highly likely to target U.S. ICS operators, unlikely to cause disruption or destruction

http://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2016/06/industrial-cybersecurity-threat-briefing.pdf

Example Attacker Threat Levels

Carnegie Mellon University

- 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*

Operational Environment

Carnegie Mellon University

- 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

Carnegie Mellon University

- 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

John Hering from Flexilis, with the new BlueSniper Rifle

Range of over 1 km

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

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

Homeland Security

Lessons learned:

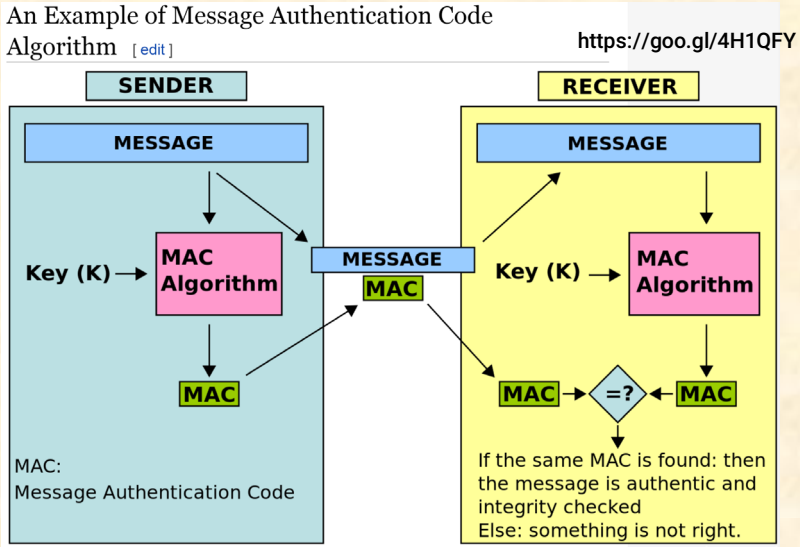
- Secure remote (trusted) access channels
- Ensure Defense-in-depth strategies with appropriate procurement requirements
- Critical patches need to be applied

https://goo.gl/hAFQUs

Integrity

Carnegie Mellon University

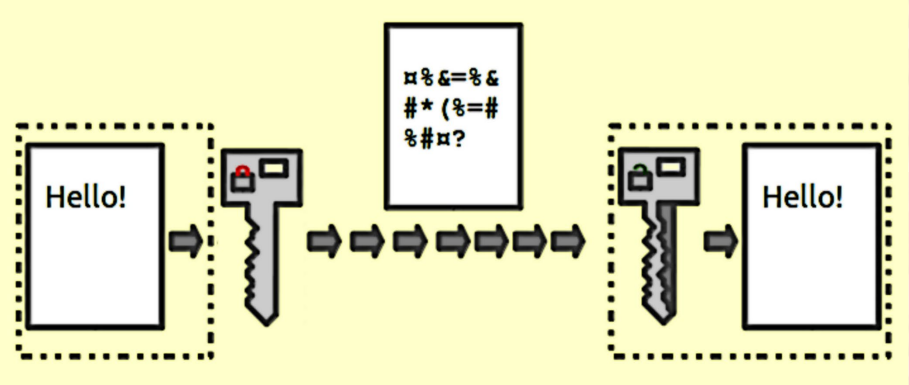
- Data Integrity – data not altered
  - Publish both data and digest of data
  - Receiver checks digest against message
  - If digest does not match, it is corrupted
- Digest techniques:
  - Checksum/CRC: insecure –accidental only
  - Message Authentication Code: symmetric key hash (shared key)
  - Secure 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

Carnegie Mellon University

- **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

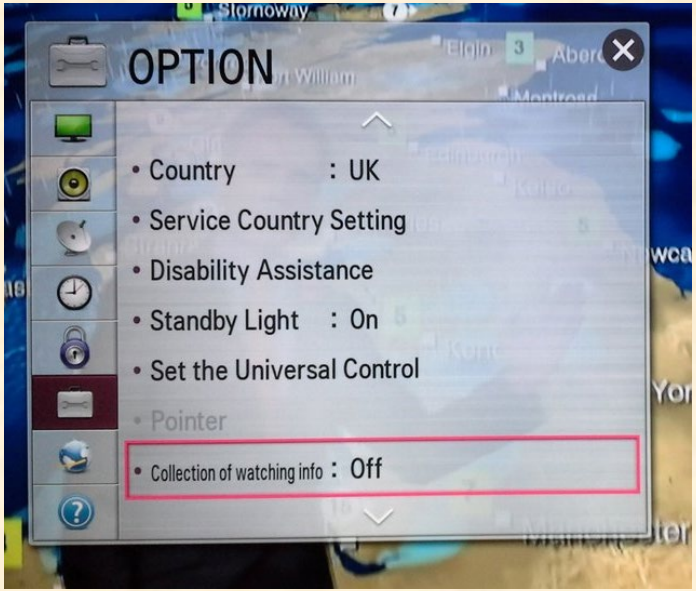
LG Smart TV Privacy Issue, Nov 2013

Carnegie Mellon University

- 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?



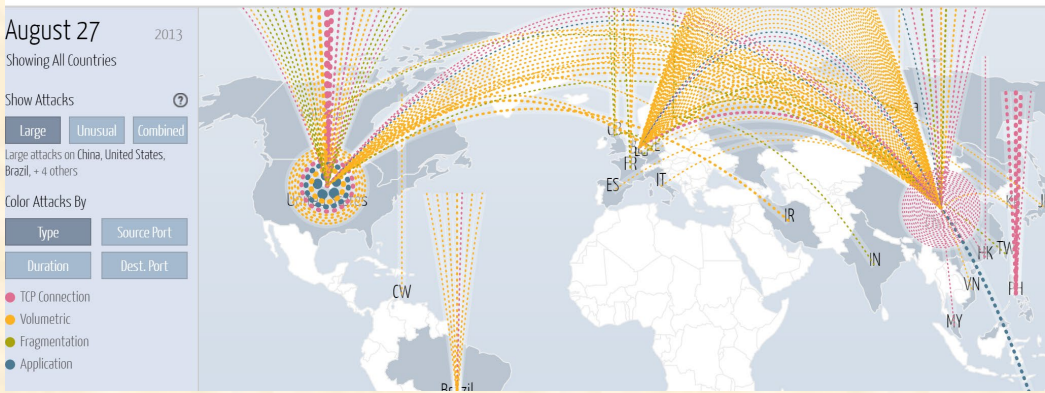
https://goo.gl/v9BZRH

Availability

Carnegie Mellon University

- 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" compromised machines)

Attack on China.cn name servers



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

- 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

Best Practices for Threat Assessment

Carnegie Mellon University

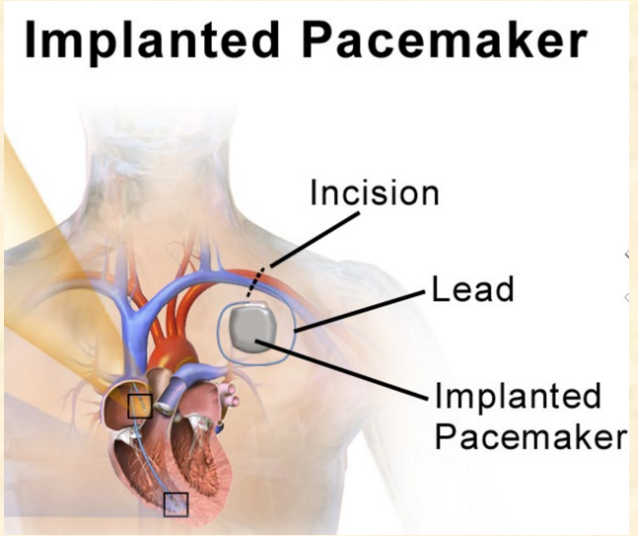
- Determine what parts of CIA you care about
  - Is secrecy really necessary? Privacy?
  - Integrity usually matters a lot
  - Does availability matter if shutdown is safe?
- Assume strong threats
  - Tool support for sophisticated attacks
  - Over time, system might be networked
  - Equipment owner might attack system
    - To recover manufacturer "secrets"
    - To subvert a particular system
- Pitfalls
  - Assuming naïve, un-motivated attackers
  - Incorrectly emphasizing secrecy (encryption)

August 2017: FDA recalls 465,000 St. Jude pacemakers

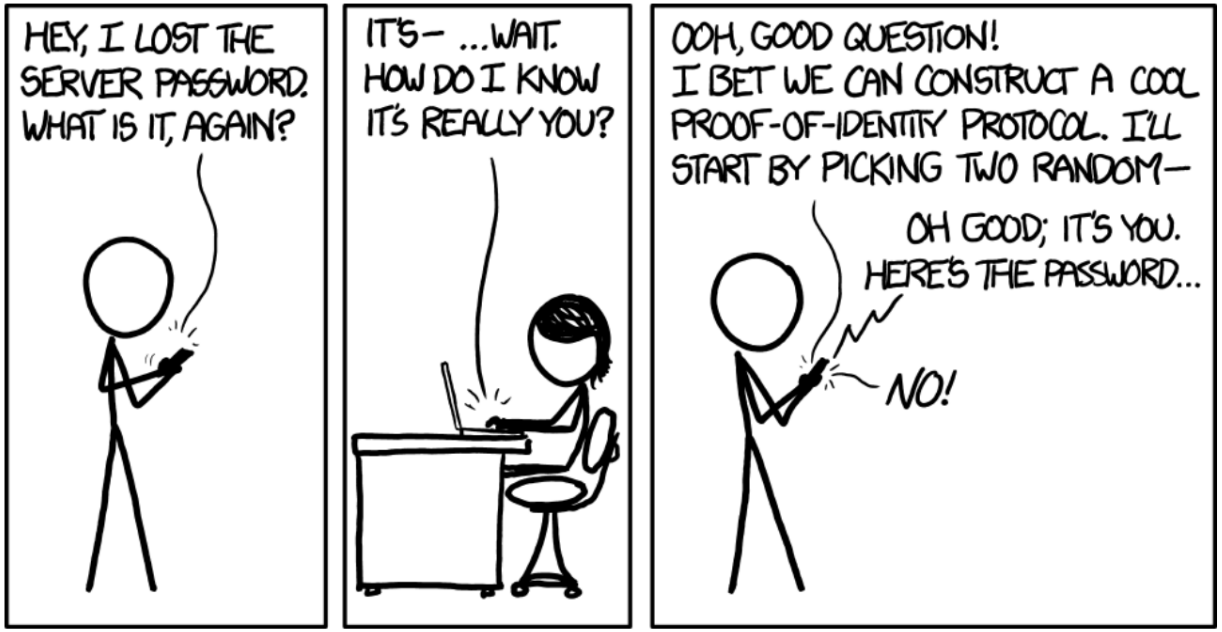
The devices must be given a firmware update to protect them against a set of critical vulnerabilities, first reported by MedSec, which could drain pacemaker battery life, allow attackers to change programmed settings, or even change the beats and rhythm of the device.

On Tuesday, the FDA issued a security advisory, warning that the pacemakers must be recalled -- and as they are embedded within the chests of their users, this requires a trip to the hospital to have the software patch applied.

https://goo.gl/NXikaL



https://goo.gl/pW2R9D



https://xkcd.com/1121/

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor ⓘ
Consumer Tech
I cover the human side of VR/AR, Blockchain, AI, Startups, & Media.

Anonymous hacker programmer uses a laptop to hack the system in the dark. Creation and infection of ... [+] GETTY

It's the first noted instance of an artificial intelligence-generated voice deepfake used in a scam.

https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#5d6e6c512241