CIS 700/002: Special Topics: Cyber-Physical Attack Steps

Thejas Kesari

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

27 January 2017

Overview

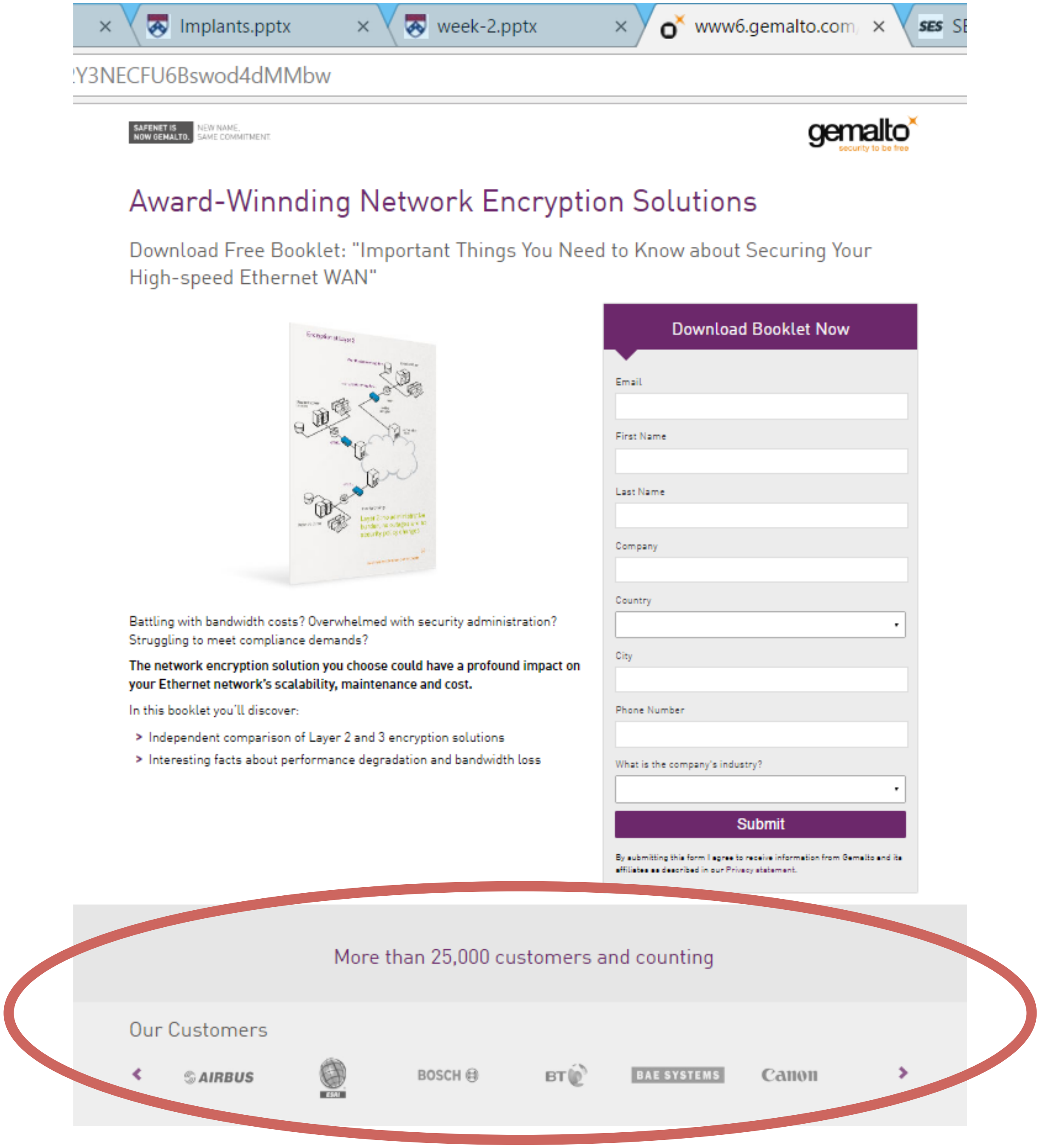
- Intro
- Preliminary Research & Reconnaissance
- Discovery of Vulnerability
- Attack Delivery
- Antiforensics

Intro

- Cyber-physical security threats are similar across platforms
- Attacker identifies entry points – tries to communicate with sensors and actuators directly or indirectly
- Discovery of such vulnerable entry points requires research and planning

Preliminary Research

- IP addresses, the topology of its network infrastructure, types and versions of software and hardware used, etc.
- Surprising how much intelligence one can gather about a potential target through a mere Google search



Award-Winnding Network Encryption Solutions

Download Free Booklet: "Important Things You Need to Know about Securing Your High-speed Ethernet WAN"

Battling with bandwidth costs? Overwhelmed with security administration? Struggling to meet compliance demands?

The network encryption solution you choose could have a profound impact on your Ethernet network's scalability, maintenance and cost.

In this booklet you'll discover:

- Independent comparison of Layer 2 and 3 encryption solutions
- Interesting facts about performance degradation and bandwidth loss

Download Booklet Now

Email

First Name

Last Name

Company

Country

City

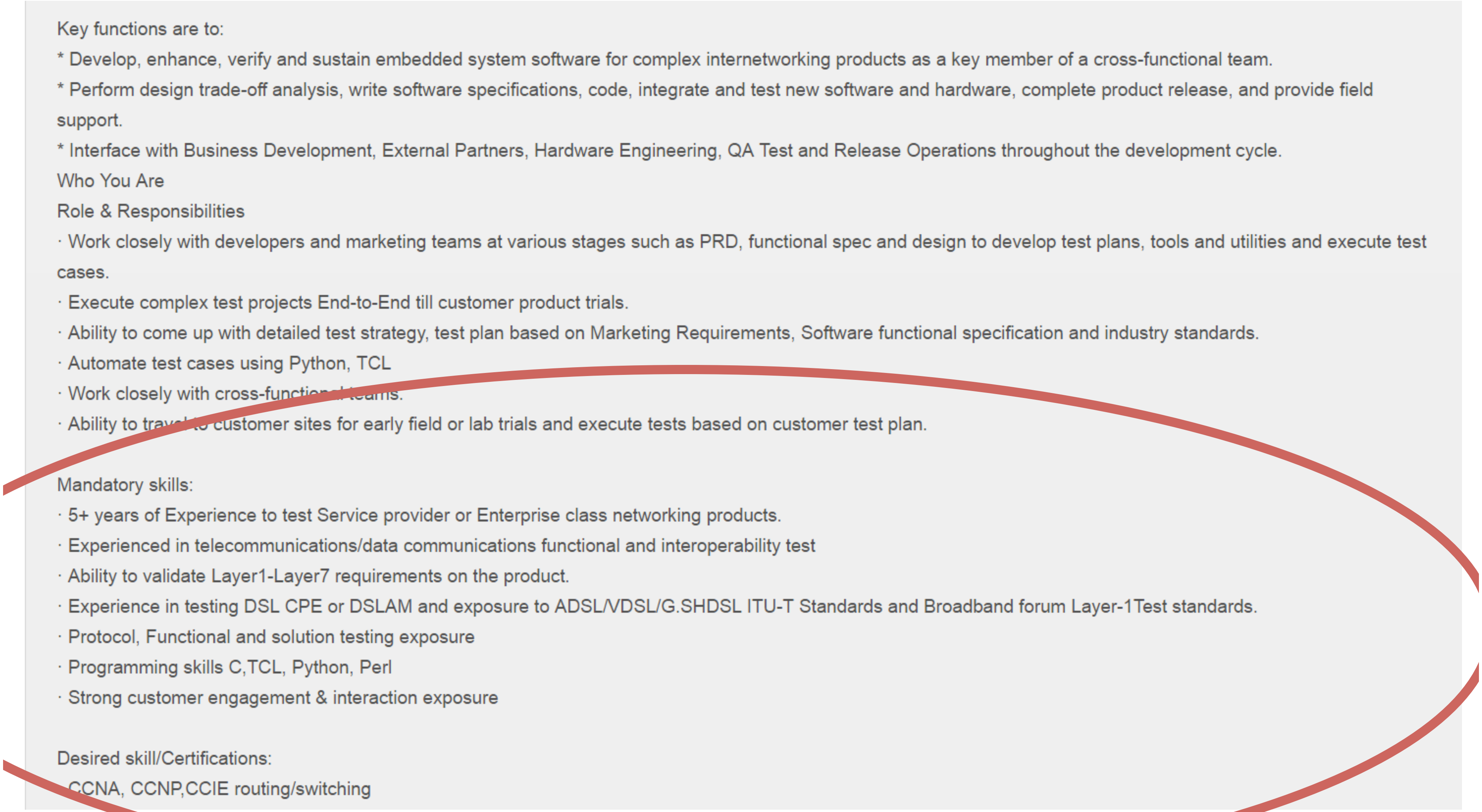
Phone Number

What is the company's industry?

By submitting this form I agree to receive information from Gemalto and its affiliates as described in our Privacy statement.

More than 25,000 customers and counting

Our Customers



Key functions are to:

* Develop, enhance, verify and sustain embedded system software for complex internetworking products as a key member of a cross-functional team.

* Perform design trade-off analysis, write software specifications, code, integrate and test new software and hardware, complete product release, and provide field support.

* Interface with Business Development, External Partners, Hardware Engineering, QA Test and Release Operations throughout the development cycle.

Who You Are

Role & Responsibilities

· Work closely with developers and marketing teams at various stages such as PRD, functional spec and design to develop test plans, tools and utilities and execute test cases.

· Execute complex test projects End-to-End till customer product trials.

· Ability to come up with detailed test strategy, test plan based on Marketing Requirements, Software functional specification and industry standards.

· Automate test cases using Python, TCL

· Work closely with cross-functional teams.

· Ability to travel to customer sites for early field or lab trials and execute tests based on customer test plan.

Mandatory skills:

· 5+ years of Experience to test Service provider or Enterprise class networking products.

· Experienced in telecommunications/data communications functional and interoperability test

· Ability to validate Layer1-Layer7 requirements on the product.

· Experience in testing DSL CPE or DSLAM and exposure to ADSL/VDSL/G.SHDSL ITU-T Standards and Broadband forum Layer-1Test standards.

· Protocol, Functional and solution testing exposure

· Programming skills C,TCL, Python, Perl

· Strong customer engagement & interaction exposure

Desired skill/Certifications:

· CCNA, CCNP,CCIE routing/switching

Preliminary Research

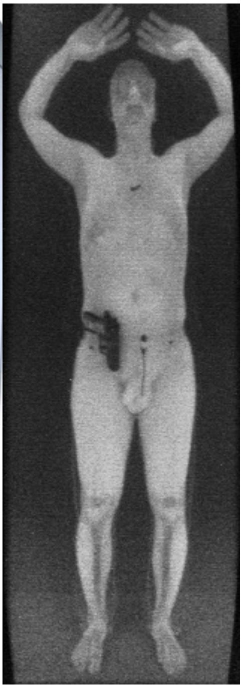
- IP addresses, the topology of its network infrastructure, types and versions of software and hardware used, etc.
- Surprising how much intelligence one can gather about a potential target through a mere Google search
- Equipment used – business success of the supplier
- Job adverts – desired skills and experience reveal the software, hardware and network technologies
- Manufacturers publish installation instructions on website – also includes default username and password that often remain unchanged

“Unchanged (end user’s) username and password is a security threat no matter how robust the encryption of the data is at rest and during transfer. Now, we prompt the user to change the default username/password during initial setup and also to update them regularly.”

-Pavan Kumar, CTO, CocoonCam

Rapiscan Secure 1000

- Full-body scanner – uses backscattered X-rays to construct an image through clothing
- Used at US airport checkpoints from 2009 to 2013
- Still in use at some courthouses and prisons

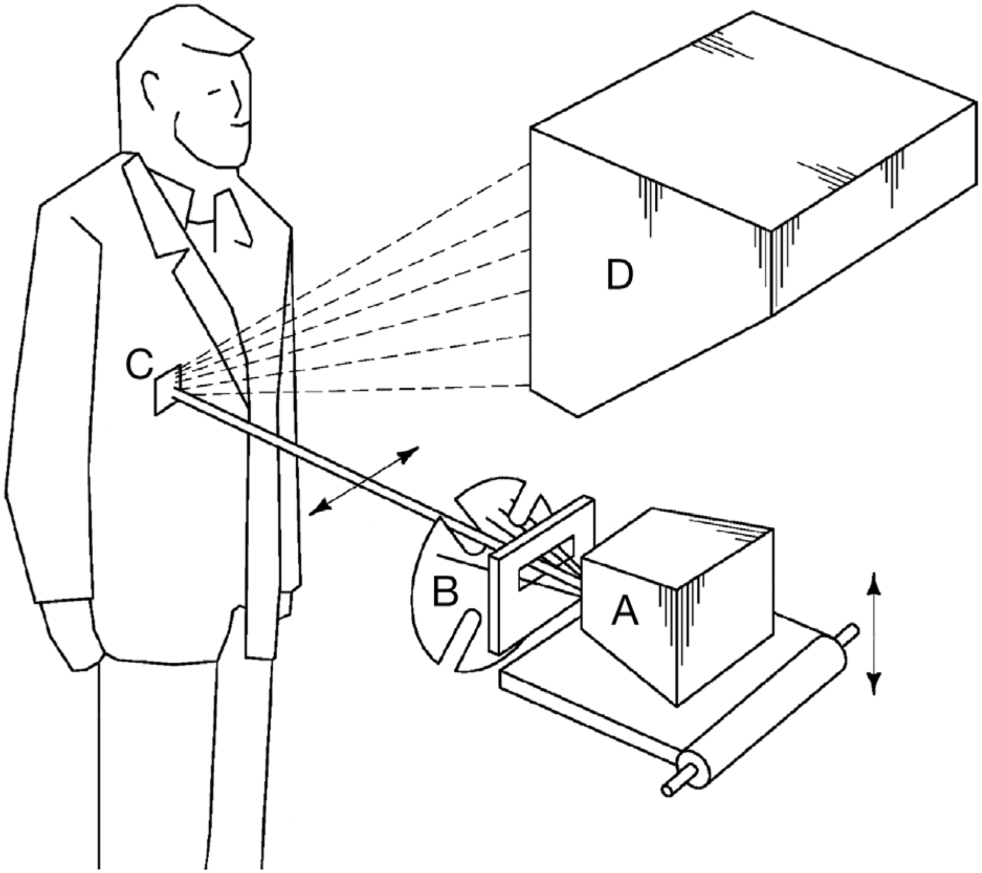


Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

Rapiscan Secure 1000

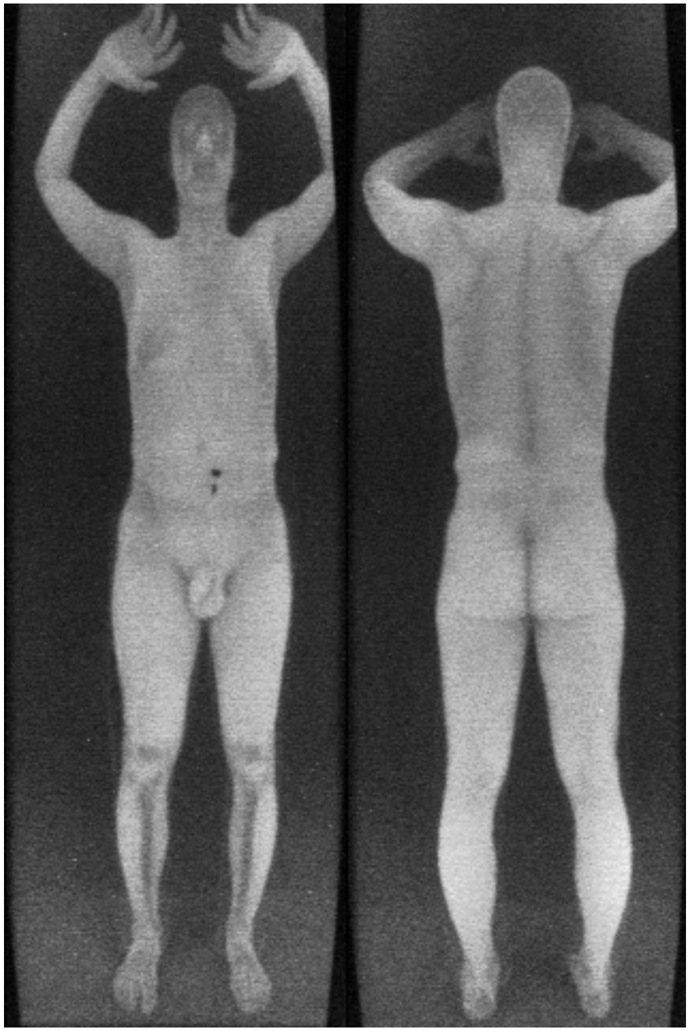
- Acquired from Ebay (a unit still seems to be available for $9900 OBO)

- A: X-ray tube
- B: Spinning disk
- C: Target
- D: Detectors



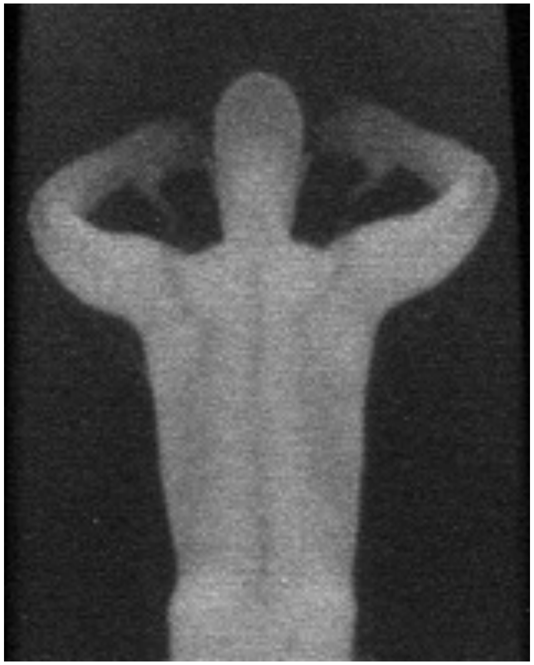
Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

Rapiscan Secure 1000

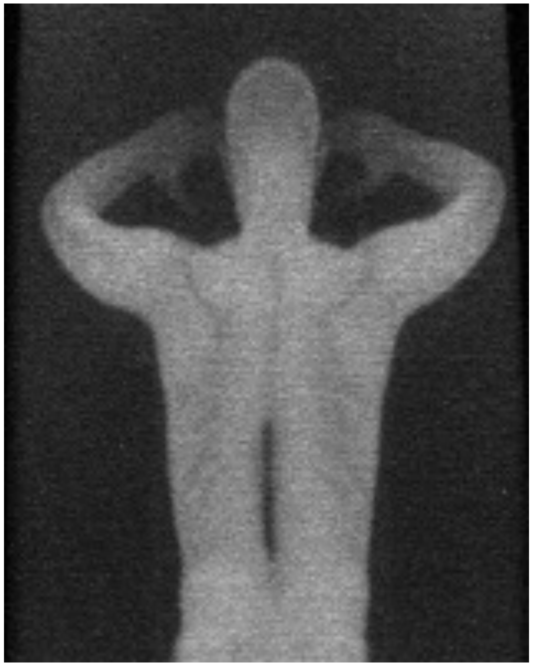


Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

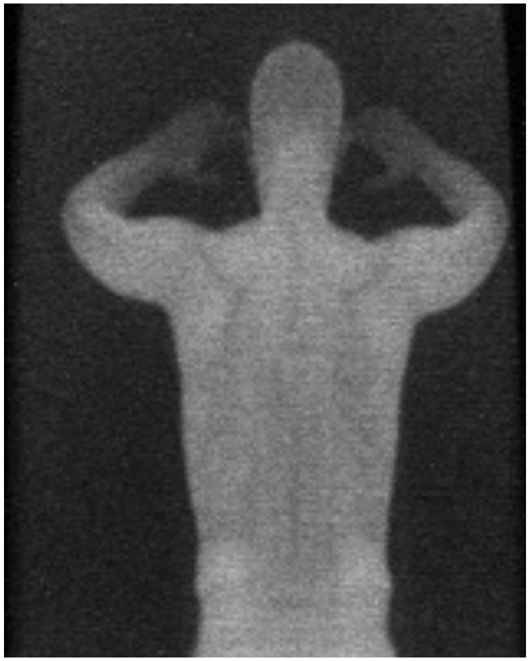
Rapiscan Secure 1000



No contraband



18 cm knife taped to spine



Knife behind 1.5 cm PTFE block

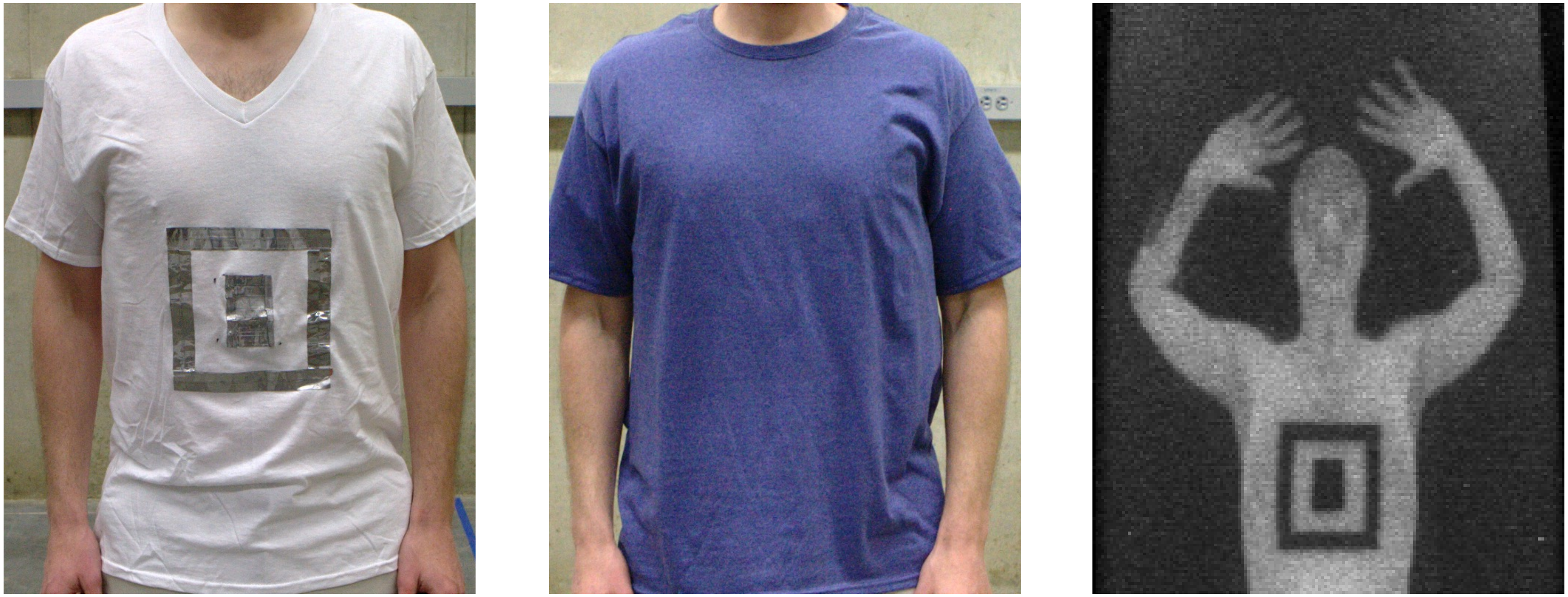
Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

User Console Malware

- MS-DOS based PC attached to the scanner via a proprietary cable
- No passwords or software verification
- Reverse engineered SECURE65.EXE, the front-end software package and created INSECURE.EXE
  - Scan image saved to a hidden location on disk for later exfiltration
  - Selectively subvert the scanner’s ability to detect contraband
  - Applies a PR algorithm to look for a “secret knock” from the attacker
  - If this pattern occurs, replace the real scan with a pre-programmed innocuous image

Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

User Console Malware



Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

Embedded Controller Attack

- Safety interlocks in place that prevent the operation under unexpected conditions
  - Circuits sense removal of the front panel, continuous motion of the chopper wheel and the vertical displacement servo, etc.
  - If any anomalous state is detected, power to the X-ray tube is immediately disabled, ceasing X-ray emission
- These sensors merely provide inputs to the SCB software, others are tied to hard-wired watchdog circuits that cut off X-ray power without software mediation – firmware CAN bypass these

Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

Rapiscan Secure 1000

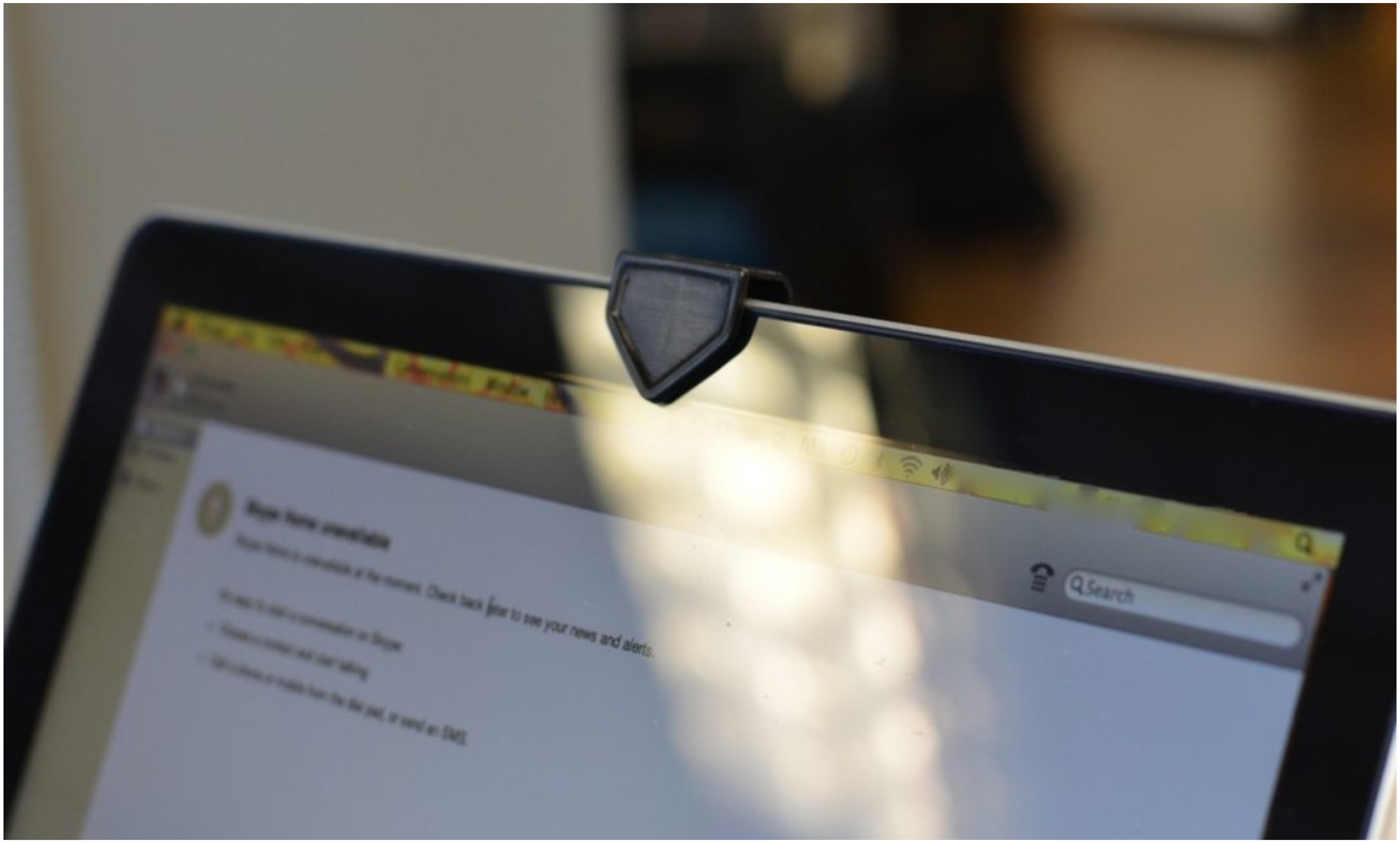
- *“Keeping the machine out of the hands of would-be attackers may well be an effective strategy for preventing reliable exploitation, even if the details of the machine’s operation were disclosed.”*

-Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014

Electronic Voting Machine - India

https://www.youtube.com/watch?v=apkSkb6Ak3I

Social Engineering



Social Engineering

- Prevalent mechanism for reconnaissance of CPS, especially industrial control systems
- Can be safely assumed that an adversary has at least attempted a social engineering attack prior to a high-impact cyber-physical attack
- Even the strongest technical security protections can be bypassed if a system's legitimate user is manipulated into letting the adversary in

- Primary target: Any cyber-physical system operated by human users or connected to a corporate network

Condor Speaks

"The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain."

-Kevin Mitnick

Poulsen, K. (2000). Mitnick to lawmakers: People, phones and weakest links. SecurityFocus, March 2000.

Social Engineering

- Can be non-technical – can start with “dumpster diving”, a fake ID or impersonation
- Also technical – exploiting human-computer interface
  - Try to approach a SCADA system engineer through social network
  - Send an email that otherwise looks legitimate but is malware
  - Phishing, spear-phishing and whaling

- Prof. Jean-Jacques Quisquater infected with an advanced piece of malware after clicking a spoofed LinkedIn invite

Watering Hole

- Same primary target
- Attack strategy where the attacker observes or guesses what website a particular target visits frequently and then implants malware on that website
- Since 2012, it has emerged as a considerable threat to national infrastructure, especially the energy sector

Candid Wueest, *Targeted Attacks Against the Energy Sector*, Symantec Security Response, January 2014

Vulnerability Discovery

- Attacker has preliminary info, now it's time to use those tools – Nmap, Nessus, Wireshark, etc.
- Collective determine a lot of stuff
  - OS running on the target
  - Scan for open network ports
  - Default passwords

Google Hacking

Whenever you have a question, whether big or small, you go to the Oracle (Google) and ask away. "What's a good recipe for delicious pesto?" "Are my dog's dentures a legitimate tax writeoff?" "Where can I read a summary of the post-modern philosophical work Simulacra and Simulation?" The Oracle answers them all. And if you configure some search preferences, the Oracle—i.e., Google—will even give your Web browser a cookie.

Ed Skoudis, foreword to *Google Hacking for Penetration Testers* by Johnny Long

Google Hacking

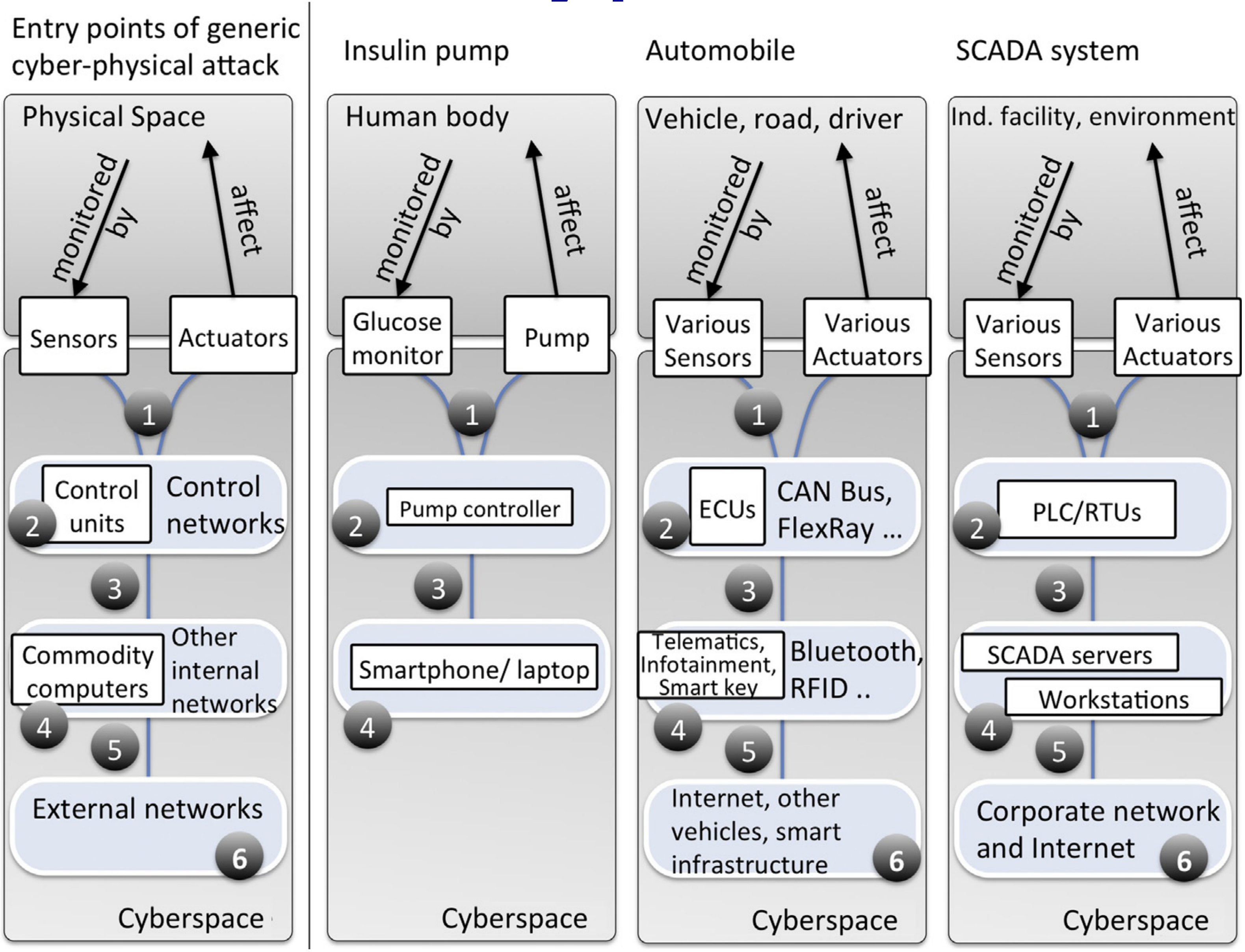
- Google offers special terms known as advanced operators to help you perform more advanced queries
- Inexhaustive list
  - *intitle:Thejas* - This query will return pages that have the phrase index of in their title
  - *inurl:admin*
  - *link* - allows you to search for pages that link to other pages

Johnny Long, *Google Hacking for Penetration Testers*

Intrusion

- Relatively easy for an unauthorized user to access system network
  - Ex-employee accessing a remote maintenance account that was never disabled/updated
  - Attacker getting hold of credentials like default password from device documentation
  - Successful phishing or watering hole attack
- Unlike conventional computer systems, where published vulnerabilities in industrial control systems and embedded systems remain unpatched for a long time
  - Hundreds of YouTube videos describing how to exploit particular vulnerabilities

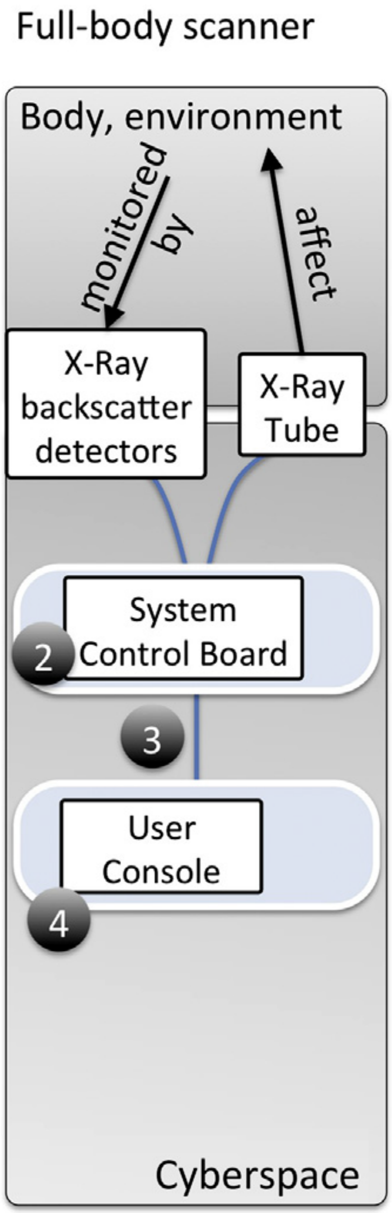
Entry points



Penn Engineering

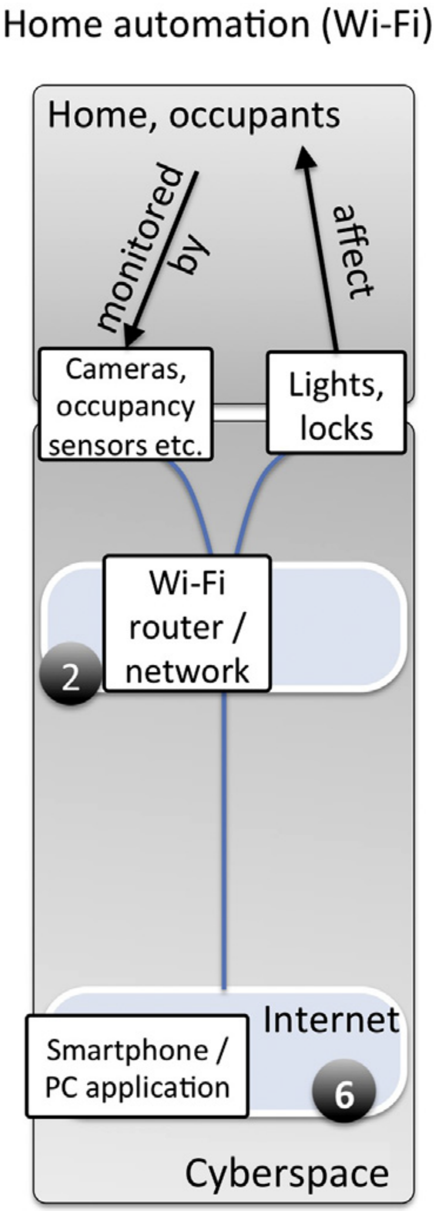
PRECISE

Entry points



2. System Control Board - Physically swap chip with a maliciously modified one
3. Serial cable - Command injection, code injection
4. User console - Malware infection

Entry points



2. WiFi Network/Router – Password cracking, packet sniffing, DoS
8. Smartphone/PC – Password cracking, malware

Attack Delivery

- The business end of the deal
- Various types of attacks
  - DoS
  - Packet Sniffing
  - Black Hole
  - Code Injection
  - Command Injection
  - Communication Jamming
  - False Data Injection
  - Firmware Modification
  - Fuzzing
  - GPS Jamming / Spoofing / Meaconing
  - Password Cracking

Command Injection

Wired: Hackers Remotely Kill A Jeep On The Highway
https://www.youtube.com/watch?v=MK0SrxBC1xs

Antiforensics

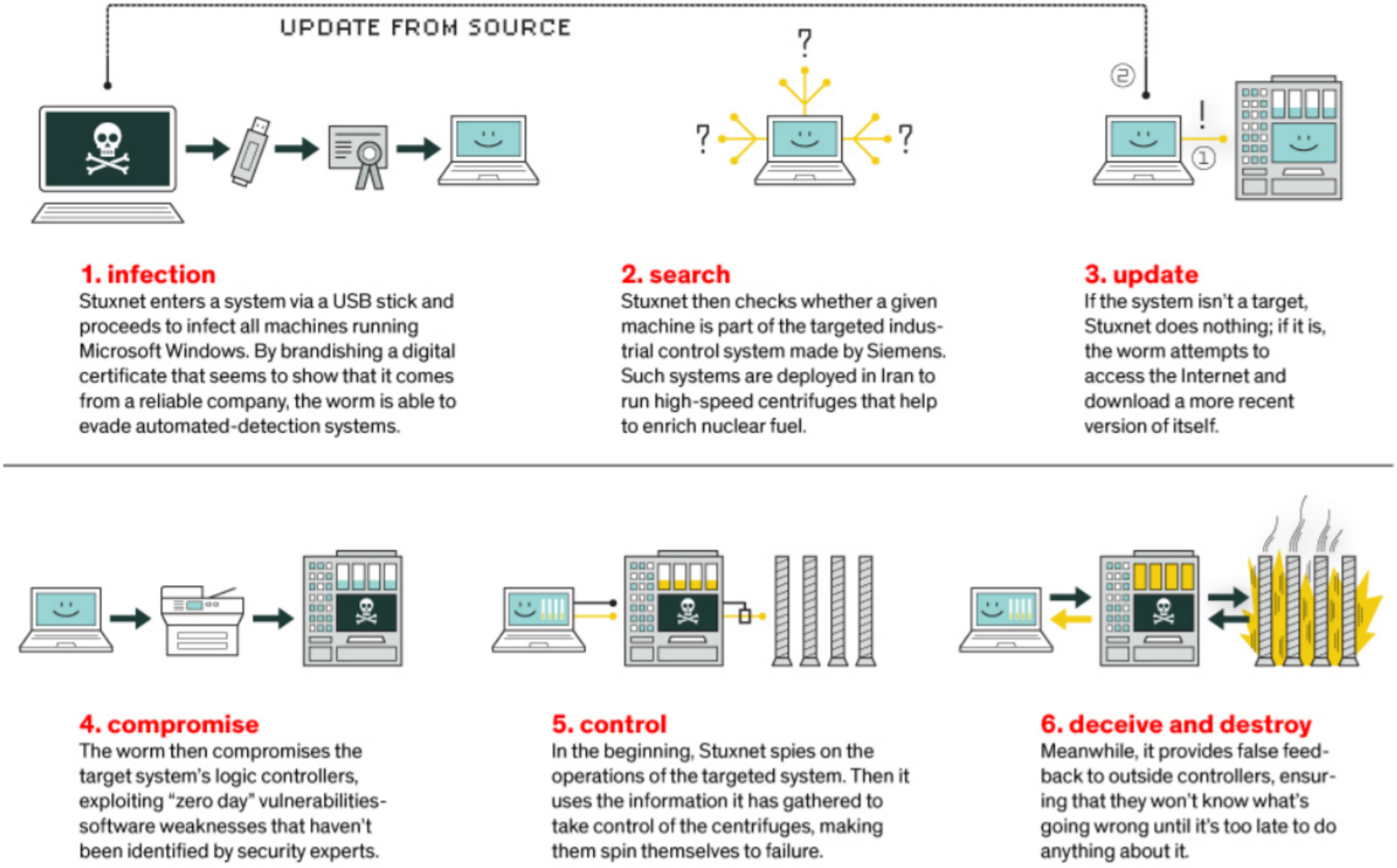
- Getting rid of traces and covering one's tracks
- *"Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct."* –Marc Rogers
- *"Anti-forensics is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found you."* –Scott Berinato

Rogers, D. M. (2005). Anti-Forensic Presentation given to Lockheed Martin. San Diego
Berinato, S. (2007). The Rise of Anti Forensics. Retrieved April 19, 2008, CSO

Antiforensics

- Deleting files created during attack
- Hiding data in seemingly innocuous files
- Temporarily disabling logs
- Use proxy servers, source address spoofing
- Wait for a few days before initiating next steps of attack – hard to connect the incidents

Recall: Stuxnet



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.

Dagaen Golomb, *CIS 700/002: Attack on Industrial Control Systems*, January 20 & 27, 2017

Recall: Stuxnet

- Arrives as an infected project archive containing both the s7hkimdb.dll and XR000001.MDX files
- s7hkimdb.dll file is executed, which then decrypts and injects the main XR00001.MDX Stuxnet binary file into the services.exe process*
- Stuxnet is now running
- A second driver, PCIBUS.SYS, is also created which causes a forced reboot by generating a BSoD 20 days after installation

Geoff McDonald et. al., *Stuxnet 0.5: The Missing Link*, Symantec Security Response, February 26, 2013

* Multiple Siemens SIMATIC Products DLL Loading Arbitrary Code Execution Vulnerability

Summary

- Breaching is not easy, requires understanding of relevant dependencies and window of opportunity
- Requires considerable planning and research
- Social engineering helps in research and to help deliver attack
- Automated tools aid in detecting and exploiting vulnerabilities
- Capable attackers use advanced antiforensic techniques to cover their tracks
- Internet is the Oracle

References

- George Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*, Elsevier, 2015
- Keaton Mowery et. al., *Security Analysis of a Full-Body Scanner*, 23rd USENIX Security Symposium, 2014
- Poulsen, K. (2000). Mitnick to lawmakers: People, phones and weakest links. SecurityFocus, March 2000
- Candid Wueest, *Targeted Attacks Against the Energy Sector*, Symantec Security Response, January 2014
- Johnny Long, *Google Hacking for Penetration Testers*
- Geoff McDonald et. al., *Stuxnet 0.5: The Missing Link*, Symantec Security Response, February 26, 2013