Digital Forensics Regarding the "Internet of Things" and Infrastructure Security

In the high tech world we live in today, technology, along with the power of the Internet has literally opened the door to hackers and cyber-criminals to steal valuable personal and proprietary information for financial gain or conduct espionage and sabotage to create confusion and chaos.

Society is extremely reliant and dependent on computerized systems for everything we do in our personal and professional lives using the "Internet of Things" that are operated or controlled by computer.

The "Internet of Things" consists of all of these computer controlled devices of our digital society that range from smart houses and self-driving cars to computer controlled industrial equipment and machinery. The consequences of cyber-warfare have the potential to be catastrophic and a specific cyber-attack against the critical infrastructure places a significant risk and potential for severe injury, chaos or societal breakdown.

Cyber-warfare is now a reality with over 90% of Fortune 500 companies along with various government and utility organizations have all had cyber-incidents of some type, although most go unreported. The cost of conducting a cyber-attack is minimal, but can impose a tremendous amount of financial or physical damage and confusion on a global scale.

Cyber is now the 5th domain of warfare and has been utilized as a war fighting function with a significant capability to eliminate or mitigate the enemy command and control, coordination, and communications. Our personal, small business, corporate and government computers, smartphones, and computer-enabled devices are part of the frontline with the ongoing threat of the continuous domestic and international cyber-attacks.

This brief will discuss the application or use of digital forensics that may facilitate real time deterrence or detection of cyber-attacks to our critical infrastructure and opportunities for law enforcement or prosecution, while generating discussion for future research.

“Internet of Things” Cheat Sheet

Acronyms:

APT - Advanced Persistent Threat
DCS - Distributed Control Systems
DOS - Denial of Service
DDOS - Distributed Denial of Service
EMI - Electro Magnetic Interference
EMP - Electro Magnetic Pulse
HMI - Human Machinery Interface
IACS - Industrial Automation and Control Systems
ICS - Industrial Control Systems
IEDs - Intelligent Electronic Devices
IoT - Internet of Things
IIoT - Industrial Internet of Things
IT - Information Technology
LAN - Land Area Network
OT - Operational Technology
PAC - Programmable Automation Controllers
PLC - Programmable Logic Controllers
RTUs - Remote Terminal Units
SCADA - Supervisory Control and Data Acquisition
SQL Injection - Structured Query Language

Terms:

Authentication - The process of confirming identity on a computer or network
Adware - software that automatically downloads unwanted advertising
Biometrics – The analysis of physical features to maintain identity for security purposes
Blue Snarfing - Theft of information from unauthorized access through a Blue Tooth device
Blue Bugging - Assumes control of cell phone and listens to conversations
BotNet - Robot network of zombie computers controlled by a server and used for cyber-attacks
Brute Force – Exhaustive testing to break a security system
DOS - Large volume of website requests by a hacker that interrupts normal service
DDOS - Large volume of website requests by a Botnet that interrupts normal service for long periods
Encryption - Process of converting information to data code for security purposes
Firewall - Monitors network traffic to prevent unauthorized access
Forensics - Electronic computer hardware and software tools to identify criminal activity or evidence
“Jus ad Bellum” - The set of criteria for the justification for war
Man in the Middle - Attacker secretly relays and possible alters information or data
Penetration Test – Used to identify external vulnerabilities in network systems
Piggybacking - Gaining unauthorized access to a network through a previously established session
Phishing - Gain personal information through email with no specific target
Ransomware - Malware that locks a network until a payment is made to the attacker
Rootkit - Conceals certain objects or activities in the computer system
Social Engineering - Method that relies on human interaction to gain access to information or network
Spearfishing – Targeted attempt to steal information through the internet and email
Spyware - Sends personal information to a third party without your consent
Tailgating - The unauthorized access by gaining entry through an authorized innocent party
Trojan - Malware that is disguised as legitimate software
Virus - Malware that can infect other computers and networks by modifying programs and software
Whaling - Cyber-fraud that targets high profile end users
Worm – Standalone malware that self-replicates to infect other computers and networks
Zero-Day Exploit – 1st day of the cyber-attack on an unknown weakness of a high value target

Links:

Addressing Urgent Cyber-Threats to Critical Infrastructure. August 2017 Retrieved from https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf

Chemical Sector Specific Plan: An Annex to the NIPP 2013 2015 Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf

China could shut down U.S. power grid with cyber-attack, says NSA Chief
Amelia Smith on 11/21/14 Retrieved from
http://www.newsweek.com/china-could-shut-down-us-power-grid-cyber-attack-says-nsa-chief-286119

Cisco Switch Flaw Led To Attacks On Critical Infrastructure In Several Countries The attack targets the Cisco Smart Install Client, and as many as 168,000 systems could be vulnerable. Conner Forrest April 6, 2018, Retrieved from
https://www.techrepublic.com/article/cisco-switch-flaw-led-to-attacks-on-critical-infrastructure-in-several-countries/

Critical Infrastructure and the Internet of Things. Tobby Simon January 2017 Retrieved from https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf

Cyber Attacks against Critical Infrastructure Are No Longer Just Theories
April 29, 2016 Bret Brasso and Business Of Security Retrieved from
https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html

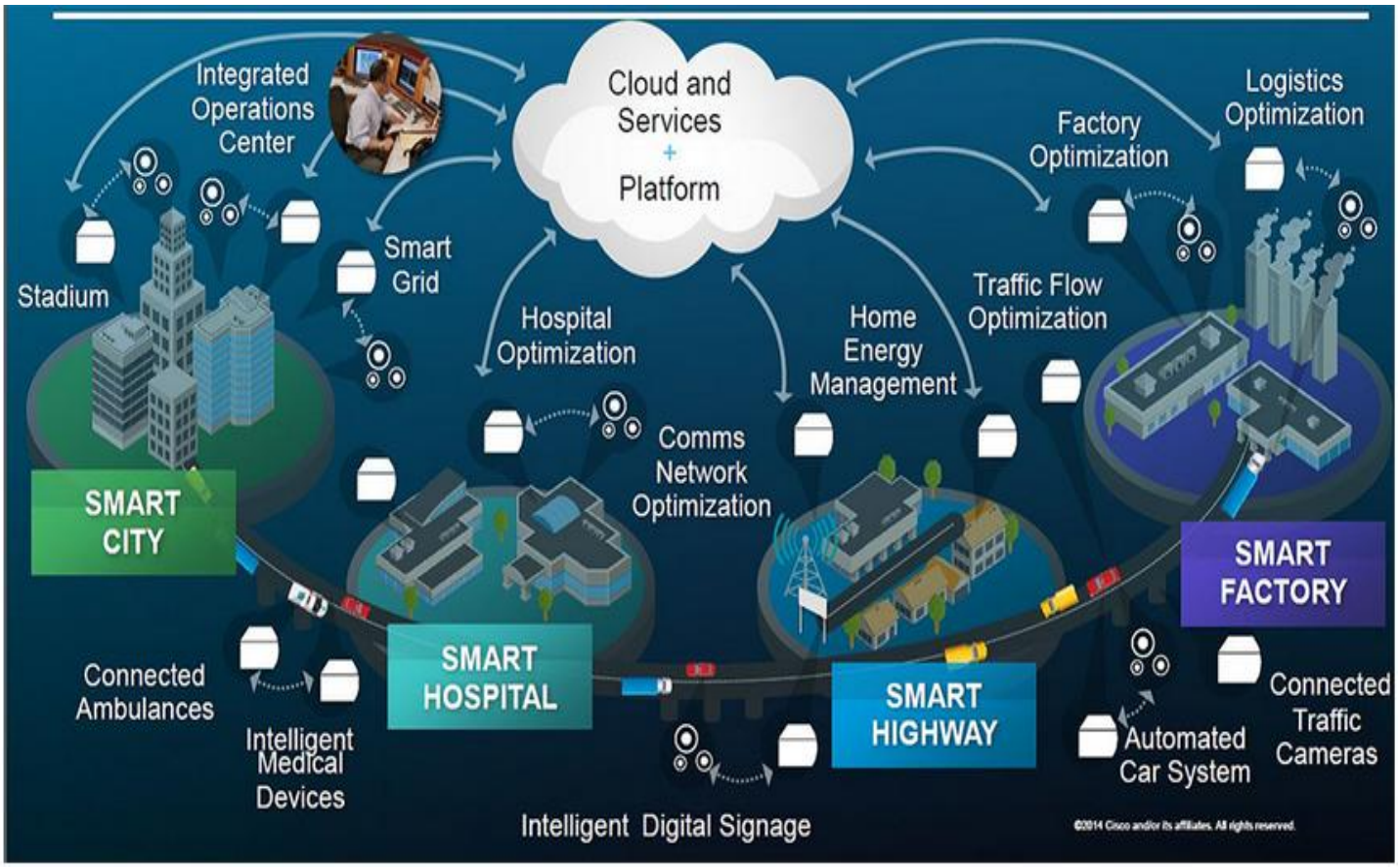
Five Insights on Infrastructure Cyber Attacks. Ryan Ayers November 22, 2017 Retrieved from
http://dataconomy.com/2017/11/5-insights-infrastructure-cyber-attacks/

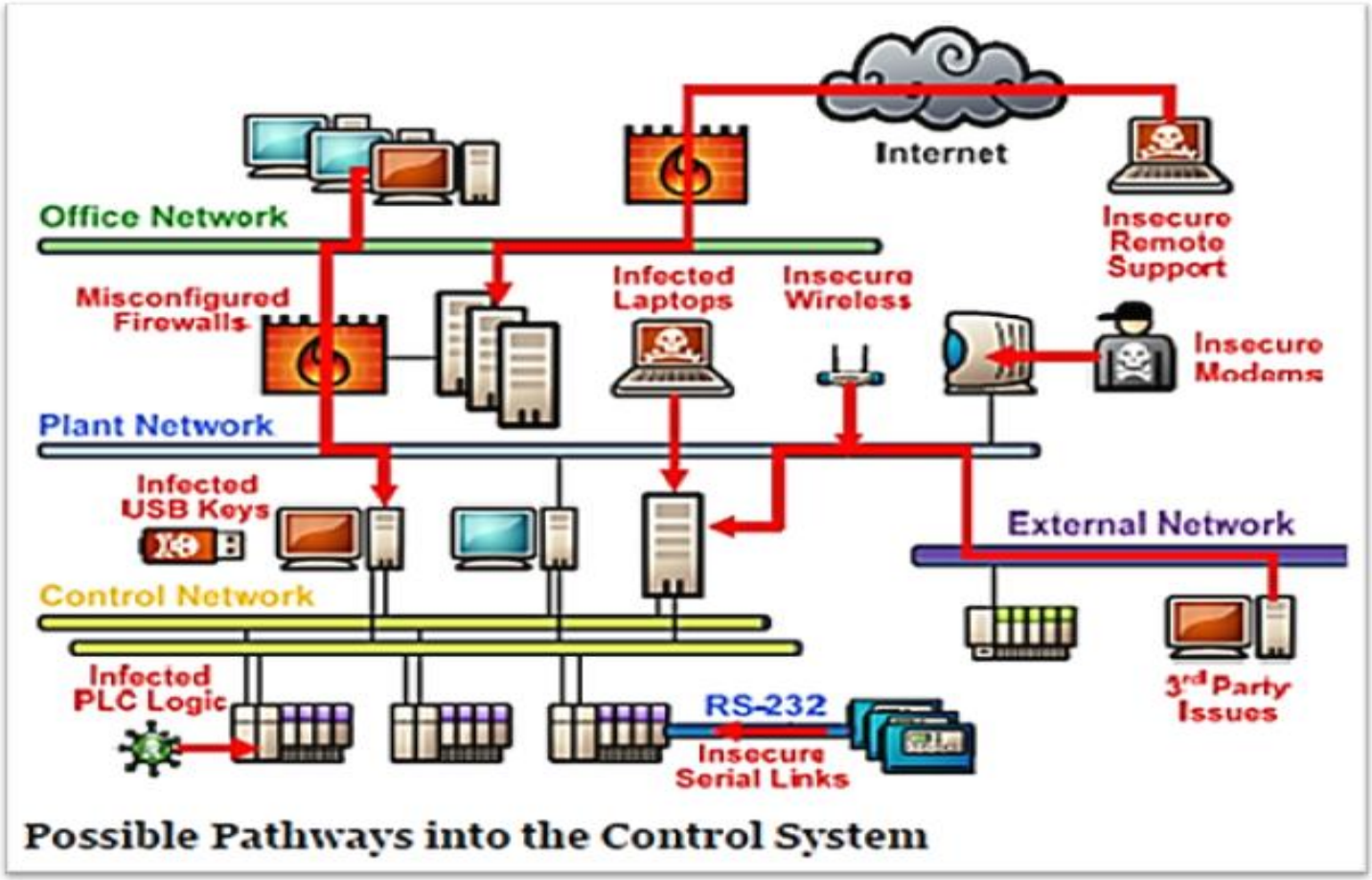
Hackers Halt Plant Operations in Watershed Cyber-Attack. Jim Finkle Retrieved from
https://www.reuters.com/article/us-cyber-infrastructure-attack/hackers-halt-plant-operations-in-watershed-cyber-attack-idUSKBN1E8271

How the Triton Malware Shut Down Critical Infrastructure in the Middle East
The December attack leveraged a zero-day flaw, and user error, to infect industrial equipment.
Brandon Vigliarolo January 19, 2018, Retrieved from
https://www.techrepublic.com/article/how-the-triton-malware-shut-down-critical-infrastructure-in-the-middle-east/

Smart Forensics for the Internet of Things (IoT) March 22, 2017 Usama Salama Retrieved from
https://securityintelligence.com/smart-forensics-for-the-internet-of-things-iot/

What Is IoT Forensics and How is it Different from Digital Forensics? Feb 27 2018
By Cyber Security. Retrieved from
https://securitycommunity.tcs.com/infosecsoapbox/articles/2018/02/27/what-iot-forensics-and-how-it-different-digital-forensics


Integrated Operations Center
Cloud and Services + Platform
Logistics Optimization
Factory Optimization
Smart Grid
Stadium
Traffic Flow Optimization
Hospital Optimization
Home Energy Management
Comms Network Optimization
SMART CITY
SMART FACTORY
SMART HOSPITAL
SMART HIGHWAY
Connected Ambulances
Intelligent Medical Devices
Connected Traffic Cameras
Automated Car System
Intelligent Digital Signage
©2014 Cisco and/or its affiliates. All rights reserved.


Internet
Office Network
Insecure Remote Support
Misconfigured Firewalls
Infected Laptops
Insecure Wireless
Insecure Modems
Plant Network
Infected USB Keys
External Network
Control Network
Infected PLC Logic
RS-232
Insecure Serial Links
3rd Party Issues
Possible Pathways into the Control System