Cybersecurity – Grid, IoT, Smart City and Smart Grid

Cyberthreats and Security

Tim Weil – CISSP/CCSP, CISA, PMP
IEEE Senior Member
SecurityFeeds LLC

University of Denver
Denver, CO
Jun 16, 2020

Objectives of this Presentation

Cyberthreats and Security

-- A Writer's Life

-- Information Security – A body of knowledge

Grid Cybersecurity Resilience (Ukraine)

-- Advanced Persistent Threats (APT)

-- Cyber Attack Strategy

-- Industrial Control Systems (ICS) Kill Chain

Security and Privacy for the Smart City

-- Roadmap of Security and Privacy for Smart Cities

-- IEEE Communications Surveys and Tutorials

Mirai Distributed Denial of Service – IoT Security

-- IoT Landscape

-- Mirai DDoS IoT Attack (Oct 2016)

-- Internet of Things (IoT) Forensics

-- How Mirai Works

Cybersecurity for the Smart Grid

-- Industrial Control Systems (ICS) – Attack Timeline 2009-2019

- Components of an ICS Attack Surface

-- Recent Publications

- MITRE ATT&CK for ICS

Table of Contents

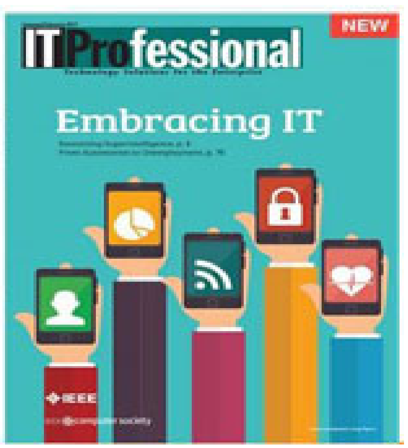
A Writer's Life –

Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...
Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ... US Department of Transportation, Washington, DC, USA	11



IT Risk And Resilience—Cybersecurity Response To COVID-19

SECURITYFEEDS / 27 MAY 2020 / 0 Comments

Download Export Citation

Home / Magazines / IT Professional / 2020.03

IT Risk and Resilience—Cybersecurity Response to COVID-19

May-June 2020, pp. 4-10, vol. 22
DOI Bookmark: 10.1109/MITP.2020.2988330

Authors

Tim Weil, SecurityFeeds LLC
San Murugesan, Western Sydney University

My article, in collaboration with SAN MURUGESAN, IT Risk and Resilience - Cybersecurity Response to COVID-19 published this month in IEEE IT Professional magazine. We look at the pandemic thru the lens of the NIST Cybersecurity Framework. This article is available through IEEE Open Access - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9098180

A Cybersecurity Body of Knowledge – IEEE Security and Privacy (May/June 2018)

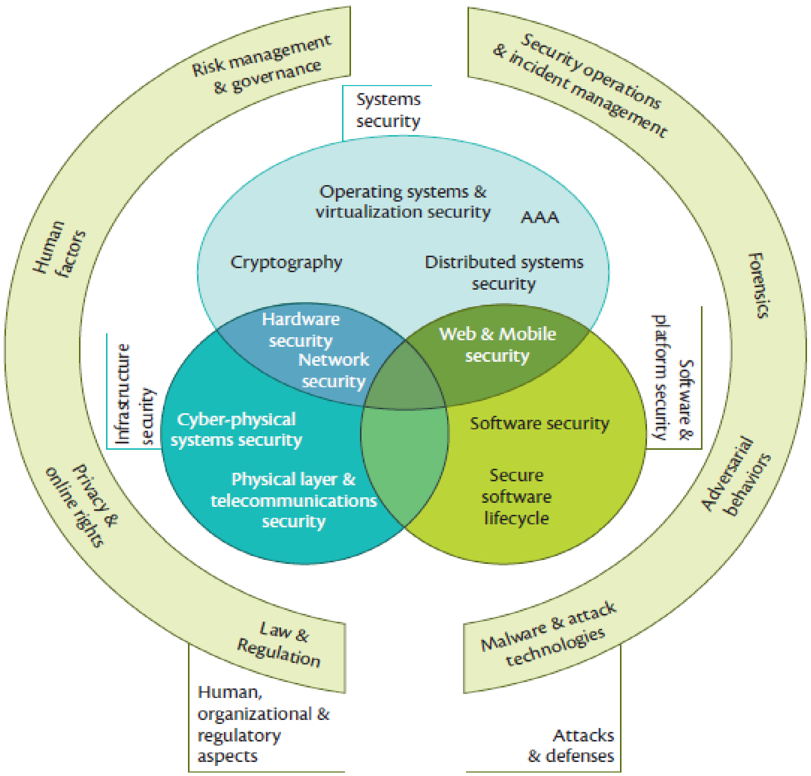


Figure 3. The 19 knowledge areas and their categorization within CyBOK.

Table 3. Overview of the 19 knowledge areas.

Human, Organizational, and Regulatory Aspects	
Risk Management and Governance	Security management systems and organizational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law and Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social and behavioral factors impacting security, security culture and awareness as well as the impact of security controls on user behaviors.
Privacy and Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.
Attacks and Defenses	
Malware and Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviors	The motivations, behaviors, and methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations and Incident Management	The configuration, operation, and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, and reporting of digital evidence in support of incidents or criminal events.
Systems Security	
Cryptography	Core primitives of cryptography as presently practiced and emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems and Virtualization Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualization, and security in database systems.

"Scoping the Cyber Security Body of Knowledge" Awais Rashid, et. al

Table of Contents

Grid Cybersecurity in the News

TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#46ecff7a3191

On December 23, 2015, the control centers of three Ukrainian electricity distribution companies were remotely accessed. Taking control of the facilities' SCADA systems, malicious actors opened breakers at some 30 distribution substations in the capital city Kiev and western Ivano-Frankivsk region, causing more than 200,000 consumers to lose power Nearly a year later, on December 17, 2016, a single transmission substation in northern Kiev lost power. These instances of sabotage took place on the tail of a political revolution in Kiev, the annexation of Crimea, and amid military clashes in the eastern Donetsk and Luhansk regions.

A Decade of Energy Cyber Infrastructure Attack Malware

http://www.aaes.org/sites/default/files/Sanders_Convocation2018.pdf

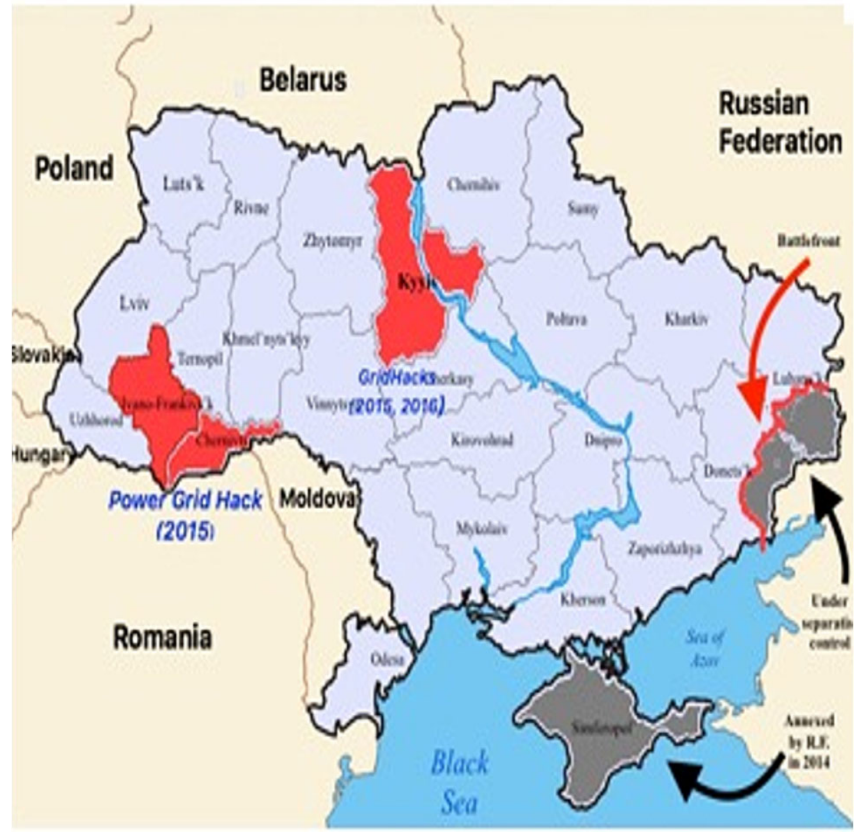
- **2010: Stuxnet:** Targeted Siemans industrial control systems in Iran. Was first discovered malware that spies on and subverts industrial systems and the first to include a programmable logic controller (PLC) rootkit.
- **2014: Dragonfly/Havex:** Focus was to collect ICS network and access control information. Evidence suggests this was provided to a well organized and funded group outside countries from which the data was collected.
- **2015: Black Energy 3:** Used in attack on the Ukraine power grid. Considered to be the first known power grid cyberattack. Hackers were able to successfully compromise information systems of three energy distribution companies and temporarily disrupt electricity supply to the end consumers.
- **2016: CRASHOVERRIDE:** Second known attack in Ukraine. Impacted a single transmission level substation. Significant increase in sophistication of attack code relative to past attacks.
- **2017: TRISIS/TRITON:** Incident at a critical infrastructure organization which targeted Schneider Electric's Triconex safety instrumented system (SIS) and where an attacker deployed malware which targeted systems provided emergency shutdown capability for industrial processes. Deployed against at least one victim in the Middle East.

Ukrainian Shale Deposits and Russian Electrical Grid Attacks

The discovery of shale deposits has prompted Russian attempts to stall their developments and sabotage much needed business deals for Ukraine's foreign capital thirsty economy. Russia's military operation on the ground solved the prospects of Ukrainian energy competition problem for Russia, albeit *partially*.[83] The warzone in the Eastern Ukraine covers the Donetsk region part of Yuzivska shale bloc, and, thus, closed it to development.

In addition, the Kharkiv region (second half of the shale bloc) has been subject to destabilizing activities. Among these actions were the recent explosions at an arms warehouse in Balaklia, in the Kharkiv region, which, according to Ukraine's defense minister Poltorak, was staged by Russia.[84] It is also worth noting that at the beginning of the unrest in the Eastern Ukraine, there were numerous attempts, however unsuccessful, to create Russia-backed third separatist enclave in Kharkiv region.[85]

To prevent the development of energy sources in Ukraine's west, Moscow has employed various methods to destabilize the region – including attacks on the electrical grid. On December 23, 2015, Russian-led cyberattack on the Prykarpattyaoblenergo distribution center created enough uncertainty to hurt the prospects of setting up industrial fracking operations in that region. Ivano-Frankivsk region that hosts part of Olesska's shale block. Russian has also financed fracking protests The map illustrates the locations of the major attacks on the electrical grid



Ukraine Grid Utility Cybersecurity Attack – FireEye

https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf

In the first publicly documented power outage attributed to a cyber attack, Russian-nexus actors caused blackouts in several regions in Ukraine. The actors used spear phishing to plant **BlackEnergy3 malware**, which was used to disable control system computer. Responders also found a wiper module called killdisk that was used to disable both control and non-control systems computers. At the same time, the attackers overwhelmed utility call centers with automated telephone calls, impacting the utilities' ability to receive outage reports from customers and frustrating the response effort.

While **killdisk does not have the functionality to open breakers** – which would cause the outages – it would impede utility visibility of breaker status,and inhibit remote control of the substations. This suggests that the attackers used another method to cause the power outage, perhaps using interactive access via compromised corporate and SCADA accounts to remotely open individual breakers or initiate load shedding, sending simultaneous trip commands to multiple breakers.

Who is behind this attack?

BlackEnergy is a Trojan that was created by a hacker known as Cr4sh. In 2007, he reportedly stopped working on it and sold the source code for an estimated $700. The source code appears to have been picked by one or more threat actors and was used to conduct DDoS attacks against Georgia in 2008. These unknown actors continued launching DDoS attacks over the next few years. Around 2014, a specific user group of BlackEnergy attackers came to our attention when they began deploying SCADA-related plugins to victims in the ICS and energy sectors around the world

Potential Power-System-Specific Cyber Attack Strategies

http://www.aaes.org/sites/default/files/Sanders_Convocation2018.pdf

- Tripping breakers
- Changing values breaker settings
  - Lower settings can destabilize a system by inducing a large number of false trips
  - Lowering trip settings can cause extraneous other breakers, causing overloading of other transmission lines and/or loss of system stability
- Corrupting Control Information: Smart Meters, SCADA Data, PMU Data, Dispatch Information, etc.
- Sophisticated lateral movement attacks
- Life cycle attacks
- Insider threats
- Physical damage by cyber means
- Combined physical and cyber attacks

Lateral Movement in Cyber Kill Chain Demands Resiliency

http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf

Reconnaissance
- Port scanning
- Media analysis

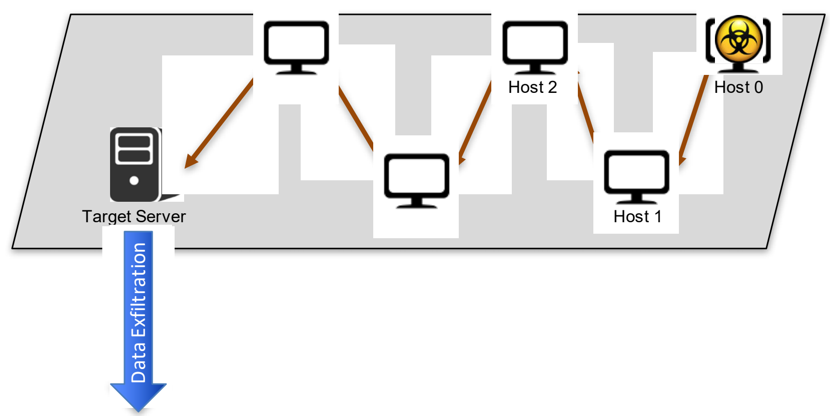
Delivery
- Spear phishing
- Zero-day exploits

Command and Control
- Control channels

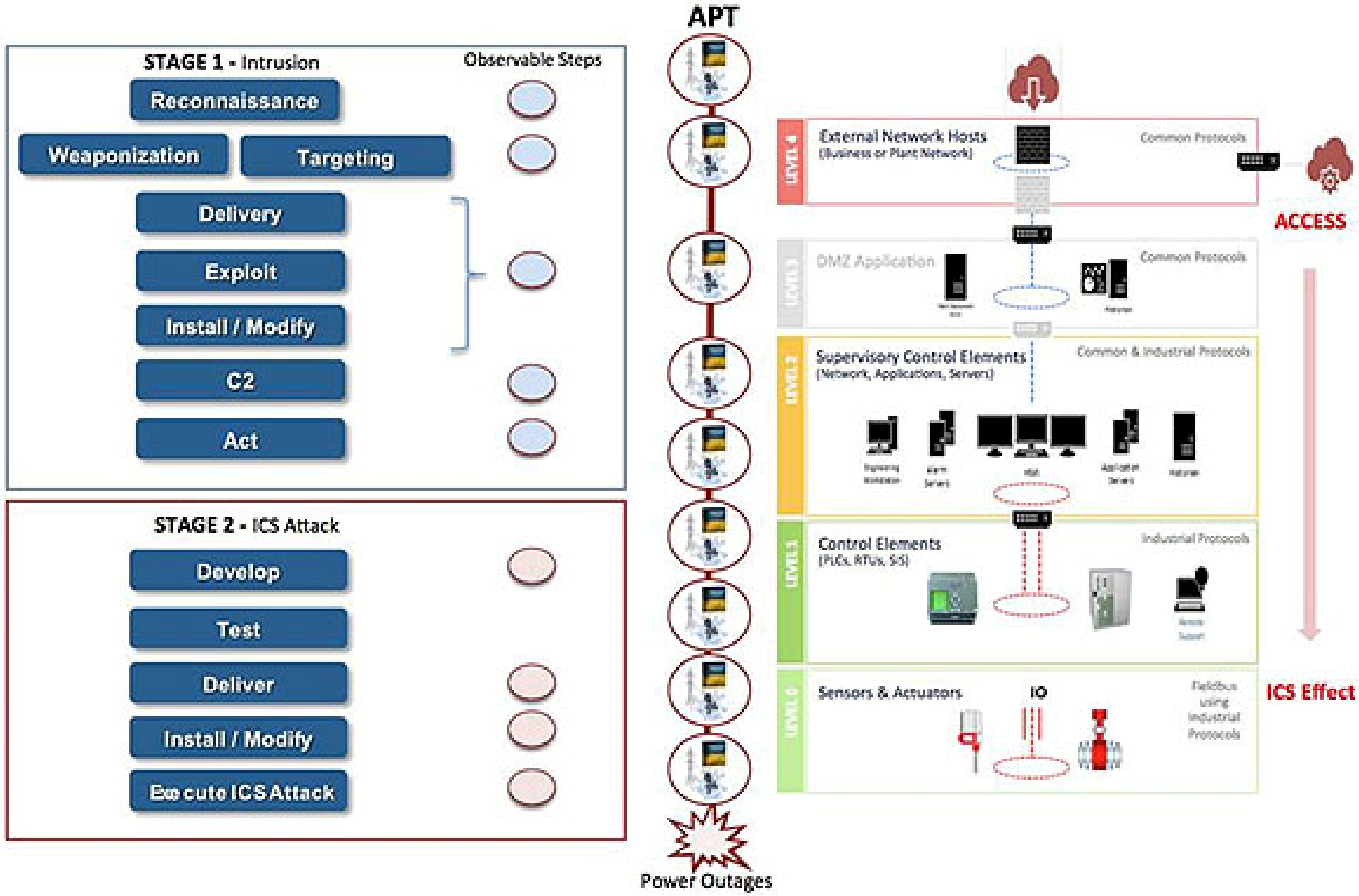
Lateral Movement
- Remote desktop
- Privilege escalation

Goal Accomplishment
- Data exfiltration
- Physical damage

During lateral movement:
- Attacker moves laterally between hosts
- Attacker uses remote desktop connections, SSH, Windows management inventory, administrator tools

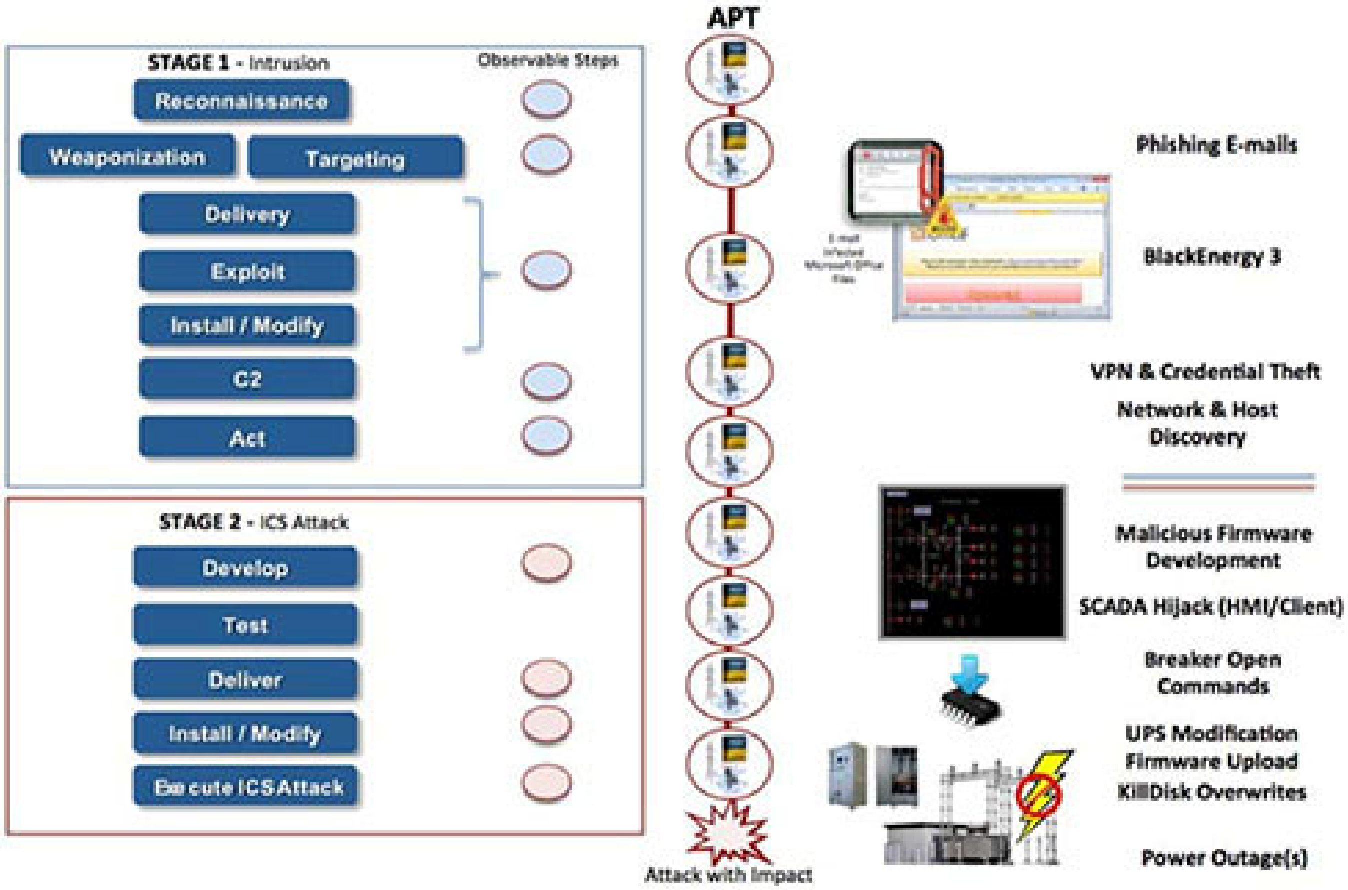


Ukraine Cyber Attack ICS Kill Chain (1 of 2)



IEEE COMMUNICATIONS SOCIETY Denver Chapter

Ukraine Cyber Attack ICS Kill Chain (2 of 2)



IEEE COMMUNICATIONS SOCIETY Denver Chapter

Ukraine Attack Consolidated Technical Components

1. Spear phishing to gain access to the business networks of the oblenergos
2. Identification of BlackEnergy 3 at each of the impacted oblenergos
3. Theft of credentials from the business networks
4. The use of virtual private networks (VPNs) to enter the ICS network
5. The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
6. Serial-to-ethernet communications devices impacted at a firmware level
7. The use of a modified KillDisk to erase the master boot record of impacted organizationsystems as well as the targeted deletion of some logs
8. Utilizing UPS systems to impact connected load with a scheduled service outage
9. Telephone denial-of-service attack on the call center

Ukraine Attack – Black Energy Malware (APT 1 of 2) -

https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

During the cyber intrusion stage of **Delivery, Exploit, and Install**, the malicious Office documents were delivered via email to individuals in the administrative or IT network of the electricity companies. When these documents were opened, a popup was displayed to users to encourage them to enable the macros in the document as shown in Figure. Enabling the macros allowed the malware to Exploit Office macro functionality to install BlackEnergy 3 on the victim system and was not an exploit of a vulnerability through exploit code.

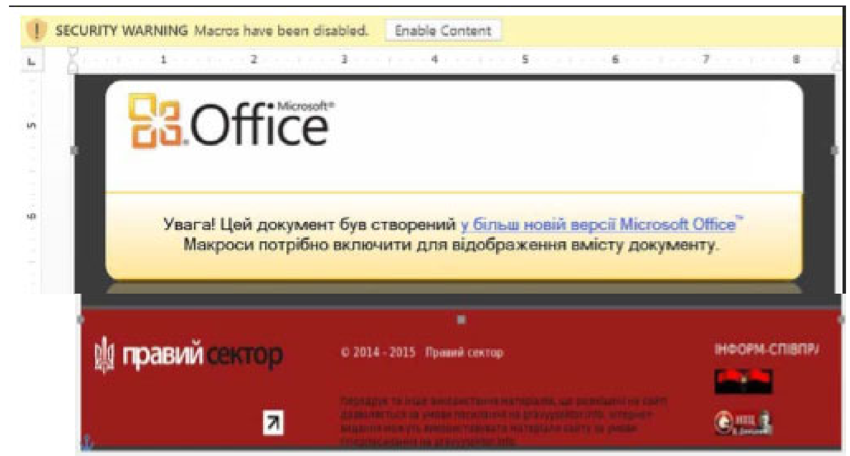


Figure 6: A Sample of a BlackEnergy 3 Infected Microsoft Office Document[27]

Upon the **Install** step, the BlackEnergy 3 malware connected to command and control (C2) IP addresses to enable communication by the adversary with the malware and the infected systems. These pathways allowed the adversary to gather information from the environment and enable access. The attackers appear to have gained access more than six months prior to December 23, 2015, when the power outage occurred. One of their first actions happened when the network was to harvest credentials, escalate privileges, and move laterally throughout the environment (e.g., target directory service infrastructure to directly manipulate and control the authentication and authorization system). At this point, the adversary completed all actions to establish persistent access to the targets.

Ukraine Attack – Kill Disk Malware -

https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

During **the ICS Attack Stage**, the adversaries used native software to Deliver themselves into the environment for direct interaction with the ICS components. They achieved this using existing remote administration tools on the operator workstations. The threat actors also continued to use the VPN access into the IT environment.

In final preparation for the attack, the adversaries completed the **Install/Mo**dify stage by installing malicious software identified as a modified or customized KillDisk across the environment. While it is likely the attackers then ensured their modifications to the UPS were ready for the attack, there was not sufficient forensic evidence available to prove this. The last act of modification was for the adversaries to take control of the operator workstations and thereby lock the operators out of their systems. Figure shows the static analysis of the KillDisk API imports following the event

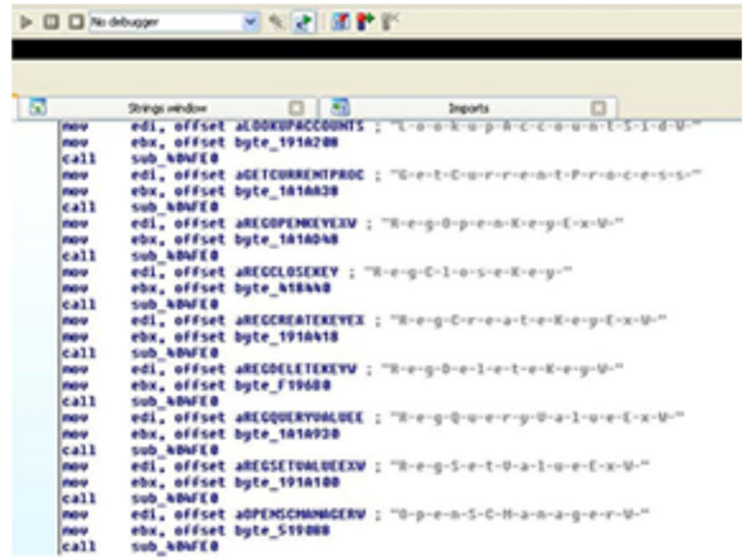
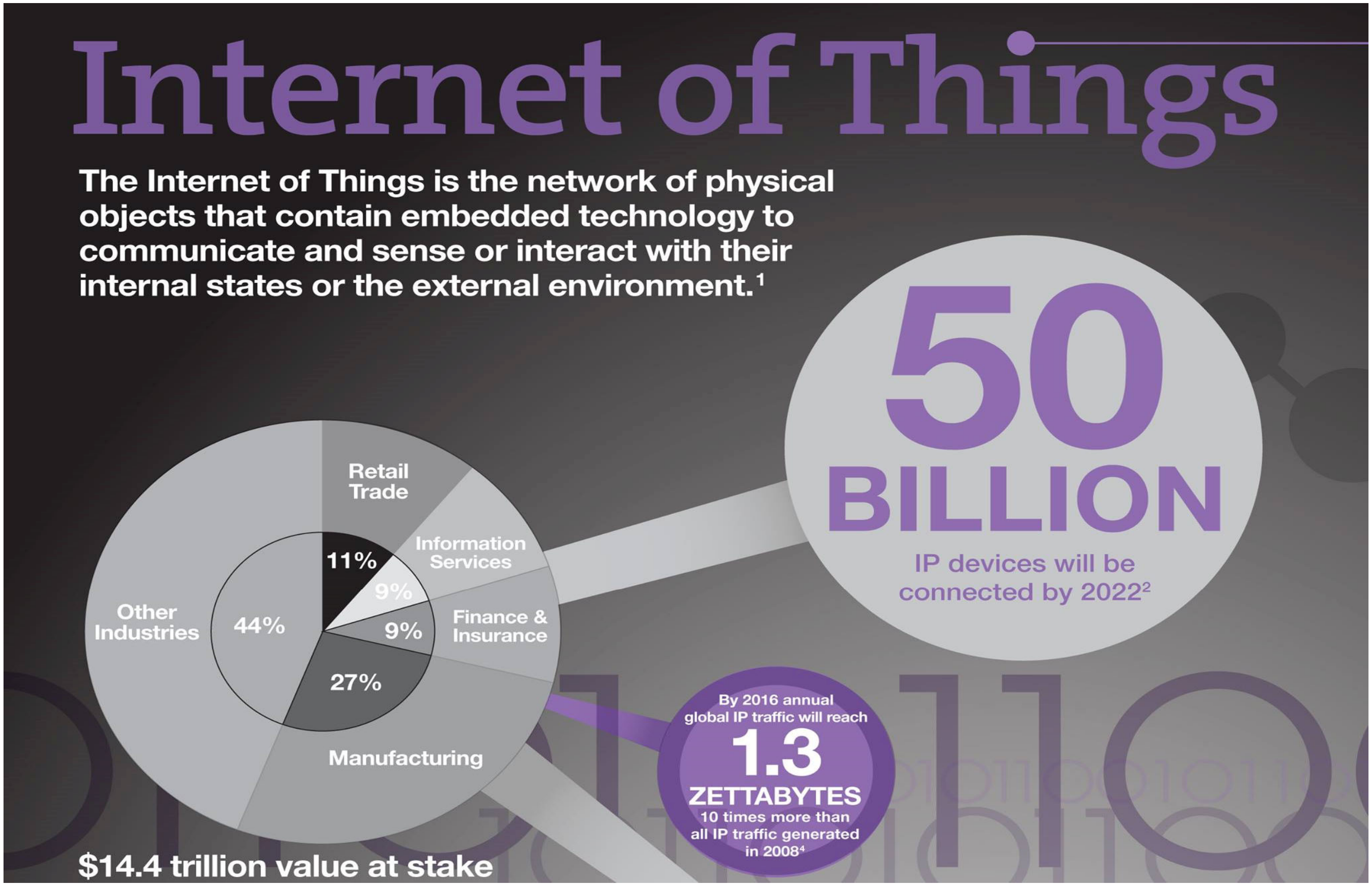


Figure 7: Static Analysis of KillDisk Identifying API Imports[32]

Finally, to complete the ICS Cyber Kill Chain and to Execute the ICS Attack, the adversaries used the HMIs in the SCADA environment to open the breakers. At least 27 substations (the total number is probably higher) were taken offline across the three energy companies, impacting roughly 225,000 customers. Simultaneously, the attackers uploaded the malicious firmware to the serial-to-ethernet gateway devices. This ensured that even if the operator workstations were recovered, remote commands could not be issued to bring the substations back online

Table of Contents

Internet of Things (IoT) Attack Surface

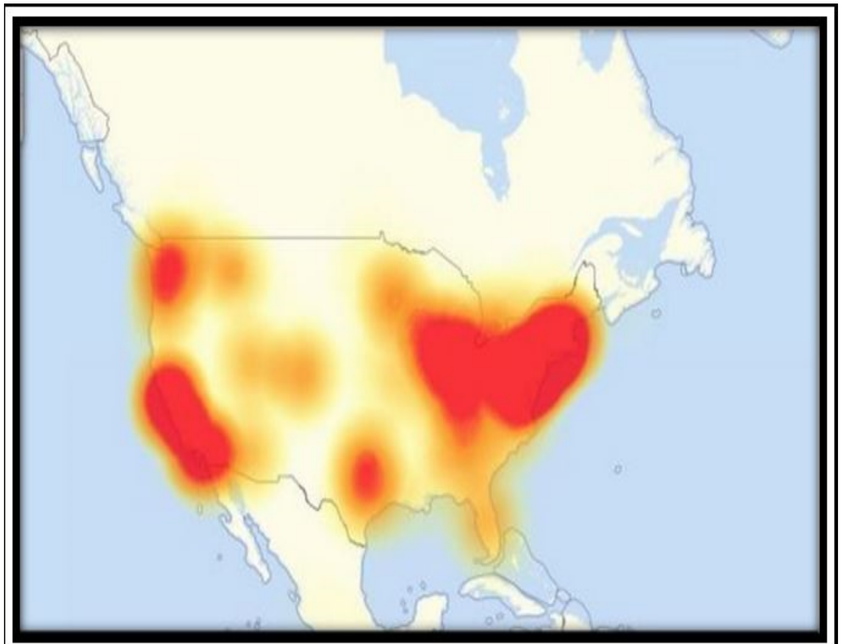


Typical IoT Devices

CCTV cameras
DVRs
Digital TVs
Home routers
Printers
Alexa
Cars
Other stuff

Security systems
Garage doors
Industrial systems
Medical systems
Home appliances
Smart Utility Meters

Mirai Botnet: IoT Botnets Performed Massive Distributed Denial of Service Attacks (Oct 2016)



What is Mirai Botnet

Mirai is a self-propagating botnet virus. The source code for Mirai was made publicly available by the author after a successful and well publicized attack on the Krebs Web site. Since then the source code has been built and used by many others to launch attacks on internet infrastructure (ref Dyn).

The Mirai botnet code infects poorly protected internet devices by using telnet to find those that are still using their factory default username and password. The effectiveness of Mirai is due to its ability to infect tens of thousands of these insecure devices and co-ordinate them to mount a DDOS attack against a chosen victim.

The Internet didn't "break" on October 21, 2016, but the attackers who launched the DDoS attacks against Dyn exploited a known DNS Weakness that negatively impacted MANY Internet-related businesses and millions of users.

http://www.billslater.com/mirai.ppsx

https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html

Mirai Impact

http://www.billslater.com/mirai.ppsx

INTERNET OF THINGS, SECURITY

Report: Mirai Botnet DDoSed 17 Dyn Data Centers Globally

BY YEVGENIY SVERDLIK ON OCTOBER 26, 2016 ADD YOUR COMMENTS

Tweet

All but three data centers where DNS provider Dyn hosts its global infrastructure came under attack in last week's massive DDoS strike that disrupted some of the internet's most popular destinations, such as Spotify, Amazon, HBO Now, Twitter, and The New York Times, among others.

Dyn's servers sit in 20 data centers spread around the world, and the attack — implemented at least in part by using a botnet created by software called Mirai, which hijacks poorly secured IoT devices, such as CCTV cameras and DVRs — was directed at 17 of those sites, according to an analysis by ThousandEyes, a provider of global network monitoring services. The three data centers that were not affected are in Warsaw, Beijing, and Shanghai.

"At the height of the attack, approximately 75 percent of our global vantage points sent queries that went unanswered by Dyn's servers," Nick Kephart, senior director of product marketing at ThousandEyes, wrote in a blog post. "In addition, the critical nature of many of these affected services led to collateral damage, in terms of outages and performance impacts on sites that are only tangentially related to Dyn (including this blog)."

WHO WAS HIT BY THE ATTACK?

Thousands of sites were hit, including:

- Twitter
- Reddit
- Spotify
- Esty
- Box
- Wix Customer Sites
- Squarespace Customer Sites
- Zoho
- CRM
- Iheart.com (iHeartRadio)
- Github
- The Verge
- Cleveland.com
- hbonow.com
- PayPal
- Big cartel
- Wired.com
- People.com
- Urbandictionary.com
- Basecamp
- ActBlue
- Zendesk.com
- Intercom
- Twillo
- Pinterest
- Grubhub
- Okta
- Starbucks rewards/gift cards
- Storify.com
- CNN
- Yammer
- Playstation Network
- Recode Business Insider
- Guardian.co.uk
- Weebly
- Yelp

How Mirai Works (1 of 3)

http://www.billslater.com/mirai.ppsx

There are two main components to Mirai, the virus itself and the command and control center (CnC). The virus contains the attack vectors, Mirai has ten vectors that it can launch, and a scanner process that actively seeks other devices to compromise. The CnC is a separate image that controls the compromised devices (BOT) sending them instructions to launch one of the attacks against one or more victims.

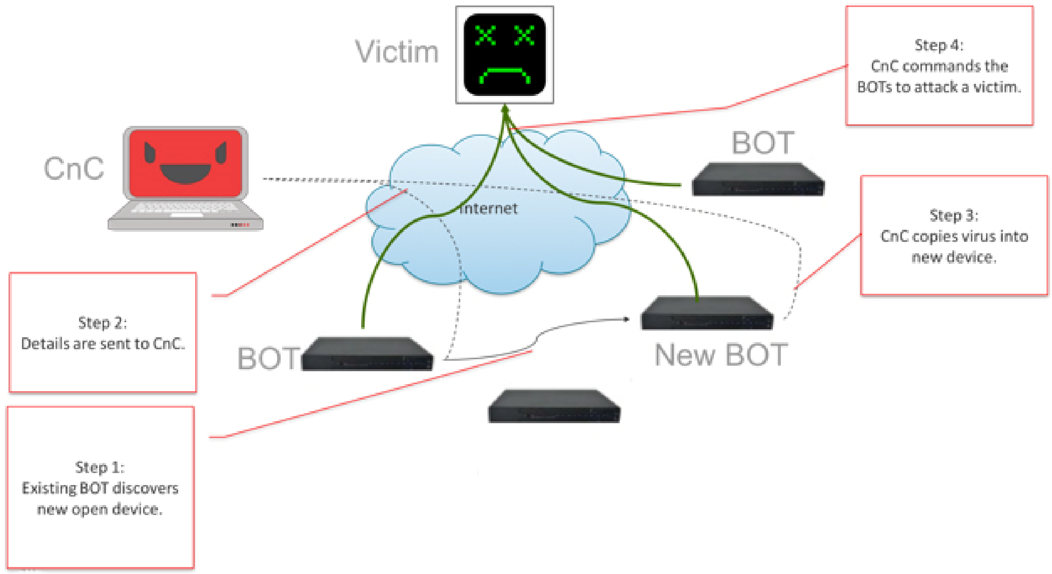


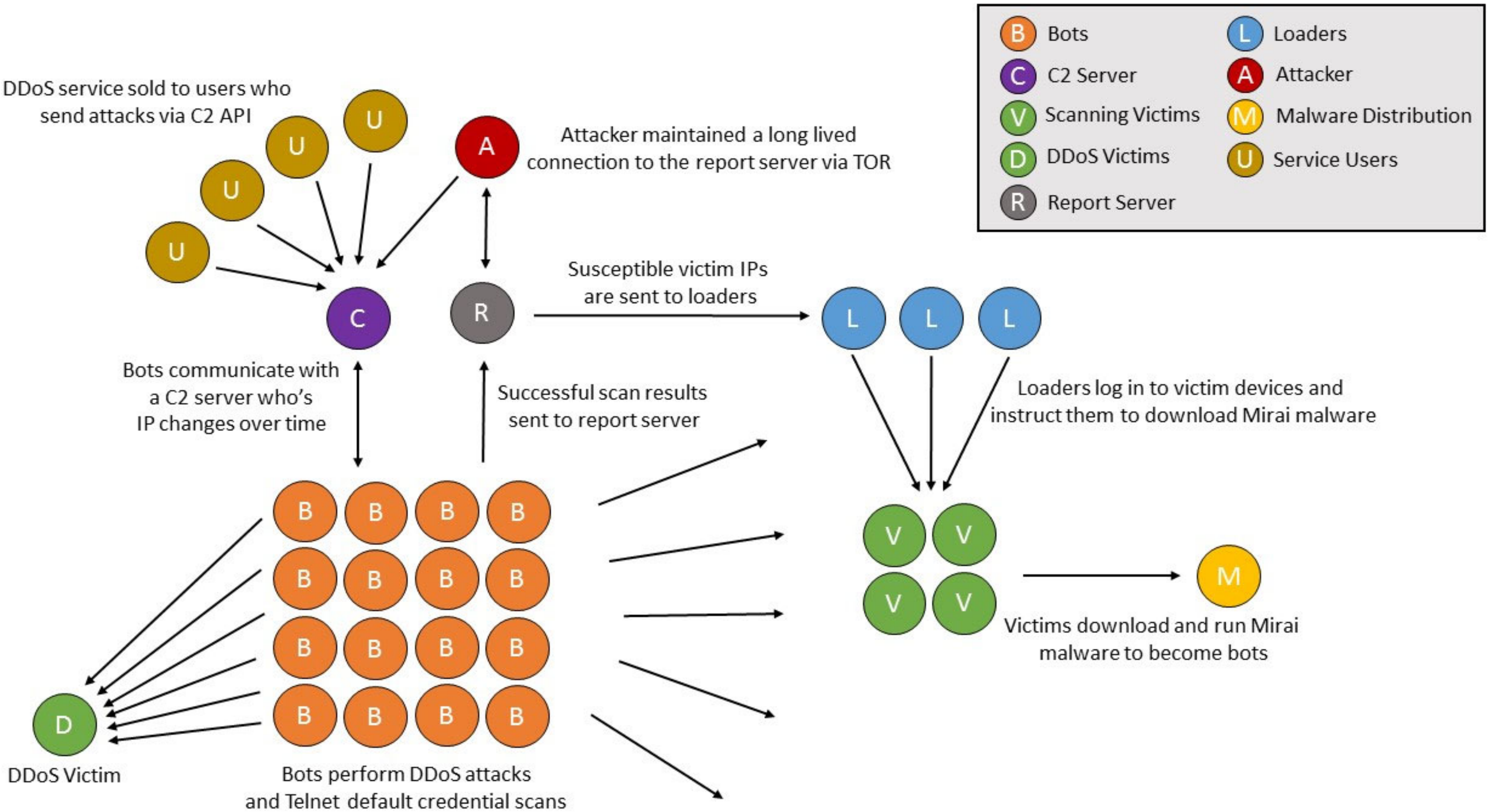
Figure 1 Mirai System

The scanner process runs continuously on each BOT using the telnet protocol (on TCP port 23 or 2323) to try and login to IP addresses at random. The login tries up to 60 different factory default username and password pairs when login succeeds the identity of the new BOT and its credentials are sent back to the CnC.

The CnC supports a simple command line interface that allows the attacker to specify an attack vector, a victim(s) IP address and an attack duration. The CnC also waits for its existing BOTs to return newly discovered device addresses and credentials which it uses to copy over the virus code and in turn create new BOTs.

How Mirai Works (2 of 3)

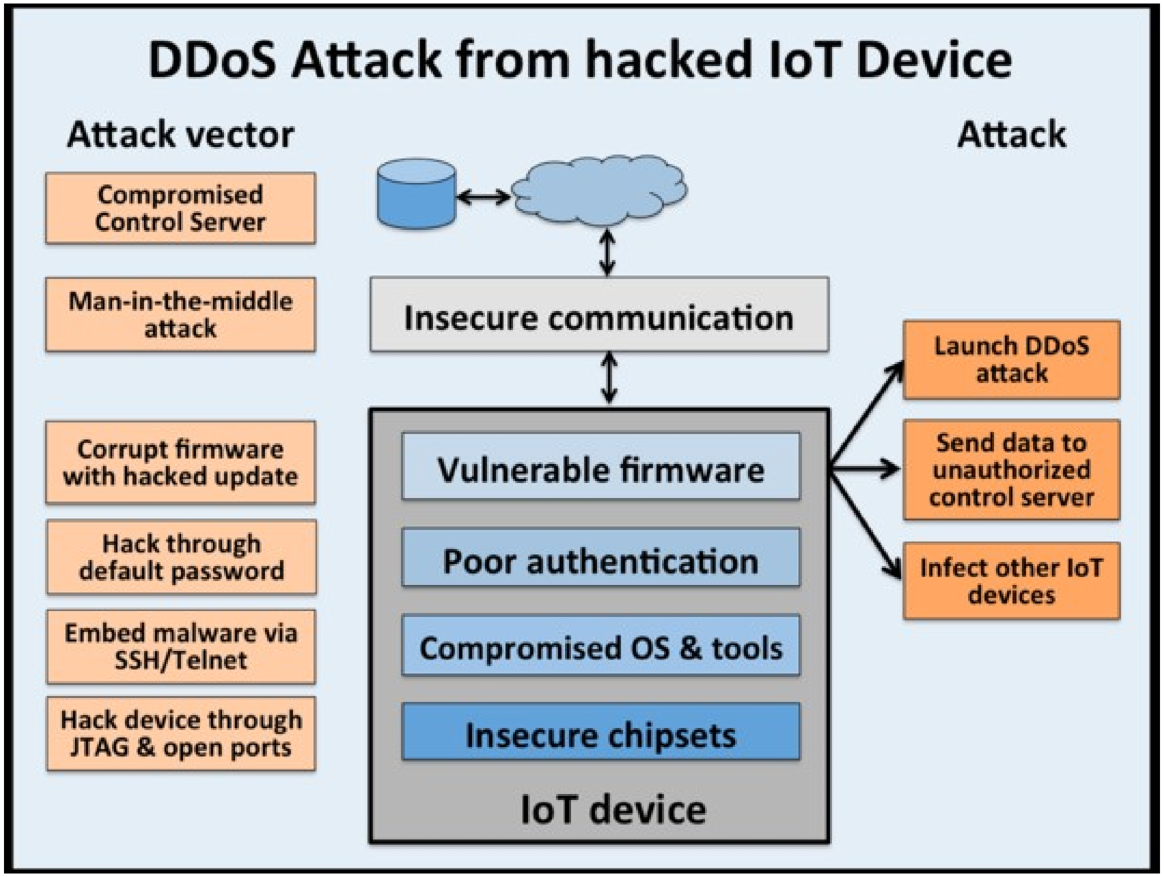
http://www.billslater.com/mirai.ppsx



IEEE COMMUNICATIONS SOCIETY Denver Chapter

How Mirai Works (3 of 3)

http://www.billslater.com/mirai.ppsx



Infected IoT Devices:

1) Launch DDoS Attacks
2) Report data to C2 Servers
3) Infect other IoT Devices

Where Mirai Botnet Attacks Came From

http://www.billslater.com/mirai.ppsx

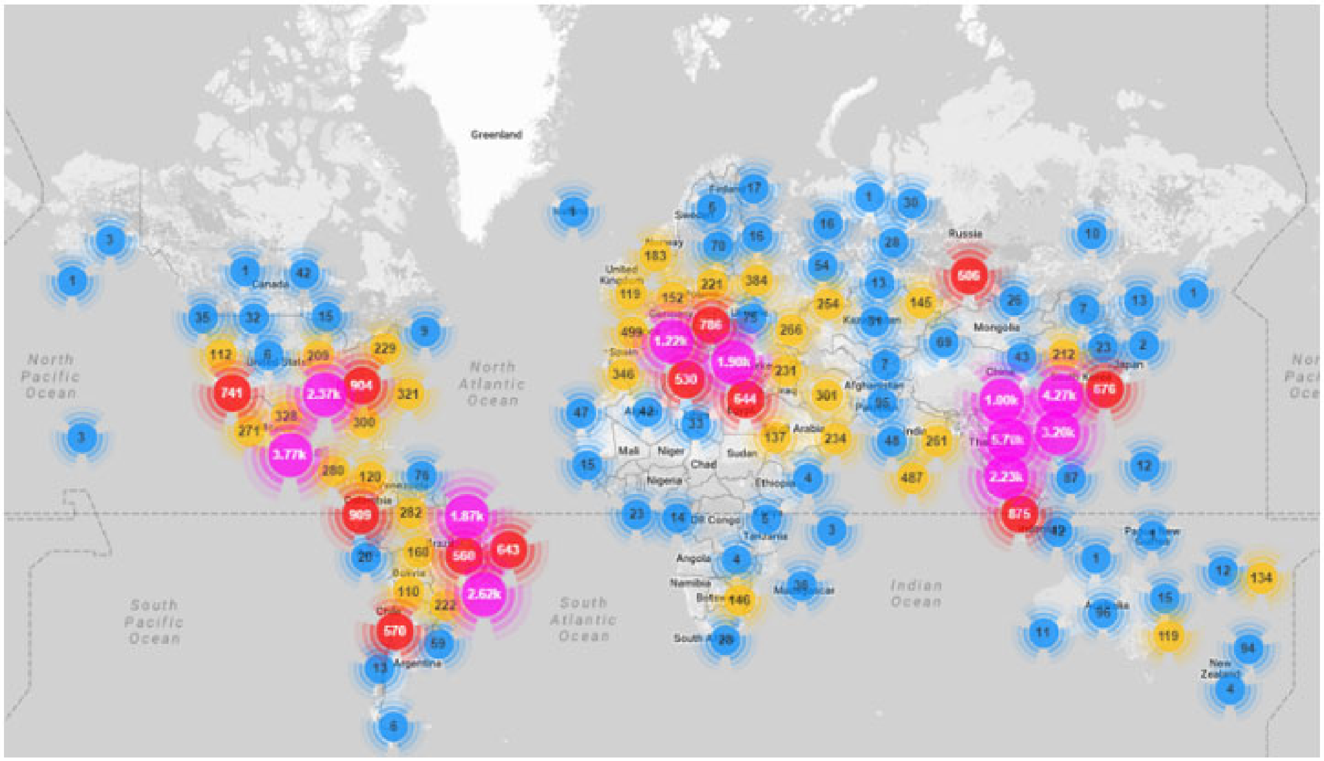


Figure 2: Geo-locations of all Mirai-infected devices uncovered so far

Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Source:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Mirai – Statistical View of the Attacks

- Mirai-powered Generic Routing Encapsulation (GRE floods), peaked at 280 Gbps/130 Mpps

- Investigation of the attack uncovered 49,657 unique IPs which hosted Mirai-infected devices. As previously reported, these were mostly CCTV cameras—a popular choice of DDoS botnet herders.

- Other victimized devices included DVRs and routers.

- Overall, IP addresses of Mirai-infected devices were spotted in 164 countries. As evidenced by the map below, the botnet IPs are highly dispersed, appearing even in such remote locations as Montenegro, Tajikistan and Somalia.

Protecting IoT Devices Against Mirai (Botnets)

http://www.billslater.com/mirai.ppsx

- ***Change Your Password.*** This is not only good advice for those of us who shop online or who have been notified that the e-commerce site we recently shopped on has been breached, but likewise for IoT devices. In fact, according to this report, these better credentials can be used to provide a bulwark against botnet attacks like Mirai by substituting the hard-coded username and password with ones that are unique to your organization and not, of course, easily guessed.
- ***Turn them off.*** For currently deployed IoT devices, turn them off when not in use. If the Mirai botnet does infect a device, the password must be reset and the system rebooted to get rid of it.
- ***Disable all remote access to them.*** To protect devices from Mirai and other botnets, users should not only shield TCP/23 and TCP/2323 access to those devices, but also to disable all remote (WAN) access to them.
- ***Research Your Purchase.*** Before you even buy a product, research what you are buying and make sure that you know how to update any software associated with the device. Look for devices, systems, and services that make it easy to update the device and inform the end user when updates are available.
- ***Use It or Lose It.*** Once the product is in your office, turn off the functions you're are not using. Enabled functionality usually comes with increased security risks. Again, make sure you review that before you even bring the product into the workplace. If it's already there, don't be shy about calling customer service and walking through the steps needed to shut down any unused functions.

Source:
https://www.pwnieexpress.com/blog/mirai-botnet-part-2

Table of Contents

A Smart City Will Create Opportunities for Energy Management

5G-Based Transmission Power Control Mechanism in Fog Computing for Internet of Things Devices

https://arxiv.org/ftp/arxiv/papers/1712/1712.09645.pdf

FogGrid: Leveraging Fog Computing for Enhanced Smart Grid Network

https://arxiv.org/ftp/arxiv/papers/1712/1712.09645.pdf

Panasonic Launches Smart City Innovation Showcase at Peña Station NEXT to Celebrate Company's 100th Anniversary

https://www.penastationnext.com/pan-clean-energy.html

OpenFog

The **OpenFog Consortium** is an association of major tech companies aimed at standardizing and promoting fog computing.

Fog computing[1] or **fog networking**, also known as **fogging**,[2][3]is an architecture that uses one or more collaborative multitude of end-user clients or near-user edge devices to carry out a substantial amount of storage (rather than stored primarily in cloud data centers), communication (rather than routed over the **internet backbone**), control, configuration, measurement and management (rather than controlled primarily by network gateways such as those in the **LTE core network**).

NEW INFORMATION ON FOG COMPUTING

OpenFog_Reference_Architecture_2_09_17-FINAL-1

OpenFog Consortium Reference Architecture – Summary presentation for Denver Summit

Helder Antunes – Fog Forum Denver2

Fog and Security (Fog Forum 2017 Denver)2

OpenFog-Architecture-Overview-WP-2-2016

The Fog Computing Paradigm: Scenarios and Security Issues

Look In 2017 Archives

References

1. **Jump up ^** *Bar-Magen Numhauser, Jonathan (2013). Fog Computing introduction to a New Cloud Evolution. Escrituras silenciadas: paisaje como historiografía. Spain: University of Alcala. pp. 111–126. **ISBN 978-84-15595-84-7**.*

http://sites.ieee.org/denver-com/technology/

IEEE Communications Society – Surveys and Tutorials

Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications

Ala Al-Fuqaha, *Senior Member, IEEE*, Mohsen Guizani, *Fellow, IEEE*, Mehdi Mohammadi, *Student Member, IEEE*, Mohammed Aledhari, *Student Member, IEEE*, and Moussa Ayyash, *Senior Member, IEEE*

***Abstract*—This paper provides an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper starts by providing a horizontal overview of the IoT. Then, we give an overview of some technical details that pertain to the IoT enabling technologies, protocols, and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues to enable researchers and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities without having to go through RFCs and the standards specifications. We also provide an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. Moreover, we explore the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing. We also present the need for better horizontal integration among IoT services. Finally, we present detailed service use-cases to illust-**

Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges

Mehdi Sookhak, Helen Tang, *Senior Member, IEEE*, Ying He, *Student Member, IEEE*, and F. Richard Yu, *Fellow, IEEE*

The Sensable City: A Survey on the Deployment and Management for Smart City Monitoring

Rong Du, *Student Member, IEEE*, Paolo Santi, Ming Xiao, *Senior Member, IEEE*, Athanasios V. Vasilakos, and Carlo Fischione, *Member, IEEE*

Next Generation 5G Wireless Networks: A Comprehensive Survey

Mamta Agiwal, Abhishek Roy, and Navrati Saxena

Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges

Mithun Mukherjee, *Member, IEEE*, Lei Shu, *Senior Member, IEEE*, and Di Wang

Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues

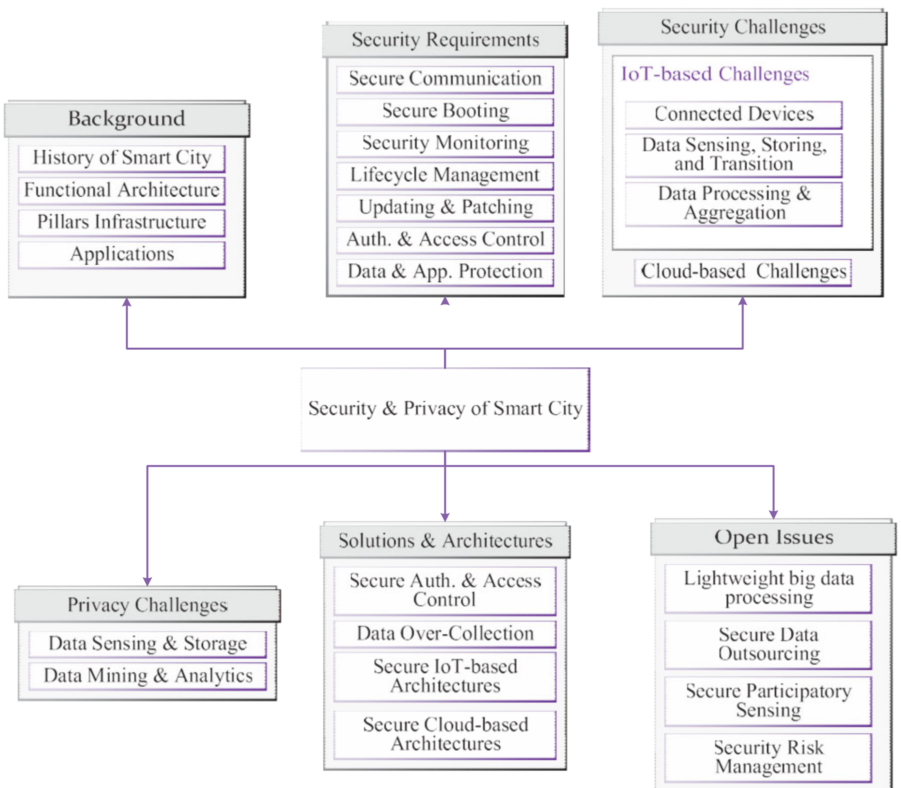
Pardeep Kumar *Member, IEEE* , Yun Lin *Member, IEEE*, Guangdong Bai, Andrew Paverd *Member, IEEE*, Jin Song Dong, and Andrew Martin *Member, IEEE*

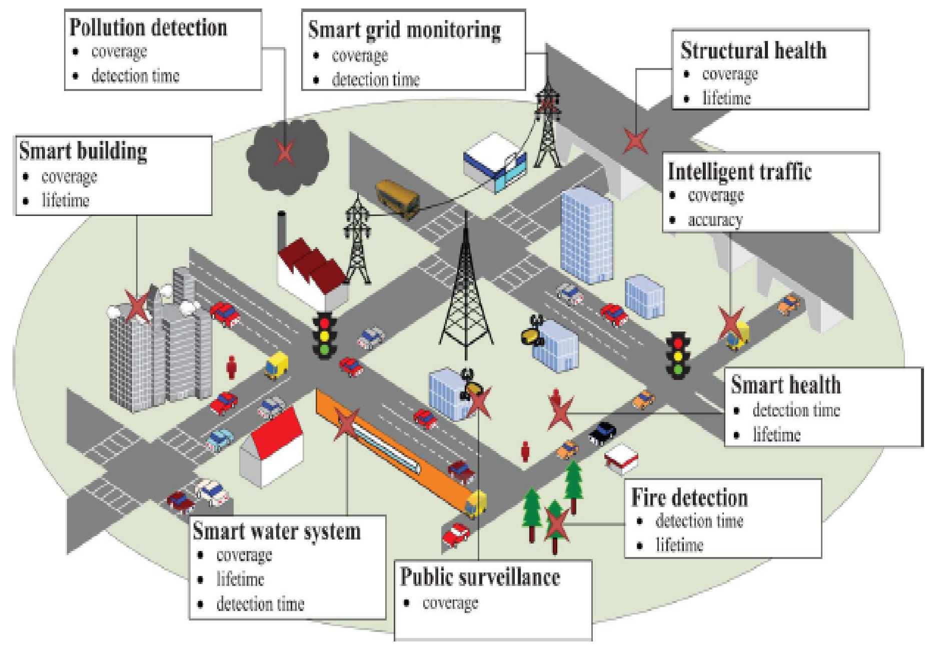
IEEE COMMUNICATIONS SOCIETY Denver Chapter

Categories of Smart Cities - (IEEE Communications Surveys and Tutorials)

Type	Ref.	Key Features
Digital City	[24]	Connecting people and city elements to gather information for creating a sustainable, greener city using new technologies
	[25]	Optimizing electrical resources, transportation, and other city operations using the deployed sensors and communication systems
	[26]	Interconnecting physical, IT, social, and business infrastructures to achieve intelligent city
	[27]	An effective solution to control the resources
ICT City	[28]	Investing in human and social capital and ICT communication to manage natural resources
	[29]	Using smart communities to achieve an ideal economy and society and increase quality of life
	[30]	Exchanging and analyzing information intelligently on the basis of a smart governance operating for achieving sustainable city
	[31]	Identifying economy, people, governance, mobility, environment and living as the main characteristics of smart city
	[32]	Promoting socio-economic, ecological, logistic and competitive performance of cities by applying knowledge-intensive strategies
Compound City	[33]	Applying ICT to promote human, social, relational, and environmental capitals
	[3]	Developing urban centers (economic, human, social, and environmental capitals) using all available technology and resources
	[34]	Including everything related to either governance and economy, or ICT, sensors, smart devices, and real-time data analysis city
	[35]	Cultivating socio-technical and socio-economic aspects of cities by using specific intellectual abilities
	[36]	Applying ICT to optimize resources and infrastructures, augment economy capitals

Roadmap of Security and Privacy of Smart Cities - (IEEE Communications Surveys and Tutorials)





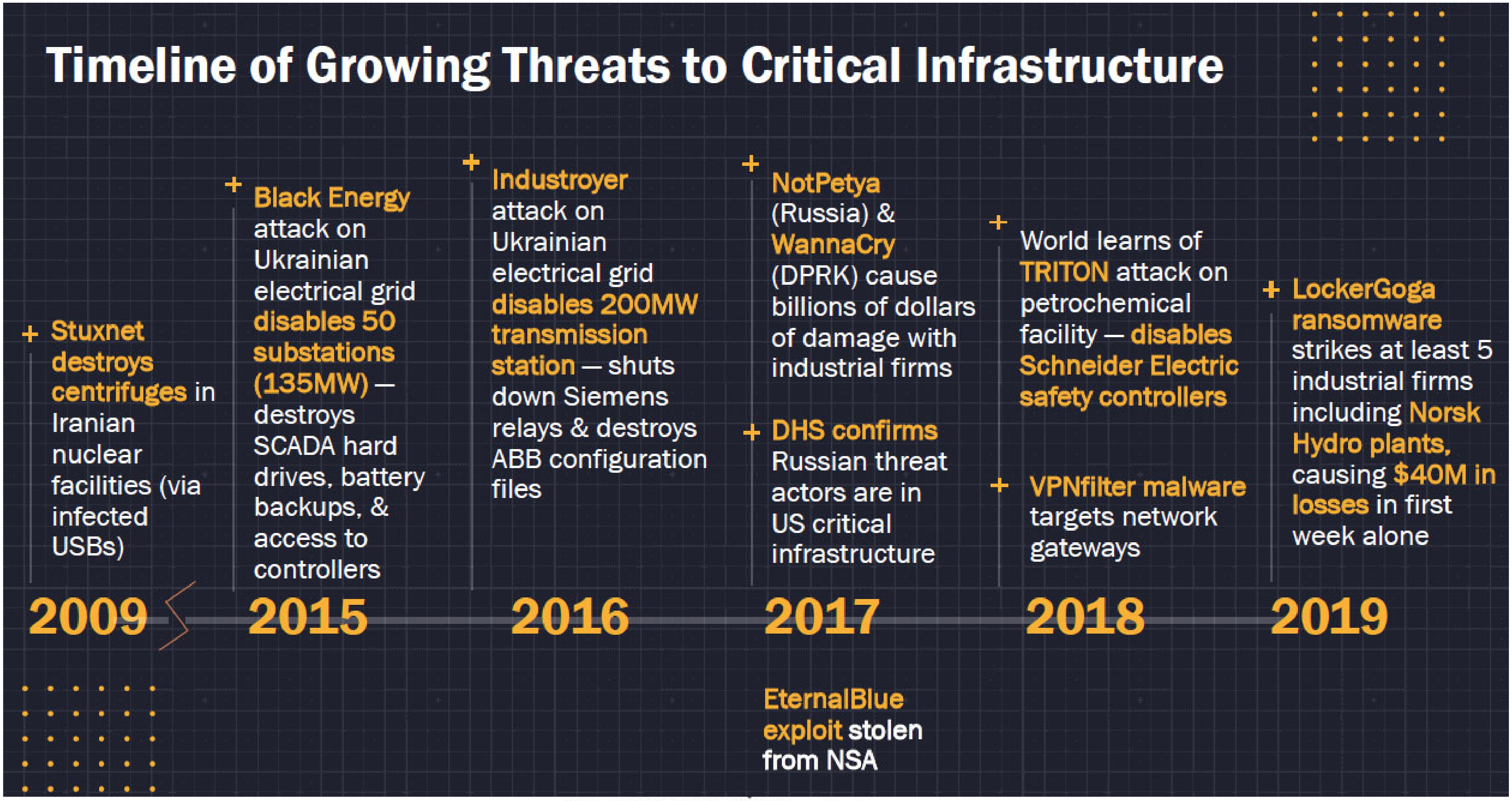
A smart city with various applications and sensing devices. Although these sensing systems target different application domains, they share common objectives on coverage, network lifetime, detection time, etc., and thus they share common research and design challenges.

Categories of Smart Cities - Security Requirements

Requirements	Method	Challenge
Secure Communication	Lightweight cryptographic Methods	Heterogeneity of Network components and devices
	Distributed key management system [51], [52]	Geographical distribution of smart cities; Draining the embedded system's resources
Secure Booting	Cryptographic boot system	Adoption to heterogeneous IoT devices
Security Monitoring, Analysis, and Response	Cisco Security Monitoring, Analysis, and Response System (MARS) [59]	Only applicable for Cisco network equipment
System, Application, and Solution Lifecycle Management	Smart City Comprehensive Data Life Cycle model [61]	Lack of security and privacy measurement
Updating and Patching	Microsoft and Linux patch updating	Authenticating the update package may reduce the IoT device functionalities; May not be applicable for old IoT devices
Authentication, Identification, and Access Control	IBE [68], ABE [69], RBAC [70]	Are only applicable for cloud-based IoT systems; May incur high computation cost on IoT devices.
Data and Application Protection	Securing IoT devices, Access permission monitoring, Securing communication links using cryptographic methods	Lack of a comprehensive framework to provide security and privacy of all layers of smart cities simultaneously.

Table of Contents

Cybersecurity for the Smart Grid



Cybersecurity for the Smart Grid

Smart grids security challenges: Classification by sources of threats

https://www.sciencedirect.com/science/article/pii/S2314717218300163

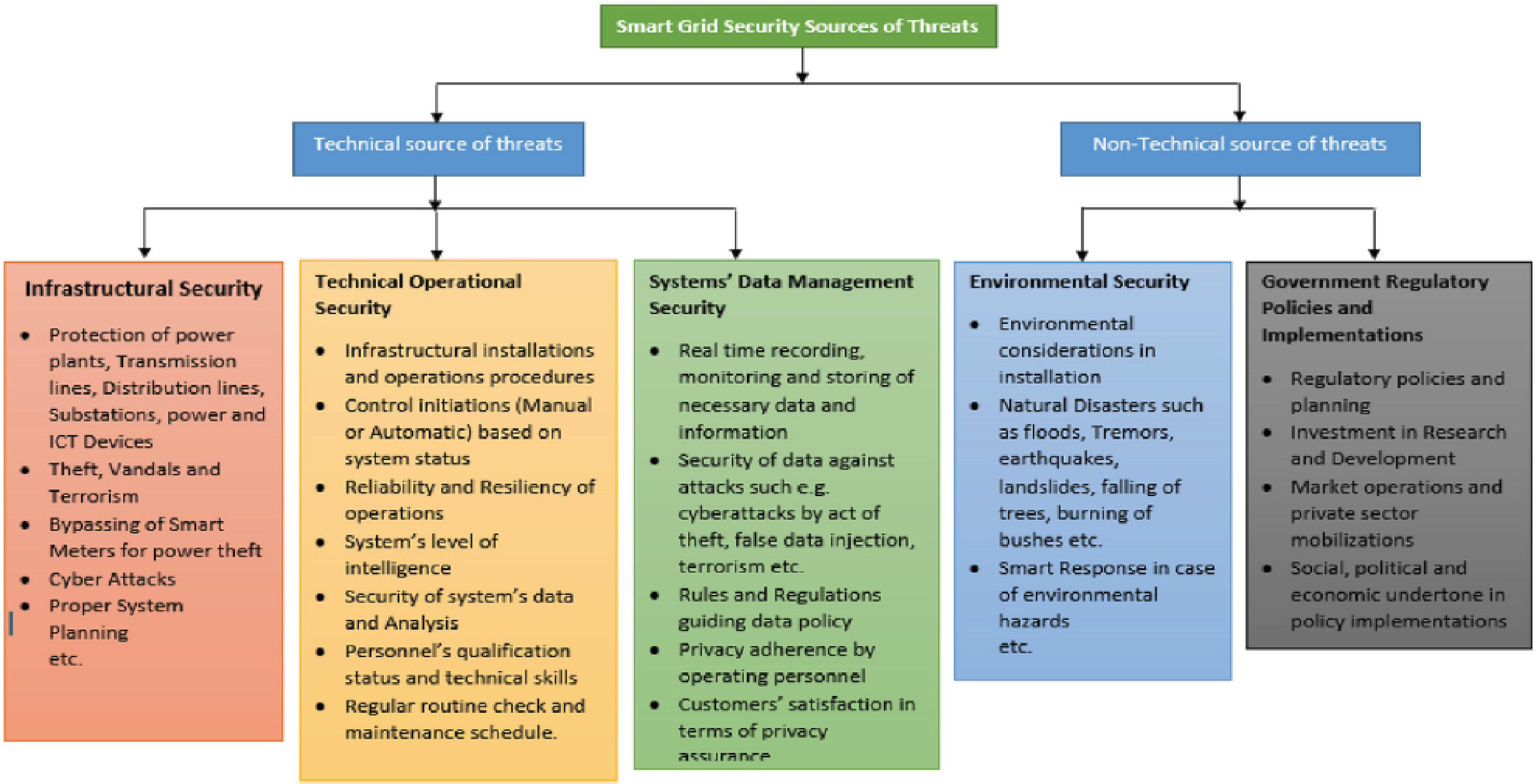
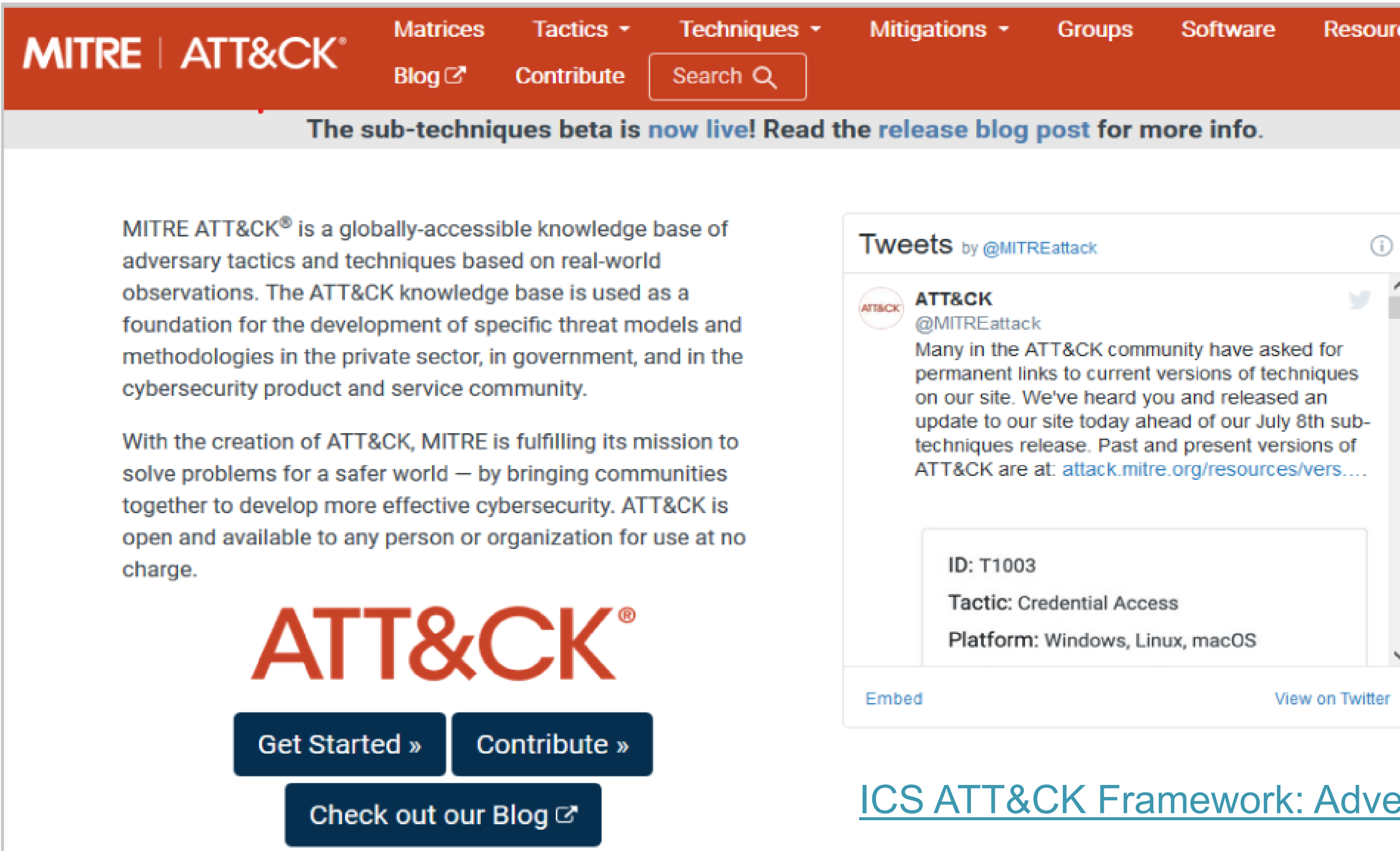


Fig. 4. Classification of SG threats by sources.

MITRE ATT&CK for Industrial Control Systems - https://attack.mitre.org/

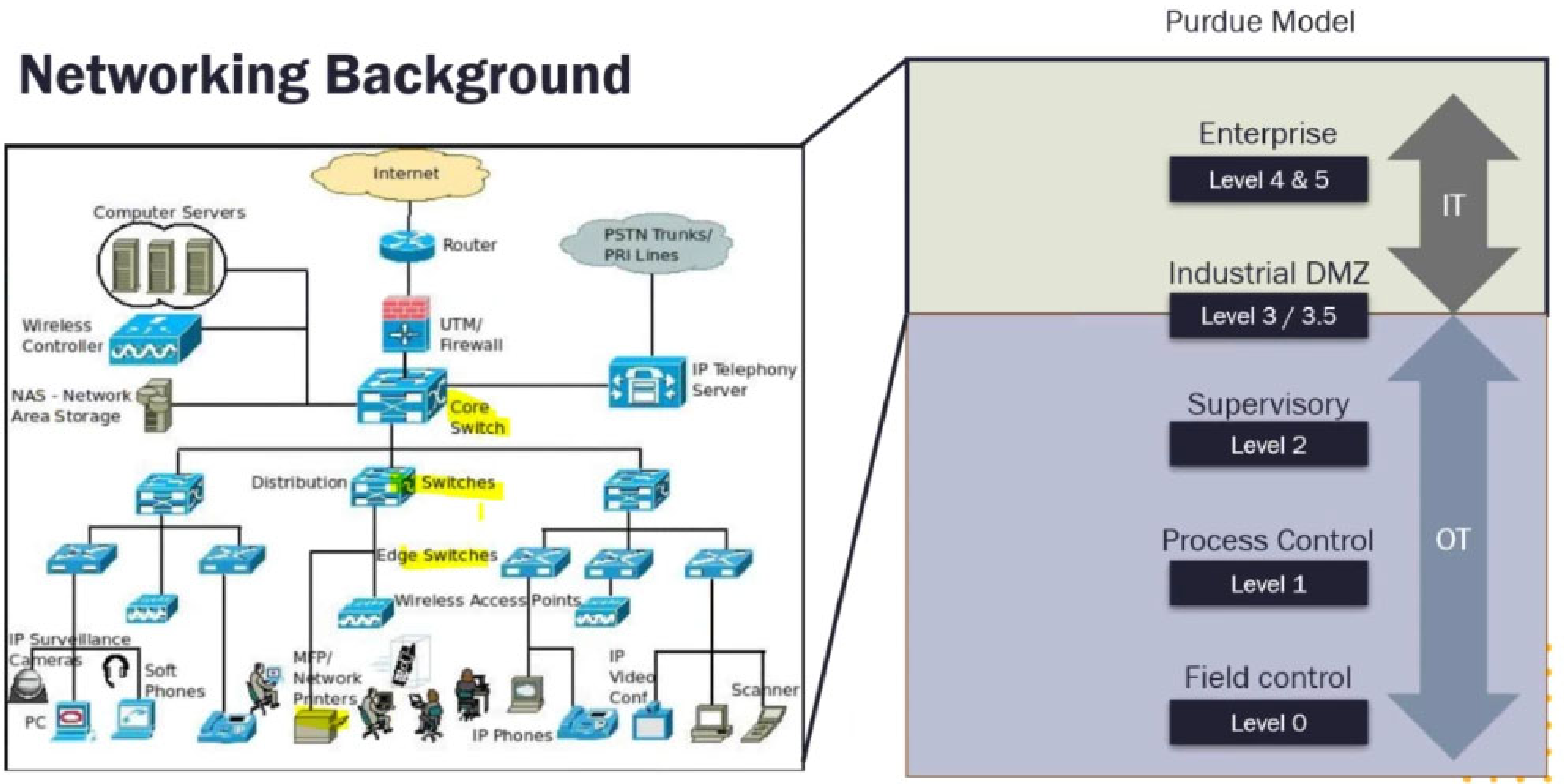


MITRE ATT&CK –

Adversary Tactics, Techniques & Common Knowledge

ICS ATT&CK Framework: Adversary Tactic and Techniques

MITRE ATT&CK for Industrial Control Systems - https://attack.mitre.org/



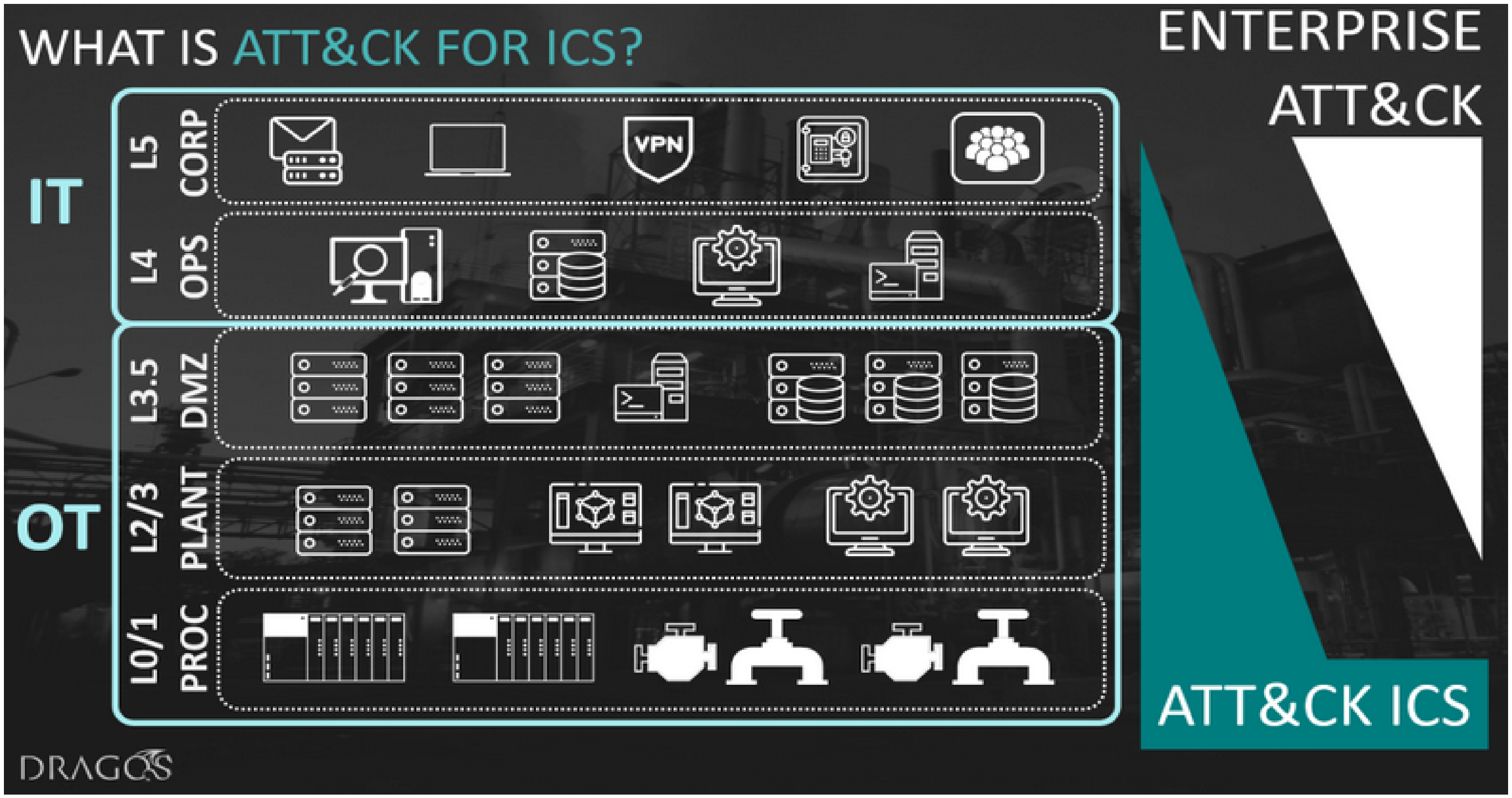
Enterprise Network (IT)

Operational Technology (OT) Network
Industrial Internet Of Things (IIOT)
Industrial Control Systems (ICS) or SCADA

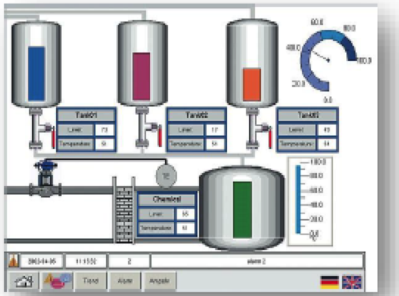
MITRE ATT&CK for Industrial Control Systems

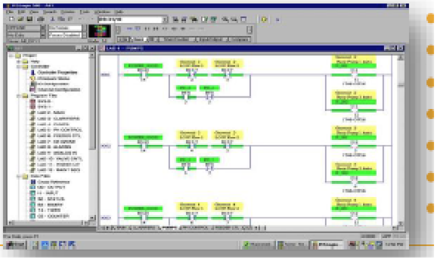
https://attack.mitre.org/

Because ICS technology operates differently than enterprise technology, it requires that Activity Groups take a unique approach to cause an impact in this arena. Even within ICS, industry verticals (Electric, O&G, Manufacturing) have unique characteristics. ATT&CK for ICS is vertical agnostic and is meant to work equally for ICS systems that support a wide range of industrial processes.



Industrial Control Systems (ICS) Components





- PLC – Programmable Logic Controller
  - PLC receives information from connected sensors or input devices, processes the data, and triggers outputs based on pre-programmed parameters.
    - ABB, Allen Bradley, Siemens, Mitsubishi, Honeywell, Motorola, Hitachi, General Electric, etc
- RTU – Remote Terminal Unit
  - RTU and PLCs perform similar functions, but used in wider geographical telemetry
    - ABB, GE Grid Solutions, Honeywell, Schneider Electric, Siemens Energy
- HMI – Human Machine Interface
  - HMI represents plant information to the operating personnel graphically in the form of diagrams
    - Mitsubishi Electric, Omron, Rockwell, Schneider Electric, etc
- EWS – Engineering WorkStation
  - Very reliable computer designed for configuration, maintenance and diagnostics of the Industrial Control System (ICS) applications
- Historian
  - Architected to pull data from a variety of systems to quickly form a complete context of the manufacturing environment.
    - Schneider Electric Wonderware, OSISoft PI, Rockwell

MITRE ATT&CK ICS Threat Matrix (1 of 2)

Initial Access	Execution	Persistence	Evasion	Discovery
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration
Spearphishing Attachment	Scripting			
Supply Chain Compromise	User Execution			
Wireless Compromise				

ATT&CK is a normalized, structured approach to classifying and describing the methods adversaries use to attack systems . ATT&CK starts out high level and provides a solid framework of concepts and relation- ships for understanding attack methods .

Tactics –

- Initial Access
- Execution
- Persistence
- Evasion
- Discovery

MITRE ATT&CK ICS Threat Matrix (2 of 2)

https://collaborate.mitre.org/attackics/

Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
	Monitor Process State		Denial of Service	Program Download	Loss of Safety
	Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
	Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
	Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
	Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information

Tactics –

- Lateral Movement
- Collection
- Command and Control
- Inhibit Response Function
- Impair Process Control
- Impact

MITRE ATT&CK ICS Threat Matrix -Tactics https://collaborate.mitre.org/attackics/index.php/All_Tactics

Below is a list of all 11 tactics in ATT&CK for ICS:

Name	Description
Collection	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.
Command and Control	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.
Discovery	The adversary is trying to figure out your ICS environment.
Evasion	The adversary is trying to avoid being detected.
Execution	The adversary is trying to run malicious code.
Impact	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.
Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
Initial Access	The adversary is trying to get into your ICS environment.
Lateral Movement	The adversary is trying to move through your ICS environment.
Persistence	The adversary is trying to maintain their foothold in your ICS environment.

ATT&CK ICS Threat Matrix Techniques - https://collaborate.mitre.org/attackics/index.php/All_Techniques

Below is a list of all 81 techniques in ATT&CK for ICS:

Name	Tactics	ID	Technical Description
Activate Firmware Update Mode	Inhibit Response Function	T800	Adversaries may activate firmware update mode on devices to prevent expected response functions from engaging in reaction to an emergency or process malfunction. For example, devices such as protection relays may have an operation mode designed for firmware installation. This mode may halt process monitoring and related functions to allow new firmware to be loaded. A device left in update mode may be placed in an inactive holding state if no firmware is provided to it. By entering and leaving a device in this mode, the adversary may deny its usual functionalities.
Alarm Suppression	Inhibit Response Function	T878	Adversaries may target protection function alarms to prevent them from notifying operators of critical conditions. Alarm messages may be a part of an overall reporting system and of particular interest for adversaries. Disruption of the alarm system does not imply the disruption of the reporting system as a whole. In the Maroochy Attack, the adversary suppressed alarm reporting to the central computer.[1] A Secura presentation on targeting OT notes a dual fold goal for adversaries attempting alarm suppression: prevent outgoing alarms from being raised and prevent incoming alarms from being responded to.[2] The method of suppression may greatly depend on the type of alarm in question: • An alarm raised by a protocol message • An alarm signaled with I/O • An alarm bit set in a flag (and read) In ICS environments, the adversary may have to suppress or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring.[2] Methods of suppression may involve tampering or altering device displays and logs, modifying in memory code to fixed values, or even tampering with assembly level instruction code.
Automated Collection	Collection	T802	Adversaries may automate collection of industrial environment information using tools or scripts. This automated collection may leverage native control protocols and tools available in the control systems environment. For example, the OPC protocol may be used to enumerate and gather information. Access to a system or interface with these native protocols may allow collection and enumeration of other attached, communicating servers and devices.

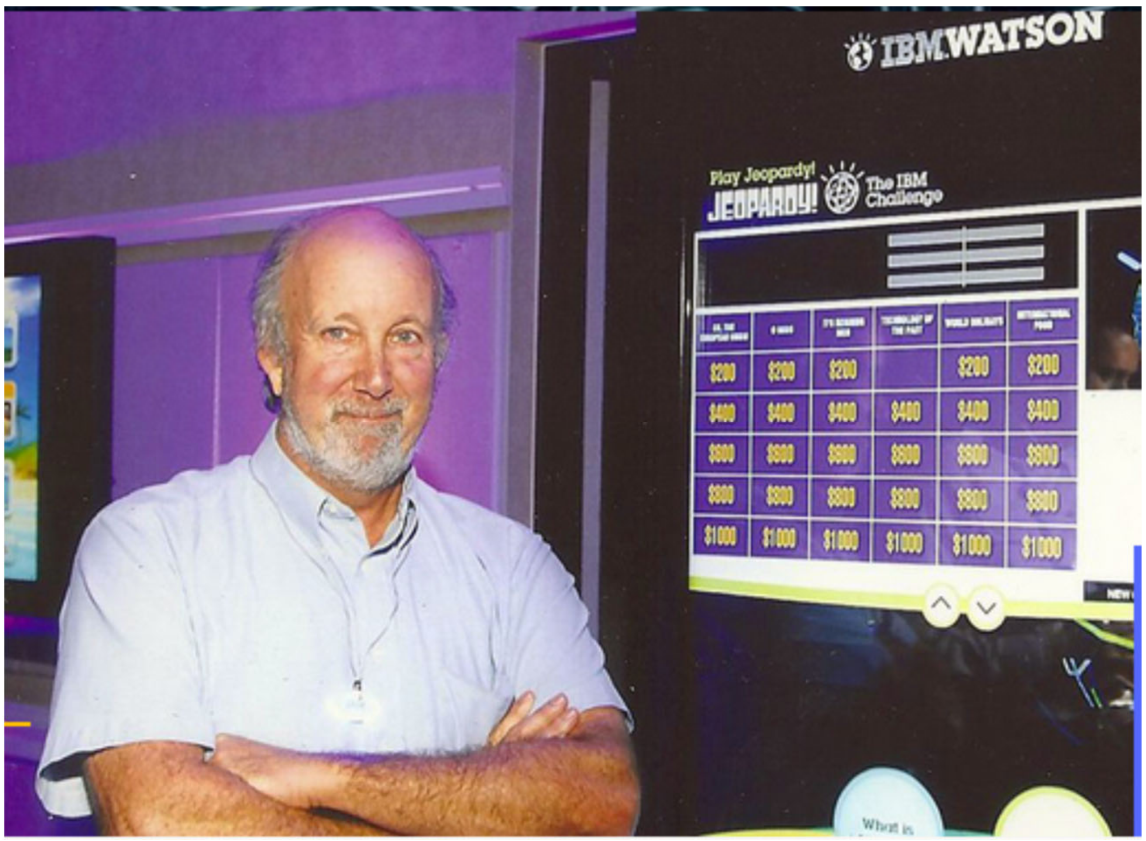
CyberX Presentation on MITRE Attack for ICS –
https://www.sans.org/webcast/recording/citrix/114775/216850

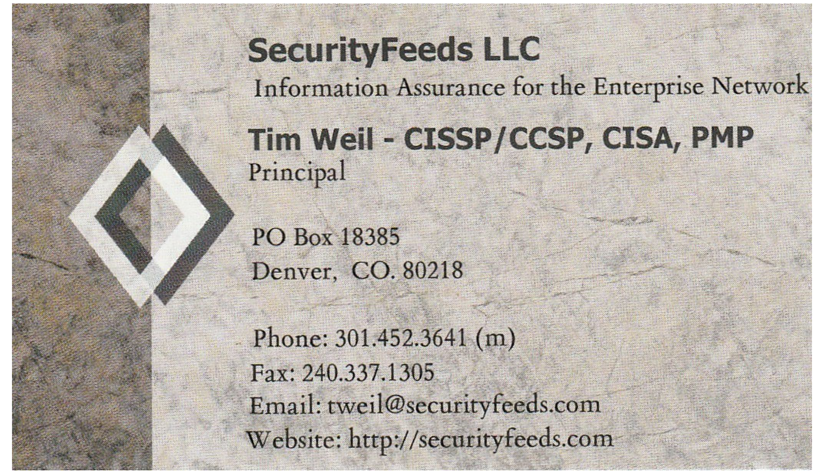
Cybersecurity for the Smart Grid – Research and Reality

Frequency Regulation with Renewables • Power Grid Reliability Concerning Wind • Why Wind Farms Need to Step Up Cybersecurity • Cybersecurity for Renewable Energy	**https://tinyurl.com/ycs2vbcx** https://www.dnvgl.com/article/why-windfarms-need-to-step-up-cyber-security-128082 https://www.osti.gov/servlets/purl/1116652
Kinetic Energy Recovery Systems (KERS) • How a layered approach keeps this F1 team's data secure • Cybersecurity and Formula One	https://www.zdnet.com/article/cybersecurity-how-a-layered-approach-keeps-this-f1-teams-data-secure/ https://www.crowdstrike.com/mercedes-f1/
Machine Learning Model to Predict the nodal prices **Fault Detection Through ML and PLC** • AI and Cybersecurity (Bruce Schneier) • Attacking Machine Learning Systems	https://www.schneier.com/blog/archives/2020/05/ai_and_cybersec.html https://ieeexplore.ieee.org/document/9089095
Using Microgrids to Improve Electrical Reliability • Assessment of Operational Energy System Cybersecurity Vulnerabilities	https://www.mitre.org/sites/default/files/publications/pr_18-1118-assessment-operational-energy-system-cybersecurity-vulnerabilities.pdf
Fast Charging Electric Vehicles • Electric Vehicles Grid Integration & Cybersecurity R&D • EV Charging Threats, Cybersecurity	https://www.naesco.org/data/energymeetings/presentations/Mohanpukar.pdf https://blog.guardknox.com/ev-charging-threats-cybersecurity-ev-charging-ecosystem

Table of Contents

Thank you for joining us!





SecurityFeeds LLC provides IT Management Consulting services

- Communications and Security Engineering
- Data Processing (Systems Engineering)
- Project and Program Management
- Risk Management (ISO 27001)

Our expertise includes Enterprise Security Architecture, Cloud Security, Program Management, and Network Engineering.

"RISK is a four-letter word"

http://www.securityfeeds.com
trweil@ieee.org

SecurityFeeds
Your source for enterprise security management

INTRODUCTION ABOUT SERVICES RESOURCES TOOLS SECURITY INDUSTRY NEWS BLOG TOOLS CONTACT

Your Source For Enterprise Security Management

Security Architecture | Cloud Security | Program Management | Systems Engineering | ISO 27001 | Risk Management and Compliance | Secure Automotive Network (V-PKI Hits the Highway) | Secure Automotive Networking for ITS

Welcome To SecurityFeeds

Tim Weil is an IT Security Program Manager with over twenty five years' experience in data processing, communications engineering, and information assurance (IA).

His areas of expertise include FedRAMP/FISMA compliance for federal agencies and cloud service providers, IT Service Management, cloud security (FedRAMP), enterprise risk management (NIST) for federal agencies and ISO 27001 compliance for commercial clients.

IEEE Milestone – Virginia Smith HVDC Converter Substation

The station's innovative control technologies act like giant shock absorbers between the eastern and western alternating current grids, allowing a reliable flow of energy between the two. Previous attempts to connect the grids without converter stations failed because frequencies on each side do not exactly match. The Virginia Smith station is capable of transferring energy in either an east-west or west-east direction by converting and inverting the AC grids to a common, controllable, high voltage direct current. Creating a reliable interconnection, the conversion process also makes it possible to maintain separation so that in times of disturbances, impacts in one grid do not adversely affec the other.

IEEE Milestone – Virginia Smith HVDC Converter Substation

The 200 MW back-to-back HVDC Virginia Smith Converter Station (SCS) was commissioned in 1987 to provide energy interchanges between the eastern and western North American alternating current (AC) power grids. The SCS facility is capable of transferring 200 MW of power in either an east-to-west or west-to-east direction.

The east and west AC networks that connect to the SCS are comprised of large but dispersed generation and transmission systems that are operated asynchronously. These power and energy systems extend from the Pacific Ocean on the west to Atlantic Ocean on the east. Before back-to-back HVDC facilities were built, it was almost impossible to transfer power and energy between the eastern and western North American power grids (see Figure 1- 1986 Map of HVDC Interconnections).

References Used in This Presentation

- Scoping the Cyber Security Body of Knowledge" Awais Rashid et al, IEEE Security and PrivacyMagazine, Volume 16, Issue 3, May, June 2018
- E-ISAC, SANS ICS. "Analysis of the Cyber Attack on the Ukrainian Power Grid" March 18 2016. p4. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
- Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks- https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
- THREAT INTELLIGENCE REPORT CYBERATTACKS AGAINST UKRAINIAN ICS https://www.sentryo.net/wp-content/uploads/2017/09/EBOOK_CYBERATTACKS-AGAINST-UKRAINIAN-ICS.pdf
- Kapersky Black Energy Spearphishing Attack Agains Ukraine ICS https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents
- A Nation Under Attack: Advanced Cyber-Attacks in Ukraine (YoutTube – 2018) https://www.youtube.com/watch?v=HgDbpTiTFdw

IoT Security References Used in the CSA Guidelines

- Data Processing Stream; Fujitsu Laboratories Ltd., Kawasaki, Japan, March 7, 2018. http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0307-02.html
- Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), Draft NISTIR 8200; National Institute of Standards and Technology; February 2018. https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200- draft.pdf
- "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures," European Union Agency for Network and Information Security (ENISA); November 20, 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
- "Internet of Things--Reference Architecture," ISO/IEC JTC 1/SC 41; August 2018. https://www.iso.org/standard/65695.html

IEEE Communications Surveys and Tutorials (Smart City)

- M. Sookhak, H. Tang, Y. He and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1718-1743, Second Quarter 2019.
- S. Tan, D. De, W. Song, J. Yang and S. K. Das, "Survey of Security Advances in Smart Grid: A Data Driven Approach," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 397-422, First Quarter 2017 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7588049&isnumber=7862305
- A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourth Quarter 2015 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7123563&isnumber=7331734
- M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617-1655, Third Quarter 2016. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7414384&isnumber=7548084
- M. Mukherjee, L. Shu and D. Wang, "Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1826-1857, Third Quarter 2018. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8314121&isnumber=8443345
- P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," in IEEE Communications Surveys & Tutorials, 2019. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8642293&isnumber=5451756