THREAT DETECTION IN THE SMART GRID

The Attacker's and Defender's Perspective

- Why is Detection so important
- The attacker's perspective
- The defender's perspective
- What Detection looks like

Jon Wells
Chairman, Technical Committee | OSGP Alliance
Jon.wells@osgp.org

OSGP ALLIANCE

About the Alliance

- The OSGP Alliance is the global non-profit association dedicated to promoting the adoption of the Open Smart Grid Protocol (OSGP) and infrastructure for smart grid applications towards a future proof modern smart grid
- Our members come from the key stakeholders in the industry, including utilities, hardware manufacturers, service providers and system integrators. All sharing a common goal and vision: promoting open standards for energy demand side management, smart grid and smart metering systems
- A global revolution on interoperability standards is needed to guarantee innovation in terms of adopting new technologies and open standards as they come available. That's where the OSGP Protocol stands out!

History of Successful Projects

Poland
400K devices

Sweden
700K devices

Sweden
400K devices

Austria
175K devices

Netherlands
65K devices

Denmark
200K devices

United States
630K devices

Finland
670K devices

Denmark
390K devices

Sweden
38K devices

Denmark
170K devices

Russia
410K devices

South Africa
35K devices

OSGP Ecosystem

Integrators

Developers

Utilities

THREAT DETECTION IN THE SMART GRID

The Attacker's and Defender's Perspective

- **Why is Detection so important**
- The attacker's perspective
- The defender's perspective
- What Detection looks like

Jon Wells
Chairman, Technical Committee | OSGP Alliance
Jon.wells@osgp.org

OSGP ALLIANCE

SECURITY THREATS CONTINUE TO INCREASE

Current Situation

- 80.7% of companies have experienced a successful cybersecurity attack.
- 36% have experience 6 or more attacks
- 62% of organizations were victimized by ransomware.

2014 and Earlier — Red October & More

There were numerous cyberattacks over the years on various companies and governments around the world.

2015 — Industroyer

This is a malware framework used in the cyberattack on Ukraine's power grid.

- Power in Kiev was out for one hour.

2015 — Black Energy

The attack targeted ICS, energy, government and media in the Ukraine and impacted other ICS/SCADA organizations worldwide.

- Power lost for tens of thousands of people.

2016 — Operation Ghoul

This new form of advanced targeted attack hit companies in many industries within the UAE and countries in Asia, Europe and the Middle East.

- 30 Countries impacted.

2017 — WannaCry

The attack was estimated to have affected more than 200,000 computers across 150 countries.

- $4B estimated losses.

2017 — Petya

Ravaged a wide range of companies. Its prime focus was to encrypt files and wipe the boot record.

- $10B estimated losses.

2018 — Shamoon3

Targeted utility, telecom and government organizations.

- 30K+ Workstations destroyed.

2019 — LockerGoga

LockerGoga and other ransomware attacks hit a variety of companies and organizations.

- $7.5B US costs in 2019.

2020 — Netwalker

A ransomware attack on Pakistan's largest power supplier, disrupting online billing services
a $3.8 million ransom demand
If not paid within 7 days, increase to $7.7 million.

2021 — US Pipeline Disruption

A ransomware attack on US pipeline company, shutting down systems, halting all pipeline operations, offline for 48H, IT system down for more that 4 days

- Supply of 45% fuel consumed on the US East Coast – cut off (50million people)

Sources:

1 – ISC2's Cyberthreat Defense Report 2020
2 – Indegy's Cyber Attacks on Critical Infrastructure – A Historical Timeline

AND NOW BEING NOTICED

Source:
https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

Utility Vulnerabilities:

- Increased awareness cyber-criminals have of the disruption that they can cause and the revenue they can generate
- Operational and geographical distribution of the utility and its impacts on its ability to protect and react in a coherent manner
- Complexity of the energy supply-chain and convergence of the physical and cyber components leading to opportunities to do major damage by attacking relatively few points

Actions to Reduce Vulnerabilities:

- ✓ Strategic intelligence on threats and actors before attacks on the network
- ✓ Programs to reduce geographic and operational gaps in awareness and communication, creating a culture of security
- ✓ Industry-wide collaboration to address the increasing convergence of physical and virtual threats

BUT, THE LOW-VOLTAGE GRID SPECIFICS ARE STILL TO BE ADDRESSED!

AND NOW BEING NOTICED…… MORE……

POWERGRID INTERNATIONAL

Generation ▾ T&D ▾ DER/Grid Edge ▾ Executive Insight Customer Service Smart Grid ▾

Safeguarding smart meters as cyberthreats surge

Eran Fine, CEO & Co-Founder, NanoLock Security 12.1.2020

https://www.power-grid.com/executive-insight/safeguarding-smart-meters-as-cyberthreats-surge/#gref

energycentral EC Webcasts Power Perspectives™ Special Issues PowerSessions™ Sponsors

Home Community ▾ Groups ▾ Topics Jobs News Calendar Resources ▾ Subscribe

AUTHOR PROFILE

Karen Marcus
Freelance Business Writer
Final Draft Communications, LLC

Follow

Contact

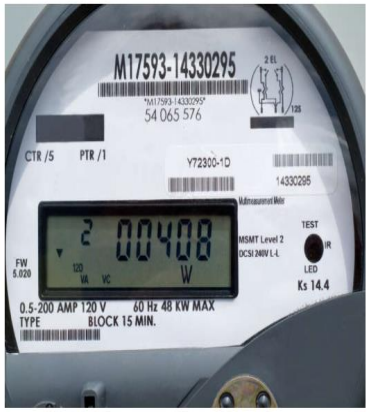
ABOUT ME

In addition to serving as an Energy Central Community Manager, Karen Marcus has over 20 years of experience as a content developer within complex industries including energy, technology...

Member since 2017
291 items added with 224,780 views

POST

Smart Meter Challenges: Customer Concerns and Cybersecurity



https://energycentral.com/c/iu/smart-meter-challenges-customer-concerns-and-cybersecurity?

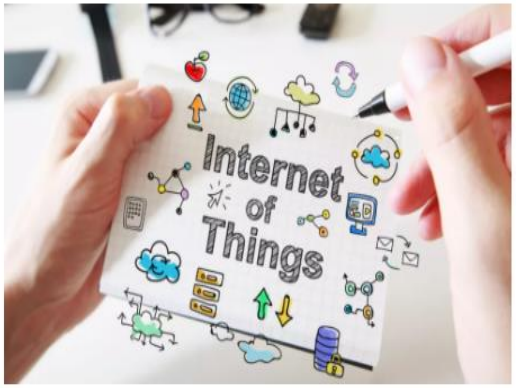
ITProPortal RSS

News Best VPN Reviews Features Resources Security Ebook Categories ▾

Internet of Things presents the next frontier of cyberattacks

By Asaf Ashkenazi January 17, 2020

As the development of IoT devices accelerates, the risk of a cyberattack accelerates as well.



https://www.itproportal.com/features/internet-of-things-presents-the-next-frontier-of-cyberattacks/

RAND

ANU NARAYANAN, JONATHAN WILLIAM WELBURN, BENJAMIN M. MILLER, SHENG TAO LI, AARON CLARK-GINSBERG

Deterring Attacks Against the Power Grid

Two Approaches for the U.S. Department of Defense

Deterring Attacks Against the Power Grid: Two Approaches for the U.S. Department of Defense (hubspotusercontent30.net)

ARE YOU WAITING OR ARE YOU ACTING?

..... MORE.....

Colonial Pipeline cyberattack

From Wikipedia, the free encyclopedia
(Redirected from Colonial Pipeline Cyberattack)

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline.[4][5][6] In response, Colonial Pipeline Company halted all of the pipeline's operations to contain the attack.[7][8][9][10] Colonial Pipeline paid the requested ransom (75 bitcoin or nearly $5 million) within several hours after the attack.[11] The hackers then sent Colonial Pipeline a software application to restore their network, but it operated very slowly.[11]

Federal Motor Carrier Safety Administration issued a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open on May 9.[12] It was the largest cyberattack on an oil infrastructure target in the history of the United States.[2] The FBI and various media sources identified the criminal hacking group DarkSide as the responsible party.[13] The same group is believed to have stolen 100 gigabytes of data from company servers the day before the malware attack.[1]

Colonial Pipeline cyberattack

Date	• May 6, 2021 (data stolen)[1] • May 7, 2021 (malware attack) • May 12, 2021 (pipeline restarted)
Location	United States
Type	Cyberattack, data breach, ransomware
Target	Colonial Pipeline
Suspects	DarkSide[2][3]

ARE YOU WAITING OR ARE YOU ACTING?

WHY IS LOW-VOLTAGE SMART GRID SECURITY SO ESSENTIAL?

The bad guys are highly motivated to attack you, and highly ingenious

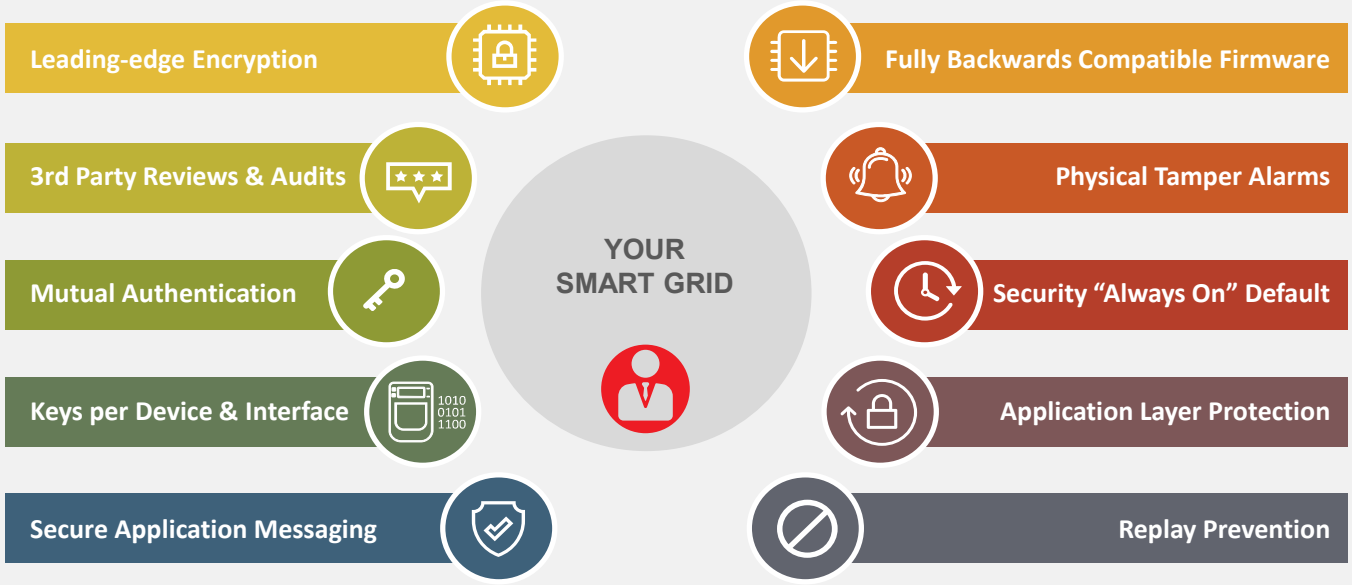
	Electricity	Data	Hardware
Your Need	Remote On / Off switch	Automation & Analytics	Remotely Upgradable
Your Risk	Power Outages	Disruption, System Compromises	Hijack or Brick Devices/Meters/DCs

Their thought process:

1. Wow, we don't need to hack SCADA to bring the grid down?
2. Wow, smart meters are not just for billing; we can steal, manipulate, disrupt
3. It is centrally managed distributed network of millions of devices, ready to be hijacked!

You have to plan as if they will succeed, eventually, one day

IS PROTECTION ENOUGH?



Have you just built one of these?

PROTECT, DETECT, RESPOND

Is it clear what is being protected?

Do we have enough protection?

What was missing here?

Who is the most important person?

Protection Goal-keeper + Defenders

Detection Seeing the threat posed by the striker and anticipating how it might develop into an attack

Response Orchestrating the defenders to block and the goalie diving the right way

THREAT DETECTION IN THE SMART GRID

The Attacker's and Defender's Perspective

- Why is Detection so important
- **The attacker's perspective**
- The defender's perspective
- What Detection looks like

Jon Wells
Chairman, Technical Committee | OSGP Alliance
Jon.wells@osgp.org

OSGP ALLIANCE

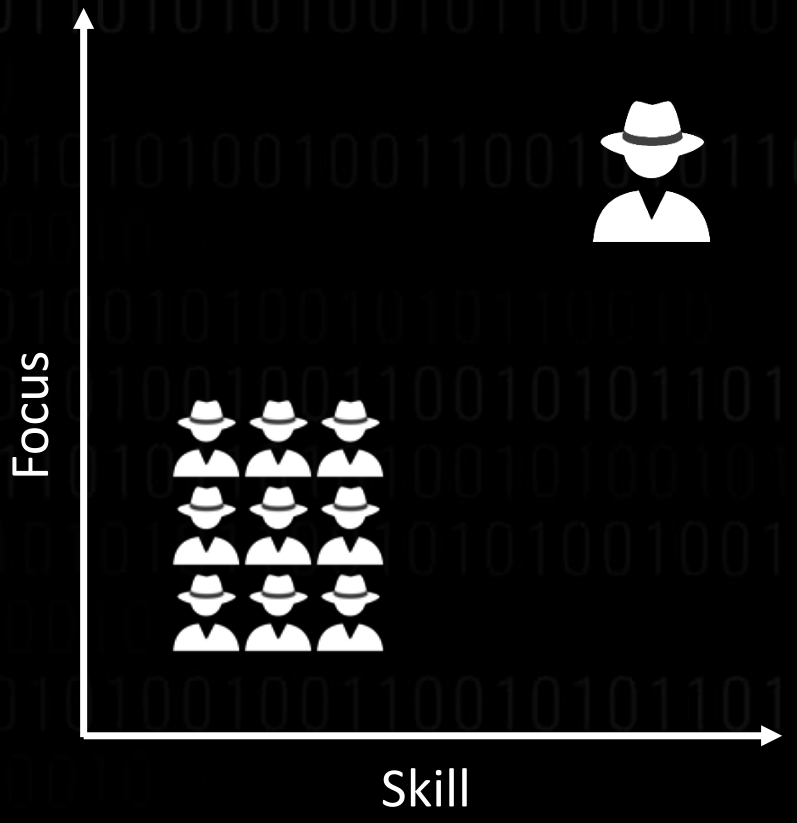
WHO

Nation-State

- Critical Impact
- High Skill
- Targeted

Criminal

- Critical Impact
- Low Skill (uses hacking-as-a-service instead)
- Ransom campaigns remain a profitable business!



There are other types of threat actors, these are just some relevant examples.

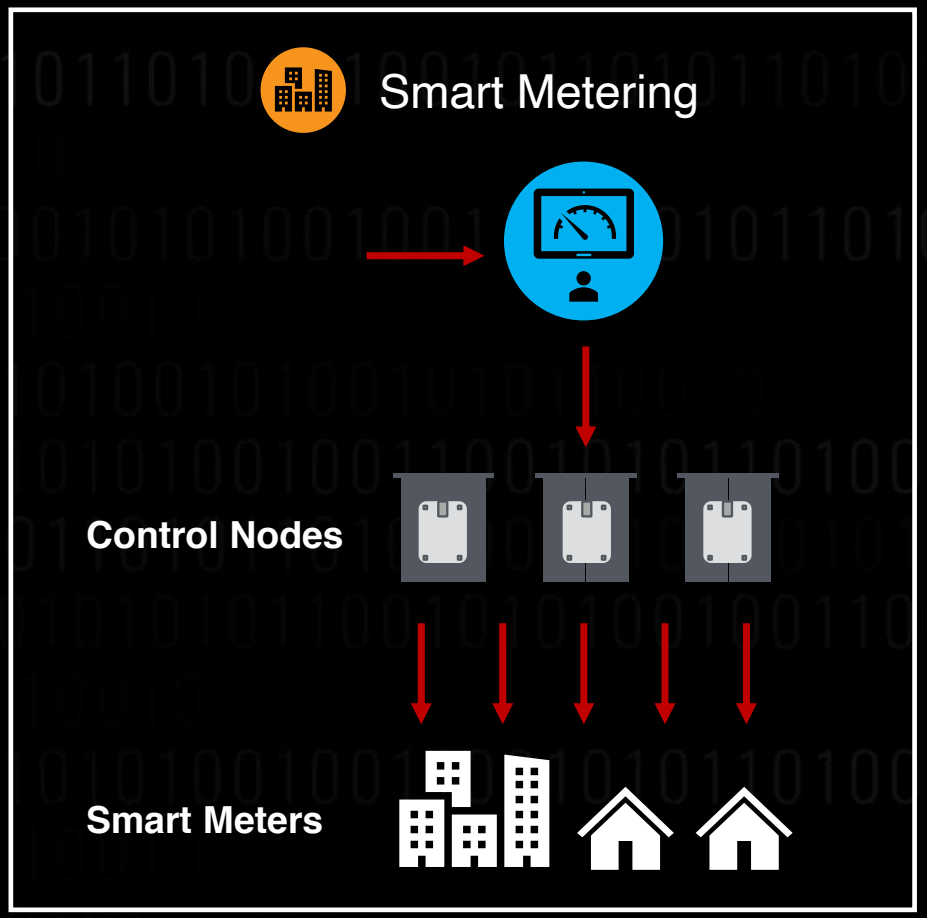
OPERATION 1: POWER OUTAGE

MISSION: TO INFLICT POWER OUTAGES

1. Hack our way into the Smart Metering control center
2. Wait until high load, then send disconnect commands to meters

⚠ HIT LIMIT OF DISCONNECT COMMANDS

3. Change power thresholds instead to complete mission



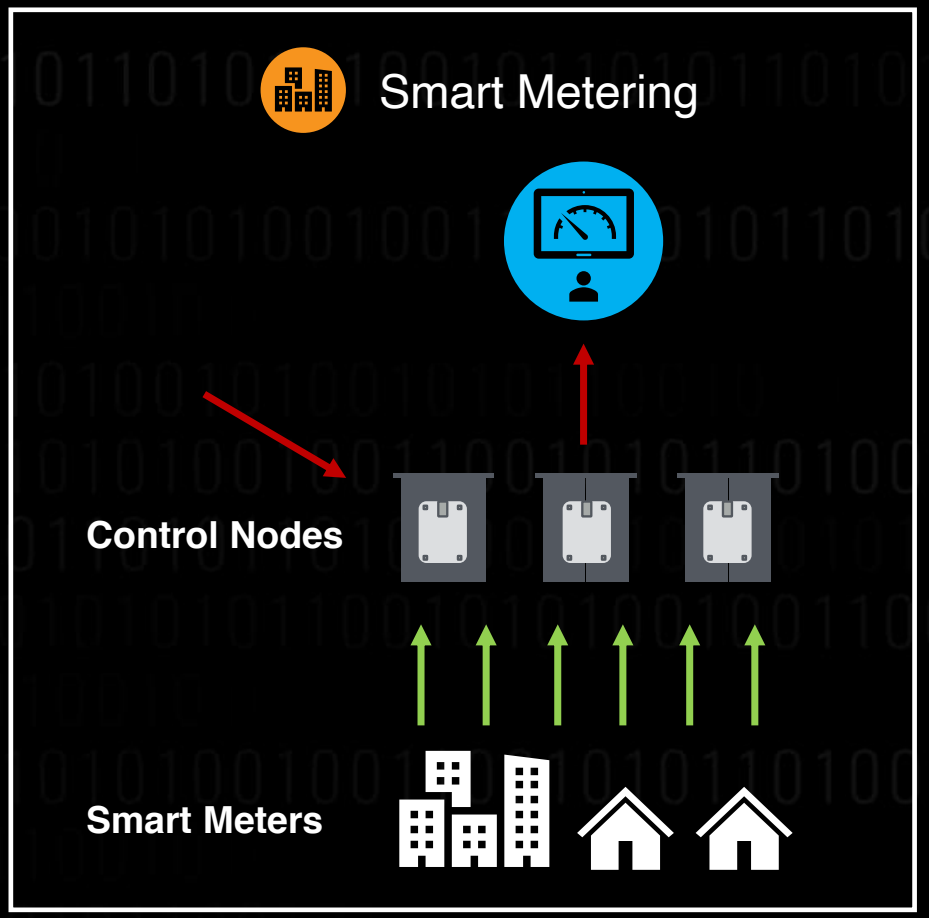
OPERATION 2: DERAIL ALGORITHMS

MISSION: TO SLOWLY DERAIL GRID AUTOMATION & CONTROL BY TAMPERING WITH GRID SENSOR DATA SOURCES

1. Hack into a select number of Control Nodes

2. Make controlled changes to the sensor data bubbling up from the smart meters

3. Watch as algorithms use our tampered data sources to derail automation & control processes, thus completing the mission



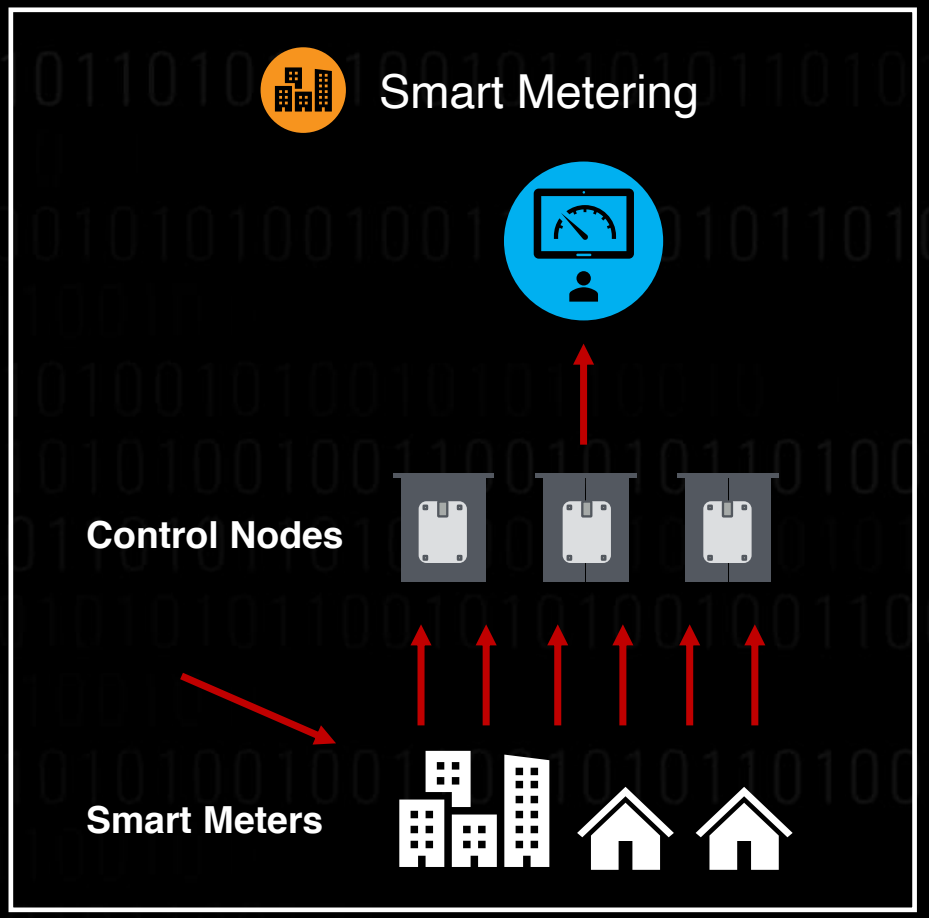
OPERATION 3: RANSOM ATTACK

MISSION: TAKE CONTROL OF THE SMART METERING INFRASTRUCTURE FOR FINANCIAL GAINS

1. Hack into thousands of smart meters via their remote interface using outsourced malware

2. Use the software update mechanism to reprogram their firmware **and/or** change their remote access keys

3. Sell back the infrastructure to the utility, threaten to leak customer data, brick devices, and shut power off to get their attention



THREAT DETECTION IN THE SMART GRID

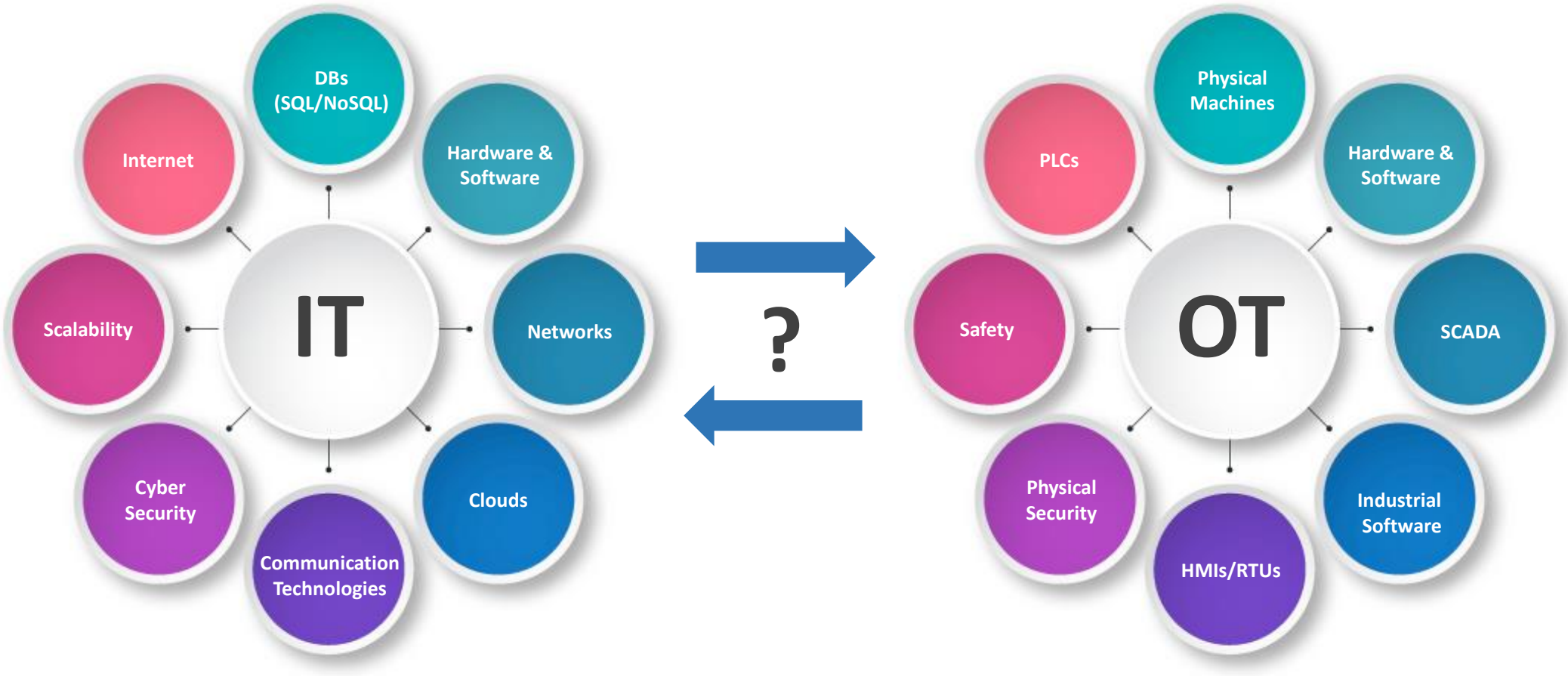
The Attacker's and Defender's Perspective

- Why is Detection so important
- The attacker's perspective
- **The defender's perspective**
- What Detection looks like

Jon Wells
Chairman, Technical Committee | OSGP Alliance
Jon.wells@osgp.org

OSGP ALLIANCE

OT & IT CONVERGENCE



ATTACKERS VS DEFENDER

VS

ATTACKER

- Highly motivated
- Educated
- Has enough time

DEFENDER

- Bored
- Knows nothing about OT
- Limited in time

DEFENDER TASKS – PART 1

- Analyzing possibly attacking surface
  - Distorting of billing data
  - Disconnecting consumers
- Risk assessment and prioritizing

Safety

- ISO 27001 doesn't take it into account
- A new challenge for the IT – an old for the OT

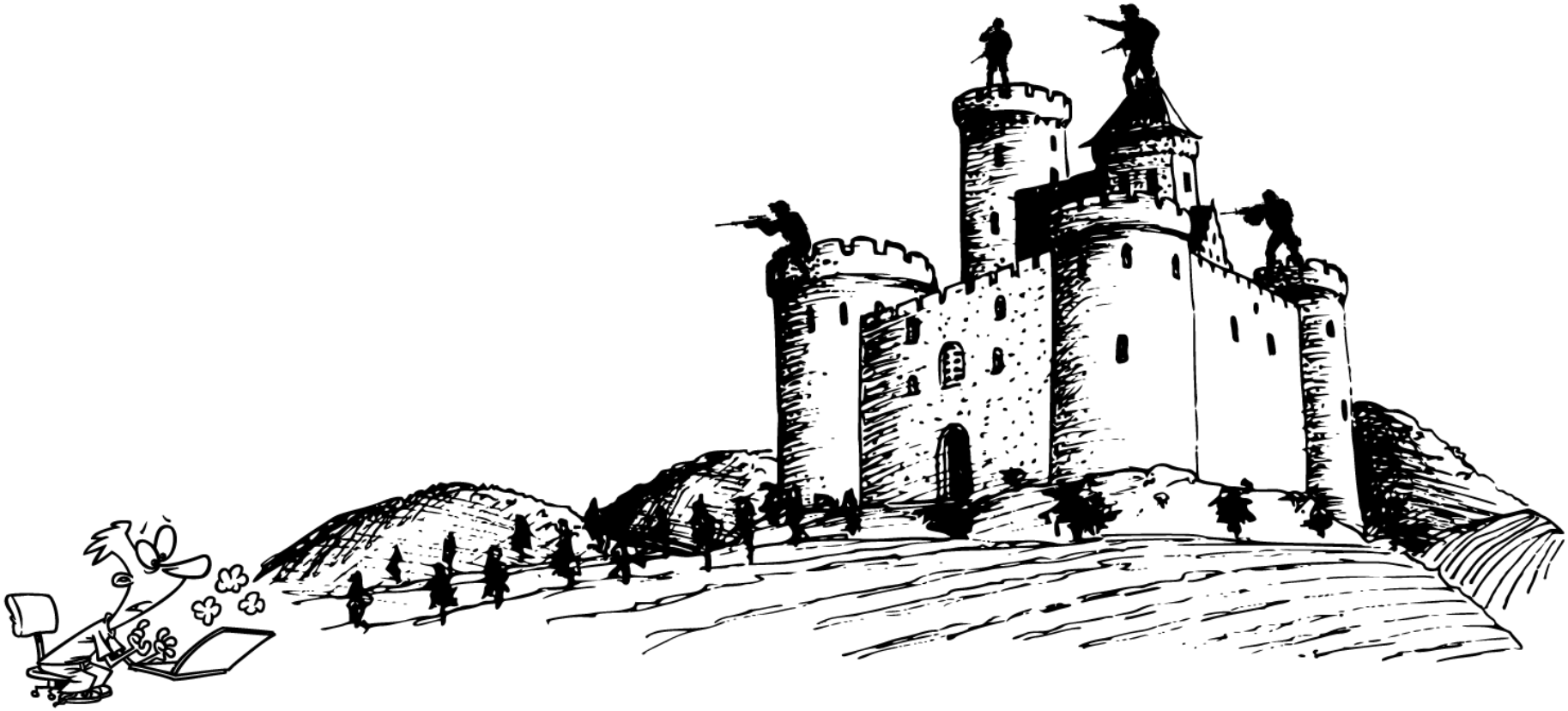
You must study the defender and give him the proper tools!

DEFENDER TASKS – PART 2

IT	
Network	IPS/IDS, firewalls, SDN
Applications	Antivirus, firewalls, behavioral analysis
Data flows	Firewalls
Infrastructure level	SIEM, SOAR
Audit	Annual by experienced auditors

OT	
Low-voltage networks (as a part of Smart Grid)	Limited options
SCADA	Limited firewalls
Data flows	Limited firewalls
Infrastructure level	No instruments
Audit	???

BE READY!



“Bad News.. It’s a cyber attack.”

THREAT DETECTION IN THE SMART GRID

The Attacker's and Defender's Perspective

- Why is Detection so important
- The attacker's perspective
- The defender's perspective
- **What Detection looks like**

Jon Wells
Chairman, Technical Committee | OSGP Alliance
Jon.wells@osgp.org

OSGP ALLIANCE

Designed by Emil Gurevitch (@networkedenergy.com) Grid Watch

Grid Watch | Overview | Incidents 2 | Alerts | Events | Settings | Sign Out

Customer Name

Incidents

Active Incidents 2

ACTIVE

- Submarine — Updated 3 minutes ago
- Echo — Updated 14 days ago

RESOLVED

- Whiskey — Resolved 24 days ago
- Foxtrot — Resolved 3 months ago
- Quebec — Resolved 6 months ago
- Bravo — Resolved 1 year ago
- Kilo — Resolved 2 years ago

Echo

Rename | Mark as Resolved | Remove | Print

Jun 29, 2019 — Jul 1, 2019

SUMMARY

Incident Type	DC Compromise, DC Integrity
Meters Impacted	0 (Meter IDs)
DC Domains	28
DCs Impacted	28 (DC IDs)
How	NES Head-End System API
Indicators of Compromise	Unexpected Fimrware Update
Time Period	Jun 17, 2019 — Now (14 days)

RECOMMENDED NEXT STEPS

Check with Operations: The logs show that the DC firmware update was pushed out on June 17, 2019 using the NES API (Web Service). Confirm with operations that this is unplanned and truly an incident. If this is a planned event, you can ignore this incident and click "Mark as Resolved"; otherwise, proceed to the next steps.

Limit & Restore: Logs show that 7 of the 28 DCs have not completed the firmware update (see Timeline below). Remove the pending firmware updates from the affected DCs. Restrict network access to the NES HES and start restoring the original firmware on the 28 affecetd DCs as they could be running malicious code. See Section 7.2 in the NES User Manual for guidance. Call NES or your local partner for further support.

Investigate: This incident could be an opertional mistake or it could be an insider attack. Regardless, the firmware update was pushed out on June 17, 2019. Find out who accessed the NES API by looking at server logs. It is recommneded that you restrict access to the NES API to prevent further misuses.

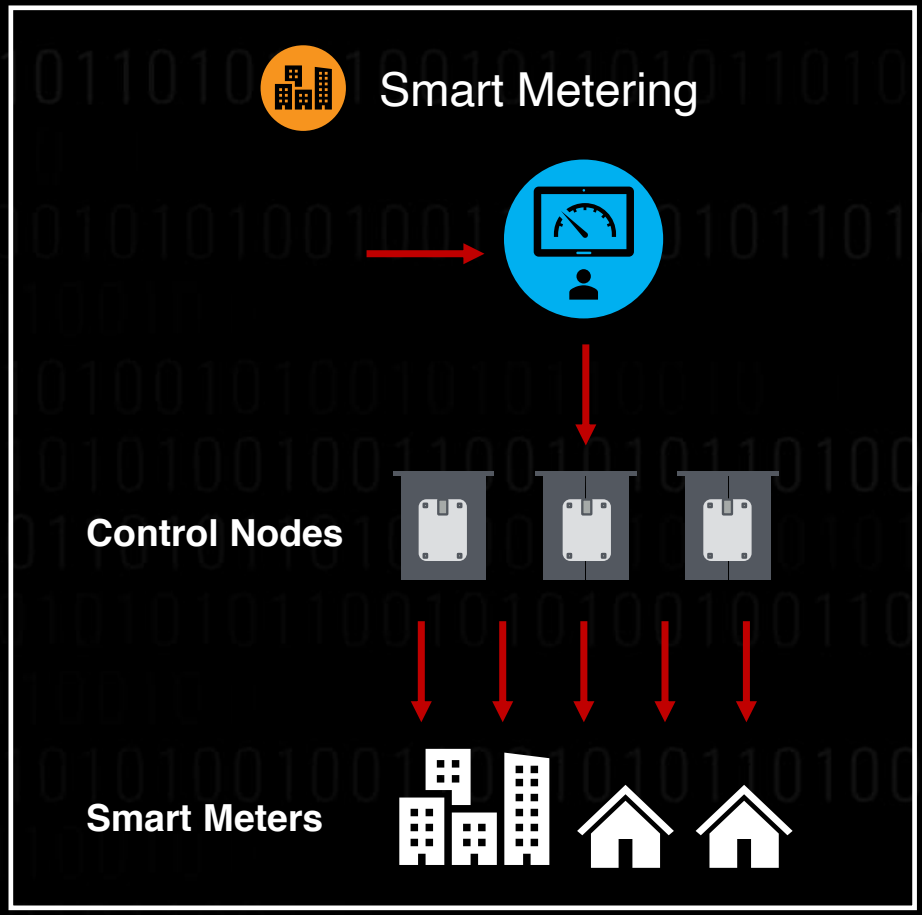
ATTACK MAP

API → HES → WAN → DCs → Meters

TIMELINE Jun 17, 2019 — Now

- **Unexpected DC firmware update pushed to 28 DCs on a Sunday** (DC IDs)
  Jun 17 2019, 10:33 PST
- **13 of 28 DCs has reproted firmware update complete** (DC IDs: complete) (DC IDs: pending)
  Jun 18, 2019, 17:03 PST
- **21 of 28 DCs has reproted firmware update complete** (DC IDs: complete) (DC IDs: pending)
  Jun 27, 2019, 17:03 PST
- NOW — **Current Status: Echo has been unresolved for 14 days and is rated critical.** (Meter IDs)
  Jul 1, 2019, 18:05 PST

Documentation Support Grid Watch v1.0.0



Designed by Emil Gurevitch (@networkedenergy.com) Grid Watch

Grid Watch | Overview | Incidents 2 | Alerts | Events | Settings | Sign Out

Customer Name

Incidents

Active Incidents 2

ACTIVE

- Submarine — Updated 3 minutes ago
- Echo — Updated 14 days ago

RESOLVED

- Whiskey — Resolved 24 days ago
- Foxtrot — Resolved 3 months ago
- Quebec — Resolved 6 months ago
- Bravo — Resolved 1 year ago
- Kilo — Resolved 2 years ago

Bravo

Rename | Mark as Unresolved | Remove | Print

Jul 3, 2018 — Jul 21, 2018

SUMMARY

Incident Type	**Meter Configuration Tampering, Unauthorized Device Access**
Meters Impacted	**321** Meter IDs
DC Domains	**1** DC IDs
DCs Impacted	**0**
Attack Vectors	**Local & Remote Meter Access**
Indicators of Compromise	**Failed Login Attempts, Mass Config Change on Suspecious PLC network**
Time Period	**Jul 3, 2018 — Jul 21, 2018 (18 days)**

RECOMMENDED NEXT STEPS

Check with Operations: Check with operations that the configuration change on the 321 affected meters was unplanned. If it was planned, you can ignore this incident and click on "Mark as Resolved"; otherwise, proceed with next steps.

Key Change & Security Patches: Remotely change both the optical and remote PLC keys on the affected meters. This will render the old and potentially compromised keys useless. The affected meters are running a firmware version that is known to have a remote vulnerability. This vunerabiity could be used in this attack. Therefore, it is strongly recommended to apply the latest NES meter firmware update to all the meters on the domain (first) and then the rest of the deployed meters.

Investigate: This incident could be indicate that keyfiles are being mishandled or misused. Use the timeline below as a starting point for piecing together a comprehensive timeline of this incident. Find out who may have had access to the keyfiles for the affected meters.

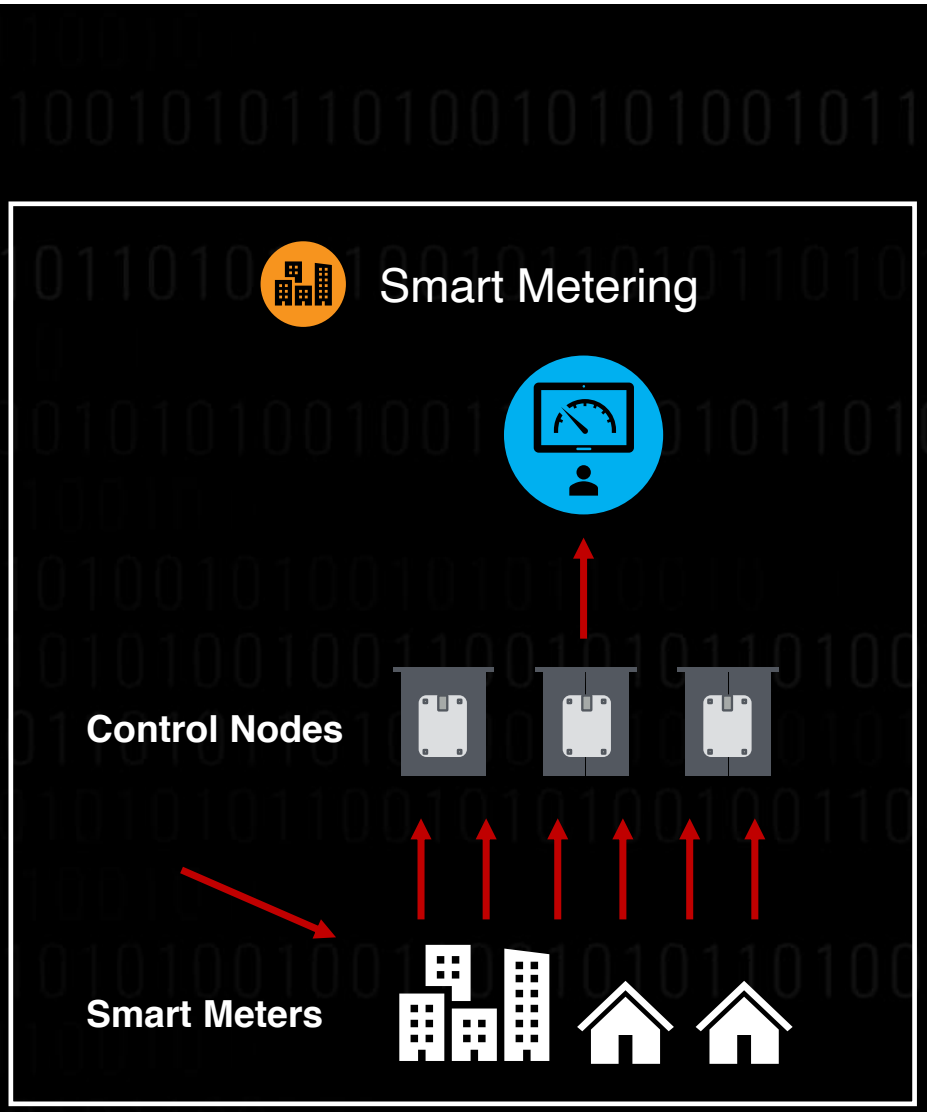
ATTACK MAP

HES
DCs
PLC
Meters
Optical

TIMELINE Jul 3, 2018 — Jul 21, 2018

- **Many failed local login attempts on 1 meter** Meter ID
  Jul 3, 2018, 19:00 PST
- **Local meter access after failed login attempts on 1 meter** Meter IDs
  Jul 5, 2018, 17:03 PST
- **Many failed remote login attempts on 1 meter** Meter IDs
  Jul 12, 2018, 18:01 PST
- **Remote change of configuraiton on 321 meters** Meter IDs
  Jul 21, 2018, 15:19 PST
- **Current Status: Bravo marked as resolved**
  Jul 21, 2018, 19:00 PST

Documentation Support Grid Watch v1.0.0



PROTECT, DETECT, RESPOND

The Key Take-aways

- The Low-voltage Smart Grid presents its own unique challenges to the defender
- Relying on standard IT/OT security practices helps but does not necessarily reflect the specifics of the low-voltage grid
- Defence is important, following regulation is important but……
- …… you have to assume a breach
- And, once you assume a breach, you need to ask yourself…..
- ….. Can you identify it and do you know how you will respond to it

THREAT DETECTION IN THE SMART GRID

The Attacker's and Defender's Perspective

- Why is Detection so important
- The attacker's perspective
- The defender's perspective
- What Detection looks like

Jon Wells
Chairman, Technical Committee | OSGP Alliance
Jon.wells@osgp.org

Any Questions?

OSGP ALLIANCE