OWASP
The Open Web Application Security Project

Smart Grid IoT Security

Kwaku Sarpong Manu

About Me

OWASP
The Open Web Application Security Project

Computer Engineer

Novice InfoSec researcher

Signals Intelligence

Cyanide and Happiness junkie

Twitter: @_kwaku__

Electricity, Water and Gas

What is Smart Grid IoT?

- Internet of things is the extension of Internet connectivity into physical devices and everyday objects
- Section of IoT devices employed in the large scale provision of Utilities as a Service
- It covers Electricity, Water and Gas production, distribution and management

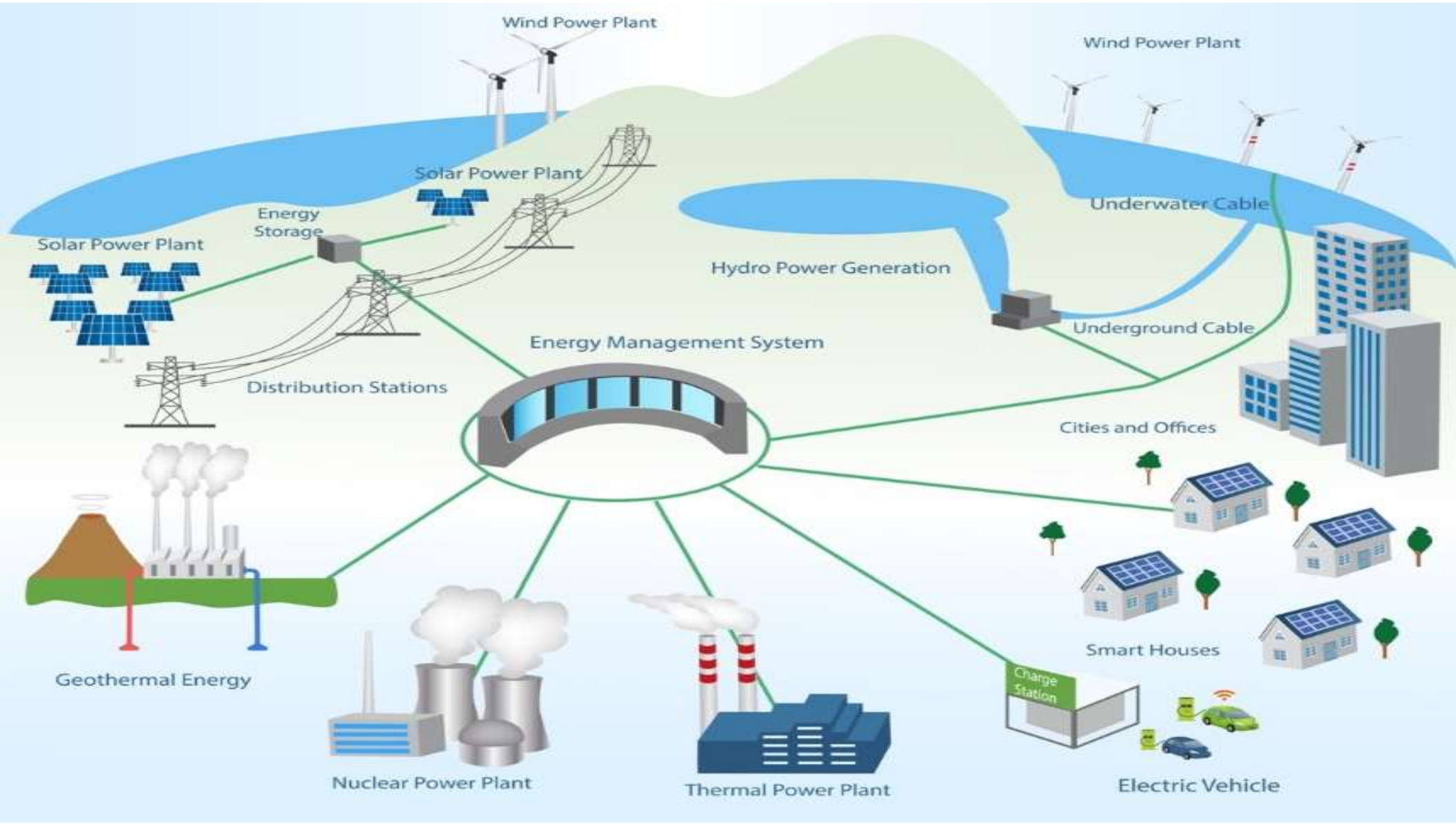
- Locale friendly examples include:

ECG prepaid meters

GWCL smart meters

Gas Meter


HANDLE WITH CARE
IF YOU THINK YOU CAN SMELL GAS
0800 111 999
METER EXCHANGE AND FIX DETAIL


Wind Power Plant
Wind Power Plant
Solar Power Plant
Energy Storage
Solar Power Plant
Underwater Cable
Hydro Power Generation
Underground Cable
Energy Management System
Distribution Stations
Cities and Offices
Smart Houses
Charge Station
Geothermal Energy
Nuclear Power Plant
Thermal Power Plant
Electric Vehicle

Some Promises of Smart Grid IoT

- Provide the capacity and incentive for customers to manage their electricity consumption more efficiently.
- Increase retail price efficiency.
- Enhanced competition in the retail electricity market associated with the timely and efficient rollout of AMI.
- Provide distributors with the capability and incentive to introduce more efficient pricing to retailers

The Urgency of Smart Grid Security

OWASP
The Open Web Application Security Project

- Utilities are essential for our daily activities; attacks can get frustrating or even scary.
- DDoS attack on a utility server could compromise the communication of 89.7 % of the total Smart Meters during the attack[1]
- In October 2016, DDoS disrupted the heating systems for at least two housing blocks in Finland. [2]
- Code for Mirai IoT botnet responsible for World's largest DDoS Attack (against OVH in France) was released online. [3]
- In March 2018, a new Office of Cybersecurity, Energy Security and Emergency Response was created and allocated $96 million as a response to Russian attacks [4]

CLOUD LAYER

Big Data Processing
Business Logic
Data Warehousing

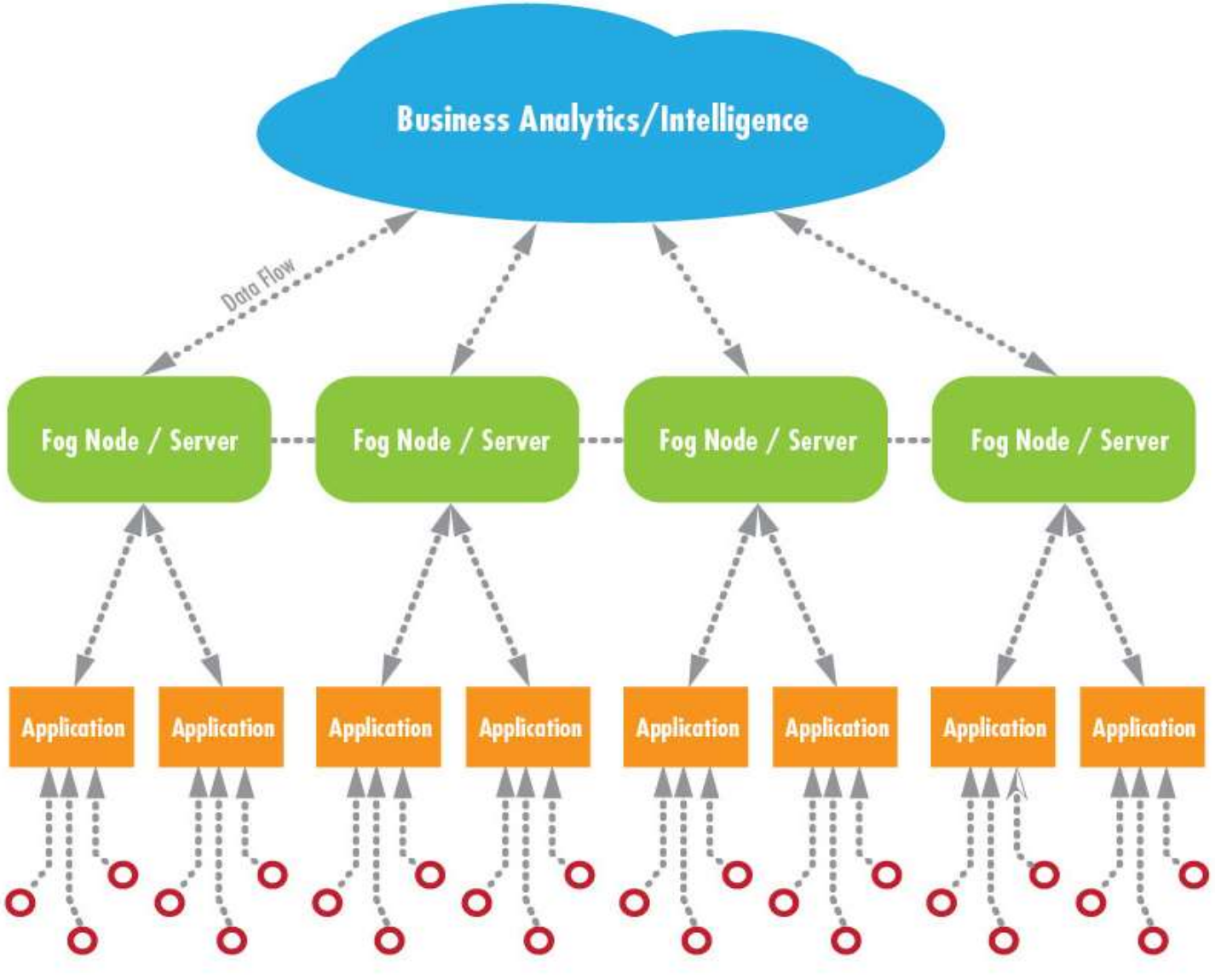
FOG LAYER

Local Network
Data Analysis & Reduction
Control Response
Virtualization/Standardization

EDGE LAYER

Large Volume Real-time Data Processing
At Source/On Premises Data Visualization
Industrial PCs
Embedded Systems
Gateways
Micro Data Storage

Sensors & Controllers (data origination)



OWASP
The Open Web Application Security Project

Attack Surface Under Consideration

Field Deployments (Edge Layer)

- Metering devices & infrastructure
- Communication infrastructure
- Data and signals

Premise Deployments (Fog Layer)

- Servers
- Databases
- Management interfaces

Threats (Field Deployments)

OWASP
The Open Web Application Security Project

Threats

- Device sabotage
- DOS
- MiTM
- Malware
- Data theft and falsification

Implications

- Financial loss
- Operations disruption
- Data fidelity
- Avenues for sophisticated crimes
- Network hijacking
- Reputation damage

Threats (Premise Deployments)

OWASP
The Open Web Application Security Project

Threats

- Malware
- Privilege abuse
- Less-than-secure operations
- Miscellaneous cyber attack

Implications

- Systems hijacking
- Unauthorised data sharing
- Unauthorized data modification
- Reputation damage

Defenses

OWASP
The Open Web Application Security Project

Attack Surface	Mechanism	Scope of effectiveness
Field Deployments	Physical security	Device sabotage
	IoT Security audits	DOS, MiTM, Malware
	Encryption and cryptography	Data theft/falsification, MiTM
Premise Deployments	Fine grain access controls, comprehensive logging/auditing	Privilege abuse, less-than-secure operations
	Software security (updates, firewall, antivirus, etc.)	Miscellaneous cyber attacks, less-than-secure operations, malware
	Cyber security policy and recovery plan	


DKF0564

OWASP
The Open Web Application Security Project

- Attacks on Smart Grid are typically aimed at disrupting Operations and Quality of Service
- No system is or can be 100% secure
- Software and Hardware security are equally important
- Regular audits are crucial for long-term security of assets

OWASP
The Open Web Application Security Project

- Less-than-secure operations risks arise from compromises
- Insider threat is a growing problem
- Few threats can be addressed by internal mechanisms
- Combine acceptance, mitigation, avoidance and transference measures
- Level of security is often influenced by culture

The Future??

OWASP
The Open Web Application Security Project

- Increased computing power and bandwidth
- Hyper secure data and communications
- Increased communication bandwidth
- Higher communication throughput and reliability
- Systems integration on steroids
- Increased skills, funding, motivation and sophistication of both attackers and defenders
- History will repeat itself!

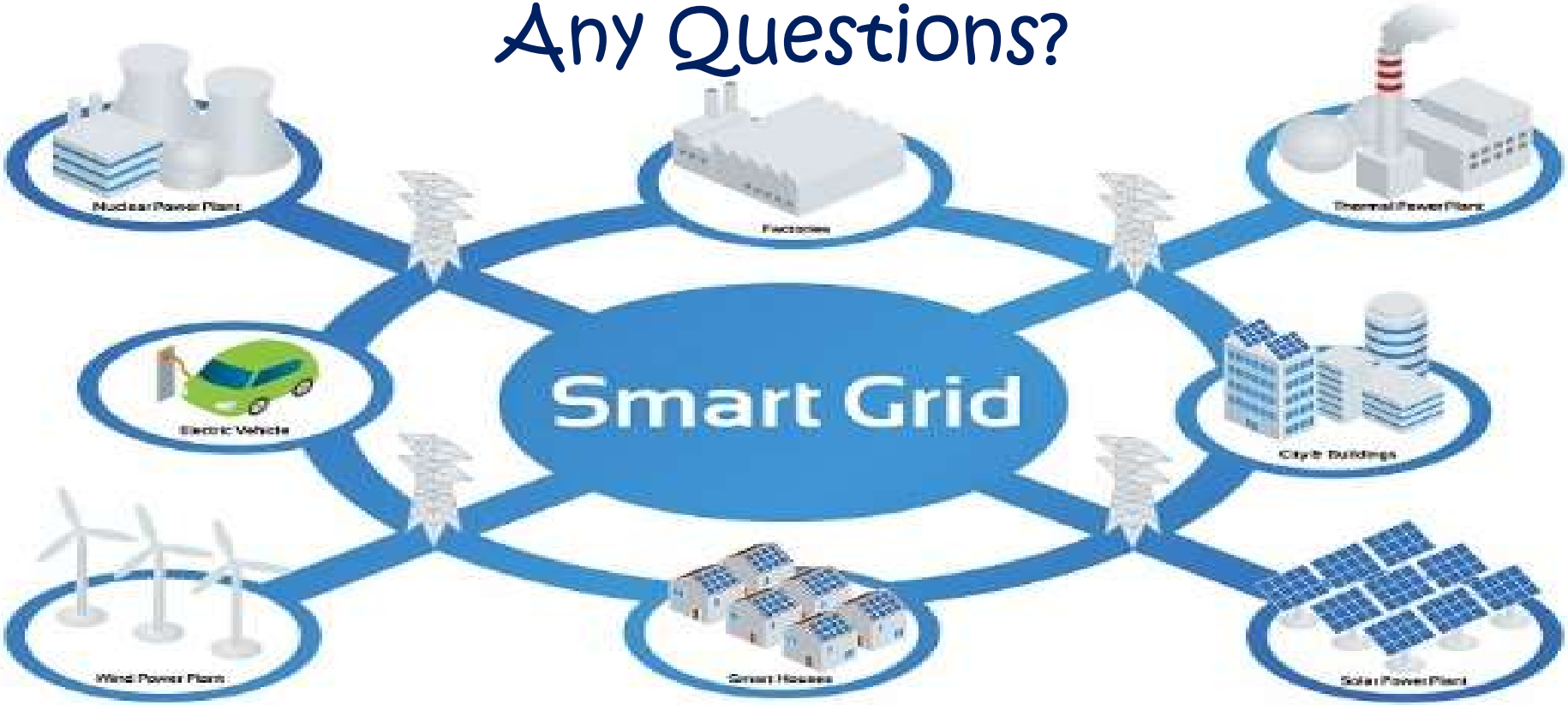
Questions for you

What is the state of security of your IoT deployments?

How are you planning to mitigate current threats?

How are you preparing to avoid future threats?

Any Questions?



References:

OWASP
The Open Web Application Security Project

[1] Cyber Attack Impact on Critical Smart Grid Infrastructures. Available from: https://www.researchgate.net/publication/260301409_Cyber_Attack_Impact_on_Critical_Smart_Grid_Infrastructures [accessed May 08 2019]

[2] Source Code for IoT botnet responsible for World's largest DDoS Attack released Online. From: https://thehackernews.com/2016/10/mirai-source-code-iot-botnet.html [accessed May 08 2019]

[3] DDoS Attack Takes Down Central Heating System Amidst Winter In Finland. From: https://thehackernews.com/2016/11/heating-system-hacked.html [accessed May 08 2019]

[4] Russia attacked the US power grid. What if they don't stop? From: https://www.smart-energy.com/regional-news/north-america/russia-attacked-the-us-power-grid-what-if-they-dont-stop/ [accessed May 08 2019]

[5] Heather Lovell (2018) The promise of smart grids, Local Environment, The International Journal of Justice and Sustainability, DOI: 10.1080/13549839.2017.1422117 [accessed May 08 2019]