Cyber Threat Information Portal for the PSGE

John Piesing

Edward Apeh

Overview

1. Who are the PSGE?
2. Can a CTIP help?
3. Current CTIPs and their issues
4. Proposed Solution

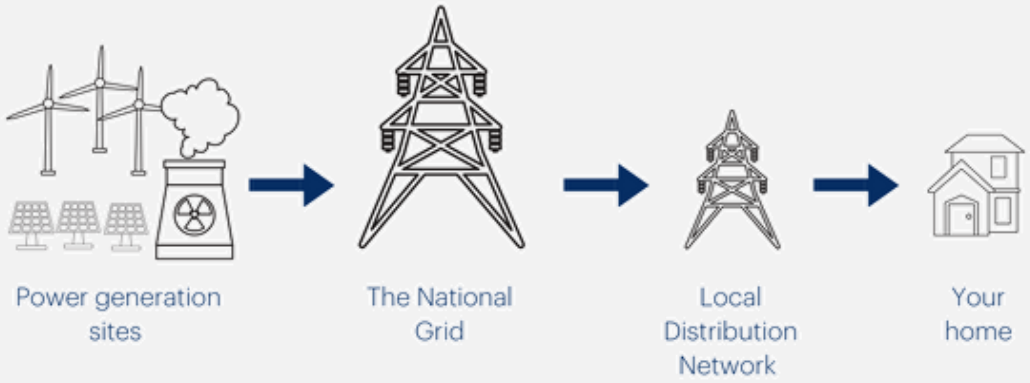
POWER

CTIP for the PSGE

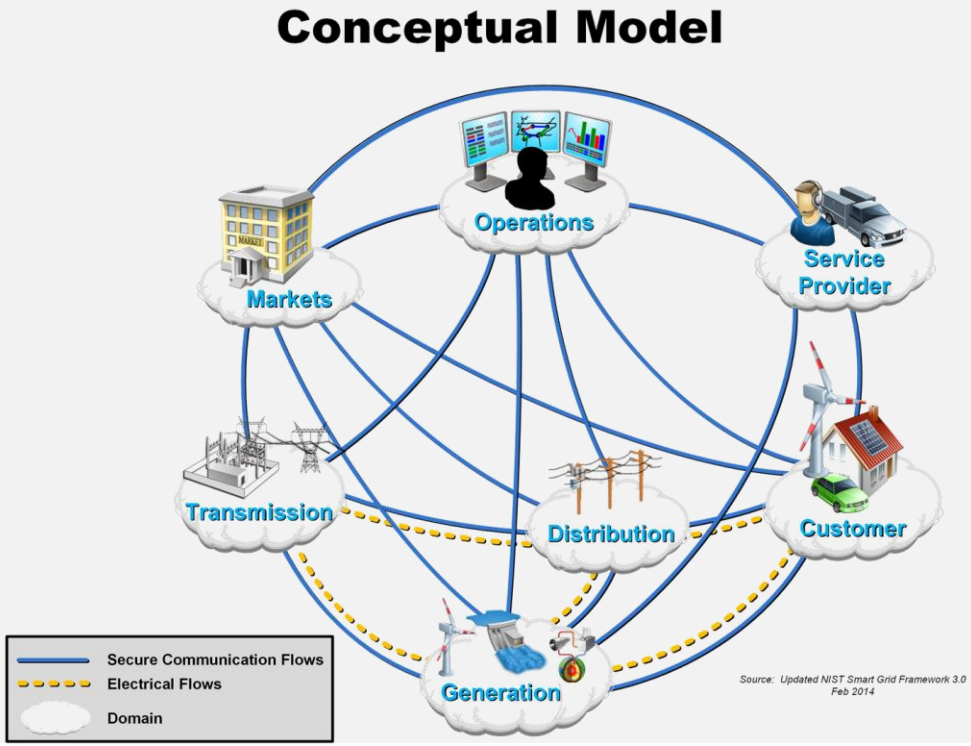
What is the PSGE?

Or *who* are the PSGE?

Traditional Grid



Power Smart Grid Ecosystem



Can CTIPs Help?

23rd December 2015

Secondary Research

"Within the Ukraine, an organization with the ability to enable appropriate information sharing and provide incident response guidance should be pursued."

Recommendation from: SANS & E-ISAC Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case.

Focus Group

Primary Research

8.8/10

Average response when asked: How important do you consider Cyber Threat Information Portals in enabling effective cyber security?

Current Problems

1. Barriers to Access
2. Users forced to “go looking” for information
3. Trust Issues

Recent Cyber News

Article (Click to view)	Publisher
Oracle Says Hackers Targeting Recently Patched Vulnerabilities	Security Week
This Week in Security News: Shade Ransomware Shuts Down, Releases Decryption Keys and WebMonitor RAT Bundled with Zoom Installer	Trend Micro
Principles of a Cloud Migration – Security W5H – The When	Trend Micro
DHS Reiterates Recommendations on Securing Office 365	Security Week
Several Vulnerabilities Patched With Release of WordPress 5.4.1	Security Week
CISA Reminds Federal Agencies to Use Its DNS Service	Security Week
Sophisticated Phishing Kit Used by Multiple Groups to Target Executives	Security Week

Threat Dashboard

8

New Threats This Month

ALL PSGE

Most Affected Area

Threats & Vulnerabilities

Affected PSGE	Threat Details	TLP Classification	CVE ID	Publish Date
ALL PSGE	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to pair a rogue keypad to an armed system.	TLP:WHITE	CVE-2020-5727	2020-05-02 16:15:00
ALL PSGE	All versions of chrome-launcher allow execution of arbitrary commands, by controlling the $HOME environment variable in Linux operating systems.	TLP:WHITE	CVE-2020-7645	2020-05-02 16:15:00
ALL PSGE	UniFi Cloud Key firmware <= v1.1.10 for Cloud Key gen2 and Cloud Key gen2 Plus contains a vulnerability that allows unrestricted root access through the serial interface (UART).	TLP:WHITE	CVE-2020-8157	2020-05-02 16:15:00
ALL PSGE	dom4j before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from	TLP:WHITE	CVE-2020-10683	2020-05-01

Twitter Threat Feed

ICS Vulnerability Feed

A Twitter list by @SCADAhacker

ICS-CERT Retweeted

Cybersecurity
@cyber

Malicious actors and cyber criminals are exploiting the #COVID19 pandemic as part of their cyber operations. @CISAgov has resources to help you better protect yourself: cisa.gov/coronavirus

Apr 29, 2020

ICS-CERT Retweeted

Homeland Security
@DHSgov

Did you know that @CISAgov is working behind the

Share Threats

Threat Name:

Affected System:

Threat Type*:

Affected PSGE*:

TLP Classification*:

TLP:WHITE

Tags:

Threat Detail*:

Share

*** Indicates a required field.**

About

CTIP for The PSGE

Power is fundamental to modern society.

Recent developments in the energy sector have led to the addition of information flows to traditional power grids. These implementations are known as Power Smart Grids, or simply Smart Grids. The PSGE (Power Smart Grid Ecosystem) refers to all those involved actors involved with Power Smart Grids. This includes all stakeholders from power generation to consumers.

The information flows in Smart Grids are bi-directional, enabling more efficient power delivery with less wastage.
However, these information flows open up the entire Smart Grid to cyber attacks.

In December 2015, Ukraine experienced the first cyber-attack targetted directly at power infrastructure. This attack alone directly affected 225,000 Ukranians for several hours, causing mass blackouts and energy providers having to resort to manual operations.
This attack demonstrates the need for appropriate protection of Smart Grids from cyber threats, as attacks are real and they are happening now.

CTIPs (Cyber Threat Information Portals) enable users to gain information about various cyber threats and vulnerabilities.
Due to the unique nature of the PSGE, this project identified a need for a CTIP to identify and inform the PSGE of the cyber threats specific to them. This will enable the PSGE to adjust their security posture to protect themselves appropriately.

How to Use

This CTIP aims to be simple to use. The Home page displays the cyber threats the PSGE face, and users are able to anonymously share threat information through the Share page.

Contact Us

Please get in touch for more information about the project.

Get in touch via e-mail

Future Work

Get Involved!

John Piesing

Email: s4913546@bournemouth.ac.uk

ResearchGate: researchgate.net/profile/John_Piesing2

Summary & Key Points

- Recent developments in power infrastructure have increased cyber risk
- Current solutions do not effectively mitigate this risk
- There is a need for a solution where stakeholders of the PSGE can get information on the cyber threats they face to better protect themselves
- This project proposed a solution aimed at solving this problem
- Feedback was positive, but the project requires wider involvement for future work

Contact
s4913546@bournemouth.ac.uk
researchgate.net/profile/John_Piesing2