



OWASP

Open Web Application
Security Project

SCADA and Other Dangerous Things

Professor Andrew Blyth, PhD.

University of South Wales, UK.

E-Mail: andrew.blyth@southwales.ac.uk

SCADA and Ukraine



The screenshot shows a web browser window displaying the Wikipedia article titled "December 2015 Ukraine power grid cyberattack". The browser's address bar shows "en.wikipedia.org". The article's main heading is "December 2015 Ukraine power grid cyberattack". Below the heading, it states: "From Wikipedia, the free encyclopedia". The article text begins with: "The **December 2015 Ukraine power grid cyberattack** took place on 23 December 2015 and is considered to be the first known successful **cyberattack** on a **power grid**. Hackers were able to successfully compromise information systems of three energy distribution companies in **Ukraine** and temporarily disrupt electricity supply to the end consumers." It then details the impact on consumers of «Prykarpattiaoblenergo» and «Chernivtsioblenergo».

Contents [hide]

- 1 Description
- 2 See also
- 3 References
- 4 Further reading
- 5 External links

Description [edit]

The cyberattack was complex and consisted of the following steps:^[2]

- prior compromise of corporate networks using **spear-phishing** emails with BlackEnergy malware;
- seizing **SCADA** under control, remotely switching substations off;
- disabling/destroying **IT infrastructure** components (**uninterruptible power supplies, modems, RTUs, commutators**);
- destruction of files stored on servers and workstations with the KillDisk malware;
- denial-of-service attack on call-center to deny consumers up-to-date information on the blackout.

SCADA Hacking

concise-courses.com

Syrian Electronic Army targets and hacks Israeli SCADA systems

concise courses

About Books Hacker Tools Courses

f

t

+

Syrian Electronic Army targets and hacks SCADA systems

For All Things IT Security Conference Related

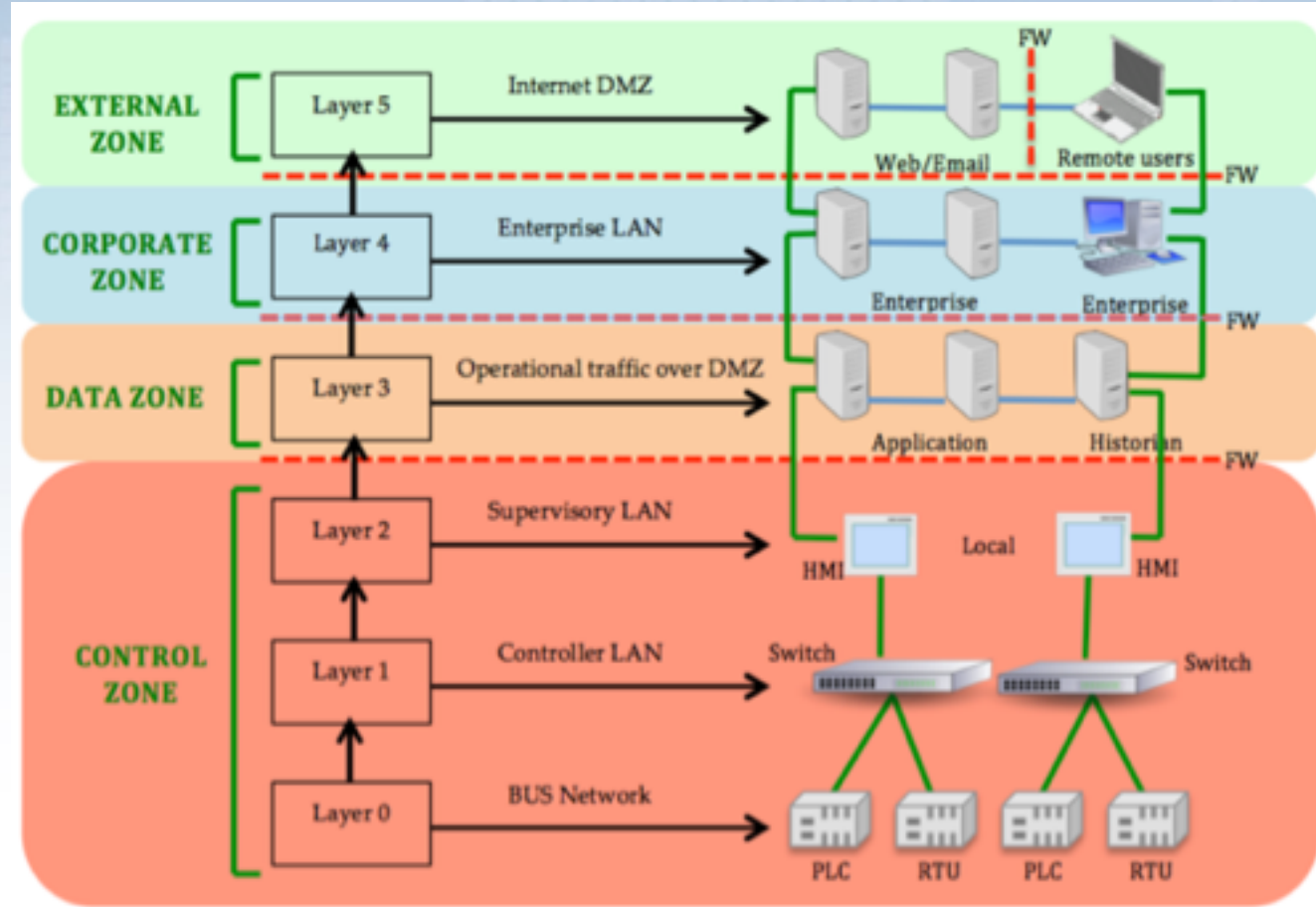
Join Our Newsletter [Over 50K Subscribers]

Let us send you information on ticket discounts, speaking opportunities and a ton more!

Yes, I want in on this...

Home / Blog / Syrian Electronic Army targets and hacks SCADA systems

Typical SCADA Critical Infrastructure Architecture



SCADA and IPC Forensic Challenges

- Why do challenges exist?
 - IPC/SCADA systems designed to automate, monitor and control Critical Infrastructure were originally designed for isolated, air gapped networks
 - Now interconnected with many networks and communicating via Internet
 - Span huge geographical areas
 - Include many proprietary and legacy devices and protocols
 - Lack of security mechanisms in SCADA protocols
 - No real guidance or methodologies for data acquisition at the control level

SCADA Forensic Challenges

- **Data Sources**
 - **Variety of data sources, amount of data sources**
- Live Acquisition
- Verification
- Response Time
- Logging and Storage
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- **Live Acquisition**
 - **Latency, interference and OOV (Order of Volatility)**
- Verification
- Response Time
- Logging and Storage
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- Live Acquisition
- **Verification**
 - **Calculating hash values**
- Response Time
- Logging and Storage
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- Live Acquisition
- Verification
- **Response Time**
 - **Span huge geographical areas, many field sites**
- Logging and Storage
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

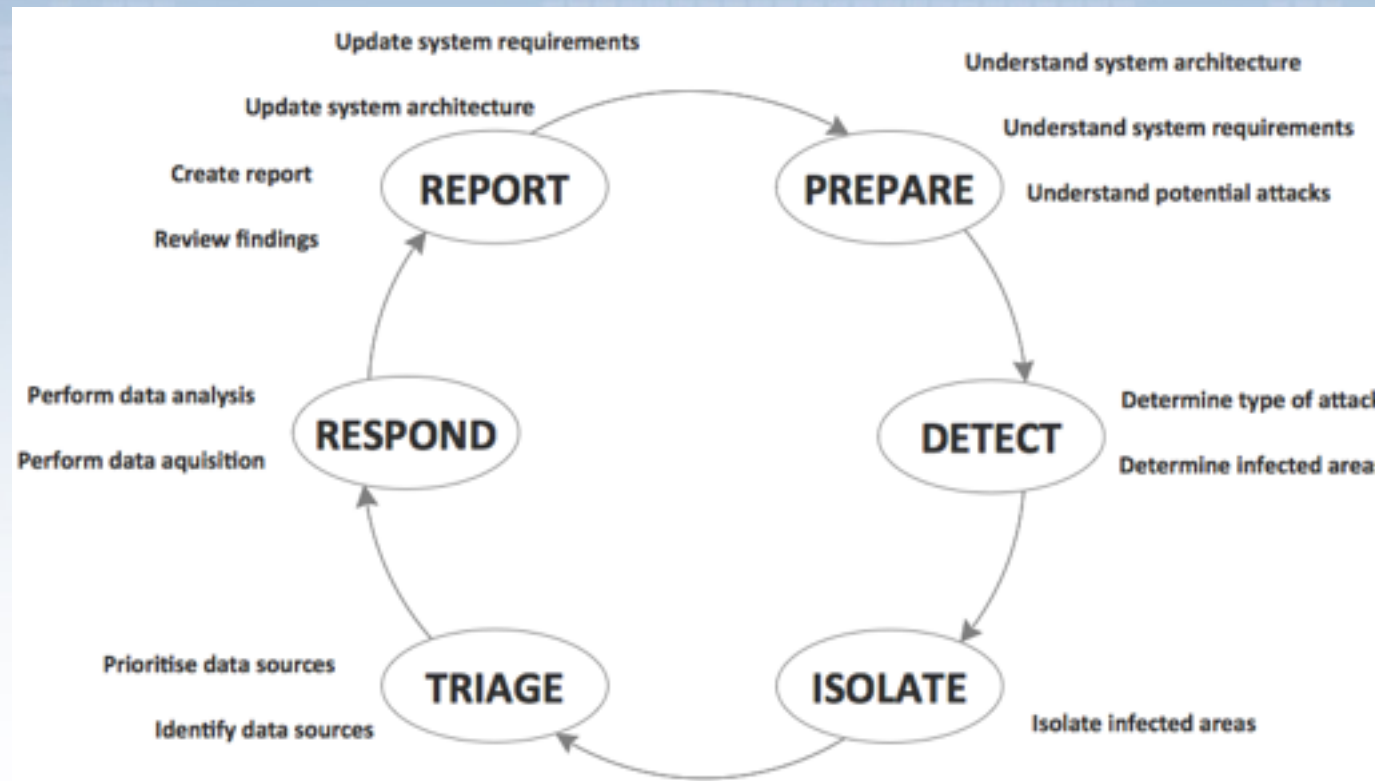
- Data Sources
- Live Acquisition
- Verification
- Response Time
- **Logging and Storage**
 - **Audit/logging functions disabled, minimal storage**
- Absence of Dedicated Forensic Tools

SCADA Forensic Challenges

- Data Sources
- Live Acquisition
- Verification
- Response Time
- Logging and Storage
- **Absence of Dedicated Forensic Tools**
 - **No real methodologies for data acquisition from PLCs**



IPC/SCADA Forensic Incident Response Model



SCADA Forensic Incident Response Model

➤ Stage 1: **Prepare**

- Understand system architecture
- Understand system requirements
- Understand potential attacks

SCADA Forensic Incident Response Model

➤ Stage 2: **Detect**

- Determine type of attack
- Determine infected areas

➤ Stage 3: **Isolation**

- Containment of infected areas in relation to business operations

SCADA Forensic Incident Response Model

➤ Stage 4: **Triage**

- Identify data sources
- Prioritize data sources

➤ Stage 5: **Respond**

- Perform data acquisition
- Perform data analysis

SCADA Forensic Incident Response Model

- Stage 6: **Report**
 - Review findings
 - Create report
 - Update system architecture
 - Update system requirements

Questions

