An Anomaly Detection Technique for Deception Attacks in Industrial Control Systems

Abdul Rahim Ahmad
College of Computing and Informatics
Universiti Tenaga National (UNITEN),
Kajang, Malaysia
Abstract

The increasing interaction of modern industrial control systems (ICS) to the outside Internet world influences making these systems vulnerable to a wide range of cyber-attacks. Moreover, the utilisation of Commercial-off-the-Shelf (COTS) products, as well as open communication protocols, made them attractive targets to various threat agents including cyber-criminals, national-state, and cyber-terrorists. Given that, today’s ICSs are deriving the most critical national infrastructures. Therefore, this raises tremendous needs to secure these systems against cyber-attacks. Intrusion detection technology has been considered as one of the most essential security precautions for ICS networks. It can effectively detect potential cyber-attacks and malicious activities and prevent catastrophic consequences. This presentation puts forward a method to detect malicious activities at the ICS networks.
Outline

- Tenaga Nasional Eberhad (TNB)
- Universiti Tenaga Nasional (UNITEN)
- Industrial Control Systems (ICS)
- Deception Cyber Attack
- Anomaly based IDS
- Solution
- Summary
Tenaga Nasional Berhad

The Tenaga Nasional headquarters in Bangar.

Type: Publicly traded government-linked company
Traded as: MYX: 5347
ISIN: MYL534700009
Industry: Electrical power
Founded: 1 February 1990
Headquarters: Kuala Lumpur, Malaysia
Area served: Malaysia (except Sarawak), Mauritius, Pakistan, India, Indonesia
Key people: Leo Maggie Iroh, Chairman
Datuk Seri Ir. Azman Bin Mohd., CEO[1]
Products: Electricity generation, transmission and distribution
Revenue: RM37.13 billion (2013)[2]
Operating Income: RM5.89 billion (2013)[2]
Net income: RM4.91 billion (2013)[2]
Total assets: RM96.03 billion (2013)[2]
Number of employees: 34,900 (2013)[2]
Parent: Khazanah Nasional
Subsidiaries: Infratrac
Website: www.tnb.com.my

<table>
<thead>
<tr>
<th>COMPANIES</th>
<th>EQUITY HOLDINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNB Engineering Corp. Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Engineers Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Energy Services Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Fuel Services Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Janamanjung Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Power Daharki Ltd</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Properties Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Repair and Maintenance Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Research Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>Universiti Tenaga Nasional Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Capital (LI) Ltd</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Ventures Sdn Bhd</td>
<td>100%</td>
</tr>
<tr>
<td>Power and Energy International (Mauritius) Ltd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Kulim Distribution Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Kulim Generation Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB International Sdn. Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>Malaysia Transformer Manufacturing Sdn Bhd.</td>
<td>100%</td>
</tr>
<tr>
<td>TNB Coel International Limited.</td>
<td>92.5%</td>
</tr>
<tr>
<td>Sabah Electricity Sdn. Bhd.</td>
<td>80%</td>
</tr>
<tr>
<td>Sepang Power Sdn. Bhd.</td>
<td>70%</td>
</tr>
<tr>
<td>Tenaga Switchgear Sdn. Bhd.</td>
<td>60%</td>
</tr>
<tr>
<td>Kapar Energy Ventures Sdn. Bhd.</td>
<td>60%</td>
</tr>
</tbody>
</table>
About UNITEN

- Website: http://www.uniten.edu.my
- Formerly Training Institute (ILSAS) for Electricity Board since 1976
- Established as a university in 1997
- 3 Main Focus areas (Engineering, Business and IT), 2 campuses, 3 hours apart
- Rough Numbers
  - 11,500 students; 50% Engineering based, 10% postgraduates, 10% Foreign students
  - 1000 staff members, 50% Academics and Research
- 3 major energy related entities
  - IEPRE (Inst of Energy Policy and Research)
  - CRE (Centre for renewable Energy)
  - PEC (Power Engineering Centre)
- Owned by TNB 100%
UNITEN
# ICS and Cyber attacks

**Cybersecurity systems**
- Protects internet-connected systems from cyber attacks.
- Security = cybersecurity + physical security
- Ensuring information availability, integrity, authentication, confidentiality, and non-repudiation.

**ICS**
- Industrial control systems - encompasses control systems and associated instrumentation used for industrial process control.

**Why systems are vulnerable to cyber-attacks.**
- Connection to outside Internet world
- Utilization of Commercial-off-the-Shelf (COTS) products.
- Use of open communication protocols

**Attackers (threat agents)**
- cyber-criminals
- national-state
- cyber-terrorists.

**How to secure ICS**
- Uses Intrusion detection technology as an essential security precautions for ICS networks.
- Detect potential cyber-attacks and malicious activities

**Why secure an ICS**
- ICSs driving critical national infrastructures.

**This presentation looks at a method to detect malicious activities at the ICS networks.**
Security in ICS

Security by obscurity
• Industrial control systems (ICS) isolated from other network systems was thought to be safe.
• But Stuxnet attack incident on the Iranian nuclear plant change that.

Security breaches on highly sensitive facilities
• 2015 - Cyber-attack induced power outage in Ukraine by compromising of the corporate networks via spear-phishing emails with BlackEnergy malware
• 2014 - Attack on German steel plant - production control software was hacked.

• Need to address the vulnerabilities and loopholes of the ICS systems to protect these systems from security threats, attacks, and malware.
• Nevertheless, activities that aid in detecting security vulnerabilities and potential breaches were not able to identify zero-day vulnerabilities or unforeseen threats.
• The need of an intrusion detection system to strengthen the security
Stuxnet

- **Stuxnet** is a malicious computer worm, first uncovered in 2010. Thought to have been in development since at least 2005, Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program. Although neither country has openly admitted responsibility, the worm is believed to be a jointly built American/Israeli cyberweapon.

- Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Exploiting four zero-day flaws.

- Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.

- Stuxnet’s design and architecture are not domain-specific and it could be tailored as a platform for attacking modern supervisory control and data acquisition (SCADA) and PLC systems (e.g., in factory assembly lines or power plants), the majority of which reside in Europe, Japan and the US.

- Stuxnet reportedly ruined almost one fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.

Stuxnet has three modules:

- a **worm** that executes all routines related to the main payload of the attack;
- a **link file** that automatically executes the propagated copies of the worm;
- and a **rootkit** component responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet.

It is typically introduced to the target environment via an infected USB flash drive, thereby crossing any air gap. The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC. In the absence of either criterion, Stuxnet becomes dormant inside the computer.

If both the conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

In 2015, Kaspersky Lab noted that the Equation Group had used two of the same zero-day attacks, prior to their use in Stuxnet, and commented that: "the similar type of usage of both exploits together in different computer worms, at around the same time, indicates that the Equation Group and the Stuxnet developers are either the same or working closely together".
Zero-day Vulnerability

- A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software).
- Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network. An exploit directed at a zero-day is called a zero-day exploit, or zero-day attack.
- In the jargon of computer security, "Day Zero" is the day on which the interested party (presumably the vendor of the targeted system) learns of the vulnerability. Up until that day, the vulnerability is known as a zero-day vulnerability.
- Similarly, an exploitable bug that has been known for thirty days would be called a 30-day vulnerability. Once the vendor learns of the vulnerability, the vendor will usually create patches or advise workarounds to mitigate it.

- The fewer the days since Day Zero, the higher the chance no fix or mitigation has been developed.
- Even after a fix is developed, the fewer the days since Day Zero, the higher is the probability that an attack against the afflicted software will be successful, because not every user of that software will have applied the fix.
- For zero-day exploits, the probability that a user has patched their bugs is zero, so the exploit should always succeed.
- Zero-day attacks are a severe threat.
BlackEnergy Malware

- **BlackEnergy Malware** was first reported in 2007 as an HTTP-based toolkit that generated bots to execute *distributed denial of service* attacks.
- In 2010, **BlackEnergy 2** emerged with capabilities beyond DDoS.
- In 2014, **BlackEnergy 3** came equipped with a variety of *plug-ins*.
- A Russian-based cybergang known as Sandworm is attributed with using BlackEnergy targeted attacks. The attack is distributed via a Word document or PowerPoint attachment in an email, luring victims into clicking the seemingly legitimate file.
German Steel Mill Attack

- Massive damage to a German steel plant in 2014.
- Specifically targeting **operators of industrial plants**
- Caused components of the plant controls to fail, resulting in an unregulated furnace, which then caused physical damage to the steel plant.
- Infiltrate the system using spear phishing and social engineering techniques.
- These two methods are proven ways by which threat actors lure their victims using emails or social media links that **appear to come from a legitimate source** but can actually introduce threats for attackers to get inside the network.
- Attacks affecting real-world operations of facilities have been ongoing but many **remain unreported** by the affected organizations.
Intrusion detection systems (IDS)

- Introduced in conventional IT networks
- Designed for the automatic and systematic detection of known cyber-attacks and unusual malicious activities.
- Collect and analyse network traffic, security logs, audit data, and information from key points of a computer or network systems, to verify the legitimacy of the examined activity and check against the security policy whether there exist security violations.
- Recently, IDS were involved in maintaining the security of ICS networks.
- During the last few years, intrusion detection technology for ICS has become a research hotspot, which has drawn great attention from both academia and industry.
- The main goal of this work is to identify the limitations of existing ICS-IDS systems and put forward a proposed method to detect malicious activities on the anomaly bases.
- We also presents an overview of industrial control systems and presents the proposed method
Industrial control systems (ICS)

- Industrial Control Systems (ICS) are used for monitoring and controlling numerous national critical infrastructure systems such as in electrical power generation and transmission, train control, chemical plants as well as in oil and water treatment and distribution systems.
- In particular, they are deriving, monitoring, and controlling the most significant and critical systems in our daily lives.
- Therefore, ICS has a strategic significance due to the potentially serious consequences of a fault or malfunction.
- As a consequence, protecting these systems against malicious attacks is a vital requirement to prevent catastrophic consequences.
- ICS typically incorporate sensors and actuators that are controlled by Programmable Logic Controllers (PLCs), Remote Terminal Units (RTU) or Intelligent Electrical Devices (IEDs) on the field sites which are themselves managed by the Human Machine Interface (HMI) at the control centre side.
Architecture of ICS

- At the field devices area; sensors, relays, and actuators offer an interface to both control and monitor the physical processes.
- As such, the RTU and the PLC are incorporated as they aggregate control (serve as master) for many field devices by passing commands and responses via a communications network to the control centre.

- The control centre commonly consists of ICS application servers to process monitoring and control, database servers for historical record storage, and in some cases, interoperability servers to interconnect the ICS control software and hardware from varied vendors.
- Moreover, the operator of the system monitors the state of physical systems’ processes through the HMI and controls the process by activating commands as required.
Deception Cyber Attack

- Our focus is on special type of attacks called **deception attacks** - defined as **false information sent by an adversary from sensors or controllers** such as wrong sender ID, wrong measurement or device status.
- Traditionally, this type of attack can be easily detected if the ICS protection system is configured to check with the expected output of a healthy system and detect whether it is being attacked or not.
- However, this technique can only work for a basic deception attack and fail to detect a more sophisticated type of attacks (i.e. **stealthy deception attacks**) [17].
- Thus, in such cases, the ICS would not be able to protect itself against such attacks. **Anomaly-based IDS** is considered as one of the outstanding solutions to this matter.
Anomaly based IDS

• A new anomaly detection method for detecting and preventing stealthy deception attacks in industrial control systems.
• The proposed method would be able to classify events generated by an RTU, PLC or IED into either legitimate or malicious behaviours.
• Preliminary analysis showed that the proposed method would be able to classify alarms in high accuracy with low false alarms.

• The detection method presented in this work is based on investigating the behaviour of normal, attack-free activities to learn how future events can be handled more efficiently.
• The proposed method is designed to classify events without using predefined knowledge of attack signatures or attack examples. Instead, it establishes a baseline model of the ICS network communication status during normal operation and attempts to discover malicious activities based on deviations from the learnt model.
• The main goal of the proposed method is to classify events generated by ICS remote sites.
Anomaly based IDS

• The main objective of this method is to **filter the incoming messages** and investigate the validity of being false or legitimate based on features extracted from the network traffic flow corresponding to the events generated by the remote sites.

• To perform this task, the proposed method has to **pre-process the monitored network traffic** to extract the required features.

• Once an event has been generated, the corresponding network traffic flow features are examined to evaluate the truthiness of the generated event.

• Prior the classification method to be able to distinguish fake events, it has to be trained with a set of legitimate events to identify normal communication patterns that tend to cause changes of remote sites’ status or readings.
Anomaly based IDS

• **During a training phase,** the proposed method has been designed to learn and model network communication states that cause the remote sites to trigger an event during benign activities using network traffic flow features identified in.

• **Off the training phase,** the event classification method utilises the constructed model to classify unlabelled events into either false or legitimate.

• The **classification method** classifies an event based on the distance between the training samples and the examined event, where those are located close to the training samples are considered false events.
Anomaly based IDS

• The proposed events classification method is composed of three processes;
  • initially, the network traffic flows are pre-processed to extract the required features. The network traffic flows are divided into uniquely time distant subsets; for each subset, flows are grouped based on the corresponding IP address and port numbers to estimate the required features.
  • After processing the training examples, the second process is initiated, in which a communication profile for each network interface is established. The communication profile is considered as the baseline model that is used in the event classification process (the third process).
  • Once the baseline model is established, the method can classify new unlabelled alarms.
Conclusion

- Today’s ICS implementations are becoming increasingly interconnected with other corporate networks and the Internet.
- ICS systems have become highly dependent on the use of Commercial-Off-The-Shelf (COTS) IT products as well as open communication standards to significantly reduce infrastructure costs and increase ease of maintenance and integration.
- This brings in substantial challenges in protecting critical national infrastructure. Moreover, as the cyber-threat landscape continues to evolve, ICS systems and their underlying architecture must be secured to withstand cyberattacks.
- The main purpose of this work is to propose a new event classification method to manage the events generated by remote terminal sites.
- The proposed method helps to filter-out malicious activities to protect the control system against stealthy deception attack.

This research was sponsored and supported under the Tenaga Nasional SEED fund (managed by UNITEN R&D Sdn Bhd)

Many thanks to the UNITEN R&D Sdn Bhd who provided their assistance during this ongoing research.
Terima Kasih