Cyber Deception for Integrated Energy Systems:

Cyber-Attacks Simulations and Defense Mechanisms

Dr Stephen Ugwuanyi*, **Research and Development Engineer, PNDC** (*Stephen.Ugwuanyi@strath.ac.uk)
Dr Kinan Ghanem, Lead Research and Development Engineer, PNDC

University of Strathclyde Engineering

UNIVERSITY of STRATHCLYDE PNDC

Abstract

This paper is based on the key lessons learned from a proof of concept collaborative review of a cyber deception framework capabilities within an Operational Technology (OT) network to detect, analyse and alert of an internal and external facing threats. As the OT domain is constantly evolving, innovative approaches are needed to enhance existing cyber security systems. By strategically hosting of intelligent 'Snare and Prowl' decoys both within and outside utilities network operator's environment to mimic faux services and targets, internet-based, in-network adversaries, and Advanced Persistent Threats (APTs) are identified, engaged, and their Techniques, Tactics, and Procedure (TTPs) tracked for attack characterisation based on their Threat Intelligence Profiles (TIPs) and narratives employed to effectively discern attackers capability to laterally progress across the network.

Background

Over the recent past, there has been a re-emergence of honeypot technologies which have been used to trap malicious users in order to identify early signs of attacks. While effective in luring inexperienced attackers, current solutions are ineffective against more sophisticated intruders given that their (static) non-dynamic nature permits easy identification. The average time to identify and contain a cyber-breach is >300 days, a significant exposure demanding the detection and mitigation of successful attacks as early as possible. Early detection is challenging as attackers constantly adapt techniques to evade embedded protection measures.

Furthermore, a 15.1% increase in successful cyber-attacks has occurred over the last year despite the plethora of solutions and tools on offer. Security Operation Centres (SOCs) report that current solutions generate between 72% and 80% False Positive (FP) alerts, resulting in increasing pressures on the Security Operations Centre personnel.

In relation to the energy sector, the potential damage and associated costs of a successful cyber-attack is exemplified by the attack on the Ukrainian Power System in 2015. The breach took the attackers 10 months from reconnaissance to execution, the goal of the attack was to cause physical damage to a transmission station. The breach resulted in 225k customers without access to power and an estimated £27m revenue loss; the average network downtime costs were £240k per hour. The estimated reputational damage cost was £1.2m and the investigation lasted for four years.

A recent report states that the potential GDP losses for the UK from a similar-sized attack may range from ~£21m for a four-substation electricity event to ~£111m for a 14-substation incident. Hence, the project objectives are:

- The co-development of a deception-enabled cyber security solution that enhances the protection of critical infrastructures for the energy networks, but also applicable to other OT sectors.
- Showcase the benefits of cyber security deception, informing cyber security operators tasked with the protection of both the corporate (IT) and OT assets.
- Provide evidence on the benefits of cyber security deception for the energy sector.

Use case

The case study is based on servers and database attack simulations critical for a more flexible, reliable, resilient, secure and sustainable integrated energy systems. In the attack scenario 1, lessons of how breadcrumbs are used to prevent an attempt to attack narrative deployment for Apache and SSH Servers is shared. The lessons from the second attack scenario show how decoys detect attacks with indicators of intelligence based on privileged access through active port scanning. Attack scenario 3 lessons demonstrate the impact of network environment change on the system's security.

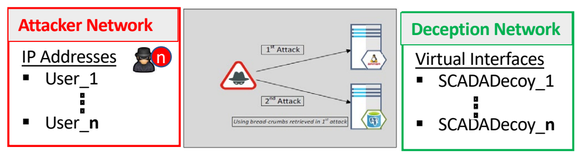
The decoy cluster co-operate to demonstrate the ability of deception-based cyber security to identify evolving threats placed into a global context, initially outside IT utility networks, enhancing the cyber security resilience on the backdrop of ever-increasing levels of sophisticated campaigns of attacks. Cyber deception solutions generate Techniques, Tactics, and Procedures (TTPs) from the data acquired, real-time from a cluster of decoys deployed within a representative DNO environment (Figure 1).

The characterisation of the showcase deployment ascertained the additional benefits of deception to enhance current cyber security practices in OT networks. The recommendations on the most appropriate deception solution and the route to deployment within utility infrastructures are insights that inform decisions on the value of deception for the sector.

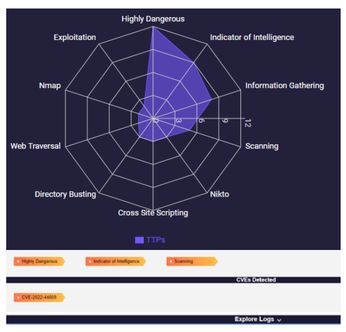
Trial summary

- Within the Snare platform, the interactions logs concerning the deployed decoys and attacking IP within the selected organization can be refined to gain other information like attacking IP address and any intelligence within the attack. Each interaction with the decoy receives a severity rating, categorized as 'informational', 'warning', or 'critical', following an analysis of the interaction.
- Analytics are applied to assess the interactions between the attacker and decoy, determining whether the connection should be identified as an attack. Each attack is assigned a threat score on a scale of 0 to 100. Interactions originating from a private IP address default to a threat score of 50, as this implies that the attacker may be within the network. Threat scores are routinely reassessed as interactions evolve.
- To strategically aligns decoy placement with the goal of detecting and responding to potential threats across different segments of the DNO's environment, deception decoys can be placed at the Corporate Perimeter Network to monitor and detect external threats from the Internet, SCADA Perimeter Network to provides insight into threats targeting the OT environment, Proxy DMZ to detect network access and signalling scanning activities from potential threats at the substation network, and at the Corporate Internal Network to identify internal related threats.

Attack Simulation Scenario:
Attempts to attack the different decoy Narratives deployed in the network



Attack Simulation TTPs Faced in a month



1 _ *ConfigureDecoysToActInNarrative*
2 _ *RunNmapAgainstBothDecoys*
a _ *RunNmap*
3 _ *RunHydraAgainstSshServerOnSpeciedPort*
a _ *CreatePasswordDictionaryToUseWithHydra*
b _ *RunHydra*
4 _ *RunNiktoAgainstApacheServer*
a _ *RunNikto*
5 _ *VerifyClonedAppOnApacheServerViaBrowser*
6 _ *VerifyBreadcrumbOnApacheServerViaBrowser*
7 _ *RunHydraOnSshServerWithBreadcrumbs*
a _ *RunHydra*

Methodology

The development and evaluation of cyber deception solution capabilities and performance helped support the creation of an energy-specific cluster of collaborating decoys which implement narratives that entices and locks attacker on paths away from critical operational assets.

- Develop POC deployment architecture and test plan for cyber deception in energy networks.
- Definition, development, and deployment of mix of decoys to demonstrate deception attack Tactic, Technique and Procedure (TTPs).
- Test and evaluation to evidence success criteria based on decoy concealments, qualitative and quantitative data, c-level and incident reporting, and actionable entities.

How it works

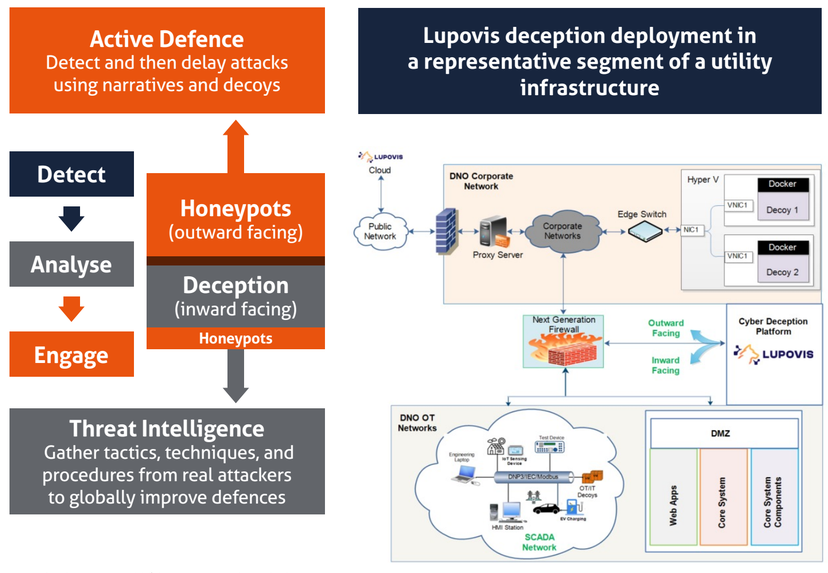


Figure 1

Stages of the development

- Dynamic deployment of deception assets inside and outside of the energy network.
- Narratives representative of attack paths in energy infrastructure created in consultation with energy network operators.
- Energy-specific decoys created and the evaluation metrics for cyber deception agreed in consultation with energy network operators.
- Breadcrumbs utilised to maintain a strong engagement with the attacker.
- The Lupovis Deception-as-a-Service platform (SNARE) served the energy-specific decoys deployed within a representative network of an energy operator.
- The Lupovis contextual threat intelligence platform (PROWL) employed to generate Internet-based attacks.

Conclusions and future work

Every energy companies will be integral to the development of the suite of most appropriate deception decoys for the sector e.g., PLC, CCTV, HMI with custom configurations, decoy concealment, and to define optimum routes for the integration of the digital intelligence generated by deception within SIEM products and Supervisory Control and Data Acquisition (SCADA) systems. By collaborating with companies in the energy sector to further demonstrate the technology through specific use cases and scenarios that help to meet NIS regulations and directives from the National Cyber Security Centre (NCSC). The trial results will inform energy networks on cyber security practices that might mitigate future risks from an evolving range of new cyber attacks.

Project partners

The project, funded through the PNDC core research fund, comprises a partnership between PNDC, Lupovis Ltd and PNDC's key DNO partners UK Power Networks, SP Energy Networks and Scottish & Southern Electricity Networks and is delivered in collaboration with UK Power Networks & Lupovis.

References

(1) Stephen Ugwuanyi & Kinan Ghanem, "Evaluation of Power Deception in Power Networks", PNDC 2024.

LUPOVIS Deception Solution
UK Power Networks DNO
UNIVERSITY of STRATHCLYDE PNDC DNO's Test & Demonstration Centre