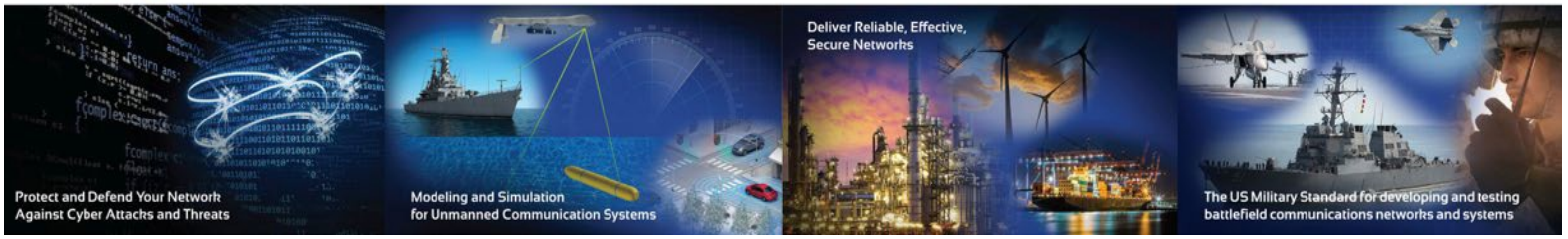
SCALABLE
NETWORK TECHNOLOGIES



Ukraine Power Grid Attack:

A Case Study on the Use of Network Digital Twins for Assessing Cyber Resilience

SCALABLE Network Technologies

Ukraine Power Grid Attack: A Case Study on the Use of Network Digital Twins for Assessing Cyber Resilience

1 Introduction

Several high-profile cyber attacks have made the headlines in the last few years, targeting organizations as varied as movie studios, retail store chains, credit agencies, and public utilities. This demonstrates that no enterprise or organization is immune to cyber attacks. The cost of these attacks has been loss of revenue, damage to business reputation, and disruption of critical services.

Some of the more prominent attacks that have made the news include:

- WannaCry 2017 Ransomware Attack: Used Server Message Block (SMB) and NotPetYa
- CxO Fraud (like spearphishing)
- Sony Pictures: 2014 Server Message Block (SMB) worm
- Target: RAM scraping
- Alteryx: Publicly exposed AWS S3 storage cache
- Equifax: Vulnerability of Apache Struts
- Marriott

As the above list makes clear, the attacks have included a variety of approaches to infiltrate the target IT system and degrade or deny critical operations and business services.

SCALBLE Network Technologies (SCALABLE) has developed its cyber range to allow their customers to assess both the impact and risks of cyber threats to their operational systems. The SCALABLE cyber range supports such assessments in a zero-risk environment using advanced Live, Virtual, and Constructive (LVC) simulations that can be used to assess resilience to myriad historical attacks (including the ones listed above) as well as so called zero-day attacks.

How Can the SCALABLE Cyber Range Help?

To prepare for the inevitable future cyber attacks, it is essential to understand and thoroughly analyze how cyber attackers can infiltrate the system, even those employing robust defense-in-depth strategies. SCALABLE's cyber range provides a convenient, cost-effective way for such analysis. More importantly, it can provide an environment in which to plan an organization's responses when their systems are attacked and to train their teams to prevent or mitigate the impact of successful attacks. An organization can use the SCALABLE cyber range specifically to:

- Uncover the weak links and vulnerabilities in the infrastructure and processes which can be exploited by adversaries
- Implement defenses to prevent breaches
- Devise methods to detect breaches quickly when they do occur
- Prepare mitigation strategies to contain breaches
- Test the effectiveness of deployed defense mechanisms, such as firewalls and Anti-Virus Software (AVS)
- Prepare methods to quickly recover from cyber attacks
- Evaluate alternatives for thwarting, containing, and recovering from cyber attacks

Benefits of Using the SCALABLE Cyber Range

Testing a live system by subjecting it to cyber attacks is time-consuming, costly, and, in most cases, impracticable. The SCALABLE cyber range, by virtue of being a digital replica of the target system, provides a zero-risk, cost-effective way to analyze how the system responds to cyber attacks and to evaluate different strategies to safeguard against them.

For a simulation to provide insight into the system behavior, the simulation model should faithfully replicate the real system such that the behavior observed in the simulation model is the same as the behavior of the real system when subjected to cyber attacks. For this, the simulation model of the target system and the analysis platform should have the following features:

- High-fidelity models of devices (hosts, routers, switches, workstations, etc.) and links connecting them
- Models of defense mechanisms such as firewalls, Intrusion Detection Systems (IDS), and AVS
- Representation of vulnerabilities at hosts that can be exploited by cyber attacks to perform malicious actions
- Models of cyber attacks and the ability to replicate chains of attacks such as those employed in the real world to breach a system
- Ability to integrate with live and virtualized devices and live applications in an LVC environment to provide a realistic simulation platform
- Human behavior models: Most attacks depend on deliberate or inadvertent actions by humans interacting with the system. The simulation platform should model those aspects of human behavior which can directly or indirectly affect the cyber state of the system.
- Ability to run simulations faster than real time
- A means to easily depict the cyber state of hosts in the network, i.e., whether the host has been cyber-compromised, and if so, to what extent
- A Human-In-The-Loop (HITL) interface using which an analyst can launch cyber attacks and set up defenses, and observe their effects
- Ability to visualize how the effects of breaches propagate within the system
- Quantify the effects of attacks on system resources, such as memory and CPU
- Produce detailed statistics which can provide insight into system behavior

2 EXata's Cyber Capabilities

SCALABLE's EXata network simulator/emulator exploits contemporary multi-core architectures and efficient Parallel Discrete Event Simulation (PDES) technologies to run high-fidelity simulations of large, real-world networks faster than real-time. It uses a network digital twin to represent the entire network, which includes detailed models of the various protocols used across all layers and replicates device configurations from the physical network. The system can interoperate, at one or more protocol layers, with real devices to provide system-in-the-loop capabilities.

EXata can also be connected to systems with real applications, which run on the network digital twin just as they would run on real networks. EXata's Cyber Library provides a comprehensive set of models for a diverse set of cyber-attacks, defenses, and vulnerabilities which can be incorporated in the network models. These models can be used to launch attacks on the virtual network. Sequences of attacks can be designed and launched to probe and exploit network vulnerabilities and gradually infiltrate the network, where knowledge or access gained through a successful attack is used to launch additional attacks. The network's response to such attacks can be studied using a cyber operating picture and simulation

statistics. This provides a highly realistic environment to evaluate the target system's cyber resilience and for training network engineers on how to defend against cyber-attacks.

Models of Network Devices and Links

The EXata model library includes high-fidelity models of network devices, such as routers, switches, servers, and workstations, as well as connections between them (point-to-point links, hubs, etc.). The device models include models of protocols at all layers of the protocol stack as well as representation of software vulnerabilities which can be exploited by cyber attackers to perform malicious actions.

Cyber Attack Library

The EXata Cyber library includes models of different types of cyber attacks, including:

- **Passive Attacks**: Network Scanning, Port Scanning, Eavesdropping, and SIGINT attacks
- **Active Attacks**: Distributed Denial of Service, Jammer, and Virus attacks
- **Packet and Timing Modification Attacks**: These attacks modify the payload and delivery time of packets, and can model a class of attacks on Supervisory Control and Data Acquisition (SCADA) and control systems.
- **Vulnerability Attacks**: These attacks exploit system vulnerabilities to compromise the victim and impact its confidentiality, availability, and integrity. The malicious actions that can be performed to compromise a victim include file or database corruption, stealing credentials and gaining unauthorized access, injecting malware, and shutting down services.
- **Malware Attacks**: These attacks infect the target system with worms and viruses.
- **Botnets**: These attacks use compromised nodes in a network to act as attackers and launch additional attacks.
- **Phishing Attacks**: These attacks direct a victim to a compromised web server or open an infected email attachment and thus inject malware into the system.
- **Scripted Attacks**: These are adaptive sequences of attacks where an attack in the sequence is selected based on the outcome of the preceding attack(s) in the sequence.

Cyber Defense Models

The EXata Cyber Library also includes models of cyber defenses, including:

- **Firewall**: The EXata firewall model is a packet-based stateless software firewall, i.e., the firewall inspects each packet to determine if the packet should be allowed or denied access and does not retain state once a packet has been processed. The EXata firewall model is based on the Linux iptables.
- **Anti-Virus Software (AVS)**: An EXata host model can be configured to run AVS, which prevents, searches for, detects, and removes viruses and other malware.
- **Intrusion Detection Software (IDS)**: An EXata host model can be configured to run IDS, which monitors incoming traffic and blocks any packets which contain malware.

User Behavior Model

An EXata host can be configured with a user profile which determines how frequently and to how many other users does the user send emails, how many web servers does the user access and at what frequency, and how many and how frequently does the user share files. The user profile also determines the probability of the user opening an infected attachment of a phishing email. The user profiles configured at

different hosts determine how far and how quickly malware spreads from an infected host to other hosts within the network.

OS Resource Models

Many cyber attacks degrade performance by consuming system resources. EXata supports CPU and Memory Resource models to monitor the impact of cyber events on system resources.

Interface to Other Simulators

EXata can interface with other simulators to provide an integrated modeling and simulation environment for holistic analysis of networks in different domains. In particular, it can interface with OPAL-RT's HYPERSIM and RT-LAB electrical grid simulators. These are real-time digital simulators which can simulate electromagnetic transients of large-scale power systems and can be used for analyzing operational and reliability issues resulting from successful cyber attacks modeled in EXata. The integration of EXata and HYPERSIM provides a means to test the resilience of power systems to cyber attacks and improve their cyber defenses, thereby helping to ensure cybersecurity.

Analysis Capabilities

To aid the analysis of network behavior, EXata supports the following capabilities:

- The EXata GUI and the companion Scenario Player provide a graphical view of the network state in real time. This visualization is useful to understand the network behavior, including how traffic flows through the network, how malware spreads from host to host, and the cyber state of devices (whether a device is compromised and to what extent).
- EXata provides a high-performance database interface that allows time-series and statistical data to be stored in an SQL database during the simulation. These statistics can be used to trace the flow of packets through the network and correlate them to network events. This analysis sheds further light on network behavior and helps understand the root cause behind unintended or undesirable outcomes.

Interaction with a Running Simulation

The EXata GUI and Scenario Player provide a Human-In-The-Loop (HITL) interface using which an analyst can interact with the network model, while the simulation is running, and launch cyber attacks and modify firewall rules.

3 Case Study: Ukraine Power Grid Attack

To illustrate how EXata can be used to analyze and understand, and hence prepare for, real world attacks, we describe the December 2015 cyber attack on the Ukraine Power grid and how it can be modeled and analyzed using EXata. This was a very sophisticated attack, planned and executed over several months prior to the actual power outage. The attackers probed the system for weaknesses and exploited them to gradually infiltrate the network. They first gained access to the corporate network, using emails with infected attachments as the initial entry point. Once they infiltrated the corporate network, the attackers were able to snoop around until they were able to steal credentials which gave them access to the SCADA network and, subsequently, the relays at the substations. This combination of deployment of different types of cyber attacks, gradual infiltration of the system through successive layers of security by probing and adapting the attacks, and exploitation of human behavior is representative of real-world cyber attacks against different types of organizations.

3.1 Description of the Attack

In the first publicly documented successful attack of its kind, three regional power control systems in Ukraine were compromised by cyber attacks, resulting in wide-spread power outage for up to six hours. Operators were unable to regain remote control of more than 50 substations affected by the incident and circuit breakers began opening and closing without input from operators. Simultaneously, the malicious actors used automated systems to overload the phone systems. This denial-of-service attack on the telephony system further complicated the situation by hampering operator communications. Power was eventually restored only when technicians were sent to the substations to manually control the power system [1].

The analysis of the power outage and the attack that lead to it determined that firmware was corrupted on serial-to-Ethernet converters at substations, Uninterruptible Power Supplies (UPS) for both the server room and the telephony system were remotely turned off, and the hard drives of numerous computers were corrupted.

3.2 Sequence of Steps in the Attack

The attack on the power systems was carried in stages [1]. Figure 2 shows the network topology at a high level. The numbers in the figure correspond to the stages of the attack, which are described below.

1. *Spear Phishing*: Several months before the power outage, the attackers used a spear phishing attack to compromise hosts within the network. Several individuals were sent emails with infected MS Excel or Word documents as attachments. Opening the attachments led to installation of Black Energy 3 on their computers.
2. *Reconnaissance and Exploration of the Network*: Black Energy 3 was used for reconnaissance and enumeration of the network over several months. Additional backdoor malware was installed on the compromised computers, providing attackers backdoor entry into the corporate network.
3. *Steal Credentials*: The attackers were able to discover and access Active Directory servers and steal credentials.
4. *Create Encrypted Tunnel*: The attackers used the stolen credentials to establish a Virtual Private Network (VPN) into the control system network. The attackers used Remote Desktop (RDT), Remote Administrator (Radmin), and Secure Shell (SSH) to gain access to computers in the network.
5. *Compromise and Reconnaissance of Human Machine Interface (HMI) Computers*: The attackers performed reconnaissance and compromised several HMIs connecting to substations. The attackers were able to interact remotely with the control system using credentials obtained from one of the compromised machines.
6. *Manipulate Circuit Breakers*: The attackers remotely manipulated circuit breakers using one compromised HMI after another. The utility operators had to shut down the entire SCADA system, which finally tore down the VPN and disabled remote access, and move to manual mode in order to regain control of control network.
7. *Additional Attack Actions*:
    a. The attackers launched a telephony denial of service attack which overwhelmed the call centers with bogus automated calls and disrupted communication between the utility operators.

b. The attackers disabled the uninterrupted power supplies.

c. The attackers corrupted the firmware on several serial-to-Ethernet devices.

8. *Execute KillDisk on Target Computers*: The attackers used the KillDisk malware to erase critical files and corrupt the master boot record, rendering the system inoperable.

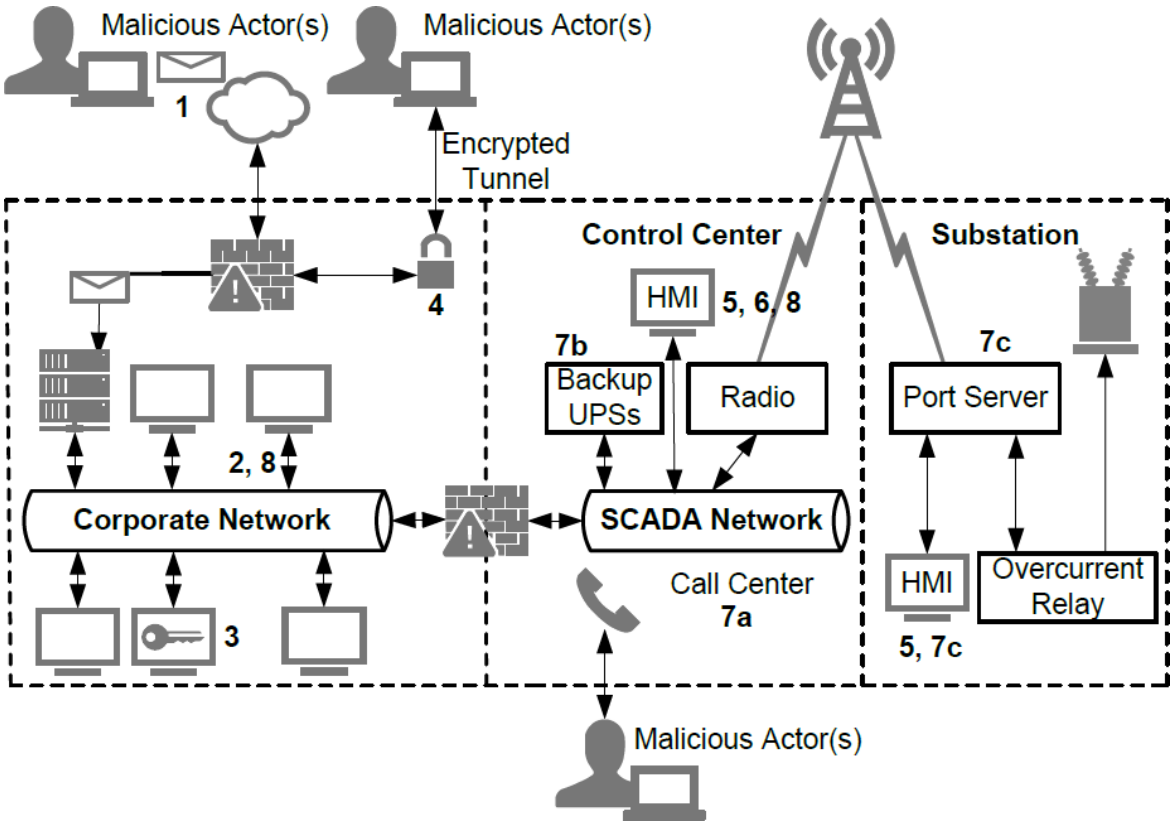


Figure 1: Progression of Cyber Attack on Ukraine Power Grid

3.3 Modeling the Ukraine Attack in EXata

The corporate network, the attacks, and their effects can be modeled in EXata in sufficient detail to understand:

- The impact of each type of attack in the sequence on the network components, i.e., the devices and resources that were impacted and the extent to which their confidentiality, integrity, and availability were compromised.
- The propagation of malware through the network, i.e., the mechanisms through which malware spread from one device to another, e.g., email or server access. This understanding can help devise more effective defensive measures, e.g., more effective firewall rules.
- The weaknesses (in network configuration, procedures and processes, and human behavior) which allowed the attack to succeed. This can help strengthen defenses and improve cyber resilience.

The EXata model can be used not only to gain insight into how the Dec 2015 attack succeeded, but can also to investigate how other attacks may affect the network and thus the operation of the power utility.

The results of such investigation and analysis can be used to develop defenses against future attacks, both in terms of hardware and software deployed in the network as well as the operational procedures and processes. In addition, such analysis can be beneficial in providing training to operators so that they can detect, counter, and contain future attacks before they cause major disruption of operations.

The model of the corporate network and control center in EXata can be connected to a simulation model of the power grid in OPAL-RT's HYPERSIM (Figure 3). EXata models the corporate IT network as well as the Operational Technology (OT) network, and the connections between them. Modeling both of these networks produces clear advantages for cyber analysis. On the IT side, user behavior may facilitate the installation of malware. The network configurations and connections will affect the malware propagation through the system as well as the success of potential unauthorized remote connections. The OT side models communication among sensors and controllers and thus, the ability of malware to affect the power grid. The simulated Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), controllers, relays, breakers, etc., in the power grid model communicate among themselves via the network digital twin created within EXata, using the system-in-the-loop interface. The sequence of simulated cyber attacks can then be launched on the simulated network and how it leads to the shutting down of the power grid (simulated in HYPERSIM) can be studied.

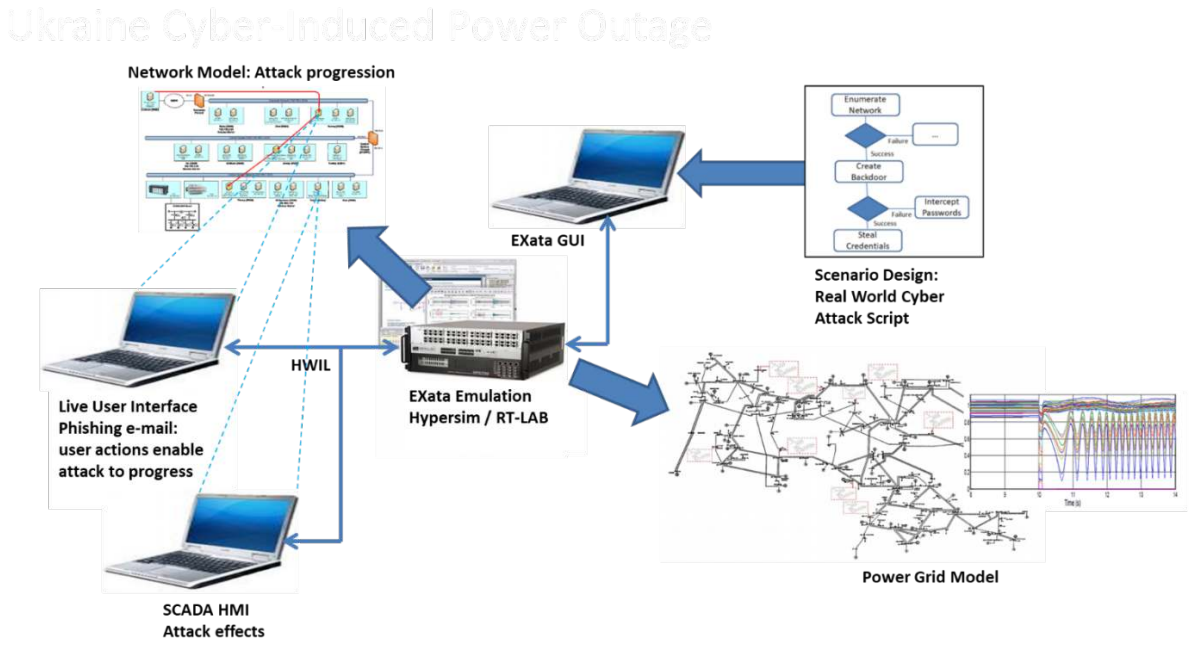


Figure 2: Modeling Ukraine Power Grid Attack Using EXata

Modeling the Network

The corporate and SCADA networks can be modeled by using EXata's user-friendly GUI and extensive library of models. The network model represents, at a sufficient level of detail, all relevant network devices and the connections between them. This includes routers, switches, and operator workstations. The models of these devices include vulnerabilities which can be exploited by cyber attacks to perform malicious actions.

Modeling Cyber Defenses

The firewalls deployed in the network can be replicated in the simulation model by EXata's firewall model, which is a packet-based stateless software firewall based on iptables. To model and analyze the Ukraine attacks, the firewalls in the model can be misconfigured in the same way as in the real network. Anti-virus Software (AVS) and Intrusion Detection Software (IDS) can also be configured in the simulation model so that the system's response to intrusion attempts can be replicated in the simulation model.

Modeling the Attack Sequence

The steps in the Ukraine attack (Section 3.2) can be modeled by EXata cyber attack models as follows:

1. Spear Phishing: This step can be duplicated in the model by EXata's Phishing attack model.
2. Reconnaissance and Exploration of the Network: EXata's Network Scanning and Port Scanning attack models can be used to duplicate the effects of this step.
3. *Steal Credentials*: This step can be duplicated in the model by EXata's Malware attack which exploits vulnerabilities to steal credentials.
4. Create Encrypted Tunnel: This step can also be duplicated in the model by EXata's encryption model.
5. *Compromise and Reconnaissance of Human Machine Interface (HMI) Computers*: This step can be duplicated by the Malware attack model integrated with a representation of the HMI, which would simulate the experience the operators had of losing control and watching commands be executed remotely.
6. *Manipulate Circuit Breakers*: This step can be duplicated by EXata's Packet Modification attack, injecting modified messages using actual SCADA protocols.
7. *Telephony denial of service attack:* The effects of this attack can be modeled by EXata's Denial of Service attack model.
8. *Execute KillDisk on Target Computers*: This attack can be modeled by EXata's Ransomware attack model.

Figure 4 shows a concept of how a Phishing attack could be launched using the EXata GUI. (Other attacks can be launched in a similar way.)

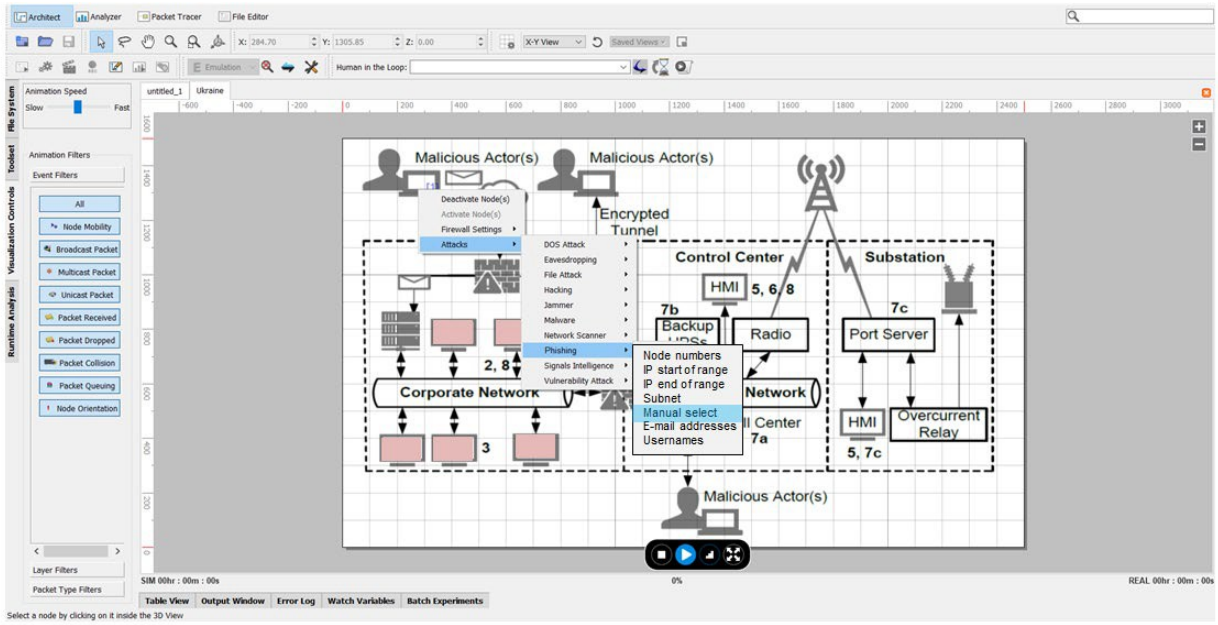


Figure 3: Launching a Phishing Attack Using EXata GUI

Modeling Operator Behavior

EXata's User Behavior model can be used to replicate the relevant aspects of operator behavior in the simulation model. These include characteristics such as how many servers a user accesses and how frequently, to how many other users does a user send emails and how frequently, and the probability with which a user opens phishing emails.

Attack Script

As in the case of the Ukraine attack, real world attacks involve a sequence of individual attacks of the type described above. EXata supports adaptive attack scripts which can be used to launch a sequence of attacks, where the outcome of an attack (success or failure) determines which attack will follow it in the sequence.

In the case of the Ukraine attack, a script is invoked at each of the targets of the phishing attack to implement the sequence of attacks shown in Figure 5.

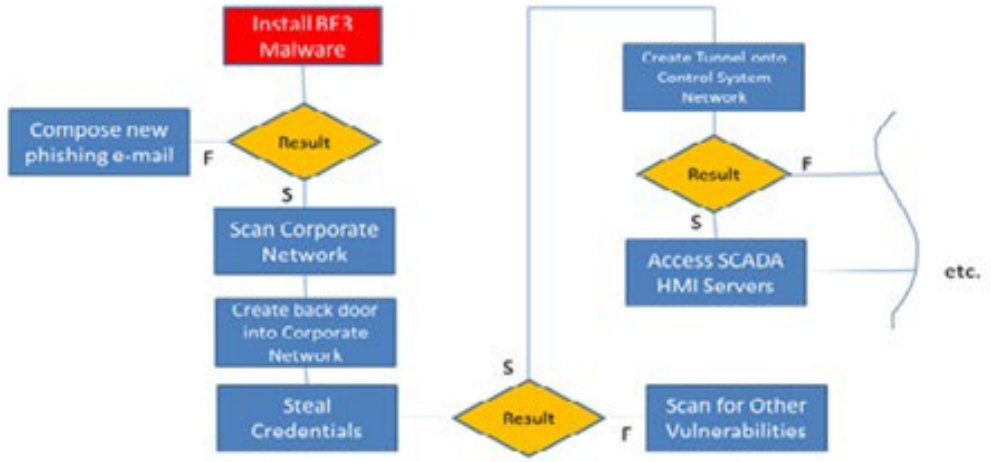


Figure 4: Adaptive Attack Script for Ukraine Attack

EXata provides a convenient Cyber Attack Editor (Figure 6) using which complex adaptive attack scripts, similar to the one shown in Figure 5, can be easily developed.

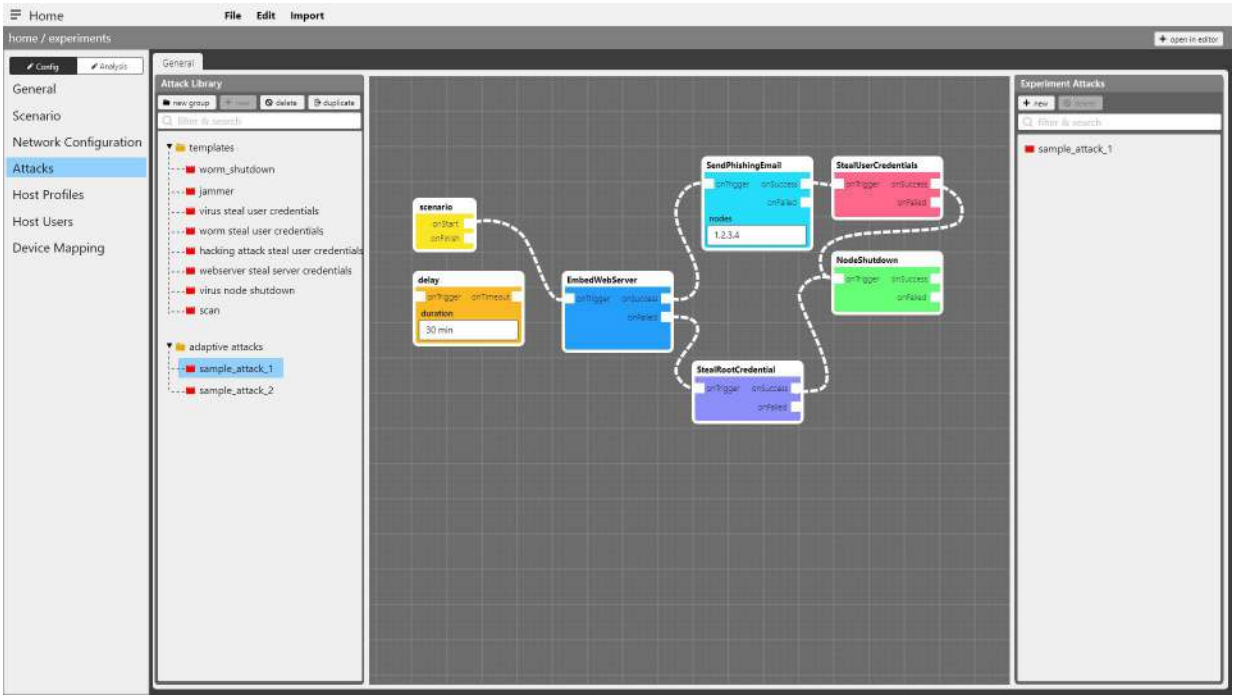


Figure 5: EXata's Cyber Attack Editor

3.4 Analysis of the Ukraine Attack Using EXata

EXata's Ukraine attack model can be used both to gain insight into the actual attack and to derive invaluable lessons to deal with similar future attacks.

Visualization and Human-In-The-Loop (HITL) Interface

The EXata GUI and the companion Scenario Player provide a graphical view of the network state in real time. This visualization is useful to understand the network behavior, including how traffic flows through the network, how malware spreads from host to host, and the cyber state of devices (whether a device is

compromised and to what extent). The EXata GUI and Scenario Player also provide a HITL interface using which an analyst can interact with the network model, while it is running, and launch cyber attacks and configure defenses.

By using the EXata GUI and Scenario Player for visualizing the sequence of steps in the attack, analysts can gain insight into how individual network components (hosts, workstations, servers, firewalls, etc.) and human operators responded to each attack in the sequence and how the network architecture, procedures, and processes enabled the attackers to infiltrate the system and allowed malware to spread. This analysis can help uncover the weaknesses in the system which can be exploited.

The integration with other simulations or live equipment extends the assessment to the impact of the cyber-attacks beyond the typical IT domain to physical systems (e.g., power grids), military missions, systems of systems, etc. For example, EXata can be interfaced with OPAL-RT's HYPERSIM or RT-LAB which models the dynamics of the power grid. Using this integrated capability, the sequence of events and the resulting effects on the power parameters can be visualized. Figure 7 shows the visualization of packets flowing through a power grid network in EXata's Scenario Player. Figure 8 shows how the power supply parameters are displayed in HYPERSIM. When the network is subjected to cyber attacks, the effects can be observed in the changing values of the power supply parameters in HYPRSIM.

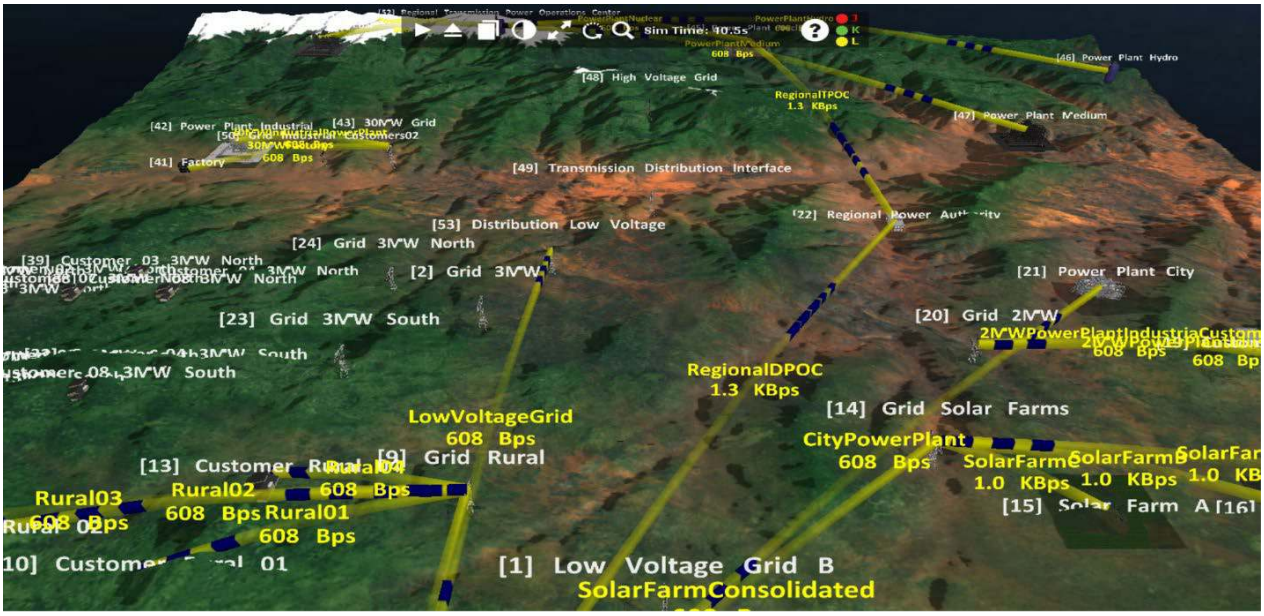


Figure 6: Visualization of Packets Traversing the Power Grid Network in Scenario Player

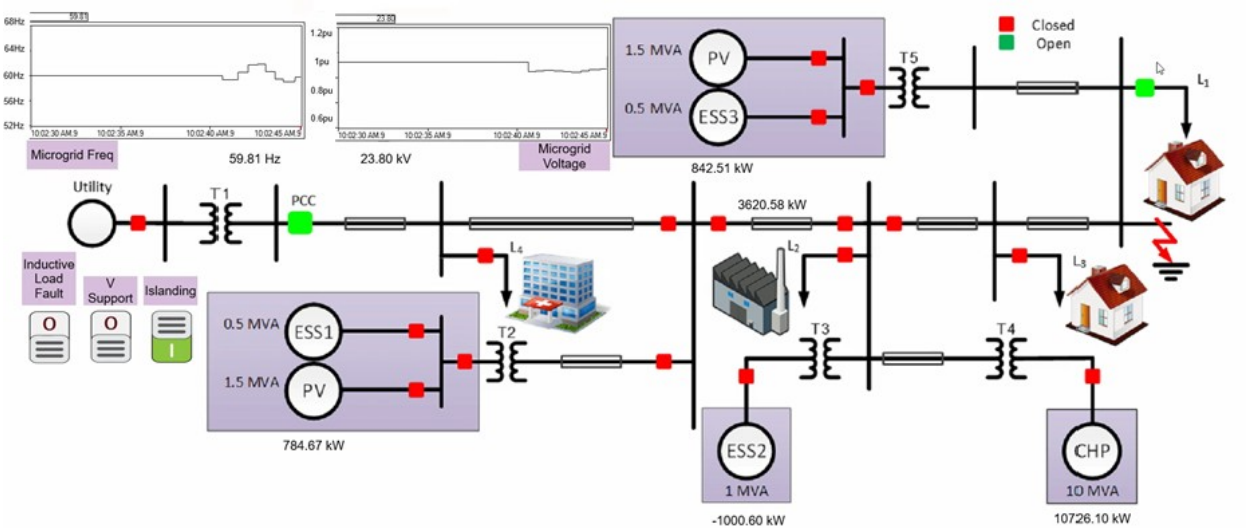


Figure 7: Simulation of a Power Grid in HYPERSIM. The Parameters Displayed in HYPERSIM Are Affected When the Network Is Subjected to Cyber Attacks.

Statistics

EXata collects detailed statistics from a simulation in an SQL database. These statistics can be used to trace the flow of packets through the network and correlate them to network events. This analysis sheds further light on network behavior and helps understand the root cause behind unintended or undesirable outcomes. Some examples of statistics generated by EXata include:

- Firewall statistics:
  - The number of packets inspected and number of packets dropped in the Input chain (packets received by the host)
  - The number of packets inspected and number of packets dropped in the Output chain (packets generated by applications running at the host)
  - The number of packets inspected and number of packets dropped in the Forward chain (packets forwarded by the host)
- IDS statistics, such as the number of signatures learned
- Attack statistics, such as
  - The number of malware propagation attempts made by a host
  - The number of attacks that were successfully launched by a host
  - The number of files infected by successful file attacks on the victim
  - The number of attackers that gained root access at the victim
  - The number of attempts to exploit vulnerabilities at a host which failed due to incorrect access vectors
  - The number of packets which were delayed arriving at the victim

What-if Analysis and Training

The Ukraine attack model can be easily modified to create ‘what-if’ scenarios, for example by changing the firewall rules or changing the network topology and access control rules to better isolate critical segments of the network. These scenarios can be easily simulated and the effects of changes evaluated, by visualization, analyzing statistics, and observing the effects on connected systems. Thus, the effectiveness of different mitigation strategies can be studied.

The visualization capabilities offer a convenient training platform where operators can interact with the simulation model, launch attacks, and modify firewall rules, and observe their effects on the system's behavior in real time. Thus, operators can be trained to recognize breaches and learn how to counter them in a timely manner.

References

[1] David Whitehead, Kevin Owens, Daniel Gammel, and Jess Smith, "*Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies*", Published in *Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions*, 2018.

[2] Robert Lee, Michael Assante, and Tim Conway, "*Analysis of the Cyber Attack on the Ukrainian Power Grid",* https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Additional Resources

- White Paper: Cybersecurity Study of Power System Utilizing Advanced CPS Simulation Tools
- Blog: Securing Cyber-Physical Systems
- Webinar: Innovative Cyber Security Training Using Network Digital Twins