Blockchain as a Solution to Cyber Threats in the Smart Grid of the Future

Jacob Mendel
*Head of the Cyber-Security Track,
Coller School of Management
Tel Aviv University*

The Smart Grid is one of the most critical infrastructure services of today's developed nations, providing electrical service to consumers through two-way digital communications. The system aims to improve supply efficiency and reliability while self-healing glitches and reducing energy consumption and costs. Governments have been working to implement these systems around the world as a step in combatting global warming and for their potential to build energy resilience and independence.

Alongside smart grids and the rise of IoT (Internet of Things) in general, smart meters are becoming widespread as well – in residential, business, and industrial buildings alike. The new smart metering is the gateway between the Smart Grid and our homes or businesses, enabling dynamic pricing and information exchange with smart home devices. In its most basic consumer application, smart meters precisely track all energy consumption and send digital meter readings to energy suppliers for more accurate energy bills.

But no matter how smart they are, smart meters still represent a serious vulnerability to the greater Smart Grid, as they are mostly a kind of interconnected communications hub between the consumers and energy providers that comprise the Grid. Malware in particular is a significant threat, both for the harm it can cause and the challenges in properly addressing it.

The combination of porous devices and the sensitive information flowing through the smart grid has left open an attractive target for malicious cyberattacks. To our collective peril, this security risk is not receiving the treatment it deserves either by cybersecurity industry research or by consumers.

Blockchain as a Solution to Cyber Threats

Smart Grid cybersecurity threats in general can come from a myriad of sources, such as cybercrime, hacking, cyberwar, etc. To mitigate cybersecurity threats, utility companies will need to share and coordinate the exchange of cybersecurity information, like intelligence and vulnerabilities, with governmental agencies and probably with other public and private sector cyber research institutes. This is one of the first places blockchain comes in.

Preventing potential cyberattacks on Smart Grid communication can be done by identifying the number of attacks, of which four have been identified. These include a device attack (aims to compromise a grid device), a data attack (attempts to maliciously insert, alter or delete data or control commands in the network traffic to misguide the Smart Grid, leading it to make wrong decisions/actions), a privacy attack (aims to learn/infer users' private information by analyzing electricity usage data), and a network availability attack (i.e. a DoS Denial of Service).

Each of the above kinds of attacks has different objectives and can often be the building blocks of more sophisticated attacks. This relates to blockchain in several ways:

1.
Attacks on the Smart Grid will likely be more advanced than the traditional attacks on IT/OT infrastructures.

2.
Additionally, for the offense to cause negative system impact, the attacker must also know how to control the cyber aspects to manipulate the physical system – including software vulnerabilities such as buffer overflows, integer overflows, and structured query language –injection.

3.
The fact that the Smart Grid does not use reliable methods to authenticate users is also a unique part of the problem/solution, and a place where blockchain can be uniquely useful. Left unaddressed, such threats may provide an attacker with the ability to bypass the authentication and take control of the Smart Grid network.

The Smart Grid cybersecurity threats – and the ways in which blockchain can be used to remediate a particularly challenging situation – are summarized in the table overleaf. As illustrated, they revolve around knowledge-based remediation (something you know); possession-based remediation (something you have); and biometric-based remediation (something you are).

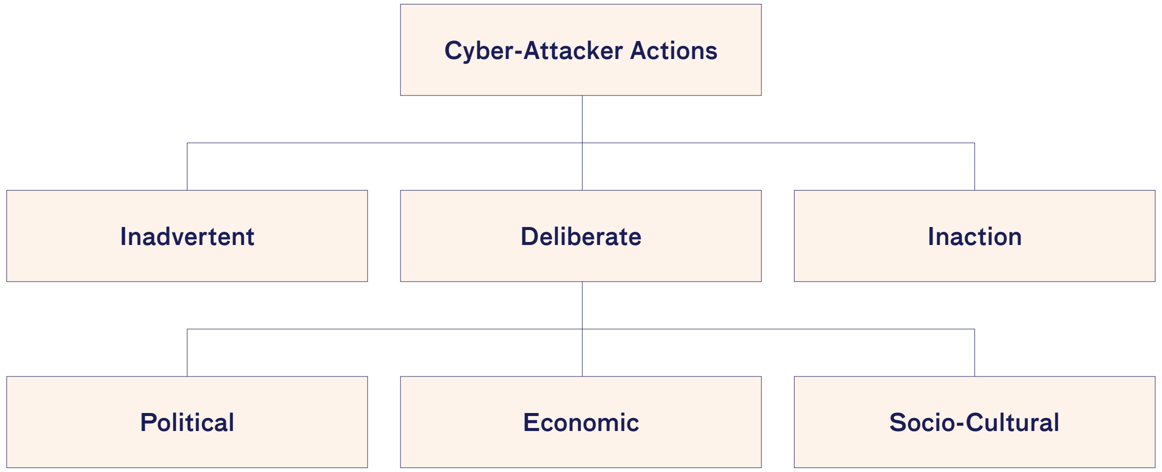
As with other essential infrastructure, blockchain is particularly relevant given that the number of attacks on critical infrastructure is continuously increasing. In this example, any deployment of a Smart Grid without suitable cybersecurity might result in severe consequences, such as grid instability, utility fraud, and the loss of user information and energy consumption data. ➔

Threat	How Blockchain Can Help
Availability	– Anti Denial of Service (DoS) (on an individual device, a group of devices or an entire subnetwork) – Anti communication hijacking/MITM attacks – Anti-jamming – Anti device theft
Integrity	– Help against fraud, stealthy manipulation of critical data such as meter readings, billing information, control commands – Anti-tampering
Personalization requires costly, potentially time-consuming tasks	– Privacy – Avoiding use of power usage data and customer account information – Smart meter aggregation of usage data for billing purposes and to support load-balancing and other monitoring functions – Avoiding backdoors and holes in the network perimeter – Defending database attacks – Protecting the smart meters' data – Preventing spoofing system operators and SCADA devices – Avoiding leakage of sensitive data
Timeliness	– Real-time needs of control systems and responsiveness aspects of the system
Human Machine Interface (HMI)	– Fraudulent information about demand or supply which will create non-existing power flows which may result in blackouts and heavy financial losses
Software Vulnerabilities	– Buffer overflows – Integer overflows – Code behavior analysis – Avoiding changes to the software or modifications to the software configuration settings – Changes in programmable logic in PLCs, RTUs, or other controllers
Authentication	– Password / authentication – Theft identification – Access control

The Psychology of Cyberattacks

The primary concern of companies and organizations are cyberattacks that are deliberate actions. Economic motivation (for example theft of intellectual property or users' private information or credit card information) is one of the most reliable motivations for attacks. By contrast, political and espionage motivations involve, for example, destroying essential web sites, DDOS (Distributed Denial Of Service) attacks, taking control of strategic or symbolic targets, blackouts or making political statements.

Given the range of the above, it is recommended that a new holistic approach be found that would automatically build a malware baseline and the corresponding detection of malicious activities, and that blockchain should be part of such a holistic approach.



A New Holistic Approach

Malware is a newly coined term for malicious software that is intentionally designed to disrupt availability, compromise confidentiality, alter integrity, and cause abusive behaviors. Research studies show that the impact of malware infection often not only leads to loss of privacy and confidentiality of data but also allows hackers to abuse the victim's computational resources when conducting larger-scale cybercrime activities.

Genge, Rusu, and Haller suggested using anomaly detection techniques to identify malware attacks. Their approach automatically generates detection rules for the IDS (Intrusion Detection System), which relies on predictive behavior. Their anomaly detection depends upon the deviation of communication patterns from regular communication. A significant improvement can be achieved by adding network traffic visualization and device identification. Because of malware disguise, multiple layers of defense are recommended, and all

> The Smart Grid is an upgrade on the old electrical power grid, and cybersecurity issues are a real threat

anti-malware efforts should be fully managed and controlled, including continuous patching and updates.

Absent advance-detection, malware advanced enough to attack a smart meter may disturb or influence the smart meter's essential rules such as periodical power consumption registration; private consumer activities, communication with the utility company, the turning of the power on or off to any electronic devices which are connected to the local grid; real-time interaction awareness and management (e.g., load balancing); and automatic switching to an alternative power source like a solar, wind, or alternative-energy storage system.

The malware may also eavesdrop on the home network traffic, which includes: pricing information, control structure, power usage, location information, and private user data.

Conclusion

The Smart Grid is an upgrade on the old electrical power grid, and cybersecurity issues are a real threat. This has led to the proliferation of industrial and academic research aimed at identifying and mitigating cybersecurity threats. This specifically includes advanced malware, which becomes a critical threat to the entire Smart Grid network, including but not limited to ICS (Industrial Control Systems) and critical infrastructures.

Adding encryption and cryptographic signatures to Smart Grid communication protocols is essential to ensure authenticity and integrity, but it will not solve the problem of advanced malware threats. For example, the unknown malicious codes, which are probably encrypted or use various programming obfuscation techniques, can bypass signature-based detection techniques.

> The complexity and heterogeneity of the Smart Grid network – as with other infrastructures – mean there will not be one golden solution, which addresses all cybersecurity threats

The complexity and heterogeneity of the Smart Grid network – as with other infrastructures – mean there will not be one golden solution, which addresses all cybersecurity threats. Blockchain can be a dominant tool in cybersecurity since it offers better methods of protection, and more flexibility, which makes it a robust tool for the changing environment. Blockchain's built-in functions (better encryption, reliability, and traceability) position it against attackers who try to bypass the authentication and take control of the Smart Grid network. Even though blockchain may help to defend many treats, Smart Grid's architecture is complicated and no single tool will protect all potential threats. Therefore, cyber protection in general and smart metering in particular are prominent research challenges and very fruitful research fields for the future.

For future research in the Smart Grid cybersecurity context, future research should also investigate the use of a machine learning-based malware detection system. In particular, it would be interesting to combine machine learning with malware intrusion detection systems (IDS) specially built for Smart Grids. ■

Supplementary references

FF. Skopik, Z. Maa, T. Bleiera, H. Grüneisb, *A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures*, "International Journal of Smart Grid and CleanEnergy" 2012, pp. 22–28, http://www.ijsgce.com/index.php?m=content&c=index&a=show&catid=27&id=16, [12.12.2016].

T. Sato et al., *Smart Grid Standards: Specifications, Requirements, and Technologies*, Wiley, 2015, http://dx.doi.org/10.1002/9781118653722

T. Baars et al.,*Cyber Security in Smart Grid Substations*, Technical ReportUU-CS-2012-017, Department of Information and Computing Sciences, Utrecht University, Utrecht 2012.

E.D. Knapp, J.T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Elsevier, Waltham 2015.

A. Hahn, *Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation*, 2013.

About the Author

Jacob Mendel is the Head of Cyber-Security study at Coller School of Management in Tel Aviv University, and former General Manager Cybersecurity COE at Intel. Mendel holds 16 approved patents in the area of cybersecurity.

Mendel's current main research interest is on the economic perspective of cybersecurity attacks, Blockchain technology with a special focus on cybersecurity attacks, privacy issues and business continuation under cyber-attack.