Cyber Security Challenges for Utilities with the Introduction of AMI

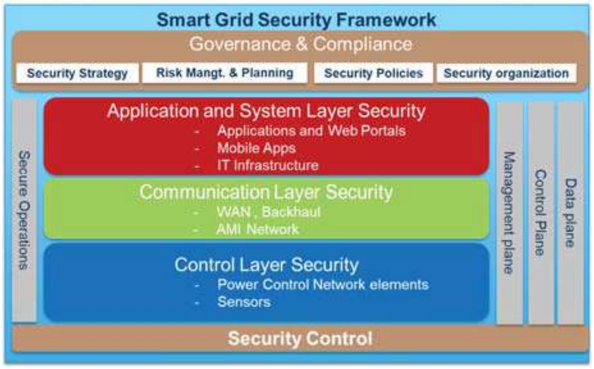
AMI is an important part of the smart grid revolution. AMI has shifted the control to the end-user and at the same time the Intelligence being shifted to millions of end devices, increasing the attack surface and threat vector exponentially. End devices (Meters, Sensors, Home automation hubs) are connected to the untrusted public Internet over wireless networks offering more entry points for an outside attacker. Security breaches are a real and imminent threat to the Utility Sector in the form of -

- Sabotage- Mass cyber-attacks - Spread of worms from meter to meter or the entire network
- Fraud - Exploiting data integrity across meters & other end devices and breaching Privacy of user data.

Cyber Security was identified as a Tier 1 threat in the 2010 National Security Strategy, alongside Terrorism, War, and Natural Disasters by UK government[1].

The consequences of a cyber-attack can be devastating: blackouts across the entire country, access to power plants, and personal data breaches. For device makers and Utilities, the loss of customers, reputation, and revenue can be difficult to recover. Lack of customer confidence and privacy may impede AMI progress and Data Management will become a bigger near-term challenge. The deployment and maintenance of a large number of AMI elements, over many years, require an appropriate level of security definitions. End-consumers and Utilities need to remain confident in the security of such infrastructure.

Security recommendations should become part of a common AMI Security framework for Utilities. In past few years, some standardization has been done for Electricity Smart Metering in the country - Standards like IS-15959 and IS-16444 define the means to interact with each meter to extract securely metering data, but granular level requirements still are to be defined to guarantee the efficient and secure end-to-end traffic between each meter and the HES over wireless networks.



There is a great focus on Application and System layer security - servers and the overall business applications running in data-center are better secured as part of Application Security Assurance. There must be equal emphasis on the security consideration for communication layer security - intermediate devices and AMI last mile wireless communication network. One of the objectives of this document is to highlight some of the key considerations to secure the data communication between end devices and the server

1 [1] https://www.gchq.gov.uk/information/cyber-threat

level HES applications, specifically when using wireless networks.

Standard IP based wireless Network

One of the key factors for security consideration for AMI is an end-to-end IP-based last mile wireless network infrastructure to take full advantage of years of IP technology development. Intellectual property conditions for IP networking technology are more favorable or at least better understood than proprietary and newer solutions.

Standards Wireless network like IEEE 802.15.4-6LoWPAN mesh networks transparently extend the reach of the Internet Protocol (IP) into devices and is most widely used for connectivity for critical AMI infrastructure like smart metering. 6LoWPAN protocol makes use of most of the Internet application protocols and tools already developed for IP networks like SNMP, NTP, UDP, TCP, ICMP, DNS, etc.

In 6LoWPAN, network elements are identified by unique IPv6 addresses by introducing the adaption layer between IP stack's link and network layer to enable transmission of IPv6 datagrams over IEEE 802.15.4 radio links similar to a standard IP network, thereby flattening the hierarchy and simplify the connectivity model and simpler gateway routers. Further, IPv6RPL and 6LoWPAN mesh seamlessly extends the devices reach and provides improved reliability through path diversity- self configuring and self-healing

End-To-End security model

An End to End security model for large scale AMI deployments shall greatly limit any large-scale attack where thousands of devices could be compromised. From AMI perspective the term End to End covers device-level security, Cryptography, Key negotiations, Network level security as well as Head End System level security. Any such security model shall include the following properties:

- Authorization: Only authorized devices can join the network
- Authentication: Only properly authenticated devices can interact with the Head End System
- Encryption: Data in-flight must be signed and encrypted to guarantee the integrity and no tampering once the data is extracted from a device until that same data gets delivered into the Head End System (HES) in the back-end.

These security requirements translate into the use of Standard-based security network protocols and the storage of security credentials in individual components of AMI infrastructure. In an End-To-End security model for authorization, authentication and encryption, security credentials (keys, passwords, hashes, etc.) shall be maintained in end devices as well as within the HES. Any network equipment on the data path, which only forward payloads between the device and the HES is much less of a concern here.

This default End-to-End Security model does eliminate any kind of concentration of security credentials in one single network device. With this model, an attacker would have to break into one thousand meters to compromise one thousand meters and would not be able to achieve the same by only breaking into one single network element.

Security credentials stored in the HES are protected because of the physical isolation & access control provided by a data center. Other standard secure designs such as the use of HSMs (Hardware Secure Modules) provide an extra layer of protection of those security credentials in a HES.

To achieve both authentication and encryption of the end-to-end data path between the HES and each end device, two types of security credentials can be considered:

- Pre-shared keys
- Public Key Infrastructure (PKI)

Pre-shared keys are not supposed to be transmitted over the air at any time and are unique passwords provisioned in each device that needs to match that same password present in the HES. This symmetrical cryptography is simple but requires that every pre-shared key be provisioned on the enterprise side (HES).

Another type of cryptography (called asymmetrical cryptography) is recommended for any large AMI roll-out. In this model, a Certificate Authority (CA) is first assigned with its unique public/private key pair for this roll-out. Then each device is provisioned with a unique

X509 certificate (public key) and a matching password (private key) during production.

A Public Key Infrastructure supports robust cipher suites, the same way the ubiquitous HTTPs secure all Web Transactions on the Internet today. Public Key Infrastructure (PKI) with a unique certificate associated with each device provides the ability to black-list or white-list any single device to deliver a security model equivalent to the HTTPS protocol used by end-consumers to browse their bank account over the web.

Once the device provisioning is completed during production, the public/private key pair of the HES server certificate and the public key of the certificate authority (CA) is the only security credentials required to set up secure sessions with millions of end devices. PKI based end-to-end security model is recommended for any large-scale AMI deployment to combine security with ease and speed.

Latency & Throughput

The wireless network selected for last-mile communication must have a built-in feature to support full-duplex mode with a good throughput path and low latency for reliable security algorithm negotiation / key negotiation as well as delivery of the commands.

The wireless communication network must have adequate effective bandwidth and broadcast capabilities to be able to successfully distribute security algorithms, upgrade keys, complete the firmware update of a large population of network elements and end devices reliably in the shortest possible time (possibly in few hours). This will ensure the longevity of system/devices and add resilience against a new vulnerability

No Untrusted Elements

Any disruption of the flow of data or insidious tampering of data in transit would have vicious consequences if perpetrated by unfriendly/rogue entities. The network devices from untrusted sources may carry malware which helps them spying, or worse, to shut down communications or the potential damage the electrical devices in the event of a cyberwar.

This is not a matter of “if” but “when” such an attack will occur. The solution to address this threat is to reduce the risk by minimizing the attack surface by removing untrusted elements from such a critical network. Our country needs to prepare to secure from hacking and infiltration into the smart grid communication networks from such bad players. The safest way is the exclusion of untrusted components from our critical AMI Infrastructure.

Conclusion

The risk of cyber threat to AMI at present is moderate to low primarily due to the low installed base. However, as the benefit of AMI system remain attractive the scenario will change in future with the increased rollout.

Overall, the Smart Grid infrastructure aims to improve the reliability and efficiency of the electrical grid by lowering the cost of distribution and generation. It is essential to implement the necessary security measures and adopt industry best practices to help build attack resistant smart grid infrastructure.

A national level statutory body must get authorized to evaluate, issue guidelines for standardization and certification for AMI security similar in line with the IT Products as per Common Criteria Standards done by STQC. http://stqc.gov.in/content/common-criteria-certification

National Institute of Standards and Technology (NIST) https://www.nist.gov/publications/cybersecurity-framework-smart-grid-profile , European Network and Information Security Agency (ENISA) https://www.enisa.europa.eu/ have developed guidelines for smart grid cybersecurity, which can be taken into consideration while developing a cohesive cyber strategy for India.

An approach document towards planning security strategy for Smart Grid will be the starting point to build a common security framework and this activity must commence without losing any more time.

Until the common framework and regulatory requirements / guidelines for smart grid security are accurately worked by the standardisation bodies , Utilities must proceed with caution while comparing and selecting technologies for their AMI projects ,understand security risks and plan for effective remediation for future Regulatory compliance requirement and safeguard their invetments. ■

Gautam Kumar

Chief Operating Officer CyanConnode Private Limited
and Co-author- Nitin Chittora, Developmeny Manager
CyanConnode Private Limited