Smart Objects: Security Challenges from the Power Sector

Barbara Fraser, Paul Duffy, and Maik Seewald, Cisco Systems, Inc.

The electric power grid is undergoing a transformation, often referred to as the evolving smart grid. A number of aspects of this ongoing transformation should inform discussions surrounding evolving security technologies for the more general Smart Objects dialog. Each will be briefly described below. This is not intended to be a comprehensive survey, rather to stimulate discussion.

First, technologies tend to live for long periods of time in the power grid. This means there will always be legacy technologies in active use alongside more contemporary technologies. This suggests that ideally security mechanisms are needed that can be used in both environments. The deployment scenarios should support security provided at various layers in the Internet stack, while allowing for uniform management.

Legacy technology often doesn't have the resources, in processing or memory, to support strong security mechanisms. This also means there is likely no secure storage for keys, certificates, etc. Sadly, this is also true of some of the newer products. There are newer meters have as little as 5K in the HAN processor only. It's likely we'll continue to have resource limitations in some devices so lightweight security protocols are needed.

Legacy devices are often deployed in remote scenarios/installations. Shared passwords are often in use for access via HMI. Remote installations are also often equipped with unsecure dial-up solutions.

Not surprisingly, legacy devices are usually not designed for patch management. Vulnerabilities may exist for critical components deployed in the field until the component itself is replaced, which could take 10s of years. Consequently, it will continue to be important to provide protections against attacks against those weaknesses.

Second, power sector applications have varying latency requirements, and maintaining reliability (and safety) is the top priority. Therefore, security mechanisms are needed that can operate within the latency restrictions. They can't be allowed to cause unreliability and safety issues.

Third, the proliferation of smart meters means millions; even tens of millions of meters will be deployed so scaling is critically important. These millions of endpoint meters need a confidentiality protection, which has implications on the aggregation

points and the control center. Management of addresses for these tunnels as well as the setup demands of traditional IPSec deployments is challenging. Exploration of use of dynamic configuration at scale is needed as well as lighter weight technologies. More generally, secured zero touch deployment (ZTD) is a critical feature in these environments. To further highlight this need is an overview of the management and security operations supporting the deployment lifecycle of Field Area Network (FAN) elements.

1.1 Day -1 (pre-deploy)

- Manufacture-time generation and placement of security credentials onto the element. IEEE 802.1AR etc.
- Depot placement of "call home" configuration upon the element (near-zero-touch deployment, optional).

1.2 Day 0 (initial deployment/reboot)

The steps below are collectively referred to as zero touch deployment (ZTD).

- Secure authentication of element to the access (L2) network.
- Element joins the access network.
- L2 connection is secured.
- Automatic population of element into FAN asset inventory and appropriate element groupings.
- IP address acquisition (assuming IPv6 ... DHCPV6 or SLAAC).
- Discovery of required services (time, configuration, applications, etc).
- Mutual authentication elements/service(s).
- Element acquires time.
- Element acquires configuration.
- Element acquires required firmware.
- Element acquires required applications.

Element is now "live" on the network.

1.3 Day 1+

Operations performed on a scheduled or intermittent basis…

- Monitoring of element status (push or pull … push highly preferred for scale reasons), comparison and trending versus thresholds, alerting out of bounds conditions, etc.
- Configuration updates.
- Firmware updates.
- Revocation/update of security credentials
- Processing asynchronous element alarms into root cause faults.

Summary

The power grid environment is but one use case where there will be huge numbers of low-resourced elements, often in contexts where there are ancient and new

technologies deployed side by side. To secure this environment, we need security technologies with the following characteristics:

- Small footprint and low processing overhead
- Latency sensitivity
- Scalability
- Manageability and zero touch deployment
- Agile deployment of mechanisms at different layers of the Internet stack, and both on-device and within the network