PROTECTING UTILITIES FROM CYBER SECURITY RISKS INTRODUCED BY SMART METERS

News / Manufacturer

Information security is a growing concern for utilities in Europe, as they deal with myriad data from their smart meters, operations, customers and the power grid.

Technology and data have completely transformed the power and utilities sector, allowing companies to use information to improve and expand services, and better engage with customers. Smart meters have played a key part in this growth for utilities. However, large data volumes also bring added and sometimes regulatory obligations around security and privacy — and the risk that sensitive data could be subject to increasingly clever cyber threats. Most utilities understand and recognise the potential cyber security risks smart meters present, but not all have the infrastructure in place to detect and respond to cyber security incidents effectively.

See original image

Image credit: Image courtesy of Unknown

What are the potential threats?

There are many different levels of potential threats that can arise from a number of different sources worldwide. These include threats from “typical” hackers outside the organisation, ethical or non-ethical, who simply want to prove that smart metering is insecure, or have the motivation to exploit companies for monetary gain. Similarly, the utility itself can be at risk from a disgruntled employee or an unhappy customer.

Some of the threats to meters include the potential to reverse engineer communications that occur between the meter and the utility, modifying the meter software or communication so that it reports incorrect energy usage, or the threat of having a meter remotely disconnected by someone other than the utility. From a security point of view, any of the above threats are equal in severity. There is no more or less, a company is either secure or not. They should be prepared to take measures - at any level and against any threat.

What is the driving force?

Data privacy and security are significant concerns for governments in the EU. Some of the larger smart meter roll-outs have been slowed down or halted for security reasons, for example in both The Netherlands and Germany where the governments have been implementing cyber security rules.

The utility is a key life-line of the country and its economy. Security breaches can potentially be catastrophic and destabilize the operation of the utility, including the loss of revenue, damaged reputation, and diminished brand value.

Security is vital for the stable operation of the economy and countries as a whole. Individual states seek to safeguard their “digital sovereignty and integrity” just as they do their territorial sovereignty and integrity.

Why are utilities hesitant to implement smart meter technology?

Smart meters can add to the complexity utilities already face in protecting their organization’s systems and data from potential cyber threats. The additional data that smart meters collect and send to the utility needs to be protected from the time it’s created within the smart meter until it’s used by the utility. Communications have to be secure, the systems in which the data resides have to be secure and there need to be clear processes for handling that data in a secure fashion.

Managing this cyber security risk is not just about adding a server, it is about changing the organisation culturally so that it thinks, acts and reacts in a more secure way.

In order to secure meters, a security infrastructure needs to be in place. This is where a utility should count on its smart meter supplier to provide the necessary infrastructure components, such as certificate policies, security baseline documents, how meters receive keys, how they are changed, and how they are destroyed.

Can regulations help?

Yes. Security requirements and regulations are becoming more compulsory worldwide, similar to other aspects of utility operations, which are helping to drive better security practices.

European governments are very concerned about privacy and security. They will impose security to a fairly deep level of detail or will demand that the utility industry, vendor or standardization committee proves to which security standard they adhere. There are many examples of “security

rulings", such as the specification by the German Federal Office for Information Security, which has a major impact on the utility industry in Germany and throughout Europe.

There are other standardization initiatives to which utilities will refer if a vendor wants to be compliant when tendering: such as DLMS standardization with its different "coloured books" (e.g. green book on protocol and system architecture and blue book on the interface classes and object identification…) or G3 PLC, which has detailed and specific sections on security,. Lastly, there are supra-national initiatives, such as the European Network for Cyber Security (ENCS). Founded in 2012, ENCS is a non-profit organisation that brings together critical infrastructure stakeholders and security experts to deploy secure European-critical energy grids and infrastructure. There is also the European Union Agency for Network and Information Security (ENISA), which issues recommendations on technical issues such as the validity of algorithms and key sizes.

What measures can utilities take to prevent incidents?

Looking at the different potential threats, cyber security needs a holistic approach. Utilities need to look at the complete solution and its processes, the overall system architecture and its system components, and sub-components.

There are two aspects of a holistic solution secrecy and trust. Secrecy is about ensuring that information cannot be retrieved or read by unauthorized parties. Trust is about being sure that the sender and the recipient of information are really the actor that you suppose them to be.

This can be translated back to smart meters; for example, they need to be sure that when a breaker command is sent to a meter, it is being sent by an authorized sender. Also, they need to be sure that the metering data that's retrieved, is not altered to reduce or increase the bill, or in the case of sub-station monitoring, data alteration to create a system or market imbalance.

At the very core of today's systems for smart meter security are secret keys (to encrypt and authenticate). These are used to verify identity and authenticity and protect confidentiality. Keys can be shared or be private/public, and they can have specific purposes such as key generation, authentication, encryption, storage, etc. Shared keys are used in symmetric security and its cryptographic algorithms; private/public keys, with certificates are used in asymmetric security and its algorithms to e.g. generate keys, or support digital signing.

Whether it's private/public or shared, keys that are used extensively throughout the whole metering solution, can become complex to manage, or difficult to securely store. So utilities do have options to secure their operations, and Honeywell has developed solutions and methodologies together with their partner Worldline, to help utilities implement security of the smart meters.

Essentially, you can't talk measures without keys (shared or private/public). For more critical processes, like switching a meter on/off, load limiting it, or updating its firmware, most utilities will opt for asymmetric security, allowing digital signing of the commands to execute the critical process.

An end-to-end security solution

Honeywell has teamed up with Worldline to provide a comprehensive, end-to-end (E2E) security solution for smart meters and their connections to utilities. Worldline is well-known for security solutions and is the market leader in Europe in securing transactions across many industries. Their solutions have millions of highly critical transactions running. With them, Honeywell has developed

a solution that enables utilities to use and manage keys and certificates in a performant and scalable manner. This solution spans the complete lifecycle of typical utility components, such as meters, data concentrators and backend systems, and it covers all processes involved, from manufacturer to utility to customer. From installation, read-out and remote and local troubleshooting to recycling and destruction of the meters.

The solution is not communication technology-specific, and is wireless through GPRS or G3 PLC. However, it goes well beyond technology and code; the Honeywell solution supports the utility in shaping and implementing proper security processes for implementing their smart meters, laying the foundation in a security baseline document with detailed process mapping, organisation structure, repair and replacement, such as key custodians, etc.

The solution has specific key storage components, also known as Hardware Security Modules, for securely storing keys, and specific key management software guaranteeing secure business operation, using private/public and shared keys in encryption, authentication, digital signing of commands and files, or generating and exchanging keys. It also supports and includes a Public Key Infrastructure (PKI) offering, to securely manage certificates; covering e.g. a certification authority (CA), registration authority (RA), etc.

As such, the solution manages trust relationships for operations between all system components: in the backend, between and amongst backend and field components like gas and electricity meters, meters and concentrators, concentrators and servers, servers and meters. It manages trust relationships for onsite operations, between customers, technicians and system components, including laptops, hand-held units and meters, concentrators, and technicians. Lastly it also supports trust relationships in factory operations, between the factory, meters, concentrators and their firmware e.g.

The Honeywell solution is compliant with DLMS security suites 0, 1 and 2, and therefore supports for example HLS6 and 7 mechanisms. DLMS Suite 0 is used at a major customer in the Netherlands, and Honeywell also has a couple of new implementations ongoing where Suite 1 & 2 are applied, or prepared to be used in the near future.

The benefits of the solution are:

- Less complexity: the system manages and uses keys and certificates, allows for high levels of automation in key management.
- Performance and scalability, e.g.:
    - About 6900 decryption operations (AES-256, GCM) per second
    - 2.9 million smart meter communication sessions are securely served in 3600 seconds

In practice

For a Dutch utility, Honeywell has implemented the key storage components (hardware security modules) and processes, and integrated it with its smart metering solution to cover all of the processes mentioned earlier; from shipping meters into the warehouse, sending them with technicians into the fields with installation, remote and secure readout. The solution can be retrofitted to an existing system, it is a standard solution applied by utilities on their metering operation and its roll out.

Utilities must increase their efforts to implement and improve their security programs against cyber intrusion. A fully integrated, E2E information security program will enhance a company’s defences against potential cyber-attacks and help protect it from potential reputational damage, regulatory

action or higher costs over the long term.

17 DECEMBER 2016

ARTICLE LINK:
https://50skyshades.com/index.php/news/manufacturer/protecting-utilities-from-cyber-security-risks-introduced-by-smart-meters