Smart Meter Security Infrastructure: Some Observations

Jan Sanders*
RVS Group, Faculty of Technology, University of Bielefeld

RVS White Paper 5

May 14, 2012 (minor revisions December 2013)

Attacker's Motivation

1 An attacker who is interested in violating the privacy of others can use Smart Metering data to infer otherwise-private life-style details of the Smart Meter user.

2 An attacker who can issue unauthorized control commands to a Smart Meter has the same degree of control as the utility company. Depending on the capability of the device, such an attacker can reset a Smart Meter, cut off electricity supply, access Smart Grid nodes via the Smart Meter, or pretend electricity use that is other than the actual use.

3 An attacker who can influence the clock of a Smart Meter can regularly use off-peak tariffs and thereby reduce the electricity bill amount.

4 Computer-based attacks are easily automated and distributed, even those which require a high level of sophistication and resources to develop initially. Attackers with limited technical sophistication can perform sophisticated attacks using such packages.

5 Utility companies must prepare for large scale failure of Smart Grid nodes. There must be fallback strategies in place to continue with electricity delivery in the face of such large-scale failures. Loss of an accounting/metering system should not lead to the loss of electricity delivery.

*Current address: Dr.-Ing. Jan Sanders, BSI, Godesberger Allee 185-189, D-53175 Bonn. BSI is the German Federal Agency for Security in Information Technology. Email: Jan@RVS.Uni-Bielefeld.de

6 Repeated attacks on Smart Meters undermine the trust bestowed on the devices by consumers. In the long run, insufficiencies in securing Smart Meters may influence case law to the disadvantage of utility companies.

Securing Smart Meter Infrastructure

7 A Smart Meter must be physically secure from possible attackers.

8 Smart Meter communications channels, e.g. sending usage data or receiving control commands, must be secure: that is, specifically, content must neither be observable nor forgeable. This is only possible using cryptographic methods if there is no dedicated, surveillance-proof channel.

9 The only way currently to secure such a large amount of devices is through a Public-Key Infrastructure (PKI).

10 Keys do not have to be installed beforehand as long as current and valid Certificates are present on the device and the Smart Meters have the capability to generate keys.

11 Prior to installation at the operational site each Smart Meter can be configured with a valid, current and non-compromised certificate. If absolutely needed, keys may be installed at the same time.

Ways to Compromise

12 To compromise keys or certificates:

12.1 A malicious insider gains access to part of the certificate chain.

12.2 A malicious customer gains physical access to the Smart Meter hardware.

13 Depending on the quality of a Smart Meter's entropy source and/or time source and chattiness, statistical attacks can be run against observed and encrypted communication.

Regaining Control after Compromise

14 A compromised communications channel means that both endpoints must be considered compromised if there are no special precautions that isolate Smart Grid nodes from compromised nodes. To clean a compromised Smart Meter and contain the threat:

14.1 The compromised device must be identified as such. Other nodes must only communicate with a compromised node if it is assured that contagion (spreading the compromise to a "clean" –known to be non-compromised– node) is not possible.

14.2 All keys and certificates of compromised devices must be revoked.

14.3 A compromised device must either be substituted with another clean device or completely cleaned and reinstalled. This not only includes all keys and certificates but also operating systems, software and firmware.

15 Revocation of keys and certificates and substitution of hard- and software must be performed by trustworthy personnel. In the absence of a guaranteed-secure connection, this must be done on site.

16 Procedures for the continuing operation of compromised Smart Meters must be devised.

17 Who will bear the obligation of proof in case of unwanted Smart Meter behaviour? This will have considerable effect on the security-economics of Smart Meters.

18 Certificate-issuing can be delegated. Containment of attacks can be improved by delegation, but at the cost of an increase in infrastructure complexity. Increasing complexity itself opens vulnerabilities, because infrastructure is only as strong as its weakest link. This is a trade off between amount of damage and likelihood of compromise.