Das Spider-Projekt

Sicherstellen der Geräteintegrität in Smart-Meter-Umgebungen

Kai-Oliver Detken

Die sichere Datenübertragung zwischen den Steuerkomponenten künftiger, intelligenter Energienetze ist zwingend notwendig, um die Anforderungen an die Stabilität und Sicherheit erfüllen zu können. Hierfür wurden Sicherheitsvorgaben vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bezug auf eine zentrale Kommunikationseinheit zur Sicherung intelligenter Energienetze, das sog. Smart Meter Gateway (SMGW), entwickelt. Das Forschungsprojekt Spider berücksichtigte diese Vorgaben bei der Entwicklung eines SMGW und erhöhte zusätzlich den Integritätsschutz.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Von der North American Electric Reliability Corporation wurden Standards entwickelt, die die Sicherheitsprobleme in Smart-Meter-Umgebungen berücksichtigen. Dazu gehört, dass Smart Grids eine bessere Integration der digitalen Geräte in den Schaltanlagen, den vermehrten Einsatz von Sensoren und weitere Regelungsschichten bieten müssen. Letztere haben allerdings ihre eigenen Sicherheitsanforderungen und benötigen daher eine eigene umfassende, integrierte Sicherheitsbetrachtung.
Die Herausforderungen für diese Entwicklung sind nicht nur technischer und wirtschaftlicher, sondern auch organisatorischer Natur. Komponenten eines Smart Grid und IT-Systeme müssen in die Lage versetzt werden, Einbruchsversuche zu erkennen, zu melden und bereits autonom darauf zu reagieren, so dass mögliche Auswirkungen minimiert werden. Um die Verlässlichkeit des Gesamtsystems sicherzustellen, ist daher eine sichere Implementierung der lokalen Systeme unverzichtbar. Zudem werden Teile der elementaren Steuertechnik in den direkten physischen Einflussbereich der Endkunden verlagert.
Anforderungen an die IT-Sicherheit in Smart Grids sollten daher sein:

- Zwingend notwendig ist eine unverfälschte Messung der Systemintegrität von Smart-Grid-Komponenten.
- Attestation: Die Gefährdung des Systems durch den Einsatz von verfälschten bzw. manipulierten Systemen sollte bei Smart Grids ausgeschlossen werden. Dazu ist eine starke Authentifizierung notwendig, um eine zertifizierte Aussage über die Integrität eines Computersystems vornehmen zu können.

Beiden Forderungen könnte mit dem Trusted-Computing-Ansatz entsprochen werden, um die von einem TPM-Chip generierten Messwerte des Systemzustands vertrauenswürdig an eine entfernte Entität (z.B. Server) zu übermitteln.
Leider wurden solche Überlegung bisher nicht ausreichend in die Planung von Smart Grids einbezogen. Energieerzeuger neigen dazu, die Sicherheitsthematik zu unterschätzen. Nichtsdestotrotz muss sie umgesetzt werden.

Das Spider-Projekt

Das BMWI-Projekt Spider (Sichere Powerline-Datenkommunikation im intelligenten Energienetz) nahm seine Arbeit im März 2013 seine Arbeiten auf. Beteiligt waren Industriefirmen und deutsche Forschungseinrichtungen, als assoziierte Partner wurden Energieversorger sowie ein Chiphersteller mit einbezogen. Sein Ziel war die Entwicklung eines SMGW-Prototyps, der den BSI-Sicherheitsanforderungen genügt. Dabei mussten auch die Interessen verschiedener externer Marktteilnehmer (EMT) wie z.B. Messstellen- und Verteilnetzbetreiber, Messdienstleister, Lieferanten und SMGW-Administratoren (GWA) in einem Smart-Grid-Szenario berücksichtigt werden. Denn die Sicherheit und Stabilität künftiger, intelligenter Energienetze hängt maßgebend von einer sicheren Datenübertragung zwischen diesen Teilnehmern sowie den eingesetzten Steuerkomponenten ab. Das BSI definierte deshalb eine Architektur, die neben den eigentlichen intelligenten Messsystemen eine lokale Kommunikationseinheit (SMGW) zum Schutz dieser Messsysteme und deren -daten vorsieht. Sie bilden zusammen die Basis eines Smart-Metering-Systems.
Das SMGW ist die zentrale Instanz. Es besitzt die Logik zur verlässlichen Verarbeitung und sicheren Speicherung der Messdaten und soll die sichere Datenübertragung zwischen den einzelnen Teilnehmern in den angeschlossenen Netzen ermöglichen. Gemäß BSI sind das folgende Netzbereiche:

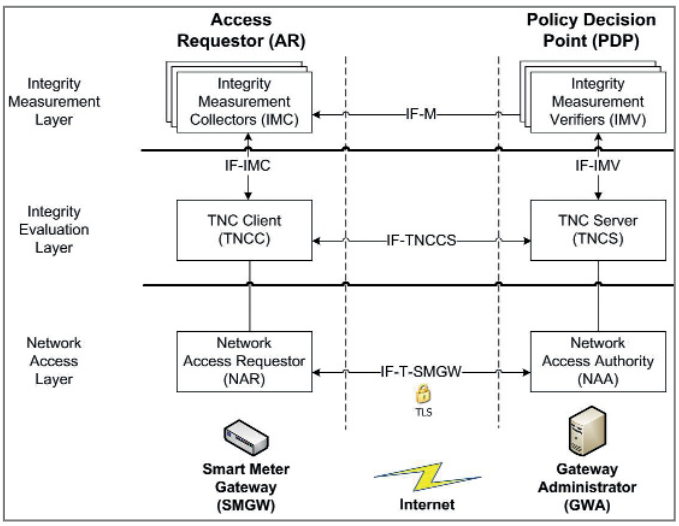

Bild 1: TNC-Schichtenmodell mit SMGW-Komponenten

- Local Metrological Network: lokale Anbindung von Strom-, Gas- oder Wasserzähler der Endnutzer (Letztverbraucher – LV);
- Home Area Network: lokale Anbindung und Steuerung von Energieerzeugern und -verbrauchern der LV sowie zur Informationsbereitstellung für LV und technisches Betreiberpersonal;
- Wide Area Network: zur Anbindung des GWA für die SMGW-Verwaltung und autorisierter Dritter (EMT) zur Datenvermittlung.

Das SMGW erfüllt zudem die Funktion einer Firewall zur Separierung dieser Netze und deren Teilnehmer. Neben dieser logischen Trennung sind die Schnittstellen im SMGW zusätzlich physisch voneinander getrennt.

Einsatz von Trusted Computing

Trusted Computing (TC) ist eine Technik, die von der Trusted Computing Group (TCG) spezifiziert wurde und die Kontrolle von Hard- und Softwarekomponenten ermöglicht. Mit ihrer Hilfe kann bei Rechnersystemplattformen wirkungsvoll nachgewiesen werden, dass die Basis eines Gerätes noch nicht kompromittiert worden ist. Hierdurch lassen sich u.a. externe Softwareangriffe, aber auch Veränderungen der Konfiguration, Sicherheitslücken oder schadhafte Anwendungsprogramme ausmachen.

Um die Integrität der SMGW-Komponente zu erhöhen, wurde daher im Spider-Projekt von Anfang an über den TC-Einsatz nachgedacht. Dabei wurden zunächst das Verfahren selbst untersucht und die Einsatzmöglichkeiten mit den BSI-Spezifikationen verglichen, um ein geeignetes Sicherheitskonzept zu definieren und abschließend ein Secure-Boot-Verfahren umzusetzen.

Bei Spider wurde der Boot-Prozess als eine Abfolge von Bootstrap-Modulen umgesetzt, die direkt miteinander verknüpft sind: Das Bootstrap-Modul Root of Trust bildet den Ausgangspunkt des Boot-Prozesses und ist als eigenständiges Hardwaremodul besonders geschützt. Erst wenn alle Module geladen sind, ist das SMGW funktionsbereit. Schlägt zwischenzeitlich eine Prüfung fehl, wird der Boot-Vorgang sofort unterbrochen und das System geht in einen Fehlerzustand über.

Die Spezifikationen der TCG können in verschiedene Arbeitsgruppen unterteilt werden. Ein Schwerpunkt ist sicherlich das Trusted Platform Module (TPM) inkl. der Sicherheitselemente. Letztere sind in der TNC-Architektur (Trusted Network Connect) wiederzufinden, die eine Erweiterung der bisherigen Sicherheitsprotokolle darstellt. Zudem definiert TNC ein Konzept von Metadata Access Points.

Trusted Network Connect

Der Fokus bei der TNC-Umsetzung lag im Spider-Projekt in der Ergänzung der BSI-Vorgaben durch die Integritätssicherung, während die Authentifizierung nach bestehenden BSI-Vorgaben realisiert wurde.

Das *Bild* zeigt das SMGW in der TNC-Umgebung als Network Access Requestor (NAR) und den GWA als Network Access Authority (NAA). Der GWA befindet sich beim Energieversorger und muss das SMGW von außen (über einen sog. Wakeup-Call) zum Auslesen von Messwerten und Abfragen des Integritätsstands kontaktieren können.

Der Integrity Measurement Collector (IMC) wertet softwarebasiert Sicherheitsaspekte aus, die die Integrität des SMGWs messbar machen. Hierfür sind Hash-Summen vorgesehen, die periodisch über ausgesuchte Komponenten gebildet werden. Die Messwerte werden auf Dateiebene gespeichert und vor Veränderungen geschützt.

Da die Dateisystemrechte auf Kernelebene geprüft werden, sind die Zugangsrechte nur schwer auszuhebeln.

Im Sinne von TNC übermittelt der IMC die Messwerte zur Attestierung an den Integrity Measurement Verifier (IMV). TNC-Client und -Server sind für die Kommunikation und die Reaktion auf die Ergebnisse der Attestierung zuständig. Bei negativen Ergebnissen muss zusätzlich der GWA eingreifen. Leider konnte bisher kein TPM-Chip implementiert werden.

Fazit

Die relevanten Aspekte zur Verbesserung des Sicherheitsgrades durch Trusted Computing sind die Integritätsmessung am SMGW und die damit verbundene Attestierung der Messwerte beim GWA in Verbindung mit TNC. Es ist hierbei besonders wichtig, die Integritätsmessung sicher durchzuführen, damit ein Vertrauen in die Messwerte möglich ist. Die Einbettung von Trusted-Computing-Mechanismen ohne TPM erfüllt diese Anforderung bereits, indem eine eindeutige Vertrauenskette erzeugt wird. Hierzu werden Integritätsmessungen während des Boot-Vorgangs sowie zur Laufzeit eingesetzt und die Messwerte zu den Hard- und Softwarekomponenten manipulationssicher gespeichert.

Noch in diesem Jahr wollen nornehmlich die an dem Spider-Projekt beteiligten Industriepartner ein BSI-zertifiziertes SMGW im Hutschienenformat auf den Markt bringen. Auch andere Konsortien entwickeln derzeit SMGW-Komponenten, um fristgerecht den Markt bedienen zu können. Der Einsatz von Trusted Computing wird dabei aber leider von den wenigsten Firmen adressiert. *(bk)*