Trusted Execution Environment-basierte Sicherheit für digitale Umspannwerke

Themenschwerpunkt: Digitales Umspannwerk und Cybersecurity

Autoren: Markus Dahlmanns (Communication and Distributed Systems, RWTH Aachen)
Andreas Wark (amperias GmbH)
Carl-Heinz Genzel (amperias GmbH)
Prof. Dr.-Ing. Klaus Wehrle (Communication and Distributed Systems, RWTH Aachen)

Immer stärker vernetzte, digitale Umspannwerke, wie sie beispielsweise für den adaptiven Netzschutz benötigt werden [1], erhöhen die Angriffsfläche für Cyber-Attacken enorm. Es sind nicht mehr nur die Stationsleittechnik, sondern auch Endgeräte, wie zum Beispiel Schutzgeräte, direkt mit der IKT-Infrastruktur verbunden. Auf der einen Seite erhöht sich so die Flexibilität, u.a. bei der Parametrisierung der Geräte, die nun aus der Ferne möglich ist. Auf der anderen Seite können allerdings auch Angreifer diese Infrastruktur für ihre Zwecke ausnutzen und beispielsweise Blackouts hervorrufen. Zwar beschreibt IEC62351 [2] u.a. die Nutzung von IEC61850 [3] via Transport Layer Security (TLS) und spezifiziert somit eine Ende-zu-Ende sichere und authentische Kommunikation. Jedoch basiert die Ende-zu-Ende Sicherheit und Authentizität auf der Annahme, dass Angreifer nicht in der Lage sind Geräte (physisch) zu kompromittieren um beispielsweise private Schlüssel zu extrahieren.

Der auf dem Poster präsentierte Ansatz sieht vor, auf Basis eines Trusted Execution Environments [4], das durch viele Arm Prozessoren, die bereits heute u.a. in Stationsleittechniken verbaut sind (z.B. [5,6]), unterstützt wird, sowohl sämtliche TLS-Schlüssel vor Angreifern zu schützen, als auch die Integrität der Geräte aus der Ferne zu attestieren. Um TLS-Schlüssel zu schützen, wird entweder nur der Authentifizierungsschlüssel in der TEE abgelegt, sodass dieser nicht einmal mehr vom Betriebssystem und somit auch nicht von Angreifern, die das System kompromittiert haben, ausgelesen werden kann. Stattdessen werden Daten, die zur Authentifizierung des Geräts signiert werden müssen, an die TEE übergeben und dort signiert. Um zusätzlich noch TLS-Sitzungsschlüssel vor einer Extraktion zu Schützen und somit zu verhindern, dass Angreifer bereits aufgebaute Verbindungen übernehmen können, kann eine vollständige TLS-Implementierung in der TEE realisiert werden. TLS-Verbindungen werden dann aus der TEE heraus aufgebaut und die Anwendungen übergeben zu verschlüsselnde Daten an bzw. erhalten bereits entschlüsselte Daten aus der TEE. Um zusätzlich (physische) Kompromittierungsversuche zu erkennen, erlauben TEEs eine Attestierung des Gerätezustandes aus der Ferne. Hierzu wird der Systemzustand aus der TEE beschrieben und durch die TEE signiert für einen Attestierungsrechner zur Verfügung gestellt. Der Abruf erlaubt es der Leitstelle bzw. dem Verifizierungsrechner zu überprüfen, ob der Gerätezustand mit den Erwartungen übereinstimmt. Sollte dies nicht der Fall sein, gilt das entsprechende Gerät als kompromittiert und kann umgehend aus der IKT-Kommunikation ausgeschlossen werden. Insgesamt erhöht die Nutzung von Trusted Execution Environments das Sicherheitslevel in digitalen Umspannwerken signifikant.

Referenzen:

[1] Matthias Lorenz, Tobias Markus Pletzer, Malte Schuhmacher, Torsten Sowa, Michael Dahms, Simon Stock, Davood Babazadeh, Christian Becker, Johann Jaeger, Tobias Lorz, Markus Dahlmanns, Ina Berenice Fink, Klaus Wehrle, Andreas Ulbig, Philipp Linnartz, Antigona Selimaj, Thomas Offergeld (2022). Interconnected network protection systems - the basis for the reliable and safe operation of distribution grids with a high penetration of renewable energies and electric vehicle. Proceedings of the CIRED workshop on E-mobility and power distribution systems 2022.
[2] International Electrotechnical Commission (IEC). IEC 61850 - Communication networks and systems for power utility automation.
[3] International Electrotechnical Commission (IEC). IEC 62351 - Power systems management and associated information exchange - Data and communications security.
[4] Siemens. SICAM A8000 Serie, CP-8050, Handbuch.
[5] SAE IT-systems. FW-5-GATE, Handbuch.