Kurzfassung

Sicherheitsarchitekturen der physikalischen Schicht für das Internet der Dinge

Eine neue Ära an Rechnern ist im Aufbruch – das Internet der Dinge (IoT). Dessen Intelligenz entspringt der Menge der allgegenwärtigen Sensoren und Aktuatoren, und der rechnerischen Fähigkeiten der Datenzentren. Schon heute besteht es aus Milliarden vernetzten Geräten, die ihre Umwelt wahrnehmen und davon Daten versenden. Große IoT Firmen erwarten, dass es in den nächsten Jahren noch mehr vernetzte Geräte geben wird. Wird dieser Trend weitergeführt, dann bietet das IoT großes Geschäftspotential für Unternehmen. Jedoch werden nicht nur Unternehmen von dem IoT angezogen. Auch Widersacher versuchen Geräte für ihr eigenes finanzielles Wohl zu kompromittieren, was noch gefährlicher wird, wenn besagte Geräte mit schlechten bis gar keinen Sicherheitsmaßnahmen ausgestattet sind.

Deswegen sollten IoT Geräte gegen Angriffe gesichert sein und ein signifikanter Anteil dieser Geräte sollte leichtgewichtige und adäquate Sicherheitsmaßnahmen haben. Aber starke Sicherheit und Kosten stehen nicht im Einklang, woraus sich das Dilemma des IoT ergibt. In 2016 wurden ungesicherte Geräte für einen sogenannten "DDoS-for-hire booter / stresser service" benutzt, was zu schlimmen Ausfällen für Internetseiten und Services führte.

Im Licht solcher aktuellen Ereignisse und Angriffen auf der physikalischen Ebene, wie Seitenkanalanalysen, scheint das Internet der Dinge nicht genügend abgesichert. Benutzer tendieren dazu schwache Passwörter mit wenig Entropie zu wählen, oder Standartpasswörter erst gar nicht zu ändern, was die Sicherheit insgesamt schwächt. Mit dem Einbinden intrinsischer Zufälligkeit von Geräten und Kommunikationen, wird die Fehleranfälligkeit von Systemen verbessert und die Sicherheitsgarantien erhöht bei einem geringen Aufwand.

Kurzgesagt verschieben wir digitale Herausforderungen, wie Schlüsselspeicher und Schlüsselgenerierung, in die physikalische Domäne. Zur Erreichung unserer Sicherheitsziele betrachten wir drei Ebenen wie man Sicherheit basierend auf der physikalischen Ebene in das Internet der Dinge bringt.

Zuerst heben wir zwei erfolgsversprechende Primitive von der technologischen Ebene hervor, wobei die Entropie durch deren physikalische Natur generiert wird. Diese Primitive sind CBKA und PUF, welche wir für Sitzungsschlüsselgenerierung und Schlüsselauthentifizierung nutzen. Wir zeigen wie MEMS Sensoren als PUF benutzt werden können, präsentieren die nach dem Stand der Technik konservativste Entropieschätzung für solche PUFs und exerzieren den Prozess einer kompletten Schlüsselrekonstruktion durch. Für CBKA erstellen wir ein neues Modell zur Energieschätzung für unsere physikalisch basierte Methode und eine nach dem Stand der Technik gewählte Alternative, nämlich ECDH. Wir geben an wann einer dieser Algorithmen besser als der andere ist im Sinne von Energie und optimieren den bestehenden Prozess der Schlüsselgenerierung.

Zweitens, da beide Technologien im unseren Fall fehlerfreie Schlüssel benötigen, wenden wir bei beiden die gleichen Fehlerkorrekturverfahren auf der Ebene der Verarbeitung an. Wir präsentieren eine umfassende Übersicht von Abgleichsmethoden, die für beide Technologien passend ist. Weiterhin leiten wir ein Abgleichsmodell ab, welches alle aktuellen und überdies zukünftige Abgleichsmethoden abdeckt. Wir demonstrieren die Tauglichkeit eines LCFE für das IoT anhand einer effizienten und leichtgewichtigen Implementierung, wobei die verrauschte Entropiequelle und der abgeleitete Schlüssel die gleiche Entropie enthalten.

Als drittes, nachdem wir die verrauschte Natur unserer gewählten Technologien bewältigt haben, nutzen wir diese auf der Ebene der Protokolle um unsere Sicherheitsziele zu erreichen. Hierbei erreichen wir ein Authentifizierungsprotokoll, das die Privatsphäre wahrt, selbst wenn der gesamte Speicherinhalt dem Angreifer bekannt ist. Desweiteren schlagen wir ein Softwareupdateprotokoll vor, wobei die Software selbst für einen Angreifer unzugänglich ist, selbst wenn das Zielgerät bereits mit Malware infiziert ist. Zusätzlich löschen wir solch eine Malware und das Gerät verbleibt in einem vertrauenswürdigen Zustand.

Innerhalb dieser Arbeit zeigen wir, dass physikalisch basierte Sicherheit wohlgeeignet für speicherbeschränkte Geräte ist. Weiterhin bleibt die Sicherheit, die auf der physikalischen Ebene basiert, selbst dann gewahrt, wenn stärkere Annahmen über einen Angreifer gemacht werden. Zum Beispiel, ein Schlüsselspeicher welcher mit einer strong PUF realisiert wurde, hält seine Sicherheitsgarantien selbst wenn der komplette Speicher einem Angreifer bekannt ist, wobei ein Schlüssel in einem nicht volatilen Speicher, wie Flash oder ROM, kompromittiert werden würde.

Schlagworte.

Internet der Dinge, physikalisch basierte Sicherheit, physikalisch unklonbare Funktion, Entropieschätzung, kanalbasierte Schlüsseleinigung, Energieverbrauch, Fuzzy Extractor, Informationsabgleich, effiziente Implementierung, Privatsphäre, Authentifizierung, Lernen mit Fehlern, Schutz von geistigem Eigentum, Software Update