FORSCHUNGSINITIATIVE Zukunft BAU

Absicherung der Gerätekommunikation im Smart Home unter Verwendung des Schutzprofils für Smart Meter Gateways

Kurzbericht

Der Forschungsbericht wurde mit Mitteln der Forschungsinitiative Zukunft Bau des Bundesinstitutes für Bau-, Stadt- und Raumforschung gefördert.
(Aktenzeichen: SWD-10.08.18.7-15.10 / II3-F20-14-1-012)
Die Verantwortung für den Inhalt des Berichtes liegt beim Autor.

Bearbeiter: M.Sc. Hannes Raddatz, M.Sc. Michael Rethfeldt, Dipl.-Inf. Martin Kasparick, M.Sc. Arne Wall

Projektleiter: Prof. Dr.-Ing. Dirk Timmermann

Universität Rostock Traditio et Innovatio

Ausgangslage

Die rasante Entwicklung des Internets und die steigende Anzahl der vernetzten Geräte, gepaart mit nicht konsequent durchgesetzter Sicherheit haben dazu geführt, dass nahezu jeder Benutzer im vollen Umfang von unbefugten Dritten überwacht werden kann. Das BSI-Schutzprofil adressiert solche Probleme für das Gateway eines Smart Metering-Systems. Das Projekt sichert die Kommunikation im Smart Home unter Verwendung des Smart Meter Gateways ab.

Gegenstand des Forschungsvorhabens

Im Rahmen des Forschungsvorhabens wurde ein Sicherheits-Framework erarbeitet, dass es ermöglicht die Kommunikation im Smart Home unter Berücksichtigung des Schutzprofils für Smart Meter Gateways und des aktuellen Standes der Technik abzusichern. Zu Beginn des Projektes wurde der Stand der Technik recherchiert und im Besonderen aktuelle Entwicklungen von Kommunikationsprotokollen im Bereich des Internet of Things (IoT) untersucht. Die Strukturen und Komponenten von Smart Metering-Systemen waren ebenso wie das Schutzprofil für Smart Meter Gateways und die zugehörigen Technischen Richtlinien TR-03109 Bestandteil dieser Analyse. Nachdem verschiedene Lösungen für Smart Home-Systeme am Markt und in der Open Source-Szene untersucht sowie Protokoll-Trends von IoT-Entwicklern ausgewertet wurden, konnten die ersten Anforderungen an das Sicherheits-Framework definiert werden. Die Basis bilden RESTful Web Services, die mit dem Constraint Application Protocol (CoAP) realisiert werden. Dies stellt eine Neuerung im Vergleich zu den BBSR-Vorgängerprojekten dar. Vorteile dieses Protokolls sind die Beliebtheit bei Entwicklern, die Möglichkeit zur dezentralen Umsetzung von Web Services und das Interesse von Marktteilnehmern (IKEA, Ericsson) und Konsortien (Open Mobile Alliance). Im Folgenden wurden weitere Anforderungen aus dem BSI-Schutzprofil und den Technischen Richtlinien abgeleitet und dabei die Teilbereiche Authentifizierung und Autorisierung als elementare Bestandteile neben der Sicherung der Gerätekommunikation identifiziert. Während für den Aspekt der Kommunikationssicherheit etablierte Protokolle wie Datagram Transport Layer Security (DTLS) existieren, gibt es kaum Lösungen für die beiden neu identifizierten Teilaspekte im Bereich des IoT. Daraufhin wurde recherchiert, ob es Bestrebungen in der Forschergemeinschaft gibt, Lösungen für diese Aspekte im IoT-Sektor zu erarbeiten. Dabei wurden die folgenden Protokolle, teilweise noch im Entwurfsstadium des Standardisierungsprozesses der Internet Engineering Task Force (IETF), als vielversprechende Kandidaten für das Sicherheits-Framework ermittelt: Concise Binary Object Representation (CBOR) und CBOR Object Signing and Encryption (COSE) als binäres leichtgewichtiges Datenformat und darauf aufbauende Sicherheitsmechanismen zum Signieren und Verschlüsseln von Nachrichten. Das Protokoll Authentication and Authorization for Constrained Environments (ACE) dient zur Autorisierung von Gerätezugriffen mithilfe sogenannter Token. Lightweight M2M (LwM2M) erweitert CoAP um Datenmodelle und ermöglicht eine benutzerfreundliche Verwaltung der Geräte. Aufgrund von Einschränkungen, die durch die Absicherung von CoAP mithilfe von DTLS entstehen, wurde Object Security for Constrained RESTful Environments (OSCORE) als Sicherheitsprotokoll in das Framework aufgenommen. Die Herausforderung bestand darin, die Protokolle in geeigneter Weise zu kombinieren, um die definierten Anforderungen zu erfüllen.

Nach der Konzeption des Sicherheits-Framework wurde die Integration von Smart Metering-Elementen in das Smart Home-Netzwerk betrachtet. Der Rollout intelligenter Messeinrichtungen in Deutschland hat gerade erst begonnen, jedoch sollen in naher Zukunft in jedem Gebäude intelligente

Verbrauchszähler installiert sein, die u. a. die Verbrauchswerte automatisiert an den Energieanbieter schicken. Dazu wird die Kommunikationseinheit Smart Meter Gateway benötigt. Dieses Gateway ist ein vom BSI zertifiziertes Gerät, welches hohen Sicherheitsanforderungen entspricht und leistungsfähige Kryptografie-Hardware besitzt. Ein Ziel des Forschungsvorhabens war es, dieses Gerät als sichere Instanz in das Smart Home-Netzwerk und das Sicherheits-Framework derart zu integrieren, dass sämtliche Smart Home-Geräte von den Sicherheitseigenschaften des Gateways profitieren können. Dazu wurde das Sicherheits-Framework entsprechend adaptiert und das Smart Meter Gateway mit zusätzlichen Funktionen aufgewertet und folglich als Smart Home Gateway bezeichnet. Abschließend wurden Prototypen verschiedener Smart Home-Szenarien mithilfe des Sicherheits-Framework entwickelt und implementiert. Dazu gehören u. a. eine Audio-/Video-Gegensprechanlage und ein Nutzerauthentifizierungs- und Autorisierungsverfahren mithilfe des neuen deutschen Personalausweises. Weiterhin wurde dargelegt, wie sich das Sicherheits-Framework zügig in existierende Smart Home-Produkte integrieren lässt.

Fazit

Es wurde mit dem Sicherheits-Framework eine Basis für Smart Home-Systeme erarbeitet, welche von Beginn an aktuelle Sicherheitsanforderungen des BSI berücksichtigt und das Smart Meter Gateway ins Smart Home-Netzwerk einbindet. Das Framework kann als eine Art Fundament eines Smart Home-Systems verstanden werden, welches Hersteller zur Implementierung eigener Smart Home-Geräte verwenden können. Es wurden darauf aufbauende Erweiterungen entwickelt, die weitere Funktionen ermöglichen. Die zu Beginn des Forschungsvorhabens durchgeführten Recherchen wurden genutzt, um trotz des wissenschaftlichen Fokus ein Konzept mit Protokollen zu erarbeiten, das eine zügige Umsetzung in die Realität ermöglicht.

Eckdaten

Kurztitel:	Secure Smart Home
Forscher / Projektleitung:	M.Sc. Hannes Raddatz, M.Sc. M. Rethfeldt, Dipl.-Inf. M. Kasparick, M.Sc. Arne Wall/ Prof. Dr. Dirk Timmermann
Gesamtkosten:	467.813,30 €
Anteil Bundeszuschuss:	327.469,31 €
Projektlaufzeit:	28 Monate

Abbildungen

Bild 1: SecureSmartHomeLogo.png
Bildunterschrift: Logo des Secure Smart Home-Projektes

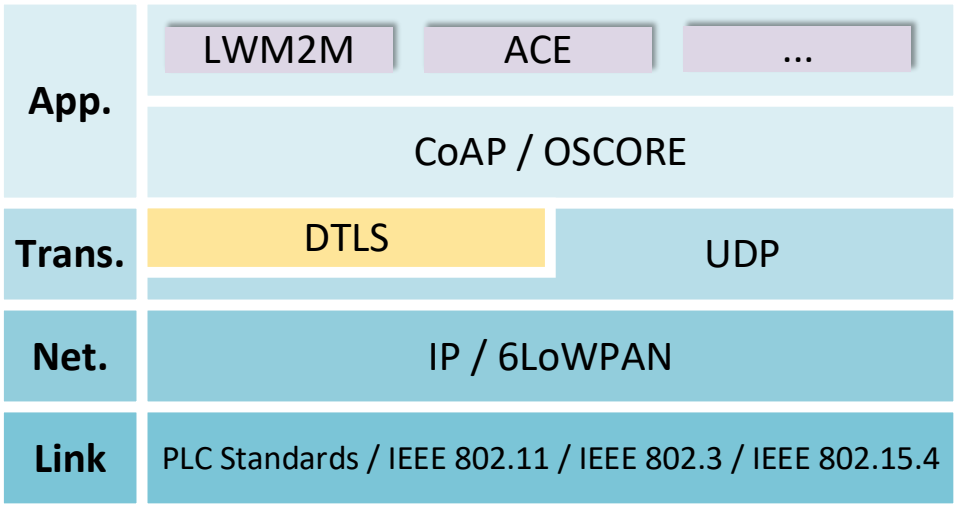

Bild 2: SecureSmartHomeStack.png
Bildunterschrift: Protokollstapel des Sicherheits-Framework

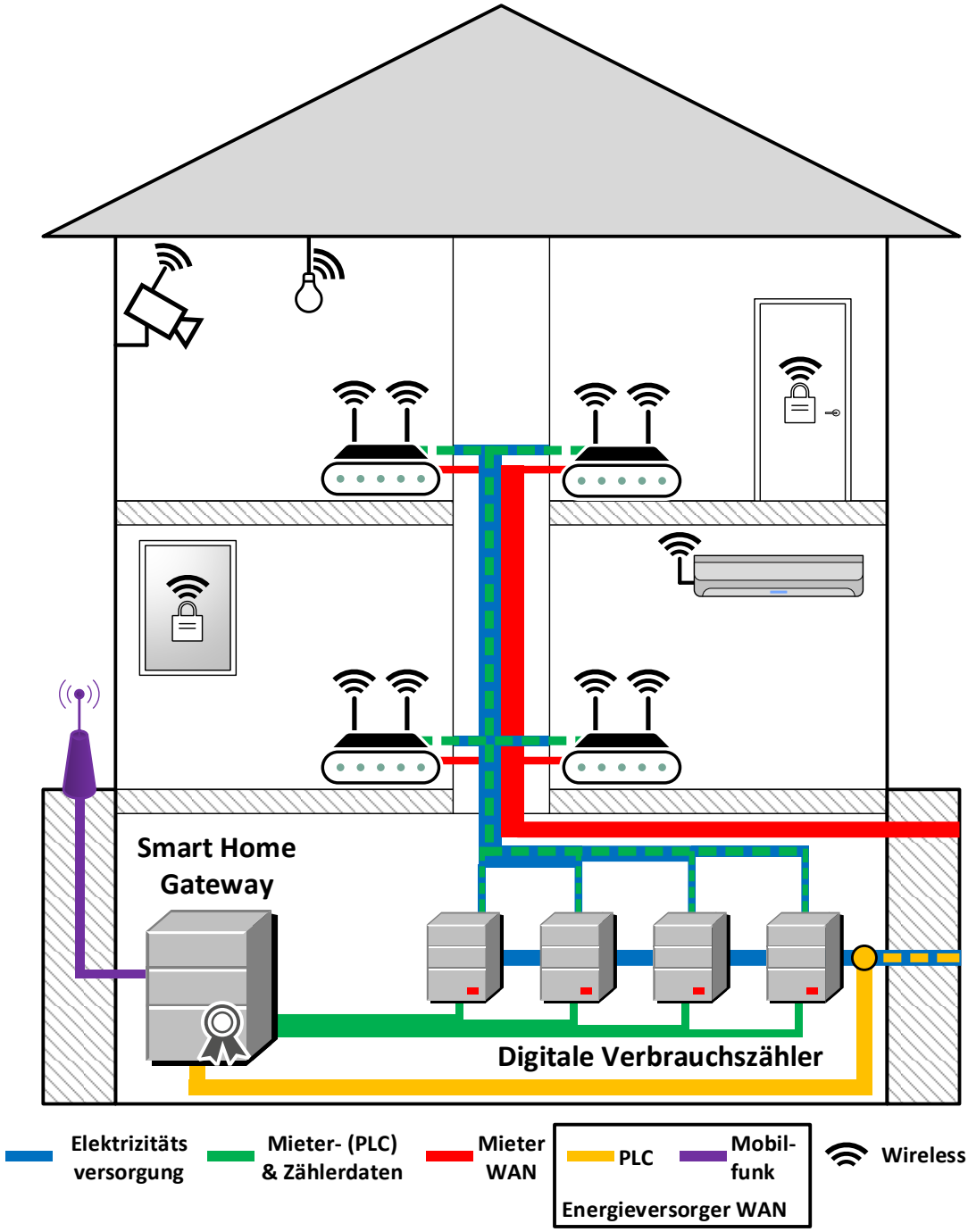

Bild 3:
SecureSmartHomeInfrastructure.png
Bildunterschrift:
Infrastruktur des Sicherheits-Framework am Beispiel eines Gebäudes mit vier Wohneinheiten ausgestattet mit Smart Home-Geräten und Smart

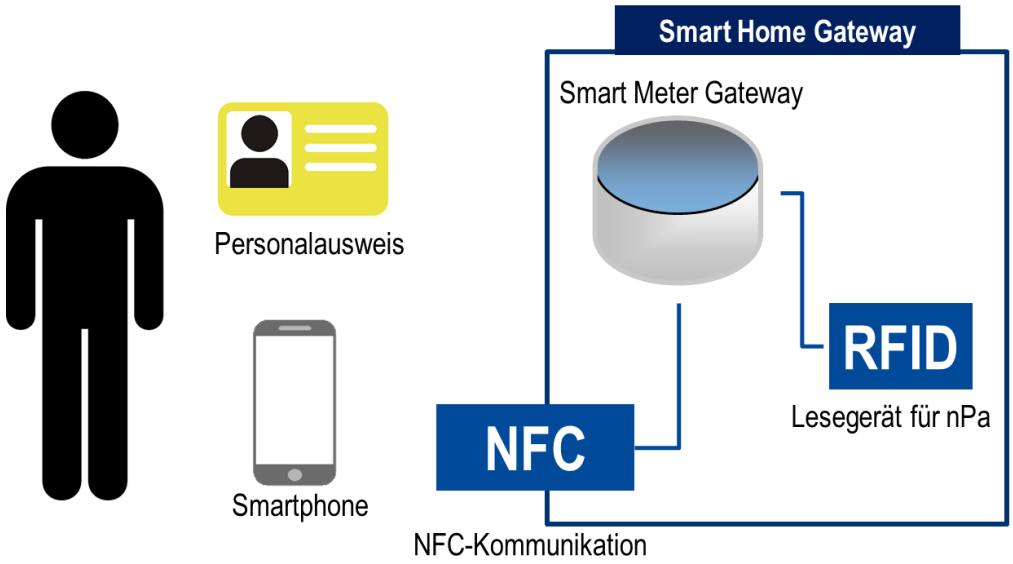

Bild 4: SecureSmartHomeNPA.png
Bildunterschrift: Registrierung neuer Nutzer und Autorisierung von Nutzergeräten mithilfe des neuen Personalausweises

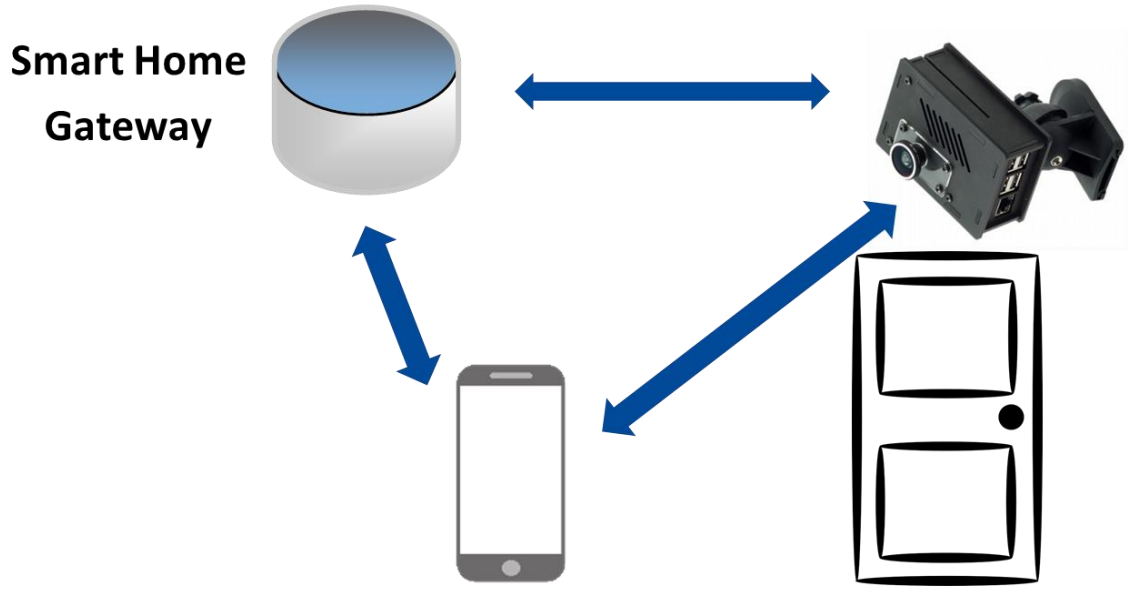

Bild 5: SecureSmartHomeIntercom.png
Bildunterschrift: Sichere Kommunikation zwischen Gegensprechanlage und Smartphone

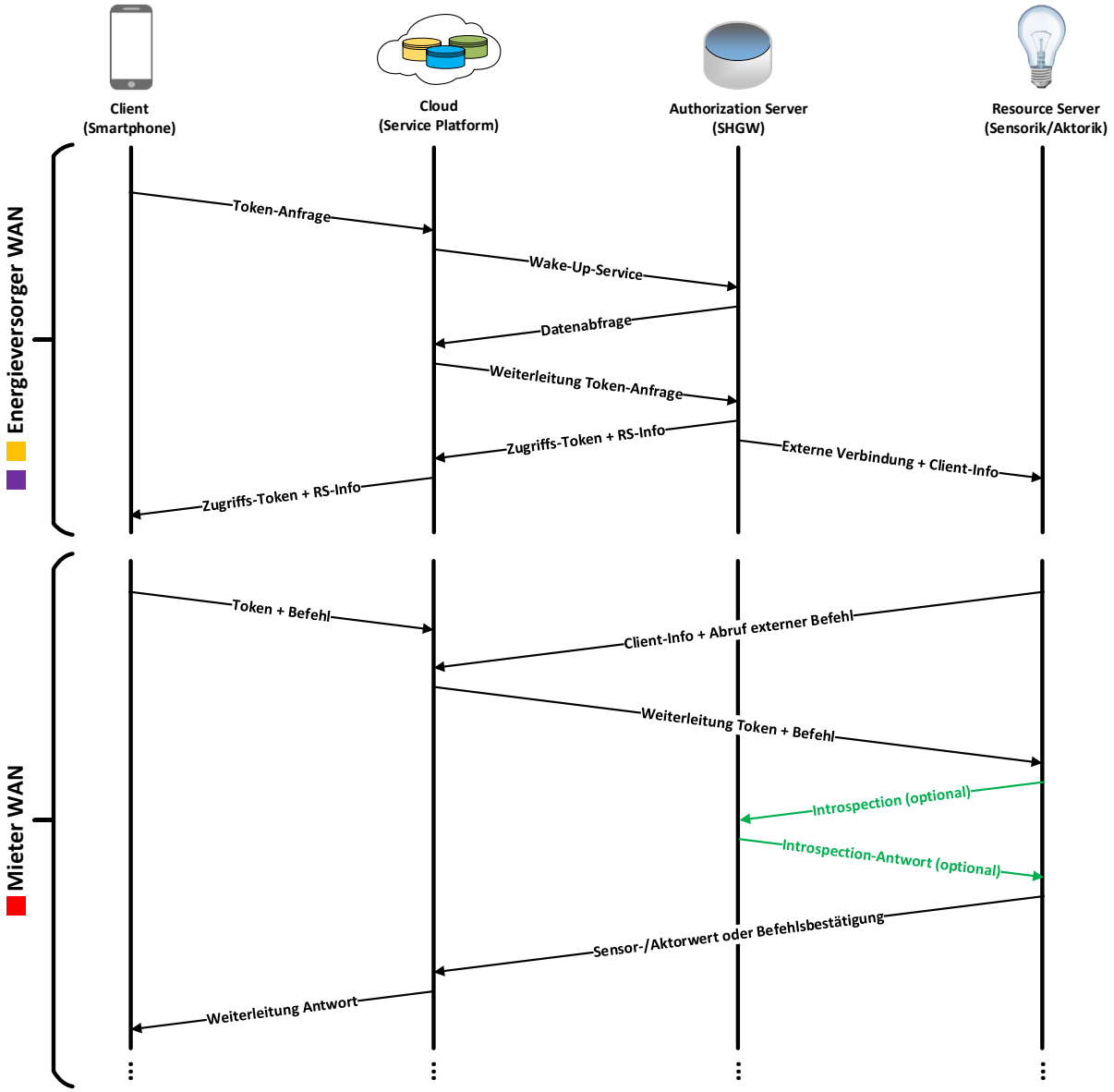

Bild 6: SecureSmartRemoteControl.png
Bildunterschrift: Sichere Kommunikation zwischen externem Nutzergerät und Gerät im Smart Home

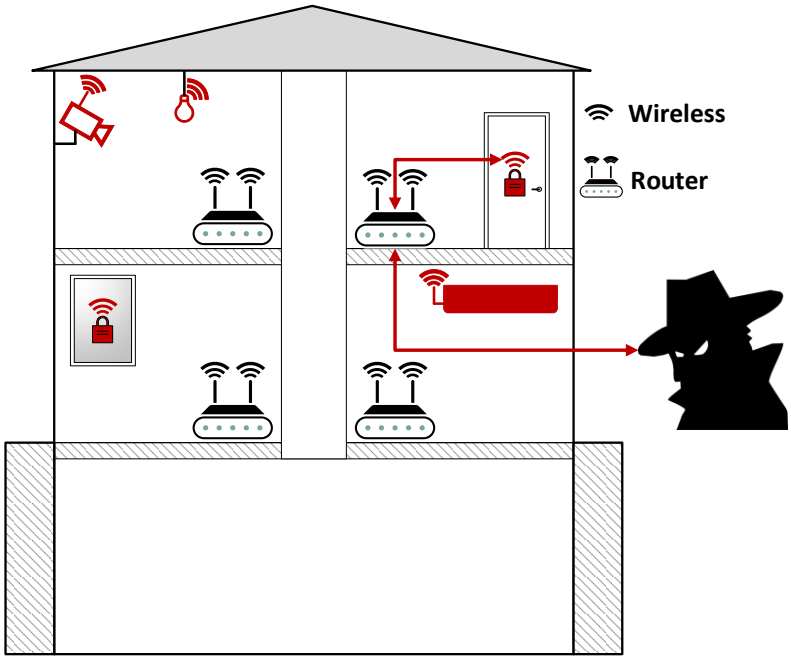

Bild 7: SecureSmartHomeAttackSurface.png
Bildunterschrift: Angriffsszenario eines Smart Home-Netzwerks aufgrund von Fehlkonfiguration

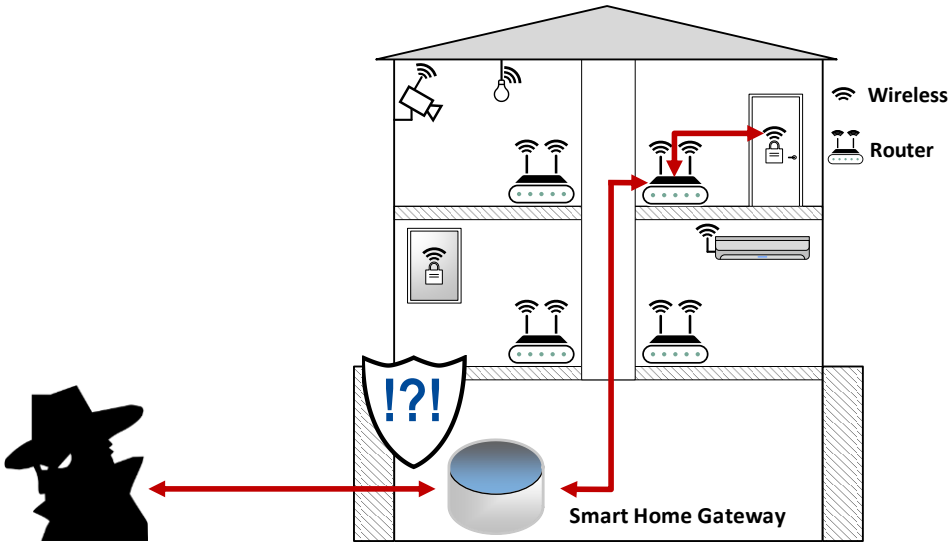

Bild 8: SecureSmartHomeProtected.png
Bildunterschrift: Angriffsszenario eines Smart Home-Netzwerks, geschützt durch Sicherheits-Framework