„Security Implications of Permission Models in Smart-Home Application Frameworks“

Die Autoren des Textes identifizieren die Berechtigungsmodelle von Smart-Home-Anwendungsframeworks als Kernpunkt in Hinblick auf Datenschutz und –sicherheit. Über diese wird definiert, wie extensiv die Rechte von Drittanbieter-Software sind – und damit auch wie viel Risiko diese darstellen kann.

Im Laufe ihrer Analyse haben die Autoren festgestellt, dass es von Framework zu Framework sehr unterschiedliche Möglichkeiten der Zugriffssteuerung gibt, auf welche sie dann kurz eingehen, um dann eine tiefere Analyse von Samsungs „SmartThings“-Framework vorzunehmen, weil dieses in vielen Aspekten stellvertretend für die anderen Frameworks gesehen werden kann.

Besonders kritisch sehen die Autoren *overprivilege*, also das überprivilegieren von Apps. Das bedeutet, dass den Anwendungen Rechte zugesprochen werden, die für deren Nutzung gar nicht relevant ist. Dies geschieht in den meisten Fällen aufgrund des Gerätemanagements, nicht aus Fehlern in der Anwendungsprogrammierung. Anhand diverser Techniken zeigen die Autoren, wie diese Überprivilegierung von einem Angreifer ausgenutzt werden könnte.

Quelle:

Fernandes, Earlence et al. (2017): Security Implications of Permission Models in Smart-Home Application Frameworks. IEEE Symposium on Security and Privacy 15, 2. S. 24-30

„Towards Territorial Privacy in Smart Environments“

Die Autoren behandeln den Themenschwerpunkt der *territorial privacy*, also den Datenschutz in einem bestimmten Territorium, welcher in der Vergangenheit relativ sicher durch einfache Häuserwände geschützt werden konnte, in Zeiten von Ubiquitous Computing, IoT und Smart Home und der Verschmelzung von physischer und virtueller Welt allerdings zunehmend gefährdet wird. Um diesen Sachverhalt zu analysieren wurde ein nutzerzentriertes Beobachtungsmodell entwickelt, welches sowohl physische als auch virtuelle Beobachter in den Blick nimmt, und diese wiederum in erwünschte (z.B. Schrittzähler) und unerwünschte Beobachter (z.B. Spysoftware) unterteilt. Im Abschluss werden dann weitere mögliche Forschungsschwerpunkte erläutert, namentlich Intrusion, Demarkation, Politik und Durchsetzung von territorialem Datenschutz.

Könings, Bastian et al. (2010): Towards territorial privacy in smart environments. Open Access Repositorium der Universität Ulm. http://dx.doi.org/10.18725/OPARU-1727

„IoT Privacy and Security Challenges for Smart Home Environments“

Auch die Autoren dieser Studie befassen sich mit den neuen Herausforderungen für Datenschutz und –sicherheit, die mit Smart Home Geräten und Anwendungen erwachsen. Nachdem sie Gefahren in den Bereichen *Confidentiality* (z.B. die Weitergabe von Temperaturdaten), *Authentication* (z.B. das fehlerhafte Öffnen von Notfallfenstern um einem Einbrecher sein Nachtwerk zu erleichtern) und *Access* (den Zugang zu den Smart Home Geräten und Applikationen) herausarbeiten. Letzteres sehen sie als am meisten gefährdet an.

Folgerichtig analysieren sie auch im nächsten Absatz den Systemzugang als Schwäche, sowohl über das Netzwerk als auch physisch. Weiterhin nennen sie unter dem Punkt *Vulnerabilities* die fehlende Rechenleistung viele Geräte, welche komplexere Sicherheitsalgorithmen verunmöglicht, die Systemheterogenität und feste Firmware, welche einheitliche Updates oder Updates im allgemeinen verhindert, und (nach Meinung der Autoren der wichtigste Punkt) das Fehlen von dezidierten Sicherheitsexperten, bzw. deren Kosten. Da Privatpersonen sich diese nämlich in den seltensten Fällen leisten können, liegt es an den Bewohnern des Smart Home selbst, sich um die komplexe Problematik von *Privacy* und *Security* zu kümmern.

Im weiteren Verlauf des Papers gehen die Autoren auf bestehende Protokolle in Hinblick auf das Smart Home ein, um schließlich die Smart Home Architektur für Sicherheit zu besprechen. Neben Middleware und Cloud Architekturen kommen sie schließlich zur Gateway Architektur, bei der ein eher rechenstarker Netzwerkprozessor als Gateway für die anderen Smart Home Geräte fungiert, welcher zusätzlich noch als Bridge zwischen den lokalen Geräten und der Cloud agieren kann. Im Gateway kann die Nutzerauthentifizierung zentralisiert und Zustandskontrolle ausgeübt werden, um ungenehmigten Zugriff auf das System zu verhindern. Weiterhin dient der Gateway als Firewall. Als konkrete Architektur wird die „Server-Based Internet-of-Things Architecture (SBIOTA)“ genannt. Weil die Gateway-Architektur einerseits kritische Smart Home Funktionen ausführen kann, andererseits auch ohne Internetverbindung das System schützen kann, ist es die von den Autoren präferierte Variante.

Als weitere Herausforderungen nennen sie Autokonfigurationssupport und IoT Software und Firmware Updates.

Lin, H.; Bergmann, N.W.: IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44.