Thema: Sicherheit / Angreifermodelle

1. Analysis of security attacks in a smart home networks

Der Artikel gibt einen Überblick über das Smart-Home Netzwerk und dessen verschiedenen Sicherheitslücken. Es wird erklärt warum es so ein einfaches Ziel für Angriffe sein kann. Ebenso werden auf die aktuellen Herausforderungen in der Forschung, sowie auf die verschiedenen möglichen Angriffe eingegangen.

U. Saxena, J. S. Sodhi and Y. Singh, "Analysis of security attacks in a smart home networks," 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, 2017, pp. 431-436.

URL: http://ieeexplore.ieee.org/document/7943189/

2. IoT based smart home: Security challenges, security requirements and solutions

In diesem Artikel geht es hauptsächlich um die Herausforderungen in Sicherheit, die von Smart Homes ausgehen können. Dabei werden auf verschiedene Angriffsmöglichkeiten, sowie deren Einfluss auf das ganze System, eingegangen. Der Artikel gibt auch einen sehr guten Überblick zu aktueller Literatur im Bereich von „Security“ und „Privacy“ von Smart-Homes. Die Autoren unterscheiden dabei zwischen 3 Hauptproblemen, device issues, communication issues und services issues.

W. Ali, G. Dustgeer, M. Awais and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, United Kingdom, 2017, pp. 1-6.

URL: http://ieeexplore.ieee.org/document/8082057/

3. Smart-Phones Attacking Smart-Homes

Dieser Artikel liefert ein Beispiel für einen Angriff auf IoT Geräte von Smart Homes. Dabei wird mithilfe einer iPhone App, welche ohne Probleme in den Apple AppStore veröffentlicht wurde, nach IoT Geräten gescannt. Dadurch können die Sicherheitsmaßnahmen des Routers umgangen werden und auf die Geräte von außerhalb zugreifbar gemacht werden. Eine Lösung für dieses Problem scheint nicht trivial zu sein.

Vijay Sivaraman, Dominic Chan, Dylan Earl, and Roksana Boreli. 2016. Smart-Phones Attacking Smart-Homes. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '16). ACM, New York, NY, USA, 195-200.

DOI: https://doi.org/10.1145/2939918.2939925

4. Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home

Der Artikel beschäftigt sich mit der Aufklärung von Sicherheit und Privacy Risiken von Smart Homes. Es wurde dafür ein Framework entwickelt, bei dem die Nutzer durch einfache Bedienung und Hilfestellung die Risiken modellieren können. Das soll besonders unerfahrenen Benutzern helfen sich mit der Thematik auseinanderzusetzen. Die Risiken werden dabei in 5 Aufgaben modelliert.

Nurse J.R.C., Atamli A., Martin A. (2016) Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home. In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016. Lecture Notes in Computer Science, vol 9750. Springer, Cham

DOI: https://doi.org/10.1007/978-3-319-39381-0_23