Security and Privacy Issues of Home Globalization

Luca Caviglione | National Research Council of Italy
Steffen Wendzel | Hochschule Worms
Simon Vrhovec | University of Maribor
Aleksandra Mileva | University Goce Delčev

Over the last few years, people have been reshaping their homes into smart hubs owing to a wide array of Internet of Things (IoT) devices, including interconnected lights, locks, sensors, cameras, actuators, wearables, and appliances accessible through the Internet that can be controlled locally via voice or remotely though mobile phones. As a consequence, modern smart homes are complex internetworks of laptops, mobile phones, game consoles, wearable equipment, and various consumer IoT nodes, which can be used for work, health, safety, and entertainment purposes. This transformation culminated in globalized homes that can be accessed from anywhere. Although the globalization process showcases many benefits, it also renders homes more insecure and less private places where individuals are exposed to an increasing variety of threats from the outside world.

For instance, IoT nodes at the basis of globalized homes are increasingly abused by adaptations of well-known attacks exploiting the variety of data and devices populating modern apartments and houses. Moreover, home-based and consumer IoT frameworks usually collect and manage information that is tightly coupled with the everyday life of individuals and can, thus, be considered a source of sensitive data valuable for profiling or reconnaissance attempts.[1] Modern homes are also technologically balkanized with services provided via different frameworks and by multiple hardware/software vendors, often through cloud- or fog-based schema, leading to complex attack surfaces with large-scale implications hard to comprehend in advance.

As an example, with the COVID-19 pandemic, many homes have been abruptly transformed into offices, bringing their insecurities into working/industrial perimeters. This is the case of the ransomware attack that targeted the Italian vaccination booking system in August 2021, which originated from the home computer of a remote worker.[2] Therefore, enforcing security and privacy requirements at the basis of the "home globalization process" entails rethinking and developing new defenses and solutions as well as addressing emerging social challenges for law enforcement agencies, policy makers, and forensics professionals.

In This Issue

The response to the home globalization theme was important. The call for papers received 17 manuscripts, and a rigorous and thorough review process led to the selection of seven articles composing this

Digital Object Identifier 10.1109/MSEC.2021.3127372
Date of current version: 25 January 2022

 Copublished by the IEEE Computer and Reliability Societies

special issue. The accepted articles demonstrate that home globalization poses a highly heterogeneous set of technical challenges, especially in terms of privacy and human aspects, hence demanding the support of multiple privacy and security requirements in a built-in and native manner.[3]

In more detail, the first group of articles is aimed at investigating and solving some key technical challenges of actual and future smart homes. Specifically, "Automated Privacy Preferences for Smart Home Data Sharing Using Personal Data Stores," "Personal IoT Privacy Control at the Edge," and "Preserving Privacy in the Globalized Smart Home—The SIFIS-Home Project" propose different solutions and ideas to enhance the privacy of smart homes. Such works attest to the wide range of theoretical and architectural aspects to consider as well as the importance of the topic, which is also supported by the European Union, e.g., through funded research projects. Indeed, security is the other core component for the success of home globalization. In this vein, "Toward Cybersecurity Personalization in Smart Homes" emphasizes the importance of suitable configuration techniques to make both machines and humans less vulnerable.

The second group of works reminds us that smart homes are about people, and this requires us to think about usability; develop mechanisms for protecting the weak; and assess a composite set of legal, social, and ethical aspects. This group of articles aims at attacking such issues. In more detail, "Citizens' Cybersecurity Behavior—Some Major Challenges" reviews and highlights the various issues awaiting to be faced in the next years, whereas "(In) Secure Smart Device Use Among Senior Citizens" and "The Ethical Smart Home—Perspectives and Guidelines" provide interesting ideas and insights on the "human" side of the conundrum of the data, hardware, and software that make our homes more pleasant and efficient.

Smart homes are about people, and this requires us to think about usability; develop mechanisms for protecting the weak; and assess a composite set of legal, social, and ethical aspects.

Finally, we would like to thank the authors who submitted their work to this special issue and the reviewers who helped in the selection process. We also would like to thank the *IEEE Security & Privacy* editors, Prof. Terry Benzel and Prof. Sean Peisert, for their continuous help and support. ■

References

1. W. Mazurczyk and L. Caviglione, "Cyber reconnaissance techniques," *Commun. ACM*, vol. 64, no. 3, pp. 86–95, Mar. 2021, doi: 10.1145/3418293.
2. L. Borghese and S. Braithwaite, "Hackers block Italian COVID-19 vaccination booking system in 'most serious cyberattack ever,'" CNN Business, Aug. 2021. https://edition.cnn.com/2021/08/02/business/italy-hackers-covid-vaccine-intl/index.html (accessed Oct. 2021).
3. O. Tene, K. Evans, B. Gencarelli, G. Maldoff, and G. Zanfir-Fortuna, "GDPR at year one: Enter the designers and engineers," *IEEE Security Privacy*, vol. 17, no. 6, pp. 7–9, 2019, doi: 10.1109/MSEC.2019.2938196.

Luca Caviglione is a senior research scientist in the Institute for Applied Mathematics and Information Technologies of the National Research Council of Italy, Genova, I-16149, Italy. Caviglione received a Ph.D. in computer science from the University of Genova. Contact him at luca.caviglione@cnr.it.

Steffen Wendzel is a professor of information security and computer networks at Hochschule Worms, Worms, 67549, Germany, where he is also the scientific director of the Center for Technology and Transfer. Contact him at wendzel@hs-worms.de.

Simon Vrhovec is an associate professor at the University of Maribor, Maribor, 2000, Slovenia. Vrhovec received a Ph.D. in computer and information science from the University of Ljubljana. Contact him at simon.vrhovec@um.si.

Aleksandra Mileva is a professor with the Faculty of Computer Science, University Goce Delčev of Štip, Štip, 2000, Republic of North Macedonia, where she is also the head of the Laboratory of Computer Security and Digital Forensics. Contact her at aleksandra.mileva@ugd.edu.mk.