Secure Smart Home Communication

Nisha Panwar and Sharad Mehrotra
Department of Computer Science, University of California Irvine
npanwar@uci.edu,sharad@ics.uci.edu

ACM Reference Format:
Nisha Panwar and Sharad Mehrotra. 2018. Secure Smart Home Communication. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Internet of Things (IoT) has a plethora of applications that revolve around user participation in routine activities such as flying ad-hoc networks, intelligent transportation, marine communication and smart communities (homes, buildings) etc. In all of these scenarios the scope of device-to-device connectivity is leveraged accross ship-to-shore, ship-to-ship, vehicle-to-vehicel, vehicle-to-infrastructure, smart home hubs, smart surveillance, data capture/sharing policies etc. Here we focus on the smart home use-case that is significantly crucial from user privacy perpective. A home owner carries multiple smart devices providing comfort, assisted-living, wearable devices, infotainment, smart documentation etc. However, the device-to-device connectivity requires sufficient security parameters to combat any external attacks through wireless communication channel. In addition, the user privacy is utterly significant such that device-to-device interaction should not reveal any personal information or cues about the user activity. For example, the most naive cue could be to detect from external world whether a home owner is currently at home or not by observing the device communication activity or pattern.

Problem Statement. The problem is to avoid any inferences to spur via passive learning on device communication activity. The passive sniffing on a wireless channel is easily doable. In addition, the side channel information can be derived based on the device activity sniffing over wireless communication channel, e.g., through the MAC address identification.

Example. Let us assume a user (u) owns a smart home (h) with devices ($D_{i\ldots n}$) capable of remote communication, e.g., through a mobile application. The remote communictaion allows the user to switch the device state from (s_{on}) to (s_{off}). The user (u) can create a schedule for devices [D_1, D_2, D_3,] as [s_{on}, s_{off}, s_{on}] such that it reduces overhead due to three explicit command for each individual device and requires a single command instead for all three devices. If user is in office and is about to leave in an hour for the home then he might want to first (a) schedule his smart car for office-to-home route, (b) auto-lock the keyfob-to-car pairing after arriving at the home, (c) switch on heating/coooling system to be as preffered, (d) switch on lights, (e) set the oven to pre-heat, (f) set the instrumental music in background mode (g) set the washing machine on. In case, the user finds a change in his/her schedule then another remote command can be send to overwrite the previous commands and schedule.

The smart home system settings can be visualized as a hub based infrastructure. The home gateway or router connects the external web with the indoor smart devices. In addition, the device-to-device connectivity is through the router and a cloud connectivity is required only in certain cases, e.g., device software upgrades, event logging, state backup etc. Therefore, our scope is to consider a local device topology that accepts user defined commands from the external web.

Threat Model. We consider both an active and a passive adversary in our threat model. The passive adversray can violate the user privacy through inferences or semantic analysis via listening on channel activity. The active adversary can mimic the device activity pattern by recording the token activity on the communication channel. In addition, the active adversary can impersonate a devcie on the communication channel through record-then-clone process where adversay generates a simialr token as an authentic device. The scheduling allows that only a device with a specific functionality will perform within a suggested time-frame as defined by the home owner. The device would not be able to pre-pone the command execution. In addition, the active adversary cannot collude with the device to reveal the secret parameters or commands.

Decoupling Channel Activity from Device Activity. Our approach is to decouple channel activity from the device activity. In some sense, a passive adversary can sniff the channel activity (without being able to decode it, in case of ciphered channel) however, through our solution the passive adversary cannot deduce whether the devices are active or not, only through passive sniffing on the communication channel. In particular, the communication channel would reflect a constant monotonous behaviour all the time, therefore, a distant adversary cannot deduce device activity through constantly behaving channel activity. In addition, we provide a scheduling ability to confirm that the devices would perform on a user given command only after a certain period of time.

REFERENCES

[1] David W. Chadwick and Kaniz Fatema. 2012. A privacy preserving authorisation system for the cloud. *J. Comput. System Sci.* 78, 5 (2012), 1359 – 1373.
[2] A. Jacobsson and P. Davidsson. 2015. Towards a model of privacy and security for smart homes. In *IEEE 2nd World Forum on Internet of Things (WF-IoT).* 727–732.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM.
https://doi.org/10.1145/nnnnnnn.nnnnnnn