Master Thesis: Security for Low-power Devices

Background and Research Area Wearable devices, such as implantable medical devices and smart wearables, are becoming increasingly popular and various applications to monitor user's health have been developed. It is wearable devices' feature to capture sensitive data and transmitted them via wireless channels. To protect data privacy and pair legitimate devices, body area networks (BANs) usually apply a security scheme based on an agreed key to encrypt the channel and authenticate devices.

A simple and unsafe scheme is to set fixed keys for wearable devices before deployment. A more sophisticated scheme requires pairing devices to generate a dynamic key independently based on a shared secret source, such as interval of heartbeats. There are two requirements for an ideal shared secret source: 1. it must be accessible by legitimate devices but potential attacker cannot derive it; 2. it must be random. In practice, a shared secret source cannot perfectly satisfy the first requirement and a sophisticated attacker can derive the key sometimes. Therefore, the new research trend is to exploit multiple secret sources together to improve the security.

Categorized by the selection of shared secret sources, there are two popular research directions: 1. exploit physiological features as shared secret sources; 2. exploit communication channel information as the shared secret source. This proposed project attempts to exploit two different shared secret sources and establish a two-tier authentication security scheme.

Thesis Objective and Content A recent paper [1] introduces Tiek, a two-tier authentication and key distribution security scheme for wearable devices. Devices under this scheme collect the user's motion characteristics (gait) with an accelerometer, and wireless channel fading information based on received signal strength indication (RSSI) of the channel. Based on collected secret sources, devices generate keys independently and correct potential mistakes using a fuzzy vault scheme.

The aim of this thesis is to implement Tiek on internet of thing (IoT) platforms and evaluate Tiek. There are two milestones within the thesis scope. Firstly, can-

didates should implement data collection for both gait and RSSI. This step may involve time synchronization, and alignment of accelerometer to earth coordinate system. Secondly, candidates should implement the key generation algorithm of Tiek so that two IoT platforms can communicate using Tiek.

IoT platforms may be selected by candidates. Suggested platforms are Raspberry Pi [2] and Arduino [3]. Most IoT platforms, including Raspberry Pi and Arduino, can collect RSSI using their radio but need to connect to an external accelerometer to collect gait.

Candidate Requirements and Application For this thesis we are looking for a highly motivated student with very good programming skills, interest in security and in programming firmware in IoT platform.

The thesis can be started as soon as possible. For the application, please provide us with a CV, your courses and grades. In addition, we appreciate an article, paper, thesis or other relevant documents you have written in your education in order to judge your ability to express yourself in English. Please send your application to thiemo.voigt@it.uu.se as one or a set of pdf files.

Contact person
Qi Lin, qi.lin@it.uu.se

References

[1] Sam Hylamia, Wenqing Yan, Christian Rohner, and Thiemo Voigt. Tiek: Two-tier authentication and key distribution for wearable devices. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–6. IEEE, 2019.

[2] Raspberry pi. https://www.raspberrypi.com/. Accessed: 2021-12-7.

[3] Arduino. https://www.arduino.cc/. Accessed: 2021-12-7.