Securing the Timestamping of Sensor Data from Wearable Healthcare Devices

Muhammad Siddiqi†, Gerard Hager†, Vijay Sivaraman†, Sanjay Jha*
†School of Electrical Engineering and Telecommunications
*School of Computer Science and Engineering
†*the University of New South Wales, Sydney, Australia
{m.siddiqi@student., g.hager@student., vijay@, sanjay@cse.}unsw.edu.au

An ageing population, coupled with increasing prevalence of chronic diseases, is placing unsustainable demands on current healthcare systems. Home-based medical monitoring, supported by wearable sensors for heart-rate, ECG, blood pressure, blood glucose, blood-oxygen saturation, etc., has the potential to alleviate the growing burden on hospitals. Timestamping data from such sensors accurately is important for correlating and reconstructing events of medical significance, and to increase trust in the context associated with the data. Unfortunately, reliable timestamping is non-trivial, and cannot be left entirely to the sensor (too resource constrained), the gateway (can be tampered by user), or the datalog server (too far from the medical device).

Timestamps on data from medically-approved wearable devices available in market can be easily altered. For example, with the Fora Diamond Cuff BP, we found that we could tamper the timestamps of measurements simply by changing the time on the smartphone clock while taking the blood pressure. We could similarly tamper with timestamps of readings from the Withings Pulse O_2 device. Even in the case when the app keeps its own clock (rather than the smartphone's clock), it is relatively easy to tamper the timestamp by hacking the app using tools such as Apktool, Androguard, Cydia, Clutch, Hopper, and iRET. We used Apktool to decompile, modify, and recompile the Android apps for the iFora BP [1] and Withings heart-rate [2] devices, and these modifications are detected neither by the device nor by the data logging servers.

Wearable sensors, although reliable, cannot timestamp data independently as their local clock is relative to their boot time and does not know the absolute time; further, they are resource constrained and cannot run time synchronization protocols like NTP. Smartphone apps cannot be trusted to timestamp data reliably, as they can be hacked (shown above). Servers are too far removed from the wearable sensors, and unpredictable network latencies make the timestamping inaccurate; moreover, data might arrive to the server in bursts due to buffering in device or the smartphone app. We propose a new solution to the timetamping problem.

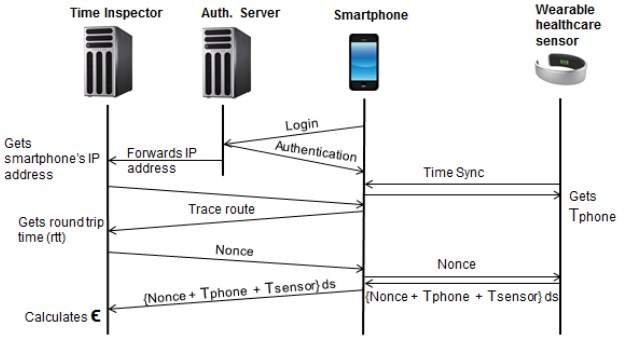

Figure 1: Protocol to validate time of the sensor

Our solution allows the device to obtain absolute time from the smartphone (to ensure accuracy), but uses a validation server (called Time Inspector) that periodically checks the accuracy of the timestamps. This solution allows the validation to be an optional add-on, and can be customized to trade-off the timetamp reliability against resource usage, to match the requirements of the deployment scenarios. The Time Inspector sends a cryptographic *nonce* (at a chosen interval) to the sensor, to which the sensor responds with a digitally signed response including its local clock value T_{sensor} and the global time value T_{phone} last taken from the smartphone. Based on the response the server calculates the time difference ϵ between the sensor's view of global time $\{T_{phone} + T_{sensor}\}$ and its own view of global time T_{server}, compensated for the network latency $\mu_{rtt}/2$. The latency is approximated by using traceroute to identify the router closest to the smartphone and then measuring latency via several ping requests. The mean μ_ϵ and standard deviation σ_ϵ of the time difference $\epsilon = \{T_{server} - (T_{phone} + T_{sensor} + \mu_{rtt}/2)\}/(\mu_{rtt}/2)$ are calculated from repeated responses to *nonce* challenges, and are used to quantify the trustworthiness of the timestamps from the sensor.

Our work[1] shows that medical timestamps are easily tampered at the smartphone, and develops a new overlay solution that can be used to increase confidence in timestamps associated with medical data.

Keywords

mHealth, wearable, provenance, timestamp, security

1. REFERENCES

[1] A modified clone app of iFora BP for research purposes. `https://github.com/sidz81/iFora-BP`.

[2] A clone app of Withings for research purposes. `https://github.com/sidz81/Withings`, June 2015.

[1]This work is funded by Australian Research Council's Discovery Grant DP150100564.

BODYNETS 2015, September 28-30, Sydney, Australia

DOI 10.4108/eai.28-9-2015.2261552