Privacy of Home Telemedicine: Encryption is Not Enough

M. Salajegheh, A. Molina, K.Fu, University of Massachusetts Amherst, USA

Implantable medical devices and home monitors make use of wireless radio communication for both therapeutic functions and remote monitoring of patients' vital signs. While our past work showed that lack of cryptographic protection results in disclosure of private medical data and manipulation of therapies [1], our present work shows that even using encryption is insufficient to protect the confidentiality of patient telemetry. Our experiment analyzes the security of data traffic patterns of two sets of real medical telemetry: a corpus from PhysioNet (an online biomedical research database) and a network trace of a live disaster drill using Harvard's CodeBlue medical sensor network [2]. Our work shows that even if a wireless medical device uses encryption, patient data can leak to unauthorized parties who need not be near the patient.

Our measurements show that data packet timing information and headers distinguish the types of medical and monitoring devices even if traditional cryptographic mechanisms are used. Furthermore, the highly repetitive nature of medical data, such as ECG or respiration signals, leads to additional privacy vulnerabilities that cannot be easily mitigated by means of encryption without significant modification. Data compression technology further exposes encrypted telemetry to cryptanalysis. The information leakage of telemetry could facilitate unauthorized tracking of a patient because an ECG is known to uniquely identify a person in a predetermined group [3]. Moreover, our study shows that data packet padding, encryption, authentication, and other common defenses against security threats require significant energy, storage, and computation that impose on the already scarce battery and space resources.

Two of our experiments show how to automatically recover data from encrypted telemetry using Bayesian classifiers. In one experiment, we encrypted an ECG signal. By observing only the length of the digitally encrypted data, we were able to reconstruct sufficient information about the original ECG data that we determined the patient's heart rate. Using similar techniques, we recovered a leaked respiration signal that visually matches the original signal. Our findings show the weakness of using common cryptographic techniques on highly periodic and often compressed medical telemetry. Our work further discusses techniques to mitigate these security and privacy risks in wireless medical telemetry systems. However, all known techniques require extra energy, computation, and bandwidth from the medical device. The lesson learned is that encryption is not enough to protect the privacy of medical telemetry, and that reasonable assurance for security and privacy will require an energy budget. Future design of medical devices will have to make difficult tradeoffs between battery life versus security and privacy.

This work was supported by NSF grants CNS-0627529, CNS-0716386, and CNS-0831244.

[1] Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., and Maisel, W. H., 2008, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," *Proc. 29th IEEE Symposium on Security and Privacy*, IEEE, Oakland, CA, pp. 129–142.

[2] Chen, B., Peterson, G., Mainland, G., and Welsh, M., 2008, "LiveNet: Using Passive Monitoring to Reconstruct Sensor Network Dynamics," *Proc. 4th IEEE/ACM International Conference on Distributed Computing in Sensor Systems (DCOSS 2008)*, IEEE/ACM, Santorini Island, Greece, pp. 79–98.

[3] Biel, L., Pettersson, O., Philipson, L., and Wide, P., 2001, "ECG Analysis: A New Approach in Human Identification," *IEEE Transactions on Instrumentation and Measurement*, 50(3), pp. 808–812.