Privacy Challenges for Wireless Medical Devices

Brent Lagesse
Cyberspace Sciences and Information Intelligence Research
Computational Sciences and Engineering
Oak Ridge National Laboratory
Oak Ridge, TN 37831
lagessebj@ornl.gov

Abstract

Implantable medical devices are becoming more pervasive as new technologies increase their reliability and safety. Furthermore, these devices are becoming increasingly reliant on wireless communication for interaction with the device. Such technologies have the potential to leak information that could be utilized by an attacker to threaten the lives of patients.

Privacy of patient information is essential; however, this information is not the only privacy issue that must be considered. In this paper, we discuss why information privacy is insufficient for protecting patients from some attacks and how information regarding the presence of individual devices can leak vulnerabilities. Furthermore, we examine existing privacy enhancing algorithms and discuss their applicability to implantable medical devices.

1 Introduction

The importance of security and privacy of patient information has long been acknowledged. As the medical community begins to rely more on networked machines for the storage of patient information the methods of securing such information has changed. Now, the medical community is moving toward medical devices for patient treatment that enable networked interaction. While it is still still essential to protect healthcare information, the connectivity provided by these networked medical devices become a vulnerability that can be exploited remotely and intelligently by attackers.

Previous work has been focused on the privacy of information from the devices [4] even when that information is encrypted [7]; however, we believe that the presence and type of devices must also be protected, especially for implantable medical devices. We make this claim for two reasons. First, knowledge of the device invites specific attacks in the physical world. For example, knowledge of a medical condition could be used against a person. Second, knowledge of the device invites specific cyber attacks. For example, knowledge of a specific model of a device, such as an insulin pump, could allow an attacker to exploit vulnerabilities or spoof a specific device controller. The challenge of device-related privacy has been previously mentioned in [5]; however, the paper only defines privacy issues that should be addressed. We extend this further and discuss why current techniques are insufficent to protect device privacy.

2 Privacy Challenges for Medical Devices

We take the position that knowledge of the types of devices (and likewise the conditions of the patients) are just as important as the information transmitted by them. Due to the constraints of personal medical devices, it is not straightforward as to how to approach this problem. Standard methods of enhancing privacy such as encryption, k-anonymity, or mixes are not suitable for many medical devices. In the following sections, we provide a brief discussion on the insufficiencies of current approaches.

2.1 Encryption

While encryption protects the information sent between components of medical devices, it is possible to derive the information from traffic analysis [7]. Even if cryptographic methods were devised that would prevent analysis of messages, it is still possible for traffic patterns could reveal device types. Masking patterns with cover traffic is possible, but would greatly reduce the battery life of some devices.

2.2 K-anonymity

K-anonymity [2] is a technique by which a data set is anonymized to the point that the identity of an entry can only be narrowed down to a set of k individuals. While this technique is historically used for static databases of information, it is feasible to use such a technique on the information transmitted by medical devices. In such a case, traffic obfuscation could mask properties of a medical device such as the make, model, or device type to a set of k devices. Such a technique would reduce the required cover traffic and extend battery-life; however, its use may be limited depending on the value of k that is achievable.

2.3 Mixes

Mixes [1] are used to anonymize the sender of traffic by reordering messages and resending them to their destinations in such a way that it is difficult for an observer to determine which (encrypted) source message correlates with which destination message. This approach may have potential applications in medical devices, but requires additional resources, primarily a mixer and additional communication devices. Furthermore, the approach may also require cover traffic to prevent timing analysis attacks [3].

2.4 Discussion

While wireless communication is a welcome convenience that can greatly enhance the usability and comfort of implantable medical devices, it also adds a risk of eavesdropping and vulnerabilities that could lead to serious attacks. In the absence of appropriate device-privacy technologies, one possible solution may be the use of unidirectional near-field communication, when feasible, for wireless device communication. Unfortunately, this may not be possible for all devices or situations due to both feasibility and usability reasons. A minimalistic design approach should be taken to prevent security and privacy issues in implantable devices. Included in such a minimalistic design would be secure protocols for initiating the wireless communications that would reduce the remote cyber attacks on the device and the privacy of the device to a physical problem (in other words, an attacker would have to come into close proximity of a specific victim and act in a way that would make the attempted attack obvious). Furthermore, such designs would prevent wide-range scanning attacks on privacy and scans would have to be focused on individual. In doing so, practical privacy could be achieved even though theoretically some privacy vulnerabilities would exist.

Existing privacy enhancing technologies may be used, but the tradeoff between their costs and benefits is uncertain in most cases. It is likely the case that no technique will be universally applicable over the range of implantable medical devices. In such a case, each device type may attempt to masquerade as another set of devices that have traffic patterns similar enough that there would be a low cost to making the traffic patterns indistinguishable (similar to the concepts introduced in k-anonymity).

3 Conclusion

Medical device privacy will soon become a significant problem as more devices become controlled wirelessly, both from the perspective of discrimination and active attacks on the systems themselves. While securing patient information is important, knowledge of the devices a person is using gives an attacker the opportunity to threaten the well-being of the person.

Current methods of achieving privacy come at a high energy cost to the devices that utilize them and many require participation from a large number of devices to achieve a useful level of privacy. It is unclear to what extent usable privacy can be achieved for wireless medical devices. It may be the case that the best privacy will be achieved through designing privacy into the networked implantable medical device such that they can be reduced from a cyber problem to a physical problem. As a physical problem, the attacker's ease of acquiring knowledge is greatly reduced and practical privacy can be achieved.

Acknowledgements

Prepared by Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37831-6285, managed by UTBattelle, LLC, for the U.S. Department of Energy under contract DE-AC05-00OR22725.

References

[1] D. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Communications ofthe ACM, vol. 4, no. 2, February 1981.

[2] L. Sweeney. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(5):557570, 2002.

[3] B. Levine, M. Reiter, C. Wang, and M. Wright. Timing attacks in low-latency mix systems. In Proc. 8th International Conference on Financial Cryptography, 2004.

[4] W. Jih, S. Cheng, J. Y. Hsu, T. Tsai. Context-aware Access Control in Pervasive Healthcare. EEE05 Workshop: Mobility, Agents, and Mobile Service, 2005.

[5] Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., and Maisel, W. H. Security and Privacy for Implantable Medical Devices. IEEE Pervasive Computing, 2008.

[6] Kotz, D., Avancha, S., and Baxi, A. A privacy framework for mobile health and home-care systems. In Proceedings of the First ACM Workshop on Security and Privacy in Medical and Home-Care Systems (Chicago, Illinois, USA, November 13 - 13, 2009). SPIMACS '09.

[7] M. Salajegheh, A. Molina, K. Fu. Privacy of Home Telemedicine: Encryption is Not Enough. Design of Medical Devices Conference, Minneapolis, MN, April 2009.