Spring 3-23-2018

THE IMPACT OF ORGANIZATIONAL CONFLICT ON THE SECURITY IMPERATIVE FOR IMPLANTABLE MEDICAL DEVICES: A CASE STUDY APPROACH

Helen B. Hernandez
Nova Southeastern University, hh436@mynsu.nova.edu

Steven D. Zink
University of Nevada, Reno, Emeritus, stevenz@unr.edu

THE IMPACT OF ORGANIZATIONAL CONFLICT ON THE SECURITY IMPERATIVE FOR IMPLANTABLE MEDICAL DEVICES: A CASE STUDY APPROACH

Helen B. Hernandez
Nova Southeastern University
hh436@mynsu.nova.edu

Steven D. Zink
University of Nevada, Reno, Emeritus
stevenz@unr.edu

ABSTRACT

Patient safety should be the primary concern in implantable medical devices (IMD). The growing threat of security attacks on networkable IMDs is an obvious risk to patient safety, because it can involve injury or death to the patient. In the case of insulin pumps, vulnerabilities are well-documented and security frameworks have been recommended. In addition, several government bodies have issued multiple advisories about security threats to IMDs. Furthermore, there is an ISO standards initiative to promote secure design for insulin pumps and associated devices. However, device manufacturers look to the U.S. Food and Drug Administration (FDA) for guidance during the pre-market approval process, and no standards are being enforced. To date, a convincing cost/benefit analysis of the security issues has remained elusive. Structuration theory has been used as a lens to understand the organizational process and the consequences of their choices.

Keywords

Implantable medical device, insulin pump, security, vulnerabilities, conflict, organization, secure design

INTRODUCTION

The advanced capabilities of implantable medical devices (IMD) that can be administered remotely have introduced a future-centric means of delivering healthcare (Aram, Shirvani, Pasero and Chouikha, 2016). IMDs connect through ubiquitous networks which places the devices within the familiar Internet of Things (IoT) vector targeting network interfaces (Marin, Singelée, Yang, Verbauwhede and Preneel, 2016) and device software (Zhang, Raghunathan and Jha, 2013). Cyber security experts have appealed to the U.S. Congress in an effort to alert policy makers about the risks inherent in this new and promising method of health delivery (Understanding the role of connected devices in recent cyber-attacks, 2016).

Medical device manufacturers have been reluctant to address security safeguards. Researchers reflect on a, “manufacturing mindset and culture established before the IoT ever sprang into being” (Khera, 2017, p. 211). To date, a convincing cost/benefit analysis of the security issues has remained elusive. To investigate this issue, this paper will use Baskerville’s (1996) third-level security notation framework for method engineering to define a security imperative for IMDs. Structuration theory and the conflict between subjective and objective realities in the organizational structure (Orlikowski and Robey, 1991) will be used as a lens to understand the organizational processes that moderate the relationship between the security imperative and design of medical devices. The insulin pump will serve as a case study of the factors that affect secure design of this type of IMD.

LITERATURE REVIEW

Limited research exists about organizational perspectives that address why insulin pump security remains a major ongoing issue despite the availability of suitable risk analysis and countermeasures. For example, processor power in insulin pumps has improved within the least five to seven years **and** enables a cryptographic AES-based solution optimized for energy consumption to function as an, “external shield” (Marin et al., 2016, p. 114) against the wireless network interface attack vector. However, current insulin pump market leaders continue to use unencrypted Bluetooth technology on the basis that limited close-range communication provides sufficient security protection. Such claims are illusory as data from medical devices can be intercepted remotely (Applegate, 2013). The hacker tool *Ubertooth One* allows attackers “more than a kilometer away” (Wolfe, 2017, p. 54) to intercept and download stored information from a device.

To establish the theoretical groundwork for sense-making of the phenomenon, this literature review introduces theoretical aspects of the security imperative by Baskerville (1996) and provides examples of structural artifacts (Jones and Karsten, 2008; Orlikowski and Robey, 1991) in the organizational context of medical device manufacture. A review of research in clinical practice allows insight about security threats for insulin pumps from the perspectives of medical professionals.

A comprehensive examination of vulnerabilities, risk models, and frameworks is important to provide a status of medical device security literature published by cyber security experts.

The Security Imperative

Traditionally, system security by design has been difficult to achieve, particularly in new products, as it frequently conflicts with functionality (Baskerville, 1996). Technology development requirements, however, continue to advance rapidly. Wireless connectivity is a key feature for IMDs, but the risk of inadequate security design accelerates with the number of devices connected to the IoT (Khera, 2017; Zhang et al., 2015). The impact on personal health and safety due to potentially inadequate security has raised the stakes to ensure appropriate safeguards. Researchers emphasize that medical device interoperability and cyber security go hand in hand for the safe use of IMDs such as insulin pumps (Jones and Katzis, 2017).

Organizational Conflict: Duality of Structural Artifacts

Conflicting “realities of organizational structure” (Baskerville, 1996, p. 13) arise when participants each construct their reality differently. Orlikowski and Robey (1991) assert the duality of such a condition because conflict is a social phenomenon and contains subjective and objective elements. As a result, development methods that include the security imperative may not reflect the reality of the structural artifact. This occurs where participants impose their [subjective] reality of meeting a deadline over [objective] concerns that the decision of building an IMD with little attention to security flaws may cause a major backlash down the road.

Security Imperative and Conflicting Realities

Baskerville’s (1996) framework for method engineering includes security elements in the design that define risks, assets, and safeguards. These are linked through the levels of artifacts and add the capacity to produce an information system responsive to the organizational structure. Baskerville’s view concurs with Orlikowski and Robey (1991) in their assumption that individuals, groups, and organizations should be treated as different levels of analysis. The elements of Baskerville’s framework illustrate the multi-dimensional structure of the artifacts contained in the security imperative.

Orlikowski and Robey (1991) positioned Giddens’ structuration theory into a framework to address the organizational consequences of using a given system development method. Their assumptions about the relationship between structure and action center on how information technology is created and used. Structuration theory explains the difference between subjective views where a lack of emphasis on consequences prevails and objective views where the focus is on characteristics and rules. This reflects the potential “collision of objects” (p. 147) in social systems such as organizations that are “created by human action and then serve to shape future human action” (p. 147). If the subjective mindset to relax security design in favor of responding to customer-centric features collides with the objective mindset that the security imperative is a logical concept, the human action that attempts to address this conflict determines further action within the organization.

Unfortunately, people in organizations may allow their actions to be affected by the power of “socially constructed abstractions” (Orlikowski and Robey, 1991, p. 147). Jones and Karsten (2008) confirm Giddens’ stance that the effect of technology depends on how social agents carry out their actions. They refer to the voluntariness of human actions and base this interpretation on Giddens’ theories when asserting that, “structure is always enabling as well as constraining” (p. 132).

Security Risks

Relevant literature identifies risks associated with medical devices as errors, malfunctions, and attack vectors (Aram et al., 2016; Bergenstal et al., 2013; Camara, Peris-Lopez and Tapiador, 2015; Heinemann et al., 2015; Khera, 2017; Ross, Milburn, Reith, Wiltshire and Wheeler, 2015). Ill-disposed adversaries who attempt to intercept and modify settings on insulin pumps are of interest for this proposed study. While no malicious hacking incidents have yet been made public (Sackner-Bernstein, 2017), clinical researchers acknowledge that improper settings on insulin pumps can lead to severe injury or death (Bergenstal et al., 2013; Ismail-Beigi, 2012) and could be induced by active adversaries (Applegate, 2013; Sackner-Bernstein, 2017).

A general assumption is that only sensitive targets are at risk, but research shows that IMDs—in their current design—are widely susceptible to exploits (Applegate, 2013; Rushanan, Rubin, Kune and Swanson, 2014; Sackner-Bernstein, 2017). Researchers point out worst-case scenarios and have demonstrated how an attacker can penetrate the system and change settings on IMDs, including insulin pumps (Kramer and Fu, 2017; Li, Raghunathan and Jha, 2011).

Assets

IMD security researchers report that patient safety, patient health, and the medical device itself require risk assessment and protection (Arney, Venkatasubramanian, Sokolsky and Lee, 2011; Blauw, Keith-Hynes, Koops and DeVries, 2016; Klonoff, 2017; Kramer and Fu, 2017). While this proposed study is limited to attack vectors pursued by active adversaries to control an IMD, the list of assets requiring protection includes potential connections to data centers via the Internet (Zhang et al., 2015).

Patient safety is at risk when IMD settings can be changed or deleted and result in an incorrect actuation of treatment. If this situation is not corrected, the patient's health is impacted because an insulin pump is an important device designed to respond to chronic health conditions and to stabilize the human endocrine system. Uninterrupted operation of the device is crucial to the patient's health.

IMD structure and firmware are not immune to damage from introduction of malware or from side-channel attacks (Arney et al., 2011; Camara et al., 2015). A damaged insulin pump could require costly technical support, a visit to the Doctor's office to reprogram individualized pump settings, or replacement of parts in question. A new insulin pump not covered by insurance can cost around $5,000 to replace.

Safeguards

Present safeguards for an IMD consist of operating integrity, access control, and error detection (Blauw et al., 2016; Sackner-Bernstein, 2017; Zhang et al., 2015). The software that controls the settings on IMDs, such as insulin pumps, should be encrypted and communicate with an appropriate authorization protocol to other devices (Blauw et al., 2016; Marin et al., 2016). Software should be subject to standards (Diabetes Technology Society, 2016), and upgrades should incorporate findings from manufacturers' post-market risk evaluations (Understanding the role of connected devices in recent cyber-attacks, 2016).

Communication directions, frequency, and protocols should be carefully assessed (Blauw et al., 2016; Kramer and Fu, 2017). In addition, alarms are crucial for error detection during the operation of insulin pumps because they frequently initiate an insulin dosage adjustment (Bergenstal et al., 2013; Heinemann et al., 2015). If an attacker disables an alarm, the user would not be aware of critical highs or lows in user blood glucose level to take recommended action (Ismail-Beigi, 2012). Third-party testing is recommended to assure that such safeguards are functioning as intended (Sackner-Bernstein, 2017).

METHODOLOGY

Theoretical Model

The proposed theoretical medical shown in Figure 1 is based on the third-level security notation framework for method engineering by Baskerville (1996) and describes the, "security element representation notation" (p. 18). Baskerville's framework is modified to reflect the specific criteria representing a security imperative for implantable medical devices (IMDs). The proposed framework to achieve secure design is moderated by the organizational conflict containing subjective and objective elements. To investigate the causality of the factors that affect the secure design of IMDs, a critical realist case study approach will be used. This allows the capturing of the participants' subjective meanings of the phenomenon. Critical realist-based research provides the foundation, "how and why a phenomenon occurred" (Wynn and Williams, 2012, p. 788). Objective elements will be captured by performing a, "categorical aggregation to establish themes or patterns" (Creswell, 2013, p. 190) appropriate for case study research, using the third-level security notation framework by Baskerville (1996) as a guide.

The Security Imperative for Implantable Medical Devices

This proposed case study will focus on risks posed by active adversaries, the protection of assets (patient safety, patient health, and the insulin pump device), and the safeguards recommended for protection (operating integrity, access control, error detection). In the case of insulin pumps where security vulnerabilities provide attack vectors that can potentially be used by active adversaries, protective safeguards are needed to ensure patient safety, patient health, and the uninterrupted operation of the device. These safeguards must consist of operating integrity, provide secure access control, and include error detection functions to alert the user when settings are changing, a possible indication that an active adversary makes an attempt to penetrate or has successfully hijacked the system.

H1: The security imperative for IMDs framework can achieve secure design in insulin pumps when risks of active adversaries are identified and when safeguards such as operating integrity, access control, and error detection are implemented to protect patient safety and health as well as the medical device itself. There is a positive relationship between the implementation of the security imperative and the secure design of the medical device.

H2: The organizational conflict that arises due to the duality of subjective and objective elements in the organizational structure is a moderator to the relationship between the security imperative and secure design when participants' realities collide.

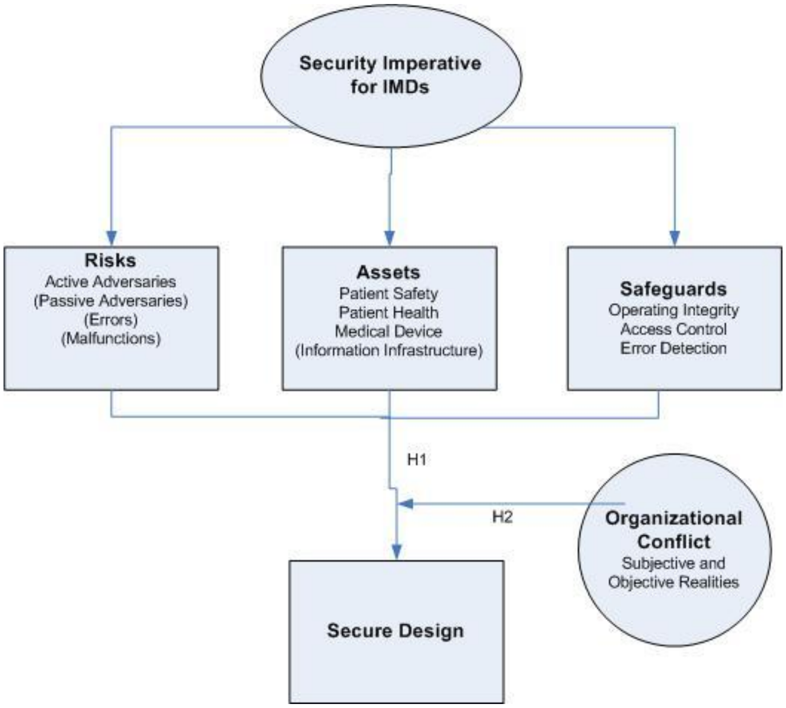

Figure 1. The Security Imperative for IMDs Model

Measurements and Analysis

This study will use purposive sampling via an Internet-based survey to collect information from a broad range of medical device stakeholders. Open-ended questions will be subject to approval by the Nova Southeastern University Institutional Review Board (IRB). Those to be surveyed include: Cybersecurity experts, who focus on medical device security; clinical researchers familiar with insulin pump therapy; government officials and lawmakers with an expressed interest in medical device security; clinical and security researchers who have focused specifically on diabetes device security; members of the IEEE standards group who recently completed the ISO/IEEE 11073 standard for Personal Health Devices (X73PHD); insulin pump manufacturer representatives; and individuals presently using insulin pump therapy. Follow-up personal contact with additional questions or to clarify any items is recommended and anticipated (Salkind, 2013).

Case study research is ideal to obtain a thorough account of what is occurring (Salkind, 2013) and to derive, “detailed, contextualized inferences” (Bhattacherjee, 2012, p. 107) to understand the dynamic process underlying the phenomenon. A purposive sampling method is appropriate when, “all participants have experience of the phenomenon being studied” (Creswell, 2013, p. 155). The Baskerville (1996) third-level security notation framework for method engineering will provide the foundation to arrive at objectives for data collection. According to Dhillon and Torkzadeh (2006), a theory is suitable as an, “initial guide for design and data collection” (p. 303).

The survey will consist of open-ended questions because little is known about the nature of the phenomenon, and this method will allow for a broad response (Salkind). According to Tan and Hunter (2002), obtaining narratives through open-ended questions is a suitable approach. It reflects how humans, “construct and organize reality” (p. 1) and serves to understand and interpret, “the social actions of developers and users involvement in the development of IS” (p. 1). A literature review of the comprehensive identification and analysis of potential IMD threats will form the basis for the topics covered by the open-ended questions.

To create a framework that would allow the assessment if and what type of organizational factors moderate the relationship between the security imperative and the secure design of IMDs, systematic classification and interpretation of the data into codes and themes will be performed using the value-focused approach to security as suggested by Dhillon and Torkzadeh (2006). This allows for the structuring of values and related objectives to be grouped according to the security notation framework into risks, assets, and safeguards. The subjective and objective realities identified in the same context will be rated based on feedback from participants to assess if those hinder or contribute to the secure design of IMDs.

A pilot survey will be distributed to graduate students of information systems and computer science to solicit feedback to eliminate poor wording choices and potential sources of confusion. This will enable a consensual validation of the instrument by seeking the opinion of other IS researchers because of their implied competence in the field of information systems and information systems security (Creswell, 2013). The literature review of IMD attack vectors and the pilot survey will serve to establish content validity and the range of each construct (Petter, Straub and Rai, 2007).

CONTRIBUTION OF THE STUDY

The primary motivation for this study is to find plausible explanations that might shed light on the apparent reluctance of IMD manufacturers to introduce comprehensive security features during the design phase. The implication being made is that manufacturers design insulin pumps with certain built-in security features that are sufficient to satisfy the requirement for FDA product approval to market. However, a more robust design is recommended based on the overwhelming volume of research, case studies, and standards efforts to reduce security risks and protect the users of IMDs from physical harm.

Statistics gathered in 2015 (McAdams and Rizvi, 2016) show that an estimated 350,000 people in the United States alone use insulin pump therapy. Applegate (2013) warns about a careless mindset that dispels the notion of kinetic cyber-attacks as an aberration. A requirements determination for the design of information technology must include the security imperative (Baskerville; 1996). Medical device security experts agree that, “security is most effective when designed into the system from the very initial development cycle” (Sametinger, Rozenblit, Lysecky and Ott, 2015, p. 80). Using the concept of duality of structures (Orlikowski and Robey, 1991) to help distinguish between objective and subjective realities, this proposed study attempts to identify organizational factors that moderate the relationship between the security imperative and the secure design. The information gathered from surveys and follow up interviews will be analyzed to identify and assess their impact on this relationship.

REFERENCES

1. Applegate, S. D. (2013) The dawn of kinetic cyber, in *2013 5th International Conference on Cyber Conflict (CyCon),* IEEE Press, 1-15.
2. Aram, S., Shirvani, R. A., Pasero, E. and Chouikha, M. F. (2016) Implantable medical devices; Networking security survey, *Journal of Internet Services and Information Security,* 6, 3, 40-60.
3. Arney, D., Venkatasubramanian, K. K., Sokolsky, O. and Lee, I. (2011) Biomedical devices and systems security, in *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE*, IEEE Press, 2376-2379.
4. Baskerville, R. (1996) Structural artifacts in method engineering: The security imperative, in Sjakk Brinkkemper, Kalle Lyytinen and Richard J. Welke (Eds.) Method Engineering, Springer-Science+Business Media, B.V., Dordrecht, Netherlands, 8-28.
5. Bergenstal, R. M., Klonoff, D. C., Garg, S. K., Bode, B. W., Meredith, M., Slover, R. H., ... and Kaufman, F. R. (2013) Threshold-based insulin-pump interruption for reduction of hypoglycemia, *New England Journal of Medicine,* 369, 3, 224-232.
6. Blauw, H., Keith-Hynes, P., Koops, R. and DeVries, J. H. (2016) A review of safety and design requirements of the artificial pancreas, *Annals of Biomedical Engineering*, 44, 11, 3158-3172.
7. Camara, C., Peris-Lopez, P. and Tapiador, J. E. (2015) Security and privacy issues in implantable medical devices: A comprehensive survey, *Journal of Biomedical Informatics*, 55, 272-289.
8. Creswell, J. (2013) Qualitative inquiry and research design: Choosing among five approaches (3rd ed.), Sage, Thousand Oaks, CA.
9. Diabetes Technology Society (2016) *Standard for Wireless Diabetes Device Security (DTSec),* May 23, 2016 Version 1.0, DTSEC-2016-08-001, retrieved from https://www.diabetestechnology.org/dtsec-standard-final.pdf.
10. Dhillon, G. and Torkzadeh, G. (2006) Value-focused assessment of information system security in organizations, *Information Systems Journal,* 16, 3, 293-314.
11. Heinemann, L., Fleming, G.A., Petrie, J. R., Holl, R. W., Bergenstal, R. M. and Peters, A. L. (2015) Insulin pump risks and benefits: A clinical appraisal of pump safety standards, adverse event reporting, and research needs: A joint

statement of the European Association for the Study of Diabetes and the American Diabetes Association Diabetes Technology Working Group, *Diabetes Week,* 38, 4, 716-722.

12. Ismail-Beigi, F. (2012) Glycemic management of type 2 diabetes mellitus, *New England Journal of Medicine,* 366, 14, 1319-1327.
13. Jones, M. R. and Karsten, H. (2008) Giddens's structuration theory and information systems research, *MIS Quarterly,* 3, 1, 127-157.
14. Jones, R. W. and Katzis, K. (2017) Cybersecurity and the medical device product development lifecycle, *Studies in Health Technology and Informatics*, 238, 76-79.
15. Klonoff, D. C. (2017) Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical Internet of things, *Journal of Diabetes Science and Technology,* 11, 4, 647-652.
16. Khera, M. (2017) Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications, *Journal of Diabetes Science and Technology,* 11, 2, 207-212.
17. Kramer, D. B. and Fu, K. (2017) Cybersecurity concerns and medical devices: Lessons from a pacemaker advisory, *Journal of the American Medical Association*, 318, 21, 2077-2078.
18. Li, C., Raghunathan, A. and Jha, N. (2011) Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system, in *2011 13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, 150-156.
19. Marin, E., Singelée, D., Yang, B., Verbauwhede, I. and Preneel, B. (2016, March) On the feasibility of cryptography for a wireless insulin pump system, in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy,* March, 2016, 113-120.
20. McAdams, B. H. and Rizvi, A. A. (2016) An overview of insulin pumps and glucose sensors for the generalist, *Journal of Clinical Medicine*, 5, 1, 1-17.
21. Orlikowski, W. J. and Robey, D. (1991) Information technology and the structuring of organizations, *Information Systems Research,* 2, 2, 143-169.
22. Petter, S., Straub, D. and Rai, A. (2007) Specifying formative constructs in information systems research, *MIS Quarterly*, 31, 4, 623-656.
23. Ross, P. L., Milburn, J., Reith, D. M., Wiltshire, E. and Wheeler, B. J. (2015) Clinical review: Insulin pump-associated adverse events in adults and children, *Acta Diabetologica,* 52, 6, 1017-1024.
24. Rushanan, M., Rubin, A. D., Kune, D. F. and Swanson, C. M. (2014) *SoK: Security and privacy in implantable medical devices and body area networks*, Paper presented at the 2014 IEEE Symposium on Security and Privacy (SP), 524-529.
25. Sackner-Bernstein, J. (2017) Design of hack-resistant diabetes devices and disclosure of their cyber safety, *Journal of Diabetes Science and Technology*, 11, 2, 198-202.
26. Salkind, N. J. (2011) Exploring research (8th ed.), Pearson, Boston.
27. Sametinger, J., Rozenblit, J., Lysecky, R. and Ott, P. (2015) Security challenges for medical devices, *Communications of the ACM*, 58, 4, 74-82.
28. Tan, F. B. and Hunter, M. G. (2003) Using narrative inquiry in a study of information systems professionals, in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, January, IEEE, 1-7.
29. *Understanding the role of connected devices in recent cyber attacks: Joint hearing before the Subcommittee on Communications and Technology & Subcommittee on Commerce, Manufacturing, and Trade*, House of Representatives, 115th Cong. (2016) (Testimony of Kevin Fu).
30. Wolfe, H. B. (2017) The mobile phone as surveillance device: Progress, perils, and protective measures, *Computer*, 50, 11, 50-58.
31. Wynn Jr., D. and Williams, C. K. (2012) Principles for conducting critical realist case study research in information systems, *MIS Quarterly*, 36, 3, 787-810.
32. Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X. and Luo, H. H. (2015) Security and privacy for mobile healthcare networks: From a quality of protection perspective, *IEEE Wireless Communications,* 21, 4, 104-112.
33. Zhang, M., Raghunathan, A. and Jha, N. K. (2013) Towards trustworthy medical devices and body area networks, in *Proceedings of the 50th Annual Design Automation Conference (DAC '13),* ACM Press, 14-19.