Towards Strengthening the Security of Healthcare Devices using Secure Configuration Provenance

Ragib Hasan
Department of Computer Science
University of Alabama at Birmingham
Birmingham, AL 35294, USA
ragib@uab.edu

***Abstract*—In modern healthcare, smart medical devices are used to ensure better and informed patient care. Such devices have the capability to connect to and communicate with the hospital's network or a mobile application over wi-fi or Bluetooth, allowing doctors to remotely configure them, exchange data, or update the firmware. For example, Cardiovascular Implantable Electronic Devices (CIED), more commonly known as Pacemakers, are increasingly becoming smarter, connected to the cloud or healthcare information systems, and capable of being programmed remotely. Healthcare providers can upload new configurations to such devices to change the treatment. Such configurations are often exchanged, reused, and/or modified to match the patient's specific health scenario. Such capabilities, unfortunately, come at a price. Malicious entities can provide a faulty configuration to such devices, leading to the patient's death. Any update to the state or configuration of such devices must be thoroughly vetted before applying them to the device. In case of any adverse events, we must also be able to trace the lineage and propagation of the faulty configuration to determine the cause and liability issues. In a highly distributed environment such as today's hospitals, ensuring the integrity of configurations and security policies is difficult and often requires a complex setup. As configurations propagate, traditional access control and authentication of the healthcare provider applying the configuration is not enough to prevent installation of malicious configurations. In this paper, we argue that a provenance-based approach can provide an effective solution towards hardening the security of such medical devices. In this approach, devices would maintain a verifiable provenance chain that would allow assessing not just the current state, but also the past history of the configuration of the device. Also, any configuration update would be accompanied by its own secure provenance chain, allowing verification of the origin and lineage of the configuration. The ability to protect and verify the provenance of devices and configurations would lead to better patient care, prevent malfunction of the device due to malicious configurations, and allow after-the-fact investigation of device configuration issues. In this paper, we advocate the benefits of such an approach and sketch the requirements, implementation challenges, and deployment strategies for such a provenance-based system.**

I. Introduction

Healthcare devices are getting smarter, with the capability to communicate with the healthcare providers as well as the ability to perform in-device computations and analysis. The combination of the Internet of Things (IoT) technology with healthcare devices has led to the development of smart healthcare devices. According to Reports and Data, globally, the market for IoT devices in healthcare settings is predicted to grow from US$ 60.83 billion in 2019 to US $260.75 billion in 2027. This corresponds to a Compound Annual Growth Rate (CAGR) of 19.8% [1]. Such devices improve health monitoring, device performance, and the ability to quickly and remotely update a device's settings by healthcare providers. For example, smart pacemakers or Cardiovascular Implantable Electronic Devices (CIED) are often paired with a mobile app running on a smartphone. Doctors can then use the smartphone app to monitor the pacemaker's performance, and update new configuration settings on the pacemaker. A recent study by Tarakji et al. [2] shows that the use of a smart pacemaker along with a mobile app based monitoring and control improves the remote monitoring of the pacemaker's performance. Similarly, other devices such as insulin pumps have been developed to improve monitoring and control of insulin delivery for diabetic patients [3]. Such developments along with the market forecasts show that the use of smart healthcare is already making important improvements to patient care and the use of these devices will continue to grow in the coming years.

However, the connectivity and smart capabilities also open the door to security vulnerabilities. In [4], Baker et al. discuss the myriad security issues and challenges that affect such smart healthcare devices. In particular, the vulnerabilities in short range and long range communication protocols can allow an attacker to compromise a smart healthcare device and change the settings and configurations, which in turn can be fatal for the patient [4]. In [5], Karunarathne et al. presented three case studies of how malicious parties can remotely take over or install malicious configurations in smart insulin pumps, pacemakers, or pain management infusion pumps. This shows the importance of monitoring and controlling the changes to configuration of a smart healthcare device. Healthcare providers also can share or distribute device configurations; for example, the on-duty nurse might update the configuration settings which was given to him or her by the doctor remotely. It is therefore extremely important to verify the integrity of such configuration updates. We must ensure that the configuration update originated from and propagated through the proper distribution paths (e.g., doctor to nurse to the healthcare device). Also, for after-the-fact forensic investigations of a device malfunction resulting in harm to the patient, we need a way to evaluate the history of the configurations in a smart healthcare device.

978-1-6654-8149-6/22/$31.00 ©2022 IEEE
DOI 10.1109/ICDH55609.2022.00043

In this paper, we propose the use of secure provenance to ensure the trustworthiness of smart medical device configuration updates as well as the configuration history of such devices. Provenance or the history and origin of objects is a widely used technique to verify the authenticity of paintings, archaeological artifacts, and manuscripts. In computing, provenance refers to the origin and propagation history of objects [6]. Secure provenance [7], [8] provides a secure mechanism to verify the trustworthiness of the provenance information itself. We argue that verifiable secure provenance provides a mechanism to ensure the security of configuration updates as well as device configuration history. It is important to evaluate the trustworthiness of a device configuration before applying it to the device. Authentication and access control alone will not provide the expected security – an otherwise trusted healthcare provider may inadvertently apply a malicious or untrustworthy configuration to the healthcare device. Therefore, it is crucial to examine not just the credential of the person applying the update, but also the provenance of the configuration update itself. Also, healthcare devices can and should maintain the provenance of their own configurations over time. This allows examination of the devices configuration changes over time so that it is possible to investigate the cause of the device's malfunction.

To this end, we provide the sketch of how secure provenance can be used in smart healthcare devices, keeping in mind the resource constraints in such devices. The contributions of this paper are as follows:

1) We show how secure provenance of configurations and device states can help improve the security of smart healthcare devices, and

2) We provide the outline of a system of secure provenance for smart healthcare device configurations.

The rest of the paper is organized as follows: in Section II, we provide background information on provenance and techniques to secure it and also give an overview of related work. In Section III, we present the outline of a scheme for secure configuration and device state provenance for smart healthcare devices. In Section IV, we present the challenges in secure provenance for smart healthcare devices. Finally, we conclude and present our plans for future work in Section V.

II. Background and Related Work

A. Secure Provenance

In the world of arts, archaeology, manuscripts, and other rare artifacts, provenance is a widely used technique to verify the authenticity of an object. Provenance refers to the origin and propagation history of such objects [9]. For example, paintings are associated with certified provenance that show when the painting was created by the artist, and a list of owners of the artwork over time all the way to the current owner. The presence of a verifiable provenance indicates the authenticity of the object. In recent years, researchers have taken the concept of provenance and applied it to digital objects such as files, clouds, and databases. Simmhan et al. [9] provides a detailed discussion of the use of provenance in various e-science applications. Efforts to provide integrity assurances for provenance information led to various secure provenance schemes. In our prior work [8], [10], we demonstrated the use of secure provenance chains to verify the sequence of events in the provenance of files. Similarly, researchers have developed such schemes for networks, databases, and cloud computing systems [11]–[15]. Techniques to secure the integrity of provenance include secure provenance chains [10], Bloom-filter based secure accumulators [14], Blockchains [16], and operating system extensions [17]. While there have been efforts to introduce provenance for Internet of Things devices [18], there has not been a lot of efforts in using secure provenance techniques for protecting device configuration updates in smart healthcare devices.

B. Smart Healthcare Device Security

Researchers have explored different techniques to harden the security and privacy of smart healthcare devices. In their seminal work, Halperin et al. [19] presented the concept of security and privacy for implantable medical devices and discussed the requirements and challenges. Karunarathne et al. [5] provide a more recent and detailed discussion of the challenges in securing healthcare devices. Researchers have developed various authentication and access control mechanisms for smart healthcare devices. For example, Wazid et al. [20] presented an elliptic curve cryptography based lightweight remote user authentication scheme for implantable medical devices. Yang et al. [21] developed a lightweight end-to-end scheme for securing the communication between smart healthcare devices and healthcare providers and data users. Taking a different approach, Tiwari et al. [22] used the concept of Smart Semantic Healthcare to ensure the secure data exchange and interoperability for smart healthcare devices. Other work include authentication [23], access control [24], and privacy [25]. However, researchers have not fully explored the use of secure provenance mechanisms in securing healthcare device configurations. In this paper, we explore this research gap and provide an outline of a provenance based solution.

III. Provenance-based Configuration Security for Smart Healthcare Devices

In this section, we discuss how a provenance based model can be used to improve the security of configurations for smart healthcare devices. We start by providing definitions of the building blocks in this model. This model is an extension of our prior work in securing file provenance [8], cloud provenance [14], and interaction provenance [26].

A. Components

The proposed model consists of the following components:

- **Configuration (C):** A configuration is a set of settings corresponding to the operation and state of a healthcare device.
- **Configuration Provenance entry (P):** A provenance entry is the basic building block of the configuration provenance. It includes information on the device type, configuration settings details, timestamps, other metadata, and identify of the entity or user who creates, modifies, or propagates a configuration setting. For example, when a physician creates a configuration setting, a new provenance entry is created. This will contain the identity information of the physician, the complete detail of the configuration settings, and the timestamp of when the entry was created. A digital signature protects the integrity of each provenance entry. Besides the creation, the modification or propagation information is also stored in a provenance entry.
- **Configuration Provenance Chain (PC):** A configuration provenance chain is a signed hash chain of a series of chronologically ordered provenance entries [10]. The hash chain approach prevents insertion or deletion of provenance entries.
- **Device Provenance Chain (DC):** For each smart device, a device provenance chain DC is also maintained. This is a chronologically ordered hash chain sequence of configurations applied to a smart medical device. For resource constrained devices, this chain can be maintained at a trusted cloud based storage service.
- **Provenance Storage Service (PSS):** Ideally, the provenance chain should accompany the configuration as it propagates from one user to another. However, since we assume operating inside a closed medical environment, it is possible to use a centralized storage service to store the provenance chain. This will improve performance and reduce the network overhead of moving provenance information along with the configuration.
- **Provenance Verification Service (PVS):** In each hospital setting, there will be a provenance verification service. Given a configuration (C) and the corresponding provenance chain (PC), the provenance verification service will verify the integrity of the provenance chain and the trustworthiness of the configuration. The trust can be measured by taking into account the reputation of the entities involved in preparing, propagating, or modifying the configuration, as well as the path or environment through which this configuration was propagated.

B. Operation and Usage Model

Here, we outline how such a provenance based system would function.

- **Configuration Creation:** When a new configuration setting is created, the first provenance entry for the configuration is also generated.
- **Configuration Propagation:** When a user receives a configuration from another user, a provenance entry containing the sender and recipient information is generated. It is added to the end of the current provenance chain PC and the hash chain information is updated.
- **Configuration Modification:** If a user modifies a configuration, the changes made are recorded in a new provenance entry P. The provenance entry is then added to the end of the current provenance chain PC accompanying the configuration.
- **Configuration Application and Verification:** Figure 1 shows the workflow for applying a new configuration on a medical device. When a device receives a new configuration setting, it first needs to verify the trustworthiness of the configuration. This step happens after authentication and authorization. To do this, the device invokes the Provenance Verification Service (PVS). PVS examines the configuration and fetches the provenance chain from the Provenance Storage Service (PSS). PVS then goes through the provenance chain to verify if the hash of the final provenance entry matches the computed hash, indicating the integrity of the provenance chain. After verifying the integrity, the PVS can use the information stored within the provenance chain to compute a trustworthiness score as well. The exact process will depend on the organization's policy. The PVS then returns the findings to the device, which then can choose to accept or reject the configuration setting C. The healthcare provider organization can set the policy on what level of trust to expect for configuration settings in order to accept it and apply to a device.

  In case of the device's provenance DC, an investigator examining the device history requests PVS to verify the integrity of the provenance chain. A process similar to the above is used to determine the trustworthiness and integrity of the device provenance chain DC.

C. Threat Model

We assume that the Provenance is stored in PSS in a trustworthy manner and a malicious adversary cannot tamper with it when it is stored in the PSS. The healthcare organization is honest and trustworthy. An attacker can spoof the identity of healthcare providers when sending a malicious configuration to other providers, but they cannot sign the provenance entries with the private keys belonging to honest healthcare providers. We also assume that honest service providers create truthful provenance entries documenting the source, modification, and propagation information of the configuration. We also assume that the provenance verification service PVS is trustworthy.

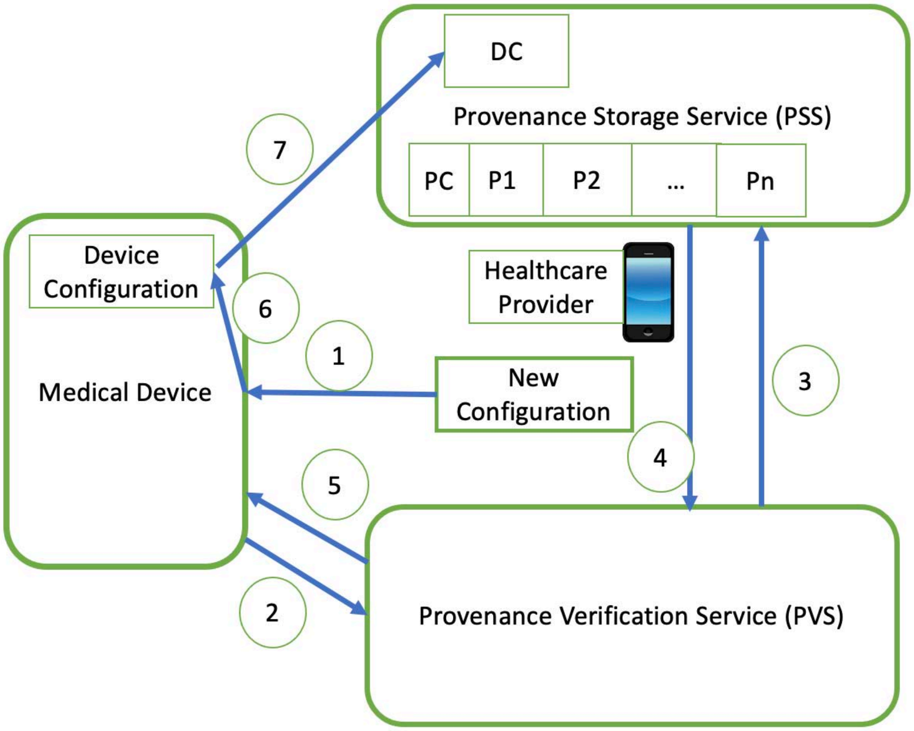

Fig. 1: Workflow for updating Configuration. (1 The healthcare provider sends a new configuration to the device, (2) The device sends it to the Provenance Verification Service (PVS, which (3) requests the Provenance Storage Service (PSS) for the provenance chain belonging to this configuration. (4) The PSS sends the provenance chain to the PVS. (5) If the provenance is verified correctly and is considered trustworthy according to policy, then the PVS sends an approval message to the device. (6) The device then applies the configuration and (7) also updates the Device Provenance chain (DC) on the PSS.

IV. Discussions

In this section, we discuss the challenges and potential issues in creating and operating such a configuration provenance based system.

A. Advantages

There are several advantages of a provenance based system for determining the trustworthiness of configuration settings:

1) First, instead of evaluating trust on a single point of time (i.e., the moment of application of the settings), provenance allows us to look over the entire source and propagation history of the configuration. This is more secure as we can look into a holistic view of the configuration, where it originated from, how it arrived at the ultimate recipient, etc.

2) Next, the use of provenance ensures that we can handle the cases where a malicious configuration is injected into the system and an otherwise honest healthcare provider is duped into applying the malicious configuration to the device. For example, if an adversary spoofs the identity of a physician and sends a malicious configuration to a nurse who unwittingly attempts to apply the configuration, a provenance based system will reject the malicious configuration since it will lack a valid provenance.

3) Also, the use of device provenance allows forensic investigations to be conducted on a device's history of configurations in order to determine any prior malfunctions.

4) Since the provenance chain is stored separately from the device, any takeover of the device does not impact the contents of the provenance chain.

B. Challenges and Deployment Considerations

While this approach is beneficial as discussed above, there are several security, operational, and deployment challenges we need to overcome. Below, we discuss these issues:

- **Device constraints:** Many smart healthcare devices, especially the implantable medical devices, are resource constrained. They have limited computational capability. Such devices are also constrained by power. Therefore, we cannot perform local verification of provenance at the device level, and have to depend on a service like the PVS to verify the provenance. This may create a trust issue as we have to assume the PVS to be trustworthy. Also, requiring the PVS to verify configuration provenance makes it a single point of failure.

To overcome this, we can deploy multiple PVS entities within the organization in order to distribute the load. We can also use a majority voting approach to reduce the chances of a system compromise due to the PVS being under the control of malicious users.

- **Centralized vs. Distributed Provenance Storage:** The provenance chain and other information can be stored centrally or it can be attached to the configuration itself and move with it. As discussed in the outline stated in Section III, we assume the use of the provenance storage service (PSS) to store the provenance. In order to do so, we must assume the PSS to be honest and not compromised by malicious adversaries. The centralized nature of the PSS creates problems similar to those discussed in the previous point. Besides performance issues due to the centralized PSS, we also need to ensure that the PSS is highly secure and trustworthy itself.

  The alternative approach of attaching the provenance information with the configuration itself reduces the load and the trust requirements of the PSS. However, it can create significant network overload as the provenance chain needs to move along with the configuration each time the configuration is sent to a new user.

- **Threat Model:** In our threat model, we assumed that the healthcare organization, the PSS, and the PVS are all trustworthy. However, depending upon the nature of the attacker and their capabilities, this assumption may not always hold. For example, if an attacker can take over the PVS, the attacker can create fake but plausible provenance history for malicious configurations.

- **Deployment and Performance Issues:** In order to deploy this in a healthcare organization, we need to ensure that all healthcare providers working on the configuration are aware of the provenance and will record the provenance accurately. In practice, this may not be feasible as it would require modifying the systems of all providers to ensure accurate recording of provenance information.

  There can be other performance issues as well. Device configuration updates under this system require verification of the provenance of the configuration. This in turn requires multiple calls to the PVS and PSS and verification of a (potentially long) provenance chain. This might impact performance. To resolve this, we can use a cloud based redundant backend to host the PVS and PSS which will improve service performance.

V. Conclusion and Future Work

In this paper, we presented the outline of a provenance-based trust assessment system for smart healthcare device configurations. The proposed system allows verification of the provenance and trustworthiness of the configuration before it is applied to a smart healthcare device. Such a system will make device configuration updates more secure and trustworthy and prevent malicious adversaries from sending flawed and maliciously crafted device configuration to the devices. It can also allow flexible security policies to be written and implemented for smart healthcare devices. Under this system, devices can choose to accept only the configuration coming from trusted and reputable healthcare providers. We believe that this approach can prevent many malicious attacks on the device configurations – for example, the attack when the healthcare provider applying configuration to a device is malicious (as discussed in the attack scenarios in Section II and in [5]). In our future work, we plan to implement the system and evaluate its security and performance in a real healthcare system scenario. In addition, we will augment the model to allow distributed deployment and propagation of of provenance chains as the configuration propagates through the system.

Acknowledgements

This research was supported by the National Science Foundation through awards ACI-1642078 and CNS-1351038.

References

[1] Reports and Data, “Iot in healthcare market to reach usd 260.75 billion by 2027.” Online at https://www.reportsanddata.com/press-release/global-iot-internet-of-things-in-healthcare-market, 2020.

[2] K. G. Tarakji, A. M. Zaidi, S. L. Zweibel, N. Varma, S. F. Sears, J. Allred, P. R. Roberts, N. A. Shaik, J. R. Silverstein, A. Maher, S. Mittal, A. Patwala, J. Schoenhard, M. Emert, G. Molon, G. Augello, N. Patel, H. Seide, A. Porfilio, B. Maus, S. L. Di Jorio, K. Holloman, A. C. Natera, and M. P. Turakhia, “Performance of first pacemaker to use smart device app for remote monitoring,” *Heart Rhythm O2*, vol. 2, no. 5, pp. 463–471, 2021.

[3] N. K. Rege, N. F. Phillips, and M. A. Weiss, “Development of glucose-responsive “smart” insulin systems,” *Current opinion in endocrinology, diabetes, and obesity*, vol. 24, no. 4, p. 267, 2017.

[4] S. B. Baker, W. Xiang, and I. Atkinson, “Internet of things for smart healthcare: Technologies, challenges, and opportunities,” *Ieee Access*, vol. 5, pp. 26521–26544, 2017.

[5] S. M. Karunarathne, N. Saxena, and M. K. Khan, “Security and privacy in iot smart healthcare,” *IEEE Internet Computing*, vol. 25, no. 4, pp. 37–48, 2021.

[6] Y. L. Simmhan, B. Plale, and D. Gannon, “A survey of data provenance in e-science,” *ACM Sigmod Record*, vol. 34, no. 3, pp. 31–36, 2005.

[7] R. Hasan, R. Sion, and M. Winslett, “Introducing secure provenance: problems and challenges,” in *Proceedings of the 2007 ACM workshop on Storage security and survivability*, pp. 13–18, 2007.

[8] R. Hasan, R. Sion, and M. Winslett, “The case of the fake Picasso: Preventing history forgery with secure provenance,” in *Proc. of FAST*, pp. 1–12, USENIX, 2009.

[9] Y. L. Simmhan, B. Plale, and D. Gannon, “A survey of data provenance in e-science,” *SIGMOD Rec.*, vol. 34, pp. 31–36, September 2005.

[10] R. Hasan, R. Sion and M. Winslett, “Preventing history forgery with secure provenance,” *ACM TOS*, vol. 5, pp. 12:1–12:43, Dec 2009.

[11] F. Zafar, A. Khan, S. Suhail, I. Ahmed, K. Hameed, H. M. Khan, F. Jabeen, and A. Anjum, “Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes,” *Journal of network and computer applications*, vol. 94, pp. 50–68, 2017.

[12] A. Bates, B. Mood, M. Valafar, and K. Butler, “Towards secure provenance-based access control in cloud environments,” in *Proceedings of the third ACM conference on Data and application security and privacy*, pp. 277–284, 2013.

[13] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. T. Loo, and M. Sherr, “Secure network provenance,” in *Proceedings of the twenty-third ACM symposium on operating systems principles*, pp. 295–310, 2011.

[14] S. Zawoad, R. Hasan, and K. Islam, “Secprov: Trustworthy and efficient provenance management in the cloud,” in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pp. 1241–1249, IEEE, 2018.

[15] S. Zawoad and R. Hasan, “Secap: Towards securing application provenance in the cloud,” in *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)*, pp. 900–903, IEEE, 2016.

[16] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, “Secure data provenance in cloud-centric internet of things via blockchain smart contracts,” in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 991–998, IEEE, 2018.

[17] A. Bates, D. J. Tian, K. R. Butler, and T. Moyer, “Trustworthy {Whole-System} provenance for the linux kernel,” in *24th USENIX Security Symposium (USENIX Security 15)*, pp. 319–334, 2015.

[18] M. Elkhodr, B. Alsinglawi, and M. Alshehri, “Data provenance in the internet of things,” in *2018 32nd international conference on advanced information networking and applications workshops (WAINA)*, pp. 727–731, IEEE, 2018.

[19] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, “Security and privacy for implantable medical devices,” *IEEE pervasive computing*, vol. 7, no. 1, pp. 30–39, 2008.

[20] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, “A novel authentication and key agreement scheme for implantable medical devices deployment,” *IEEE journal of biomedical and health informatics*, vol. 22, no. 4, pp. 1299–1309, 2017.

[21] Y. Yang, X. Liu, R. H. Deng, and Y. Li, “Lightweight sharable and traceable secure mobile health system,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 78–91, 2017.

[22] S. M. Tiwari, S. Jain, A. Abraham, and S. Shandilya, “Secure semantic smart healthcare (s3hc),” *Journal of Web Engineering*, vol. 17, no. 8, pp. 617–646, 2018.

[23] M. Rostami, A. Juels, and F. Koushanfar, “Heart-to-heart (h2h) authentication for implanted medical devices,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1099–1112, 2013.

[24] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, “Proximity-based access control for implantable medical devices,” in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 410–419, 2009.

[25] W. H. Maisel and T. Kohno, “Improving the security and privacy of implantable medical devices,” *The New England journal of medicine*, vol. 362, no. 13, p. 1164, 2010.

[26] R. Khan and R. Hasan, “Fuzzy authentication using interaction provenance in service oriented computing,” in *Proc. of SCC*, IEEE, Jun 2015.