Toward a Safe Integrated Clinical Environment: A Communication Security Perspective

Denis Foo Kune, Yongdae Kim
{foo,kyd}@cs.umn.edu
University of Minnesota

Krishna Venkatasubramanian, Insup Lee
{vkris,lee}@cis.upenn.edu
University of Pennsylvania

Eugene Vasserman
eyv@ksu.edu
Kansas State University

ABSTRACT

With a vision emerging for dynamically composable and interoperable medical devices and information systems, many communication standards have been proposed, and more are in development. However, few include sufficiently comprehensive or flexible security mechanisms to meet current and future safety needs. In this work, we enumerate security requirements for the communication stack of a medical composition framework. We then survey existing medical and non-medical communication standards and find significant gaps between required properties and those that can be fulfilled even by combinations of currently standardized protocols. This paper is meant to inform future work on building such a comprehensive protocol stack or standardizing protocols and protocol suites that satisfy the properties needed for safe and secure next-generation device coordination.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Data communications, Security and protection*; K.6.5 [**Computing Milieux**]: Security and Protection—*Authentication, Unauthorized access*; J.3 [**Computer Applications**]: Life and Medical Sciences—*Medical information systems*

Keywords

Medical device, integrated clinical environment, security

1. INTRODUCTION

Preventable accidents can be avoided with the introduction of communicating devices in modern clinical settings. For example, during laser procedures in a patient's larynx, an endotracheal tube can be held in place by a high pressure cuff. Reports of the ignition of that cuff due to stray laser strikes have been reported [16], with the situation made worse by the high oxygen levels favoring the ignition. A system that can detect a loss of pressure in the cuff, could instruct a connected laser system to switch off in a fraction of a second, mitigating the possibility of ignition.

Various agencies and standards bodies, including the U.S. Food and Drug Administration, have signaled that *the future of medical technology lies in medical device interoperability*, that can integrate information from multiple clinical sources in a context-sensitive way to guide patient care or prevent common critical mistakes [27, 34]. The benefits of connected integrated clinical environments however, have to be balanced against the possibility of attacks on the communication protocol stacks. Recently, vulnerabilities in standalone medical devices [18] have lead to efforts in building security features into them in addition to the traditional safety focus[12]. The next step is the security and safety of *interconnected and dynamically composable* medical systems. While there is a general agreement that security is important, few existing standards mention specific security considerations or mechanisms for medical systems [6, 8, 20, 25]. Even when discussed, security standards are incomplete, optional, or both, preventing strong security guarantees even when implementing standards-mandated methods. *Gaps in available standardized security mechanisms* can lead to failures in the safety of resulting systems in the presence of insider or outsider adversaries. The purpose of our work is to: (1) draw attention to this increasingly important problem, (2) describe security requirements for communication in integrated clinical environments, and (3) demonstrate the gaps between requirements and features provided by currently standardized protocols.

Interoperability Architecture. In this work, we focus on the ASTM F2761 standard architecture [6] shown in Figure 1, also known as the MD PnP Integrated Clinical Environment (ICE). The idea is to do for medical devices what USB and Bluetooth did for personal computing: devices conforming to the ICE standard, either natively or using an after-market adapter, would be able to inter operate with other ICE-compliant devices, regardless of manufacturer. Logically ICE is separated into the *Supervisor, Network Controller, and devices*, although many components may be implemented on the same physical hardware. Logging and external interfacing, such as off-site patient Electronic Health Records (EHRs), are also supported by dedicated logical components.

Devices perform sensing and/or actuation automatically or on command, i.e. a device may take a blood pressure reading or infuse medication. Coordinating devices may temporarily suppress a high blood pressure alarm if all other

MedCOMM'12, August 13, 2012, Helsinki, Finland.

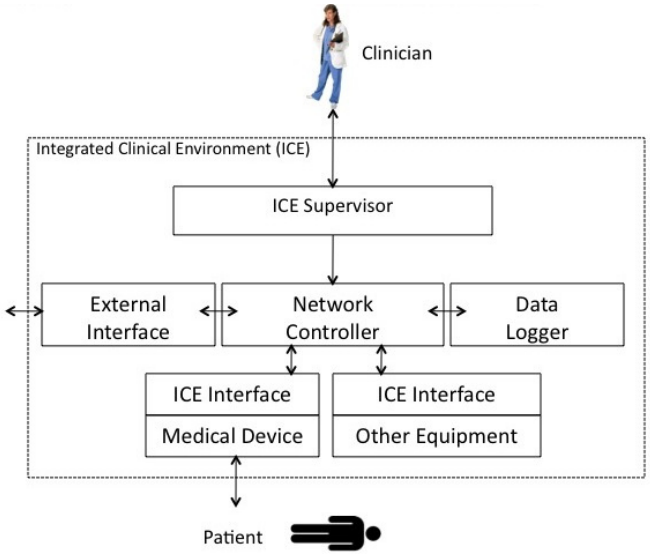

Figure 1: Interoperability architecture of MD PnP ICE

patient vital signs are normal and the just-infused medication is known to elevate blood pressure. Currently, devices from different manufacturers cannot communicate except in very limited ways, so even this simple level of coordination is hard to achieve without a standardized interoperability protocol. ICE allows such coordination — each device communicates with the Network Controller, a sort of "medical router" which does not have any medical/clinical functionality itself, but is responsible for data routing, translation, and quality of service (QoS) enforcement, facilitating communication between devices and the Supervisor. The Supervisor is responsible for executing "clinical workflows," from common and easily scriptable tasks such as taking blood pressure at predefined intervals and recording the results, to more complex procedures like medication interaction monitoring and suppression of likely false alarms. Each component has different connection security, authentication and authorization, logging, and physical protection requirements, which need to be considered in the overall system architecture.

Threat Model. Because ICE makes medical systems *composable at deployment time*, we do not a priori know the target network topology, communication protocols, or transmission media (e.g. wireless or wired). Thus we assume a strong adversary in clinical care contexts, who have access to the communication medium[1]. Therefore the adversaries can eavesdrop on all communication and arbitrarily delay, inject, reorder, or forge packets in the network. Authorized medical staff members are assumed to be trusted.

2. SECURITY REQUIREMENTS

We consider the design of secure interoperable medical systems by focusing on security requirements specific to each OSI communication layer, as well as cross-layer requirements. We evaluate available communication standards against those requirements while keeping the assumptions about deployed systems to a minimum. Table 1 summarizes these requirements and organizes them by the layer at which they must be addressed. We note that physical tamper resistance/evidence, while important, are not protocol issues and are thus out of scope for this paper. The requirements are as follows.

1. **Secure medium access control**: An attacker with access to the wired or wireless medium should not be able to generate forged layer 2 protocol messages that would be accepted by a receiving interface. Confidentiality may be added as needed.
2. **Secure sessions**: Applications hosted by devices should be able to set up end-to-end secure (confidential, authenticated, and timely) communication channels.
3. **Authenticity of application objects**: Each application should be able to authenticate and determine the trustworthiness of its remote communicating principals. Note that even if a device is trusted, not all of its applications may be trusted to generate/access certain data blocks.
4. **User authentication**: The system should ensure that the medical staff and patients are properly identified before granting the appropriate level of access.
5. **Access control of application data**: The system should provide granular access control to application data blocks to enable clinicians and patients to retain control as well as record access to those data blocks.
6. **Timely and secure logs**: Security events anywhere in the stack may generate logs at the application layer, depending on the applicable policy. Those logs should be timestamped and transmitted to a central repository with minimum delay to enable both reconstruction of past events and estimation of likelihood of future events. Once generated, logs should be immutable and maintain accountability for log access.
7. **Alerts for unexpected behavior** (†cross-layer): The system should support the generation and delivery of alerts based on local policy. Alerts generated at each layer of the communication stack may be reported up to the next layer, or directly to the application layer for logging and/or user notification.
8. **Device provisioning and management** (†cross--layer): The system should support binding of devices to a facility-local trusted keying infrastructure to track their life cycle, ensuring revocation when required.
9. **User management** (†cross-layer): The system should enable the management of users interacting with the devices within the system including addition and deletion of new and old users.

3. SURVEY OF EXISTING PROTOCOLS

We focus on single-patient systems with devices connected in a star topology with the coordinator, such as the ASTM F2761 network controller [6], in the center. At layer 2, interface pairing only provides pairwise single-hop protection, but data transferred over a shared hospital network remain unprotected.[2] We thus leverage the properties of layer 4

[1]Proximity allows an attacker to physically harm the patient, but we assume that more subtlety or delay is desired to e.g. prevent detection.

[2]The proposed model might not be a direct fit to existing clinical networks. We thus consider mechanisms that are independent of lower layers to allow a smooth migration path.

Table 1: Requirements satisfied at OSI layers 2, 4 and 7. Items marked '†' span multiple layers.

	Requirement	Layer 2	Layer 4	Layer 7
1	Medium Access	√		
2	Session Security		√	√
3	Data Provenance			√
4	User Authentication		√	
5	Data Access Control			√
6	Logging	√	√	√
7	Alerts†	√	√	√
8	Device Management†	√		√
9	User Management†			√

protocols for end-to-end protection of multi-hop communication. We use layer 7 protocols (which amalgamate layer 5 and 6 functionalities as well) to ensure security, at data unit-level granularity, between components which may only be partially trusted.

In this section, we summarize existing healthcare-specific communication standards, as well as existing layer 2, 4, and 7 protocols specified in those standards, and compare them with our requirements. We begin with a short description ISO 11073 and the Continua standards, discuss the specified layer 2 and 4 protocols, and then examine layer 7 standards, including IHE and HL7.

3.1 Full-stack protocols

ISO/IEEE 11073. The 11073 standards family, though spanning all the layers of OSI stack, only appears to partially satisfy a subset of our requirements. The standards are made up of 4 main groups, namely Device Data, Application Services, Internetworking, and Transport, numbered by group. The *00101-2008, wireless guidelines* document [19] refers to sections typically covered in parts 305xx, including parts of mobile cellular networks, wireless broadband, WLAN, and WPAN. It considers data and network security, leaving physical security out of scope.

The *Data Security* recommendations are limited to U.S. legal requirements for health information, wherein system integrators and operators are ultimately responsible for the risk analysis and choice in the appropriate security mechanisms. We note that some protocols mentioned in this document do not provide adequate building blocks due to weak or broken security, e.g. [31]. The document also recommends the use of encryption only after patient identifiers have been included, leaving a potential window of vulnerability at earlier stages. A follow-up recommendation suggests avoiding security mechanisms between the sensing circuit and the "amplifier" (presumably the processing component of the same device) due to concerns regarding cryptographic overhead. The document focuses on encryption techniques and provides very little detail on message integrity, thus only partially addressing requirements **2** and **3**.

For *Network Security*, the document focuses on 3 components: authentication (presumably of users, which would address requirement **4**), encryption, and firewalls. It mentions 802.1x protocols for authentication (requirement **3**) and AES (in modes of operation specified in current 802.11-series wireless protocols) for encryption and integrity, addressing requirement **1** if the appropriate modes are chosen. Malware is also discussed, but there is no recommendation for reducing this threat short of referring to the FDA's cybersecurity efforts. The document also discusses denial of service (DoS) attacks and intrusion detection and prevention as mitigation mechanisms, which may address requirement **7**, though it is not clear exactly how. Substitution attacks are cast as network security issues, and the document recommends the use of message authentication/integrity codes such as AES in CCMP mode of operation, partially addressing requirements **1** and **2**.

30x series (Transport) documents including *30200 (Cabled), 30300 (Infrared), 30400 (Inter-LAN)* mention little in regard to security, perhaps because they have no built-in security mechanisms. At the time of writing, a document for *305xx(Wireless)* has not yet been finalized, but may offer more insight once released due to security mechanisms already built into the wireless protocols under consideration.

20x series (Internetworking) includes a security section[3] that appears to still be in draft, and no publicly circulated copy was available at the time of writing.

Continua. The Continua reference architecture [9] mentions the Bluetooth Health Device Profile [7] for wireless interfaces, the USB Personal Healthcare Devices [11] protocol for wired interfaces, and the IEEE 11073 Personal Health Device standard [8] for the application data format. Although security is identified as a technical issue, it is not yet clearly addressed in the Continua effort and so cannot be evaluated in our work.

3.2 Layer 2 and 4 protocols

Since most medical standards either mandate or recommend certain data link and transport protocols, it is useful to summarize the available standards here.

Wired. ISO/IEEE 11073 has specifications for cabled serial connections, e.g. RS-232 [1], Ethernet (802.3 family [10]), USB [35], and FireWire [22]. Part 30200 [23] specifies a transport profile for cabled connections. It defines the physical layer, but inherits the upper layers from IrDA [24], so there are no security mechanisms built into the profile. At the physical and data link layers, the document appears to assume that data security relies on physical security. The IEEE 802.3 family of protocols [10] also rely on physical security. The above protocols were not designed with our threat model in mind and do not defend against an attacker with access to the communication medium. Therefore, they do not meet the requirements from Section 2.

Wireless. Due to space constraints, we will focus on the most widely deployed protocols mentioned in the P11073-00101 document [19], namely cellular networks, 802.11 [21], and 802.15 [2, 36] families. Cellular networks can be grouped by generation: 2G includes GPRS and EDGE on GSM networks, 3G has UMTS and CDMA2000, and 4G incorporates LTE and WiMax. While all provide varying levels of security protection, the schemes implemented in 2G networks are known to be weak [31]. UMTS [4] and LTE [3] protection mechanisms, on the other hand, have not had significant vulnerabilities reported. In wireless local area networks (WLAN) we look at the widely-deployed 802.11 [21] family, which appear to satisfy requirement **1** with WPA2 and **4** with 802.1x. Wireless personal area networks (WPAN), Bluetooth, and 802.15.4 [36] provide security mechanisms including device authentication, message encryption, and integrity, thus fulfilling requirements **1** and **4**. However, the key exchange and interface pairings must be controlled by the upper layers, parts of which are not explicitly mandated by 802.15.4, leaving requirement **8** incomplete.

[3]ISO/IEEE 11073-20500 Security - Framework and overview

Due to the nature of radio frequency communication, disruptions in the medium (e.g. jamming) is almost always possible. A large body of work exists on jamming detection, avoidance and resistance, e.g. [37, 38], but these mechanisms are not explicitly mandated in current standards, and so we do not consider them in our evaluation.

Transport. At the transport layer, we consider the TLS v1.2 [14] and DTLS v1.2 [15] protocols for streams and datagrams, respectively. They rely on a public key infrastructure for key/certificate distribution and update, the details of which are not addressed at this layer, and are instead considered at the application layer.

TLS v1.2 provides unidirectional or mutual authentication for secure transport sessions, allowing devices to authenticate in an end-to-end session if they both have certificates signed by a trusted entity, fulfilling requirements **2**, **3**, and **4**, but leaving requirement **8** to the implementer. It supports cryptographic algorithms known to be secure at the time of writing; as far as we are aware, TLS session are considered secure and can provide confidential authenticated end-to-end L4 (OSI transport) channels as long as a good key and certificate management infrastructure is in place.

DTLS v1.2 is the datagram counterpart of stream-focused TLS, but some successful attacks on implementations of DTLS v1.2 have already been disclosed [5], meaning DTLS v1.2 addresses, but does not fully satisfy the same requirements as TLS (**2**, **3**, and **4**).

3.3 Layer 7 (application) protocols

At layer 7, we consider two existing standards for medical device interoperability: Integrating the Health Enterprise (IHE) [25], a healthcare industry consortium that publishes standards to improve the way computer systems in healthcare share information, and Health-Level 7 (HL7) [20], a medical data exchange standard. Table 2 summarizes the extent to which these protocols satisfy the requirements specified in Section 2.

3.3.1 Integrating the Health Enterprise

IHE defines a number of profiles meant to solve specific interoperability issues among medical devices. The current profile list covers a wide range of issues from Anatomic Pathology to Radiology, but only two of the eleven profiles deal directly with security issues when medical devices interoperate, addressing them the transport layer and above.

The **Audit Trail and Node Authentication** (ATNA) profile establishes security measures for patient confidentiality, data integrity, and caregiver accountability [26]. It specifies access control, security audit logging, and secure inter-device communication. The profile defines the notion of a *Secure Node* (SN), which establishes a trusted base for secure interaction with other nodes, and uses access control mechanisms in conjunction with user authentication to secure user-to-node interaction. The SN is most similar to the ICE Network Controller [6]. All aspects of the SN device are assumed to be secure, including data storage and operating system. All interacting Secure Nodes are collectively called a *Secure Domain* (SD), which can be established at the hospital, departmental, or other level of granularity. All machines within this SD are assumed to be "host-authenticated," i.e. known to the operating facility.

Table 2: Summary of Layer 7 standards addressing our security requirements. '$^{\triangle}$' and '*' denote optional and partial fulfillment.

Requirement	IHE	HL7	ICE	11073
2 Session Security	Yes$^{\triangle}$	–	–	Yes*
3 Data Provenance	–	–	–	Yes*
4 User Authentication	Yes*	–	–	Yes
5 Data Access Control	Yes*	Yes	–	–
6 Logging	Yes$^{\triangle}$	Yes$^{\triangle}$	–	–
7 Alerts	–	–	–	–
8 Device Management	–	–	Yes*	Yes*
9 User Management	Yes*	–	Yes*	–

The ATNA profile has two requirements — node authentication and auditing. The authentication aspect has two parts, the first requiring node-user interaction authentication, and the second authenticating inter-node interaction. Node-user authentication enforces and limits the level of access a user gets to various applications on the node, though the details of the access control mechanism are left to the implementer, only partially addressing requirements **4**, **9**, and **5**. Inter-node authentication is certificate-based, requiring mutual authentication, and proposes the use of TLS (assuming v1.2) for end-to-end secure channels between the nodes. Details of the requisite public key infrastructure (generation and maintenance of the certificates for individual devices) are not specified. Finally, the profile does not mandate confidentiality/encryption, focusing instead on the integrity of the channel. As it makes confidentiality optional, this profile only partially addresses requirement **2**.

The *Logging and Audit Trail* aspect of ATNA ensures that all security-related events are logged by the SNs. These events include accesses to a patient's personal health information (PHI), the user performing the access, and node or user authentication failures, and will be generally stored in a centralized repository.

The ATNA profile mandates the use of the DICOM vocabulary [13] for auditing purposes, extended by RFC 3881 [33]. These standards provide the data definitions for reporting security and privacy events.[4] During normal operation, every user login attempt to an SN generates an audit event for both successful and failed actions. The audit messages (or audits) are sent to the repository for storage using the standard Syslog protocol defined in RFCs 5424 and 5426 [17, 32]. To address confidentiality and integrity concerns, RFC 5425 proposes an alternative that sends Syslog messages over TLS [28]. However, this only partially fulfills requirement **6** as we shall see in the next section. IHE also defines an ATNA Radiology-option which is an extension of the profile for radiology purposes. Its requirements mirror those of the base ATNA profile except it mandates that communication between SNs be encrypted, given the sensitivity of the radiology information.

The **Enterprise User Authentication** (EUA) profile has two main tasks — (1) provide centralized authentication management for users thereby enabling single sign-on over the healthcare enterprise, and (2) seamlessly allow a users' context to be transferred between applications on a single machine [26] using a users' authentication credentials, enabling authenticated interoperability between applications. Authentication in EUA is done using Kerberos, the centralized key distribution scheme that provides temporary and

[4]Note that the auditing framework assumes that all the devices and systems are time-synchronized and have the correct timestamp for every event record.

Table 3: Summary of protocols which address various requirements at different layers. '$^{\triangle}$' and '*' denote optional and partial addressing, respectively.

	Requirement	Layer 2	Layer 4	Layer 7
1	Medium Access	11073*, 802.15.4$^{\triangle}$, 802.11i-2004$^{\triangle}$		
2	Session Security		TLS, DTLS*	11073*, IHE$^{\triangle}$
3	Data Provenance		TLS, DTLS*	11073*
4	User Authentication		TLS, DTLS*	11073, IHE*
5	Data Access Control			HL7, IHE*
6	Logging			HL7$^{\triangle}$, IHE$^{\triangle}$
7	Alerts	–	11073*	–
8	Device Management	11073*, 802.15.4$^{\triangle}$, 802.1x	–	11073*, ICE*
9	User Management			IHE*, ICE*, 802.1x

revocable keys for a user and a service to communicate securely [29]. One of the services provided is authenticated user access to the Context Manager (CM) on the machine to which the user is trying to log on. The CM and different client applications use the specifications of the HL7 Clinical Context Object Workgroup (CCOW) [20] to provide seamless movement of a user's context between applications on a single machine. The EUA profile is primarily used to improve the effectiveness of addressing requirement **4**. The use of Kerberos partially fulfills requirement **9**.

3.3.2 Health Level 7

HL7 provides a framework for exchange, management, and integration of electronic health information to support clinical practice and management of healthcare delivery services. Interoperability in HL7 is supported by standardization at five levels of abstraction: conceptual (e.g. RIM), document (e.g. CDA), messaging (e.g. HL7 v2.x and HL7 v3), application (e.g. CCOW), and service (e.g. Arden). Most of the discussion below focuses on HL7 v3 which contains more details of the security specification than HL7 v2 [20]. Security in HL7 is defined in v3 as a service standard in the form of *Privacy, Access and Security Service*. The focus of these standards is from the standpoint of data rather than individual medical devices.

The **Privacy, Access and Security Service** (PASS) defines a set of loosely-coupled service components that enable confidentiality and integrity of healthcare information. The PASS-Audit service describes, at a conceptual level, the requirements that relate to the functional behavior of auditing in a healthcare environment. The service provides two capabilities that would address (partially) requirement **6**: (1) audit submission in response to events generated by Audit Event Sources, and (2) retrieval of audit records with respect to access of personal health information. Further, it specifies that the audit service must have the ability to validate any requests that can be submitted and it must establish a secure communication channel with the querying entity. Events (audits) can be generated by users, information systems or devices. The model used is a generalization of the one used in DICOM, based on RFC 3881 as referenced in the ATNA profile described above.

The PASS-Access Control service presents functionalities required for access to resources in a distributed healthcare setting. The document also specifies the lifecycle of the policies involved in access control. Both these are are currently in the form of unconstrained conceptual specification and do not provide any implementation details. The access control system is responsible for generating audit records based on security relevant information, addressing requirements **5** and **6**. In general terms, HL7 specifies a *Role-Based Access Control* system, and a framework for role engineering, using scenario-based approaches as described in [30], but does not provide details regarding specific roles or permissions, which is left to the implementers.

Table 2 summarizes the requirements satisfied by the IHE, HL7, ISO/IEEE 11073, and ICE standards.

4. DISCUSSION

Table 3 summarizes the various standards examined in this document, and the extent to which they fulfill each security requirement from Section 2. It is clear that not only is there no standard that satisfies all requirements, but even combinations of currently-available standards would not satisfy all the requirements. Moreover, some requirements are not completely addressed by any standard.

Due to the inclusion of physical access to both the wired and wireless medium of the clinical environment in our threat model, we find that wireless protocols may have an advantage with built-in security mechanisms. Using a VPN, such as IPsec in tunnel mode, could help bridge this gap by protecting the packets from the network header in, but this would have to be a deployment architecture decision. This would also aggravate the problem of certificate and key management, and support for all devices in the VPN, some of which may be resource constrained embedded devices. In addition to defenses on the lower layers of the stack, an end-to-end security mechanism at layer 4 is required and good options such as TLS and DTLS exist, but the standards surveyed do not mandate them.

At the application layer, the focus on dynamic composability makes it difficult to consider security without making assumptions about the properties of the underlying network architecture and communication layers. This leads us to conclude that standards specifying a complete stack would be better able to address the requirements comprehensively with size and complexity trade-offs. Both IHE and HL7 discuss security, but the suggested mechanisms are only partial solutions. We also note that a secure time synchronization, critical to addressing requirements **7** and **6**, doesn't appear to be specified in surveyed standards. For this reason, we consider satisfaction of requirement **6** by IHE and HL7 as partial. The IEEE 11073 documents we surveyed define vertical profiles through the communication stack with different data-link components, each with different security properties. Due in part to those options for transport layers and a lack of specification of how application-level user access controls feed into security at the lower layers of the stack, 11073 does not appear to fulfill all requirements.

We developed security requirements in a clinical context, and while we were not expecting current standards to ad-

dress all proposed requirements, we were surprised at the large gaps that exist. Current standards developed for the healthcare industry could benefit from the inclusion of existing secure communication standards. Specifying the use of such existing standards would also simplify the maintenance of already large healthcare standards.

Acknowledgments

This work was supported in part by the National Science Foundation NSF award CPS-1035715 and the NIH/NIBIB Quantum program grant NIH-1U01EB012470.

References

[1] Interface between data terminal equipment and data circuit terminating equipment employing serial binary data interchange. TIA/EIA-232-F, 1997.

[2] Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). *IEEE P802.15.1/D6*, 2005.

[3] 3GPP TS 36.201 V10.0.0 — LTE physical layer; General description (Release 10), 2010.

[4] 3GPP TS 36.331 V10.3.0 — Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification, 2011.

[5] N. AlFardan and K. Paterson. Plaintext-recovery attacks against datagram TLS. In *NDSS*, 2012.

[6] ASTM F-29.21. Medical devices and medical systems — essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE), 2009.

[7] Bluetooth, SIG. Health device profile v1.0. 2008.

[8] M. Clarke, D. Bogia, K. Hassing, L. Steubesand, T. Chan, and D. Ayyagari. Developing a standard for personal health devices based on 11073. In *EMBS*, 2007.

[9] Continua health alliance. `http://www.continuaalliance.org/`.

[10] CSMA/CD access method and physical layer specifications. *IEEE 802.3-2005*, 5, 2005. (Revision of 802.3-2002).

[11] Definition, U.S.B.D.C. USB personal healthcare device profile. *V1.0*, 2007.

[12] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *HotSec*, 2008.

[13] The DICOM standard. `http://medical.nema.org/standard.html`.

[14] T. Dierks and E. Rescorla. The transport layer security (TLS) protocol version 1.2. RFC 5246, 2008.

[15] J. Fischl, H. Tschofenig, and E. Rescorla. Framework for establishing a secure real-time transport protocol (SRTP) security context using datagram transport layer security (DTLS). RFC 5763, 2010.

[16] M. Fried. A survey of the complications of laser laryngoscopy. *Archives of Otolaryngology- Head and Neck Surgery*, 110(1):31, 1984.

[17] R. Gerhards. The Syslog protocol. RFC 5424, 2009.

[18] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Security and Privacy*, 2008.

[19] Health informatics — point-of-care medical device communication — technical report — guidelines for the use of RF wireless technology. *IEEE Unapproved Draft P11073-00101/D03*, 2007.

[20] Health level seven international. `http://www.hl7.org/`.

[21] IEEE. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 1997.

[22] IEEE standard for a high-performance serial bus. *IEEE 1394-2008*, 2008.

[23] IEEE standard for health informatics — point-of-care medical device communication — part 30200: Transport profile — cable connected. *ISO/IEEE 11073-30200:2004(E)*, 2004.

[24] IEEE standard for health informatics — point-of-care medical device communication — part 30300: Transport profile — infrared wireless. *ISO/IEEE 11073-30300:2004(E)*, 2004.

[25] Integrating the healthcare enterprise. `http://www.ihe.net/`.

[26] IHE Integration Profiles. Technical Report, 2011.

[27] K. Lesh, S. Weininger, J. Goldman, B. Wilson, and G. Himes. Medical device interoperability-assessing the environment. In *HCMDSS-MDPnP*, 2007.

[28] F. Miao, Y. Ma, and J. Salowey. Transport layer security (TLS) transport mapping for Syslog. RFC 5425, 2009.

[29] C. Neuman, S. Hartman, and K. Raeburn. The Kerberos network authentication service (V5). RFC 4120, 2009.

[30] G. Neumann and M. Strembeck. A scenario-driven role engineering process for functional rbac roles. In *SACMAT*, 2002.

[31] K. Nohl. Wideband GSM sniffing. `http://events.ccc.de/congress/2010/`, 2010.

[32] A. Okmianski. Transmission of Syslog messages over UDP. RFC 5426, 2009.

[33] G. L. Simmons. Security audit and access accountability message XML data definitions for healthcare applications. RFC 3881, 2004.

[34] D. Tillman and L. Kessler. Medical device interoperability — assessing the environment. In *HCMDSS-MDPnP*, 2007.

[35] USB 2.0 specification, 2000.

[36] Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPANs). *ANSI/IEEE*, 802(4), 2003.

[37] A. Wood and J. Stankovic. Denial of service in sensor networks. *Computer*, 35(10), 2002.

[38] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *MobiHoc*, 2005.