Published in final edited form as:
Inform Secur Appl (2013). 2014 ; 8267: 213–217. doi:10.1007/978-3-319-05149-9_13.

Foundational Security Principles for Medical Application Platforms* (Extended Abstract)

Eugene Y. Vasserman and **John Hatcliff**
Kansas State University

Abstract

We describe a preliminary set of security requirements for safe and secure next-generation medical systems, consisting of dynamically composable units, tied together through a real-time safety-critical middleware. We note that this requirement set is not the same for individual (stand-alone) devices or for electronic health record systems, and we must take care to define *system-level requirements* rather than security goals for components. The requirements themselves build on each other such that it is difficult or impossible to eliminate any one of the requirements and still achieve high-level security goals.

1 Introduction

This position paper is a first step in deriving and elucidating security properties needed for safe operation of next-generation medical systems – sets of medical devices and health information systems, dynamically composable as needed. and enabled by **medical application platforms**. MAPs are safety- and security-critical real-time *open computing platforms* for (a) integrating *heterogeneous devices*, medical information systems, and information displays via a communication infrastructure and (b) hosting application programs (clinical logic and/or workflow automation) that provide medical utility via the ability to both acquire information from, and update/control integrated devices, IT systems, and displays [1]. A MAP can be implemented in a number of ways and environments such as clinical, home-based, mobile, or distributed.

While security alone cannot guarantee safety, it is unlikely that we will be able to achieve safety without security. Current safety evaluation and verification and validations techniques are designed primarily to deal with environmental failures and stand-alone devices or collections of devices that are integrated by a single manufacturer. For medical systems that do include some form of limited dynamic integration and reconfigurability of components such as central station monitors, current safety approaches often dictate that each combination of components requires evaluation as a complete system. This implies that for a system with interchangeable constituents, the manufacturer must gain regulatory approval for every possible permutation of constituent devices forming the composite medical system (which has been termed “pair-wise” approval).[1] For example, if a new type of medical

*Position paper

[1]Details of issues with the current pair-wise regulatory approach can be found in [2].

device is added to the central station monitoring system, then the entire system must be reevaluated. Security is rarely taken into account, dismissed with blanket statements of precautions such as usage of antivirus software on desktops and intrusion detection/prevention in networks. Note that we are referring to the security of medical *platforms* as a whole rather than individual devices. Device security is vital [3, 4], but *does not capture the all security requirements for a system of interoperating devices*.

Experience in consumer electronics with interoperability standards such as USB, WiFi, etc. has shown the success of the "component-wise" certification approach: manufacturers submit their products to third-party certification organizations that verify that the products conform to interfacing and communication standards. These components are then integrated into larger systems/-configurations with high degrees of confidence and without the need to verify each possible combination of components. Of course, the challenges in the area of safety/security-critical medical systems are much greater. However, in the critical systems space, Integrated Modular Avionics [5] and the MILS Security architecture [6] are examples where standards-based architectures and interfaces are being used to encourage the development of a commodity market of safety-critical components, taking security into account explicitly. We believe that lessons learned in these frameworks can help in constructing standards that will allow medical systems to be verified and receive safety evaluations in a component-wise, as opposed to a pair-wise, fashion.

2 Unique Security Challenges

Medical systems are a unique instance of cyber-physical systems (CPS). They often require real-time guarantees which are more strict than other CPSes such as the smart grid. Avionics, power plant control systems, and other industries with federal safety regulations come to mind as the closest analogs, but these systems are *closed* to the outside and physically protected from tampering. Hospitals and other care facilities, on the other hand, rarely incorporate physical access control except for controlled substances, and individual devices are almost never tamper-resistant. Several additional quirks make medical applications unique within the CPS realm. One is the regulatory *requirement for emergency override* – human caregivers must be able to disable safeguards that are designed to ensure safety and security but may, in an emergency, inhibit delivery of needed care. *Medical systems themselves are assumed to be unreliable in determining when such an emergency is taking place.* Therefore, security controls must be subject to disabling – termed "break-glass," [7] such as when pulling a fire alarm breaks a glass rod before activating. Security is especially challenging to implement when it can be disabled. Further, while we cannot rely on authentication during emergencies – it may slow down emergency response – we must maintain (in fact, increase) accountability and logging to ensure that post-hoc event reconstruction and auditing is possible.

3 Minimal Requirements

We suggest a list of security properties (for component-wise evaluated systems) that must be enforced in order to ensure:

- no harm can come to the patient through deliberate tampering with data;

- confidential patient data is not obtained by unauthorized parties;
- regulatory authorities and medical system operators can be confident that only components that are authorized for use are incorporated; and
- in case of an adverse incident, authorities have sufficient information available to support audits to determine the root cause(s) of the incident.

These properties are inspired by, and partially draw from, Anderson's model of clinical information systems [8], but encompass individual composable devices as well as middleware/support system architecture rather than focusing on databases of patient health records or individual devices.

1. **Integrity** to prevent unauthorized alteration of data or code[2] in transit[3] or at rest, and prevent unauthorized physical modification.
2. **Authenticity** for trustworthy *identification* of principals.
3. **Authorization** to codify the actions that an entity is allowed to perform.
4. **Attribution** to allow unambiguous identification of proximal causes of events or sources of data.
5. **Provenance** to record the original source *and chain of possession* of data (i.e., series of attributions). This should be securely and reliably logged.
6. **Availability** to guarantee that the system is reliable for predefined (possibly very small) periods of time.
7. **Timeliness** and transparency of system availability state, i.e., messages are delivered in a timely fashion[4] or not at all, and exposure to the components of the status of the system – whether or not it is *currently* available/reliable.
8. **Confidentiality** to ensure data is not readable by anyone who does not have the correct cryptographic credentials.
9. **Privacy**, which is broader than confidentiality, and is meant to partially control information leakage and inference.

Figure 1 shows property dependencies, but they may differ depending on the point of view. Moving from the bottom up, **provenance** (and secure logging of data and metadata) achieves accountability of original source *as well as intermediate entities*, providing full traceability of data custody and alteration. This can only be achieved by systems providing **attribution** of data to its previous custodian. Attribution in turn relies on the **authenticity** and **integrity** of the data and the device that authored it. Note that **authorization**, while requiring **authenticity** and **integrity**, is somewhat orthogonal, since actions may be allowed under certain circumstances without prior authorization (such as break-glass), as long as they are logged and can later be audited and their provenance traced. **Confidentiality** and **privacy** are likewise orthogonal, since in most cases they are not required for safe operation

[2]Code can include "virtual" software-only "devices".
[3]Data left its producer but has not yet arrived at the final consumer (destination).
[4]As defined by the receiving component

(although they are required by law in some jurisdictions to protect private health information [9, 10]). **Availability** and **timeliness** of events are both required, but not to the same extent in all systems. Not all medical interactions require full real-time guarantees and continuous connectivity, but these properties must be taken into account: **availability** because the system must be functional at least part of the time, even if only long-enough for initial programming and a "start" command, and **timeliness** or temporal ordering awareness because in cases where real-time control is needed, we must reliably notify communicating components when that property has been lost, so they can engage their fallback failsafe states. Certainly temporal ordering is also required for logging, in order to allow for accurate forensic reconstruction of events [11, 12].

4 Conclusion

The properties enumerated above are required for effective component-wise clearance, and eliminating each one presents a problem for technical operation, regulatory approval, or both. Some properties build upon others, and their requirements can be traced to the desirability of the "top-level" property. For instance, if we want **provenance** information as part of a log, we must also have **attribution**, which requires **authenticity** and **integrity**.

Acknowledgments

This work was supported by National Science Foundation grants CNS 1239543, and CNS 1224007, and National Institutes of Health grant 1U01EB012470-01.

Bibliography

1. Hatcliff, J.; King, A.; Lee, I.; MacDonald, A.; Fernando, A.; Robkin, M.; Vasserman, EY.; Weininger, S.; Goldman, JM. Rationale and architecture principles for medical application platforms; Proceedings of the International Conference on Cyber-Physical Systems (ICCPS); 2012.
2. Goldman JM. CIMIT/TATRC symposium on developing a plug-and-play open networking standard for the operating room of the future. 2005 May.
3. Burleson, WP.; Clark, SS.; Ransford, B.; Fu, K. Design challenges for secure implantable medical devices; Proceedings of the Design Automation Conference (DAC); 2012 Jun.
4. Clark, SS.; Fu, K. Recent results in computer security for medical devices; International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth), Special Session on Advances in Wireless Implanted Devices; 2011 Oct.
5. Conmy, P.; Nicholson, M.; McDermid, J. Safety assurance contracts for integrated modular avionics; Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software (SCS); 2003.
6. Objective Interface Systems, Inc. Multiple independent levels of security (MILS) — technical primer. 2011 http://www.ois.com/Products/mils-technical-primer.html.
7. Brucker, AD.; Petritsch, H. Extending access control models with break-glass. Proceedings of the ACM symposium on Access control models and technologies; ACM; New York, NY, USA. 2009. p. 197-206.
8. Anderson, RJ. A security policy model for clinical information systems; Proceedings of the IEEE Symposium on Security and privacy; 1996. p. 30-43.
9. United States Congress. Health Insurance Portability and Accountability Act, Privacy Rule. 45 CFR 164. 1996
10. United States Congress. Gramm-Leach-Bliley Act, Financial Privacy Rule. 15 USC §6801–§6809.

11. Accorsi, R. Safe-keeping digital evidence with secure logging protocols: State of the art and challenges; International Conference on IT Security Incident Management and IT Forensics; 2009. p. 94-110.

12. Arney, D.; Weininger, S.; Whitehead, SF.; Goldman, JM. Supporting medical device adverse event analysis in an interoperable clinical environment: Design of a data logging and playback system; International Conference on Biomedical Ontology (ICBO); 2011 Jul.

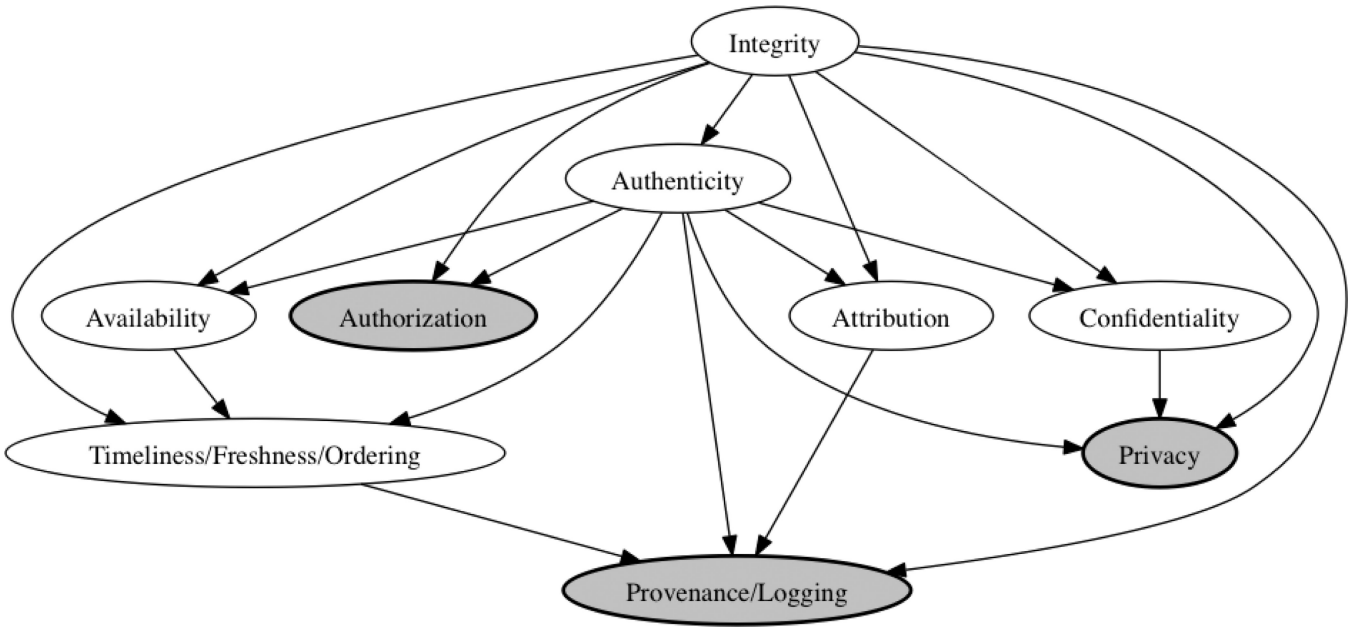

Fig. 1.
Requirement interdependencies. Children depend on parents.