Issues in Information Systems

Volume XII, No. 1, pp. 106-113, 2011

THREATS TO HEALTHCARE DATA: A THREAT TREE FOR RISK ASSESSMENT

J. Harold Pardue, University of South Alabama, hpardue@usouthal.edu
Priya Patidar, University of South Alabama, priya.vpatidar@gmail.com

ABSTRACT

The American Recovery and Reinvestment Act of 2009 authorizes the payment of incentives to hospitals, clinics, and practices that adopt meaningful use of electronic health records by the year 2015. The promise of making health data readily available for manipulation any place, any time, and in multiple formats is reduced medical and medication errors, lower healthcare costs, and improved healthcare outcomes. However, control over availability is no small challenge. This paper represents a preliminary effort at cataloging threats to electronic healthcare data associated with unauthorized access, data loss, and data corruption as a threat tree. The purpose of the threat tree presented here is to facilitate risk assessments and inform health care policy and legislation. The paper concludes with a brief discussion of ways to vet and extend the proposed threat tree.

Keywords: Health Care Information System, Security Threats, Risk Management

INTRODUCTION

The year 2015 looms on the horizon for hospitals, clinics, and practices as a deadline set by the American Recovery and Reinvestment Act of 2009 for implementation of meaningful use of health information technology and electronic health records. The goal of this legislative act is the development of a nationwide health information technology infrastructure that will transform healthcare by integrating technology into the flow of clinical practice. This infrastructure should be interoperable, private and secure [1].

Properly implemented, this infrastructure holds the promise of minimal unproductive data entry, streamlined patient flows and processes comparable to other industries, and improved clinical decision making through real-time access to patient data. This transformation requires that information technologies be easily adapted to the day-to-day workflow of clinicians and caregivers and that data flow seamlessly between systems and processes. A major obstacle to this integration is the proliferation of disparate proprietary systems with no standard data formats [1]. Even within a given hospital, each unit tends to purchase separate "best of breed" systems that best fit their own workflows and processes.

As the healthcare industry moves toward an information technology infrastructure common in other industries such as banking, a similar host of threats to security and privacy emerge. Like other systems, healthcare systems are a very complex interplay of technologies, people, policy, and legislation. However, because the information technology must be easily adapted to the clinician's daily workflow, technology must be brought to point-of-care, that is, technology must be both mobile and wireless. Data entry and manipulation cannot be separated from the task of providing patient care. This creates a very challenging data security environment to manage.

One approach to managing security of data is through risk assessment. In risk assessment, the analyst seeks to assign a quantitative or qualitative value to the risk of a threat being exercised in the context of a particular environment or situation. Risk assessment provides a means of allocating relatively scarce resources, conducting sensitivity and cost-benefit analysis, and computing residual risk. There are many methods for performing risk assessment. The method described in this paper involves the use of threat trees [2, 3, and 4].

Threat trees model risk in terms of source/vulnerability pairs organized as a hierarchy of threat actions. Each threat action defines a potential means for a threat source to exploit a system vulnerability. Threat actions also define unintentional exploitations such as those resulting from an unintended or unanticipated sequence of events or a failure. Here we define a vulnerability using the NIST 800-30 guidelines: "A vulnerability can be defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exploited to accomplish a security breach or a violation of the system's security policy" [5].

This paper describes a threat tree intended to model threats to unauthorized manipulation, loss or corruption of healthcare data. The remainder of this paper is organized as follows. The next section provides a brief overview of threat trees. The next section describes the threats comprising the healthcare data threat tree. This is followed by a discussion of uses of the threat tree. The paper concludes with a brief discussion of ways to extend and vet the proposed threat tree.

THREAT TREE OVERVIEW

Threat trees organize threats as a hierarchy. A threat action is modeled as a node. Subordinate nodes can be thought of as sub-nodes or actions. Figure 1 contains a simplified threat tree in indented, outline numbered list format. Threat trees can also be represented as nodes connected by directional edges.

Subordination of nodes is defined by indentation and outline numbering. The simplified threat tree in Figure 1 contains two threats: Threaten healthcare data and Disclose healthcare data. The threaten healthcare data threat is decomposed into three sub-actions: gather knowledge, gain insider access, and subvert equipment. The first node "A 1" is an AND node denoted by the capital letter "A". This means that all directly subordinate nodes must be accomplished for the vulnerability to be exploited. Nodes prefixed with an "O" are "OR" nodes mean they define optional ways of exploiting the vulnerability. An attacker can subvert equipment by either subverting hardware OR subverting software. Nodes prefixed with a "T" are "TERMININAL" nodes mean they are atomic actions and the analyst does not wish to decompose them further. The depth of the tree is determined by the analyst. However, the goal is to create a tree that is sufficient for risk analysis but not overly complex. All things being equal, a simple tree will be more useful than a complex one.

```
Node type - Outline number - Threat action
A 1   Threaten asset
  O  1.1 Gather knowledge
  O  1.2 Gain insider access
     T  1.2.1 at targeted site
  O  1.3 Subvert equipment
     O  1.3.1 Subvert hardware
        T 1.3.1.1   Swap external media
        T 1.3.1.2   compromise configuration
     A  1.3.2 subvert software
        T 1.3.2.1   develop malware
        O 1.3.2.2   select targets
          T  1.3.2.2.1  select locations
        O 1.3.2.3   inject malware
A 2   Disclose private data
```

Figure 1. Simplified Threat Tree

HEALTHCARE DATA THREAT TREE

The threat tree presented in this paper is based on existing research, frameworks, and taxonomies of threats to health information systems [6, 7, 8, and 9]. The study by Kotz [7], proposes a taxonomy of 25 threats organized by identity threats, access threats, and disclosure threats. Samy, Ahmad, and Ismail [9] identified 22 categories of health information systems threats. Their research suggested five critical areas: power failure/loss, acts of human error or failure, technological obsolescence, hardware failures or errors, and software failures or errors.

The healthcare data threat tree presented in this paper focuses on unauthorized manipulation, data loss, and data corruption. Documented risks of exploited vulnerabilities of healthcare data include exposure to economic harm, mental anguish, social stigma, identity theft, and poor healthcare outcomes. The healthcare data threat tree is

depicted visually in Figure 2. The threat tree in Figure 2 represents threats to data integrity. What follows is a brief description of the threats cataloged in our threat tree.

node type - outline number - threat action
1 manipulate health data
T 1.1 by vandalism
O 1.2 by loss or corruption of data
T 1.2.1 due to faulty hardware
T 1.2.2 due to faulty software
T 1.2.3 due to human error
T 1.2.4 due to malware
T 1.2.5 due to a natural disaster
T 1.2.6 due to a database attack
T 1.2.7 due to unauthorized access

Figure 2. Healthcare Data Threat Tree

Vandalism

Vandalism of health information systems (1.1) can be thought of in the broader context of cyber protest. Cyber protest is an expression of a social movement through the use of communication technologies [10]. Controversial healthcare such as abortion or medical animal research and their information systems has long been a target of vandalism [11, 12, and 13].

Hardware and Software

In a 2010 study by Samy et al [9], hardware and software failures (1.2.1, 1.2.2) were ranked among the top five out of 22 threats to hospital information systems. Dealing with hardware failure has been a significant part of the history of the application of information technology to healthcare data management [14 and 15]. Failures range from hard drive crashes and backup technology failure to poor planning of storage needs leading to inadequate storage space.

Despite the promise of healthcare software systems to reduce medication, human, and medical errors and reduce healthcare costs, at least two studies found that computer physician order entry (CPOE) systems actually facilitated medication errors and lead to an increased mortality rate among patients dependent on time-sensitive therapies [16, 17, and 18]. Two major reasons emerge from these studies. First, healthcare data comes from a myriad of sources and formats. If the data are not integrated correctly in the database and positioned correctly on computer screens, data errors can occur. Second, software systems alter the normal flow of events in a hospital. Health care professionals are not information workers. A computer screen data-entry flow optimized to ensure transactional completeness for a clerk sitting alone in a cubical will not likely match well with the frenetically multi-tasked, communication rich interactions of hospital staff leading to human error (1.2.3). Data values may not be entered correctly or at all. As a result, time-sensitive therapies such as early resuscitation may be delayed to the determinant of the patient's health and chances of survival. Figure 3 provides a sample threat matrix entry for a software failure (1.2.2).

Threat Attribute	**Value**
ID-Node Type-Outline No.	24 – T – 1.2.2.2
Source	Human-unintentional
Action	Manipulate health information by loss or corruption of data due to faulty software
Health Information Asset	Patient health and survival
Vulnerability	Dosage information and dosage schedules based on preset defaults or "outside" data such vendor specifications rather than clinical guidelines
Potential Controls	Do not assume a healthcare software system will reduce or mitigate medical or medication errors. Assess mortality effects and evaluate medication error rates. Plan and look for unintended consequences during system integration. Dedicate an additional physician or staff member to enter and verify orders. Implement preprogrammed order sets (of medication and treatment).
Scenario(s)	System integration failure and human-machine interface flaws cause adverse changes in bedside care and delivery of time-sensitive therapies leading to increased mortality rates. Example: patient antibiotic administration is not timed to the initial dose but with preset defaults causing the dosage schedule to be automatically deleted by the system without notifying staff or physicians [17].

Figure 3. Healthcare Data Threat Tree

Malware

The 1982 Tylenol cyanide contamination case is a stark reminder that there exist malicious threats to the world's drug supply and infrastructure. The software and data systems that manage the flow of drugs and information about treatments are no less susceptible to their corollary malicious threat: malware [19] (1.2.4). Malicious software that performs unauthorized manipulations on sensitive health data can be written and introduced into health information systems the same way they are introduced to any other software system. A recent class of Tylenol-like threats is malware in embedded medical devices [20, 21] . The wireless nature of these new devices makes them vulnerable to both security and privacy threats.

Natural Disaster

When disaster strikes (1.2.5), just as in any other information system, the key to avoiding data loss or corruption is a comprehensive data security and recovery plan [22] . Health information systems are critical systems and therefore planners must consider such options as hot, warm, and cold sites, uninterrupted power, and off-site storage [23]. Some health information system providers create mobile, mirrored sites that can be trucked to and set up at a disabled site.

Database Attack

Because health information systems are built on database technologies, these systems are at risk to the threat of database attacks (1.2.6). Most databases can speak a common language: structured query language (SQL). With the advent of networking and scripting technologies, SQL became a powerful language to access and manipulate health records. However these scripts running on a network are vulnerable to database attacks such as SQL injection and denial of service worms such as SQL slammer [24, 25, 26, 27, 28]. SQL injection attacks involve a malicious user inserting a SQL expression into a string of text that is processed by the database. If written correctly, such a SQL expression can directly manipulate or destroy medical data stored in a database. Counter measures to SQL injection include: changes to the networking infrastructure that isolates the database, improved user input cleansing, improved auditing of database changes, allowing applications to have the lowest level of privileges required, and disallowing customized or dynamic SQL, that is, placing all database access language inside tested, correctly constructed stored procedures.

Unauthorized Access

Electronic health records are intended to increase the availability and accuracy of health information. However, with availability comes the threat of unauthorized access to data (1.2.7). Unauthorized access takes many forms and occurs for many reasons. For example, a malicious attacker may gain unauthorized access in order to acquire medical treatment with a different person's insurance (identity theft) [8] (Nematzadeh and Camp, 2010). Another form of unauthorized access arises from the fact that health care facilities routinely deal with emergency situations where action must be immediately taken. The first directive of a physician is to do no harm and to save life. Data access policies often must be circumvented in these so-called "break-the-glass" life-or-death moments [26, 28] . Although necessary, this circumvention exposes the system to the threat of unauthorized access to health care data. Several countermeasures are proposed in the literature such as digital rights management technology [8] , reflective database access control [26] , and the definition of policy spaces that use composition algebra to regulate traditional access control systems [28] .

USE OF THREAT TREE

The purpose of the healthcare data threat tree is to facilitate risk assessment and inform health care policy and legislation. One approach to risk assessment is to rank-order threats [3]. Rank-ordering can be arrived at in a number of ways. One approach is to assign a qualitative value of high, medium, and low to each of the threats in the tree for a given context assuming a given set of controls. A control is any counter-measure designed to reduce the risk of exploitation of a vulnerability. The assignment of a value is based on the analyst's knowledge, expertise, and experience. Because a threat tree is an abstraction, the analyst can reason comparatively about threats as well as

compare their assessment with the assessment of other analysts. The branch in the threat tree provides a common point of reference. Analysts can compare their rank-ordered lists and discuss where they differ and why.

Risk can also be assessed by assigning quantitative values to the risk of each threat in the threat tree. The analyst can develop metrics for each node which facilitates the application of formal methods to the estimation of risk [4]. Metrics can include such quantitative variables as dollar cost, man-hours of effort, number of attackers, level of expertise, and risk of detection [29, 30]. Not only does quantitative analysis enable rank-ordering of threats, it allows for an assessment of the relative magnitude of each threat. For example, the threat hardware failure might be ten times higher than the threat of malware. Because the threat tree abstracts the essence of the threats, it provides a common point of reference across contexts, sets of mitigations and analysts.

The healthcare data threat tree can also facilitate group risk assessment. For example, the threat tree could be used as the basis for a facilitated risk analysis process (FRAP) [31]. In a FRAP, a facilitator and a team of 5 to 8 domain experts prioritize a list of threats. The goal is not to produce accurate point estimates of risk but rather a ranking of the threats. FRAP participants document their assumptions about context and controls for each threat or node in the tree and the rationale for their ranking of the threats.

CONCLUSION

The purpose of this paper is to present and describe a preliminary threat tree for threats to healthcare data. This tree is not presented as comprehensive but as a work in progress. What follows is a brief description of how the authors plan to proceed with extending and vetting the threat tree prior to use in risk assessment.

The threat tree presented here was produced by the authors using the extant literature, and their own knowledge, expertise, and experience. The next step is to circulate the healthcare data threat tree to a group of domain experts for asynchronous evaluation. This group will include hospital administrators, healthcare informaticists, security specialists, and academics. The group will be asked to do three things: add additional threats, expand existing threats into sub-threat actions, and modify the structure of the tree where necessary. Group size will be between 8 and 12 participants. The authors will integrate this feedback into the existing threat tree. The authors will contact domain experts for clarification.

The second phase will be to convene a panel of domain experts to collaboratively modify and vet the healthcare data threat tree. The panel will meet for one to two days for a face-to-face synchronous meeting in a location such as a hotel conference room. The meeting will be managed by an impartial facilitator. It is expected there will be 10 to 12 participants similar in composition to the phase 1 group evaluation. The panel will work through each threat and sub-threat actions until all nodes of the tree have been evaluated. Audio of the meeting will be recorded and notes transcribed. The authors will integrate this feedback into the revised threat tree.

The third phase is risk analysis. An explanation of our risk assessment process is beyond the scope of this paper.

REFERENCES

1. President's Council of Advisors on Science and Technology (2010) "Report to the President Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward. Available: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf
2. Schneier, B. (1999). "Attack trees" *Dr. Dobb's Journal of Software Tools*, 24. 21–29.
3. Pardue, J. H., Landry, & Yasinsac, A. (2009). "A Risk Assessment Model for Voting Systems using Threat Trees and Monte Carlo Simulation". *First International Workshop on Requirements Engineering for E-voting Systems*, Atlanta, GA.
4. Yasinsac, A, and Pardue, H, (2011) "Voting System Risk Assessment: A Process Using Threat Trees," *Journal of Information Systems Applied Research*, 4(1), pp. 4-16. http://jisar.org/2011-4/ ISSN: 1946-1836.
5. Stoneburner, G., Goguen, A., & Feringa, A. (2002). "Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology." Gaithersburg, Md: U.S.

Dept. of Commerce, National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

6. Appari, A. and Johnson. M. E. (2010) "Information security and privacy in healthcare: current state of research", *International Journal of Internet and Enterprise Management*, 6, 4, 279 – 314.
7. Kotz, D. (2011) "A threat taxonomy for mHealth privacy", in *Workshop on Networked Healthcare Technology (NetHealth)*, January 4, 2011, Bangalore, India.
8. Nematzadeh, A. and Camp, L. J. (2010) "Threat analysis of online health information system, in Fillia Makedon, Ilias Maglogiannis, and Sarantos Kapidakis" (Eds.) *Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '10)*, June 23-25, 2010, Samos, Greece, 31, 1-7.
9. Samy, G. N., Ahmad, R., and Ismail, Z. (2010) "Security threats categories in healthcare information systems", *Health Informatics Journal*, 16, 3, 201-209.
10. Zimbra, D., Abbasi, A. and Chen, H. (2010) A cyber-archaeology approach to social movement research: Framework and case study, *Journal of Computer-Mediated Communication*, 16, 1, 48-70.
11. Curran W. J., Stearns B., and Kaplan H. (1969) Privacy, confidentiality and other legal considerations in the establishment of a centralized health-data system, *New England Journal of Medicine*, 281, 5, 241–248.
12. Forrest J. D., and Henshaw S. K. (1993) Providing controversial health care: abortion services since 1973, *Womens Health Issues*, 3, 3, 152-157.
13. Jackson, T. (2001) Website of the week: Animal research, *British Medical Journal*, 322, 7280, 244.
14. Hersh ,W. (2004) Health care information technology: Progress and barriers, *The Journal of the American Medical Association*, 292, 18, 2273-2274.
15. Kilbridge, P. (2003) Computer crash—lessons from a system failure, *New England Journal of Medicine*, 348, 881-882.
16. Ash, J. S, Berg, M., and Coiera, E. (2004) Some unintended consequences of information technology in health care: the nature of patient care information system-related errors, *Journal of the American Medical Informatics Association*, 11, 2, 104-112.
17. Han Y. Y., Carcillo J. A., Venkataraman, S.T., Clark, R. S., Watson, R. S., Nguyen, T. C., Bayir, H., and Orr, R. A. (2005) Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system, *Pediatrics*, 116, 6, 1506-1512.
18. Koppel, R., Metlay J. P., Cohen, A., Abaluck, B., Localio, A. R., Kimmel, S. E., and Strom B.L. (2005) Role of computerized physician order entry systems in facilitating medication errors, *The Journal of the American Medical Association*, 293, 10, 1197-1203.
19. Keese, J., and Motzo, L. (2005) Pro-active approach to malware for healthcare information and imaging systems, in *CARS 2005: Computer Assisted Radiology and Surgery*, June 21-25, 2005, Kuessaberg, Germany, 943-947.
20. Fu, K. (2009) Inside risks: Reducing risks of implantable medical devices, *Communications of the ACM*, 52, 6, 25-27.
21. Maisel, W. H. and Kohno, T. (2010) Improving the security and privacy of implantable medical devices, *New England Journal of Medicine*, 362, 1164-1166.
22. Simpson, R. L. (2001) What to do before disaster strikes, *Nursing Management*, 32, 11, 13-14.
23. Hannah, K, Ball, M., and Edwards , M. (2006), Disaster recovery planning, *Health Informatics*, Part IV, 243-253.
24. Chryssanthou Anargyros, Iraklis Varlamis, and Charikleia Latsiou. 2009. Security and trust in virtual healthcare communities. In Proceedings of the *2nd International Conference on PErvasive Technologies Related to Assistive Environments* (PETRA '09). ACM, New York, NY, USA, , Article 72 , 8 pages. DOI=10.1145/1579114.1579186 http://doi.acm.org/10.1145/1579114.1579186
25. Fonseca, J., Vieira, M., and Madeira, ,H. (2008) Online detection of malicious data access using DBMS auditing, in *Proceedings of the 2008 ACM symposium on applied computing (SAC '08)*, March 16 - 20, 2008, Ceará, Brazil, 1013-1020.
26. Olson L. E., Gunter, C. A., and Olson, S. P. (2009) A medical database case study for reflective database access control, in Camp, Jean (Ed.) *Proceedings of the first ACM workshop on security and privacy in medical and home-care systems (SPIMACS '09).* November 13, 2009, Chicago, IL, USA, 41-52.
27. Goedert J. (2007) I.T. threats: obvious, unknown or hyped? *Health Data Management*, 15, 5, 54-58.

28. Ardagna, C. A., De Capitani di Vimercati, S., Foresti, S., Grandison, T. W., Sushil Jajodia, S., Samarati, P. (2010) Access control for smarter healthcare using policy spaces, *Computers & Security*, 29, 8, 848-858.
29. Jones, D. W. (2005). Threats to voting systems, *Position paper for the NIST workshop on Threats to Voting Systems*. Gaithersburg, MD.
30. Tipton, H. F. & Henry, K. (2007). *Official (ISC)2 Guide to the CISSP CBK*. Boca Raton, FL: Auerbach Publications: Taylor and Francis Group.
31. Peltier, T. R. (2001). *Information Security Risk Analysis* (2nd ed.). Baca Raton, FL: Auerbach Publications.