CERIAS Tech Report 2014-2

Reliability and Cyber-Security Assessment of Telehealth Systems

by Karla Welch, J. Chris Foreman, James H. Graham, Mostafa Farag, Melinda Whitfield Thomas, Phil Womble
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Reliability and Cyber-Security Assessment of Telehealth Systems

Karla Welch[1], J. Chris Foreman[1], James H. Graham[1], Mostafa Farag[1], Melinda Whitfield Thomas[2], and Phil Womble[3]
[1]Intelligent Systems Research Laboratory
University of Louisville, Louisville, KY 40292
[karla.welch, jcfore01, jhgrah01@louisville.edu]
[2]Cyber Defense Laboratory
Western Kentucky University, Bowling Green, KY 42101
[melinda.whitfield@wku.edu]
[3]EWA Government Systems Inc., Bowling Green, KY 42101
[pwomble@ewa.com]

Abstract

This paper presents the results from a recent evaluation of the reliability and cyber-security vulnerability of telemedicine/telehealth systems used today in the United States. As this technology becomes more widely used in an effort to reduce costs and better serve remote and isolated populations, these issues will undoubtedly become more pronounced. This paper presents some background information about telemedicine/telehealth systems and an overview of recognized reliability and cyber-security risks. It then discusses a national survey of equipment and software vendors for telemedicine/telehealth, discusses a risk scoring system that was developed as part of the project, and presents overall results and recommendations for future work in this area.

1 Introduction

The Healthcare and Public Health (HPH) Sector is responsible for the direct delivery of medical care to the population. Increasingly, many people are provided healthcare remotely using telehealth systems. This shift to utilize cyber systems within provider networks is primarily due to physical constraints, such as distance, preventing access to traditional healthcare systems; however, costs are also beginning to play a role as telehealth affords more frequent healthcare delivery and monitoring than multiple site visits. As such, telehealth plays a major role in the influence of the public's healthcare. It is considered a critical infrastructure of interest by the Department of Homeland Security's (DHS) National Critical Infrastructure Prioritization Program (NCIPP).

Reliability and cyber-security are key issues to the HPH Sector and telehealth. However, most attention has been on privacy and compliance with HIPAA, while the importance of the cyber-security of medical devices has been overshadowed. In recent years, however, cyber-attacks on medical devices have become noticeable and these will continue to grow as such attacks gain publicity [1]. Some of these attacks have included malicious software and activities aimed at IT solutions that are coincidentally part of telehealth systems [2]. However, newer attacks are beginning to target telehealth systems specifically [3], including direct influence of the actual medical devices that provide healthcare to patients [4].

As a first step towards realizing a solution for mitigating risks in reliability and cyber-security for telehealth systems, a research team represented by the authors have conducted a landscape analysis, developed an assessment survey, and analyzed the results of this survey, citing conclusions and future work.

Section 2 will discuss the landscape assessment of telehealth systems including how such systems are used/deployed, the market share of major vendors, and vulnerabilities to reliability and security. Section 3 will discuss the development of a vendor survey to assess these vulnerabilities. Section 4 will describe the scoring system for evaluation of these surveys. Section 5 will present the results of the survey assessment. Section 6 will provide conclusions and directions for future work.

2 Landscape of Telehealth Systems

Telehealth, telemedicine, and to a lesser extent cyber medicine, have generally been accepted as near synonyms. To avoid confusion, telehealth will be used in this paper and refer inclusively to any healthcare services provided at a distance through Information Technology (IT) based systems. Some other definitions for telehealth in agreement with this term are:

- "Telehealth is the use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, public health and health administration" [5].
- "Telemedicine is the use of medical information exchanged from one site to another via electronic communications to improve patients' health status. Closely associated with telemedicine is the term 'telehealth,' which is often used to encompass a broader definition of remote healthcare that does not always involve clinical services" [6].

2.1 Organization of the Telehealth Sector

Telehealth systems are used when logistic or financial motivating factors indicate that healthcare is best provided remotely versus in a traditional healthcare provider's facility. A common example is when a patient resides in a remote, rural setting where frequent travel for minor services is not feasible. In this case, the healthcare network is virtually extended to facilitate healthcare at a distance. Fig. 1 illustrates the organization of a typical telehealth network.

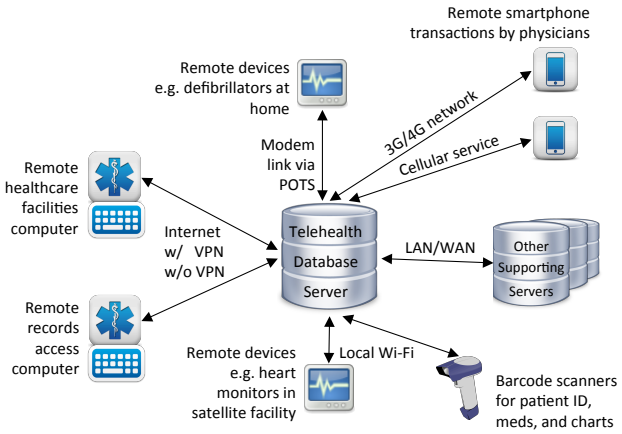

Figure 1. A typical telehealth information network [15].

There are 430 telehealth vendors that represent over 50,000 contracts with associated healthcare providers. The top eleven vendors by U.S. market share are listed in Table 1 according to the Definitive Healthcare Database (DHD) [7]. These eleven represent a combined 67.4% of the U.S. market share. Telehealth solutions are provided as either stand-alone software systems or Software as a Service (SaaS). Solutions may also include IT hardware such as depicted in Fig. 1.

Table 1. U.S. market share of top eleven vendors.

Vendor	Market Share
Meditech	23%
E.P.I.C.	12.5%
Cerner	10.6%
McKesson	5.2%
CPSI	3.3%
Infor Healthcare (Lawson)	3%
Siemens	3%
Vista	2.1%
Allscripts	2%
Healthcare Management Systems	1.7%
CGI	1%

2.2 Vulnerabilities in the Telehealth Sector

Through the review of existing media exposure of telehealth vulnerabilities [2-4], the HIMSS (Healthcare Information Management and Systems Society) survey [8], and the consensus of the team, the following five vulnerability categories were established and some of the associated threats identified [9].

1. Lack of safeguards against unintentional errors
   a. Data entry error
   b. Not logging off, unattended access points
   c. Unintended privilege escalation
2. Vulnerabilities in IT practices
   a. Lack of security training
   b. Unauthorized access
   c. Exploitation of improper systems configuration
   d. Exploitation of poor IT security policies
3. Lack of safeguards against malicious intrusion
   a. Successful malware/virus attack
   b. Malicious misuse by users
4. Hardware infrastructure vulnerability
   a. Severe weather events
   b. Collateral damage from physical attacks
   c. IT Network outages
   d. Counterfeit devices
5. Software vulnerability
   a. Compromise of database integrity
   b. Lack of proper data backup procedures
   c. Improper application of reliability/security software patches

In some cases, these threats span multiple vulnerability categories, e.g., unauthorized access is a threat in all categories. The risks posed by these threats fall into three basic categories as follows [1].

1. Costs – disclosure of sensitive data may result in HIPAA violations and fines, other recovery costs for lost data and/or equipment damage, and malpractice costs for patient injury and death.
2. Recovery time and effort – lost data and compromised systems require recovery effort by personnel. This risk also delays access to telehealth systems by healthcare providers.
3. Patient injury or death – telehealth systems are responsible for health-sustaining care and their compromise can directly harm patients.

3 Development of the Telehealth Survey

A telehealth survey was developed to quantify awareness of the vulnerabilities and detect deficiencies. This survey was designed to assess vendors' efforts to address these risks in their telehealth solutions. To form the survey, the driving concerns that had originated the vulnerability categories were generalized to determine the root concerns. From these root concerns were determined key words that would be integral parts of the associated survey questions. This process is illustrated in Fig. 2 as read from left to right.

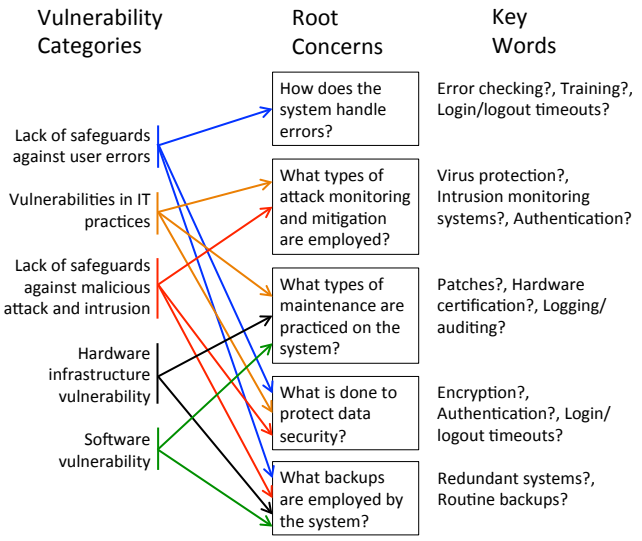

Figure 2. Survey development process [10].

Once the key words had been uncovered through this process, the formation of survey questions could proceed. Based on a few examples of specific threats as in Section 1, and the team's expert knowledge of IT and telehealth systems, candidate survey questions were developed. Since the survey questions are based on the root concerns derived from the vulnerability categories, it was expected that these questions would engage reviewers and uncover new information regarding specific vulnerabilities and the mitigating factors that might address them [10].

The first objective of the process was to create questions such that they connect with telehealth solutions for ease of understanding and engagement by vendors. The second was to phrase the questions concisely and reduce the number of questions in an attempt to improve participation. We set a target of 10-15 questions and an estimated completion time of approximately 10 minutes.

The questions utilized a multiple-choice, Likert scale to encourage uniform responses. The resulting telehealth survey of vendors is as follows [10].

1. Does your health information technology software check the validity of data input based on common trends or real-world applications (for example, not allowing lethal doses of medicine)?
   a. No error detection
   b. Simple data type and/or spelling detection
   c. Intelligent error detection correlated with a medical database
2. Does the software monitor and log user activity?
   a. Yes
   b. No
   c. Unknown/Not applicable
3. Does the software automatically alert anyone in the case of suspicious activity?
   a. Yes
   b. No
   c. Unknown/Not applicable
4. Does your health information technology software require input of user credentials before allowing the retrieval/adding/editing of data?
   a. Yes
   b. No
   c. Unknown/Not applicable
5. Is provider data stored and transferred in an encrypted format?
   a. Yes
   b. No
   c. Unknown/Not applicable
6. Is access to data limited to specific devices?
   a. Yes
   b. No
   c. Unknown/Not applicable
7. Are phones allowed to access the system and its data?
   a. Yes
   b. No
   c. Unknown/Not applicable
8. Is an intrusion detection system in place to monitor network traffic?
   a. Yes
   b. No
   c. Unknown/Not applicable
9. Does the health information technology monitor and store which devices apply changes to the software?
   a. Yes
   b. No
   c. Unknown/Not applicable
10. How often is the health information technology database backed up?
    a. Never
    b. Monthly
    c. Weekly
    d. Daily
    e. More than once a day
11. How often are security patches released?
    a. Never
    b. Less than once a month
    c. Monthly
    d. Weekly
    e. More than once a week

Six of the vendors listed in Table 1 completed the survey. This sample still constituted 55.3% of the market share. Many of these responses were also partial or from information given out to all inquirers. Reasons given for partial or refused participation were: (1) survey responses would constitute a HIPAA violation, (2) survey responses would violate confidentiality with their clients and customers, (3) survey responses would disclose proprietary infor-

mation. Some vendors cited being overwhelmed with survey requests and could not spare the resources to respond.

The process depicted in Fig. 2 facilitated the formation of survey questions; however, when read from right to left, the process also provides a basis for mapping the responses back to specific vulnerability categories. This mapping and subsequent scoring will be discussed further in Section 4.

4 Survey Risk Scoring Methodology

The risk scoring methodology followed an amalgamation of practices from the following three sources.

- Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology (NIST) 800-30 [12]
- An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, NIST 800-66 [13]
- Information Technology Risk Management Guideline, Virginia Information Technologies Agencies, SEC506-01 [14]

The risk score is assessed as likelihood multiplied by impact. Likelihood and impact levels are defined in Tables 2 and 3. Risk likelihood is scaled as (low, moderate, high) => (0.1, 0.5, 1.0). Risk impact is scaled as (low, moderate, high) => (10, 50, 100). The total risk score can thus take on nine discrete values in a range from 1 to 100 [9].

To determine the impact level for each of the specific threats from Section 2.2, the team employed the Delphi method. The likelihood level was determined by the Likert scale response of each survey question. For example, in question #1 from Section 3, the vendors could respond with either *a*, *b*, or *c*, which mapped to a risk likelihood level of either high, moderate, or low respectively. For question #2, a *yes* response mapped to a risk likelihood of low while a *no* or *unknown* response mapped to a risk likelihood of high.

Table 2. Risk likelihood level definition [9].

Level	Likelihood Definition
High (1.0)	The threat-source is highly motivated and sufficiently capable while controls to prevent the vulnerability from being exercised are ineffective.
Moderate (0.5)	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. Alternatively, the threat-source may lack motivation or capability, but controls are also ineffective.
Low (0.1)	The threat-source lacks motivation or capability, and controls are in place to prevent, or significantly impede, the vulnerability from being exercised.

Table 3. Risk impact level definition [9].

Level	Impact Definition
High (100)	Exercise of the vulnerability (1) may result in the loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Moderate (50)	Exercise of the vulnerability (1) may result in the loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low (10)	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Once these levels were assessed, the survey responses were then quantized and mapped back to the associated vulnerability category as discussed in Section 3 and illustrated in Fig. 2. These results are presented in Section 5.

5 Survey and Risk Scoring Results

From the eleven original vendors surveyed, only six responded in a meaningful way. This represented 55.3% of the U.S. market share. These six vendors are anonymously listed from A-F in Table 4 with the associated vulnerability category as discussed in Section 2.2 and the total risk vulnerability scores assessed as in Section 4. For example, a value of 10/1 indicates that the range of responses was from a high of 10, to a low of 1, on a scale of 100 for the threats within that vulnerability category. An asterisk indicates that some of the associated questions, from Section 3, were left unanswered and thus, the total risk is not fully assessed for this vendor/vulnerability.

Table 4. Vendor vulnerability risk summary.

Vendor / Vulnerability	A	B	C	D	E	F
#1: Unintentional errors safeguards	10/1	*50/5	50/5	50/1	*50/5	*10/5
#2: IT practices	*	*	5	50	*	*
#3: Malicious intrusion safeguards	*10/5	*10	10/5	50/10	*10/5	*10/5
#4: Software	*10/1	*	10/1	100/1	*	*
#5: Hardware	*50/5	*	10/5	100/1	*	*

As discussed in Section 3, vendors claimed a number of reasons for not participating in the survey, either partially or fully. Vulnerability in IT practices (2) seems to have elicited the least response. For this vulnerability, healthcare providers' IT networks play a significant role over which vendors may not have influence. This also seems to be the category which was most guarded in terms of disclosure, again citing HIPAA. While unintentional errors (#1) elicited a moderate rating, there is a trend in industry to minimize manual data entry in favor of barcode scanners and simple cut-and-paste operations. Software (#4) and hardware (#5) each had the broadest ranges, primarily from un-

certainty in patch application and management on the software side, and physical failure on the hardware side from either lack of redundancy or counterfeit devices [14, 15].

6 Conclusions and Future Work

Despite problems in obtaining information from telemedicine/telehealth equipment and software vendors, this work succeeded in developing a rough-cut assessment of the reliability and cyber-security vulnerabilities that currently exist in most of these systems. A first effort, such as this project, always results in a set of outcomes that is limited by the choice of methods and the time available. Only through an initial evaluation can future refinements be made. For example, the risk summaries in Table 4 can be reevaluated as further survey questions are answered and/or additional vendors participate.

As technology changes, the risks to telemedicine/telehealth systems will change and thus, the risk assessment must be continually updated. Using the lessons learned from this survey, it is suggested that a more comprehensive national risk assessment should be performed. By utilizing the Regional Extension Centers (REC), there should be much improved access to the hospital and healthcare IT personnel, and greatly improved quality of the risk assessments by obtaining information that is more accurate and more detailed.

A good next step in understanding the risks associated with telemedicine/telehealth systems would be to perform collaborative assessments, commonly known as Blue Team assessments, at a number of hospitals and healthcare facilities. The Blue Team assessments would allow us to correlate vulnerabilities in a number of facilities and examine if there are common causes. Furthermore a prevention program could be generated from these assessments.

Another possible extension of this effort would be the development of a comprehensive education and prevention program that can be disseminated to hospitals and other health providers to enable hospital personnel to better secure telehealth systems. The team would develop training materials and informational resources of "best practices" for securing telehealth systems and then work with the RECs for dissemination of this information.

It is the opinion of the authors, that, taken together, the three thrusts outlined in the preceding paragraphs: continuance and expansion of the National Risk Assessment, conducting collaborative assessments of telehealth installations, and development and dissemination of "best practices" information, could significantly mitigate the systems vulnerabilities identified in this project.

Acknowledgement

This work was sponsored under a contract from the Department of Homeland Security (DHS) administered through the National Institute for Hometown Security (NIHS). The opinions expressed in this paper are solely those of the authors.

References

[1] Melinda Whitfield Thomas, Cassie West, Ryan Moore, Karla Welch, J. Chris Foreman, James H. Graham, Mostafa Farag, Phillip Womble, Morgan Phillips, and Nathan Alexander, "Landscape Assessment of Telehealth / Telemedicine Systems: A National Perspective," DHS/NIHS contract: Risk Assessment of Telemedicine / Telehealth Systems, Project Deliverable 1, Oct 2012.

[2] Ellen Messmer, "Are Healthcare Organizations Under Cyberattack?" *NetworkWorld*, accessed at http://www.pcworld.com/article/142926/article.html, Feb 2008.

[3] Tom Sullivan, Editor "DHS lists top 5 mobile medical device security risks," *Government Health IT*, accessed at http://www.govhealthit.com/news/dhs-lists-top-5-mobile-device-security-risks, May 2012.

[4] Clive Akass, "Killer hackers could target cardiac implants," *The Inquirer*, accessed at http://www.theinquirer.net/inquirer/news/1556846/killer-hackers-target-cardiac-implants, Sep 2009.

[5] Health Resources and Services Administration, accessed at http://www.hrsa.gov/ruralhealth/about/telehealth/, 2012.

[6] ATA American Telemedicine Association, accessed at http://www.americantelemed.org/i4a/pages/index.cfm?pageID=3333, 2012.

[7] DHD Definitive Healthcare Database, accessed at www.definitivehc.com (subscription required), November 29, 2012.

[8] HIMSS Healthcare Information Management and Systems Society, "5th Annual HIMSS Security Survey, sponsored by Experian" accessed at http://himss.files.cms-plus.com/HIMSSorg/content/files/2012_HIMSS_SecuritySurvey.pdf, 2012.

[9] Melinda Whitfield Thomas, Cassie West, Ryan Moore, Karla Welch, J. Chris Foreman, James H. Graham, Mostafa Farag, Phillip Womble, Morgan Phillips, and Nathan Alexander, "Risk Assessment Scoring System," DHS/NIHS contract: Risk Assessment of Telemedicine / Telehealth Systems, Project Deliverable 2, Nov 2012.

[10] Melinda Whitfield Thomas, Cassie West, Ryan Moore, Karla Welch, J. Chris Foreman, James H. Graham, Mostafa Farag, Phillip Womble, Morgan Phillips, and Nathan Alexander, "National Survey Questionnaire and Methodology," DHS/NIHS contract: Risk Assessment of Telemedicine / Telehealth Systems, Project Deliverable 3, Dec 2012.

[11] Melinda Whitfield Thomas, Cassie West, Ryan Moore, Karla Welch, J. Chris Foreman, James H. Graham,

Mostafa Farag, Phillip Womble, Morgan Phillips, and Nathan Alexander, "National Survey Results," DHS/NIHS contract: Risk Assessment of Telemedicine / Telehealth Systems, Project Deliverable 4, Mar 2013.

[12] National Institute for Standards and Testing, Report 800-30 Risk Management Guide for Information Technology Systems, access at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, Nov 2012.

[13] National Institute for Standards and Testing, Report 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, accessed at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf, Nov 2012.

[14] Virginia Information Technology Risk Management Guideline – Appendix D, accessed at https://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/unmanaged/library/RiskAssessmentInstructions12142006.pdf, Nov 2012.

[15] Melinda Whitfield Thomas, Cassie West, Ryan Moore, Karla Welch, J. Chris Foreman, James H. Graham, Mostafa Farag, Phillip Womble, Morgan Phillips, and Nathan Alexander, "National Risk Assessment Survey Analysis," DHS/NIHS contract: Risk Assessment of Telemedicine / Telehealth Systems, Project Deliverable 5, Apr 2013.

[16] Melinda Whitfield Thomas, Cassie West, Ryan Moore, Karla Welch, J. Chris Foreman, James H. Graham, Mostafa Farag, Phillip Womble, Morgan Phillips, and Nathan Alexander, "Comprehensive Final Report," DHS/NIHS contract: Risk Assessment of Telemedicine / Telehealth Systems, Project Deliverable 6, May 2013.