;login:

DECEMBER 2014 VOL. 39, NO. 6

ELECTRONIC SUPPLEMENT

Conference Reports

HealthTech '14: 2014 USENIX Summit on Health Information Technologies

Safety, Security, Privacy, and Interoperability of Health Information Technologies

August 19, 2014, San Diego, CA

Summarized by Yuzhe Tang and Tariq Yusuf

Keynote

Summarized by Tariq Yusuf

Software Loved by Its Vendors and Disliked by 70% of Its Users: Two Trillion Dollars of Healthcare Information Technology's Promises and Disappointments

Ross Koppel, Ph.D. FACMI, Sociology Department and School of Medicine, Senior Fellow, LDI, Wharton, University of Pennsylvania

Dr. Koppel's research focuses on Healthcare Information Technologies (HITs) and how they interact with healthcare workers and their systems. HITs used by most clinics cost anywhere from $300–400 million. However, these components are only a small part of the full systems that are implemented in these facilities. There are around 300–400 separate components and systems that have to interconnect from other software vendors and data sources, with each connection between these systems being a potential vulnerability. A fully integrated HIT can cost around $1.5 billion.

HITs are provided by seven major vendors, the largest being Epic systems. Epic holds about 70% of the HIT market, touches the lives of about 52% of healthcare patients, and is implemented in one out of every two clinics. These systems have several components that have to be connected to the main hospital, such as ambulatory systems. However, the HIT industry has very few data and data format standards, and that severely limits interoperability. In terms of government regulation of these data format standards, they have typically followed the industry, which hasn't done much to combat the problem.

These systems are not only riddled with potential vulnerabilities from integration and implementation, but present several usability issues that Dr. Koppel pointed out. Some of his examples included the improper viewing of systolic and diastolic blood pressure. In some systems, these two critical measurements were not even displayed close to each other. Several of these usability and display issues could cause everything from improper diagnosis to downright dangerous errors in prescription amounts.

Other issues with these systems included potentially life-endangering workarounds involving a system refusing to accept the unusually low blood pressure of an emergency room patient to smart infusion pumps unable to deal with obese patients.

In recent surveys given to the hospitals about their HITs, hospital staff were asked about their need of funds and tech support. However, the surveys failed to ask hospitals about the functionality of their systems. Many developers make assumptions about the needs of HITs without consulting the healthcare professionals that end up using this system. Furthermore, there is a failure to analyze the implementation of this software in the context of the social system of healthcare and the technical and physical infrastructure that is present. It is already known that HITs influence the healthcare social system, but, Dr. Koppel argues, the healthcare social system also influences new HITs and how they are implemented in the future.

The system, as it stands, contains conflicts between healthcare regulation/patient protections and sales/promotion. Instead of fixing these problems, the HITs' solution has been to talk about the problem differently. Instead of becoming frustrated at the problems in the system, vendors like Epic have started distributing posters on what healthcare workers are supposed to say when talking about these systems.

When hospitals request fixes or changes to the HITs, they're typically told to either buy the newest version or additional components, that the system is "hard-wired" to work this way, or that the problem is not reproducible and therefore is not a legitimate problem. On the small chance that your fix is acknowledged, vendors will take at least 30 months before the fix is implemented (and the hospitals will have to purchase this new version).

So how can these issues in HITs be fixed? Dr. Koppel believes that the first step is to allow an easy method to communicate software issues to the vendors. Perhaps hiring a third party to identify and track these problems will help. If a vendor refuses to fix the problem, expose it publically so they will be forced to repair it. Most of these solutions will inevitably require contractual changes between HIT vendors and the healthcare facilities they serve, increased regulation and oversight from the government, and demands from insurance companies. Despite the large changes that need to take place, Dr. Koppel says it will work to demand a more responsive HIT that molds to the needs of the industry and not to the wants of the vendors.

Session 1

Summarized by Yuzhe Tang (yztang@gatech.edu)

Differentially Private Genome Data Dissemination through Top-Down Specialization

Shuang Wang and Xiaoqian Jiang, University of California, San Diego; Noman Mohammed, McGill University; Rui Chen, Hong Kong Baptist University; Lucila Ohno-Machado, University of California, San Diego

Shuang Wang presented research centered around the iDASH (http://idash.ucsd.edu/) challenge, which primarily includes two tasks: (1) privacy-preserving SNP data sharing and (2) privacy-preserving release of top-*K* most significant SNPs. Here, SNP is a DNA sequence variation that identifies biological species. Task one aims at understanding the privacy-utility balance in the publicly released SNP data set after proper anonymization in GWAS (http://en.wikipedia.org/wiki/Genome-wide_association_study). The utility was considered as the number of significant SNPs identified by the chi-square association tests (http://en.wikipedia.org/wiki/Chi-squared_test). Privacy protection aims at anonymizing sensitive genome data and making it resistant to the likelihood-ratio test. The second task aims at evaluating the residual utility in the anonymized results of GWAS. In particular, the utility is measured by the likelihood that the top-*K* SNPs of the ground-truth result can be preserved in the test result (by using the chi-square tests). Privacy is measured by a differential privacy under budget: epsilon=1.0.

The workflow regarding the iDASH challenge is that a publisher who maintains the raw data set on behalf of its owners anonymizes the data set based on anonymization algorithms and releases the anonymized data set to recipients. While the anonymization algorithm provides privacy guarantees, the utility is measured on the data-recipient side. The metric of differential privacy is considered in the work; differential privacy is realized by adding noise based on a Laplace mechanism. Through the study on task one, the authors identify the difficulty of keeping data undamaged while preserving privacy. For task two, the study result is that the algorithm works well when *K* (as in top-*K*) is a small value, such as $K < 5$, but the performance degrades when the value of *K* increases, which presents a design challenge for the future research.

Malware Prognosis: How to Do Malware Research in Medical Domain

Sai R. Gouravajhala, Amir Rahmati, Peter Honeyman, and Kevin Fu, University of Michigan

Sai R. Gouravajhala started with the observation that medical devices are vulnerable. This is partially due to the fact that the owners of those devices, being physicians or other non-experts in computing, are reluctant to patch the embedded systems.

The research work then focused on malware detections in medical devices. In this new research domain regarding medical-device malware, Gouravajhala raised valuable questions, such as what could be the dominant sources for malware infections. Better understanding this question helps in malware detection and even helps to determine what actions will best fix the infected system. In reality, a medical device may be infected through different channels, such as from the Internet, the private LAN inside a hospital domain, or a USB thumb drive.

To detect the dominant malware source in the medical domain, the authors devised experiments to reproduce the vulnerable scenarios; those are done through using network trace data to find the malware fingerprint. The authors studied several standard data sets such as Darknet, Netflow, and blacklist. Several techniques were chosen for malware detection in those data sets, including port scanning and timing analysis. The study results implied that the Netflow data set contains several anomalous behaviors, such as several hosts operating over Bitcoin ports, and from the blacklist data set, it found that tens of devices did contact the blacklist IPs. Gouravajhala concluded by suggesting several solutions, such as relying on IT administration and device-level investigation to fix the problems.

An attendee asked about a scenario where there might be no IT administration department in the hospital; such a scenario is not addressed by the current work, and Gouravajhala acknowledged that it presents possible future research directions.

Microbiome Sequencing

Justin Wagner and Hector Corrada-Bravo, University of Maryland, College Park

Justin Wagner addressed the privacy problems regarding personal biomedical data. The particular biomedical data in question is the OTU (operational taxonomy unit) data, which indicates species information regarding a creature. Such data can be analyzed for various types of modern medical applications, such as disease prediction. In particular, the workflow to create OTU data starts from the human microbial samples that are part of a publicly available data set (e.g., the "personal genome project" (http://www.personalgenomes.org/)); it then moves on to extract DNA from which OTU data can be built.

While the OTU data analysis can have various new applications, it may raise privacy concerns, because once disclosed such personal OTU data could allow other people to predict the possible diseases that a patient may develop in the future, something not every patient feels comfortable about disclosing. To be specific, the research formulated such personal data as the presence/absence of data between a patient and OTU. Based on this data format, applications such as disease prediction are translated into similarity/diversity measures such as the Bray-Curtis dissimilarity index. Wagner then addressed the privacy preservation regarding these computations, which will be elaborated. By using this technique, they disabled the reidentification with regards to the publicly posted microbiome data sets.

Privacy-preserving computations and storage are handled by formatting data selectively. The sensitive data (e.g., original OTU data) is stored securely and processed using either additive secret sharing or generic multi-party computations—more specifically, SharedMind (http://code.google.com/p/sharedmind/)—while the nonsensitive data (e.g., the analyzed result regarding disease prediction) is stored non-securely, and is made available to the end users.

Session 2

Summarized by Yuzhe Tang (yztang@gatech.edu)

Securely Connecting Wearable Health Devices to External Displays

Xiaohui Liang and David Kotz, Dartmouth College

Xiaohui Liang said that wearable health devices, such as smart bracelets, are booming. These devices are unique in the sense of their portability and always-on feature. Smart TV is becoming a reality in different places (e.g., the screen on a treadmill), which enables effective information visualization. Bridging a smart bracelet with a smart TV for a better user experience in health care raises security issues and design challenges.

When pairing smart TV and bracelet, there are several unique properties about the scenarios: a smart TV is shared by many users while a smart bracelet is usually owned by a specific patient. Also, the two devices are usually connected in an ad hoc manner. Secure device pairing in this scenario is challenging since the setup of a secure channel requires computation-intensive key-management operations that may be prohibitive for power-limited mobile devices such as a bracelet.

Liang discussed several baseline approaches with detailed analysis of their respective pros and cons. To make it practical, they considered various properties that are desired, such as security and ease of setup among many others. Liang then presented possible solutions that leverage the built-in hardware components of wrist-worn devices to securely and effortlessly establish connections to ambient display devices.

An Evaluation of ECG Use in Cryptography for Implantable Medical Devices and Body Area Networks

Michael Rushanan, Johns Hopkins University; Denis Foo Kune, Daniel E Holcomb, and Colleen M Swanson, University of Michigan

Michael Rushanan pointed out that existing authentication protocols for implantable medical device and body area networks, such as the Heart-to-Heart protocol, relies on measuring IPI (inter-pulse interval) or the time between heartbeats. The protocols assume that the randomness from IPIs must be measured with physical contact, which presents obstacles for practical use.

Their research work challenged this conventional assumption and proposed a new concept of remote observability, which aims at correlating ECG signals (electrocardiography) with observable features, such as involuntary movement and skin color changes. With this new feature, the IPI data can be obtained (through indirect inference) without patient physical contact, which is expected to improve the practicality. The presentation included a pre-recorded demonstration for showing the feasibility of using image/video processing techniques for IPI inferences. To further improve the precision of inference results, Rushanan talked about the possible solutions of using a high-speed motion camera.-

Rushanan also briefly mentioned possible attacks and defense mechanisms such as signal injection and unobservable physical values.

"Dr. Hacker, I Presume?" An Experimentally-Based Discussion about Security of Teleoperated Surgical Systems

Tariq Yusuf, Tamara Bonaci, Tadayoshi Kohno, and Howard Jay Chizeck, University of Washington

Tariq Yusuf began by saying that, as a new technology expected to be approved soon (by the FAA), teleoperated systems have various advantages over conventional approaches. They are cost-effective and more affordable nowadays than ever before. The medical domain finds various applications of this new technology, such as in the Da Vinci® system, where robots are used to assist in medical procedures. Teleoperated surgical robots have the advantages in more extreme application scenarios such as battlefields, natural disasters, and human-caused catastrophes.

Yusuf addressed the security aspect of teleoperated surgeries. He demonstrated several interesting attacks targeted at the surgical robot. The system setup consisted of three machines interconnected by a network hub that transferred modified UDP. The network packages were transferred between a surgeon control console, where the surgery physically occurred, and a Raven machine, where the physician provides the surgeon with instructions. The attacking machine running Kali Linux was in the middle of the two machines, capturing network packages flowing through. While the vulnerability can be exposed on end machines, the research work mainly considered the network communication security. Several attacks were then demonstrated, such as dropping things on the surgeon control console (which could lead to wounding the patient, or even death), or hijacking the mechanical arms during the surgery, which may not move as intended.