1st USENIX Workshop on Health Security and Privacy (HealthSec ’10)

August 10, 2010
Washington, DC

INVITED PANEL: MEDICAL DEVICE SECURITY AND PRIVACY

Summarized by Leila Zucker (leila@motherzucker.com)

- ***Ten Years of Insulin Pump Therapy: From User to Researcher***
  Nathanael Paul, Research Scientist, Oak Ridge National Laboratory

Nate Paul told us that he received his first insulin pump in 2000. He gave a brief overview of diabetes, how the insulin pump works, and how the systems may be vulnerable. The pumps can be very complicated, and there are classes to teach you how to use them. Newer pumps have an increasing number of features, including remote wireless programming and the ability to update settings by personal computer. While these features improve effectiveness, they also represent the threat of exploitable vulnerability and decreased safety. Approximately 13 different attacks have been described to the FDA. In looking for solutions we must address both issues.

Session chair Kevin Fu asked each of the presenters to describe the biggest research problems for security and privacy. Paul answered, data transmission. Don’t get attached to a specific device, but focus on the entire system. Fu then asked about incentive systems for improving security when there is shared responsibility. Paul responded that manufacturers are aware of compliance, safety, and security. Revealing source code would be a good step, or the FDA could review source code. Carl Gunter (University of Illinois) asked whether the 13 problems with the insulin pump could be solved by best practices or whether they required a novel approach. Paul felt that general solutions were needed that would apply to all devices, both implanted (e.g., pacemaker) and partially embedded (e.g., insulin pump).

- ***FDA Regulatory Perspectives on Cybersecurity***
  John F. Murray Jr., Software Compliance Expert, United States Food and Drug Administration, CDRH/Office of Compliance

John Murray said that confusion seems to exist about what the law requires vendors to do. The FDA rules only apply to manufacturers, not to software vendors or clinical facilities. Manufacturers must validate patches. Viruses have caused major disruptions to clinical information systems, but there is no formal reporting of cybersecurity issues. Vendors have reportedly told hospital IT staff that they can’t install security patches “because of FDA rules.” Therefore we need FDA outreach to the clinical IT community.

The law requires that deaths be reported to the FDA and the manufacturer, serious injury to the manufacturer only, and potential injury or death to MedWatch on a voluntary basis. The manufacturer must report if there is any chance a device may cause a death or any indication of quality deficiency (go to http://www.fda.gov and search for “cybersecurity”). The FDA addresses safety, not security, concerns. To solve the problem of medical device security will require the efforts of IT infrastructure vendors, healthcare IT administrators, and medical device manufacturers.

Paul Jones at the FDA is doing research on device tracking, secure record transfer, and the question of whether to allow patients to take records home. The current focus is on functionality, but security and safety issues need more attention. The IAC standards organization is addressing the issue of different stakeholders negotiating safety and security, and voluntary standards will be published soon. However, the FDA will be highly dependent on the cooperation of device manufacturers. The FDA’s inability to review every line of code supports the idea of having medical device software all be open source. Please feel free to contact Murray with any questions (see http://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/ucm127922.htm).

- ***Killed by Code: Software Transparency in Implantable Medical Devices***
  Karen Sandler, General Counsel of the Software Freedom Law Center

Karen Sandler told us that two years ago she got a pacemaker/AICD (automated implantable cardioverter-defibrillator). She was very concerned about the safety of the software in the device, particularly when she found out that she could not obtain the code to check it herself. She finally settled for an older device with no wireless component She is now researching pacemaker software, which on average has one defect per 100 lines; 98% of software failures could be detected by all-pairs testing. Security through obscurity just doesn't work. However, with free and open source code, users have the ability to independently assess the system and risks, patch bugs easily and quickly, and remove dependence on a single party. Shared software does not mean unprotected devices—you can still use encryption.

The FDA does not review source code, only manufacturer reports. There is no clear set of mandatory requirements for software and no repository of source code, which prevents patients from suing under state product liability laws. All software should be made safe: medical devices, cars, voting machines, financial markets. See www.softwarefreedom.org.

In the discussion, Sandler emphasized that with wide adoption of implantable medical devices, the biggest research problems for security and privacy concern the need for open-ended transparent solutions so that security can be verified. Since the open source world is about collaboration, with shared systems it is more likely that everyone will understand them. Avi Rubin (Johns Hopkins) interjected that the many-eyeballs theory works in Linux, but in the real world a hacker can find vulnerabilities, so patches might not come out quickly enough. Sandler replied that it's been seen that not publishing does not stop attacks. Umesh Shankar (Google) felt that it's really about transparency. While there are not many hackers, plenty of people want to test for vulnerabilities, but there is a question of manufacturer liability. Sandler said that she can think of hacks for her pacer, and primarily wants transparency.

SENSORS, CLIENT DEVICES, AND MOBILE HEALTH

Summarized by Leila Zucker (leila@motherzucker.com)

- ***Protecting E-healthcare Client Devices against Malware and Physical Theft***
  Daisuke Mashima, Abhinav Srivastava, Jonathon Giffin, and Mustaque Ahamad, Georgia Institute of Technology

Daisuke Mashima said that in their setup, data is stored in online repositories and a threshold keys system is used to control access. The client device includes one VM for the user interface and another that holds one key and handles communication. The other key resides at a logging service, although a human administrator can also provide a key. Mashima went over ways to handle issues if a client device is compromised and for eliminating single point of attack, including the threshold signature scheme, human authority, online monitoring system, user virtual machine, and firewall.

- ***Can I access your data? Privacy Management in mHealth***
  Aarathi Prasad, Dartmouth College; David Kotz, Dartmouth College and ISTS

Aarathi Prasad said that if you want patients to use EHR, you need to instill confidence in them. For example, a patient sharing jogging data from her mobile phone with a wellness advisor might not want the advisor to see her jogging route. What data do we need, then, and when do we collect it? A patient may remove sensors and forget to reattach them. Another issue is that many doctors believe patients cannot tell what data to share. Several items were mentioned for consideration: Do we retain old data? Should backups be retained, with or without the patient's knowledge? Query and response should be fixed format. There should be user interface requirements that are unambiguous and use few medical terms. Finally, future work includes learning patient privacy concerns, identifying benefits and trade-offs, and determining what to delegate to doctors.

Attendee Vince (last name and affiliation not stated) inquired about what to do if a patient revokes access. Prasad replied that they are researching this now. The session chair, Tadayoshi Kohno, asked about patient privacy. Prasad replied that while doctors need access, patient privacy is an important consideration. Kohno then asked about emergency situations, people who can't afford a phone, and other countries. Prasad responded that researchers can take phones to rural areas to collect information. An attendee noted that most people don't have a single point of access to the healthcare system or even always know their doctor's name, and privacy laws vary by country. Prasad added that some cultures don't have the concept of privacy, so how much of their data can you use? Kohno said that consent management is important; doctors should take only information needed for care. He then asked if there is research on how much patients want to be involved with management of their EHR. Prasad said they are working on that.

- ***Using Trusted Sensors to Monitor Patients' Habits***
  Alec Wolman, Stefan Saroiu, and Victor Bahl, Microsoft Research

Alec Wolman addressed the problem that patients often do not follow doctors' instructions. It can be difficult to manage chronic diseases such as high blood pressure and diabetes outside the office. Smartphones can be used with sensors to change the status quo by assisting patients in monitoring their habits: an accelerometer can be used for exercise, a camera for diet, a pressure sensor for their pillbox, body sensors for heart rate and blood pressure, and so on. Financial incentives can also be used to change patient behavior. But data gathering must be done in a trustworthy manner. Trusted sensors include laptops with TPM chips or smartphones with ARM's TrustZone. We can use trusted computing primitives to preserve the integrity of sensor readings with digital signatures and verification. He outlined two approaches: software only (trusted VM) with no barrier to deployment but also with no wireless security, and simple hardware changes such as tamper-resistant casing. Trusted sensors must protect against malicious use and ensure that users do not fabricate readings.

An attendee wondered who would benefit financially from attacking. Generating false claims is a bigger risk than monitoring sensor data. Wolman said thatraw data does have significant financial impact. Hackers want raw data for making fraudulent claims. In response to the chair asking about the future of medical sensors, Wolman said that monitoring eating disorders with weights recorded by sensors would be useful, as patients often report false weights. Carl Gunter (University of Illinois) observed that his cell phone surreptitiously spying on him and reporting to his doctors would not be his idea of a killer app. Wolman said the user could be in control of what readings are taken and what is revealed to whom. How likely are these apps? Mobile devices can take pictures of checks to be filed with your bank. Security is a big challenge; so are energy management and battery life. The Chair asked how one could monitor a patient who cheats. Wolman replied that there is no way to stop this currently unless you use multiple sensors.

Nate Paul (Oakridge National Labs) pointed out that smartphones have been used with insulin pumps, but that means carrying an additional device. Wide-scale attacks on insulin pumps could have some financial advantage. Jack Lacy of Intertrust asked about data integrity vs. privacy and a patient needing selective control over sharing data. Perhaps offer incentives: if you don't opt in, you are penalized by insurance companies. Chase replied that it's a question not only of who gets access, but also of what they do with the data. The chair next commented that some EHRs allow a designation to not reveal certain data, but it might be revealed in a free text note. Wolman said that it's critical to put the patient in control. Is there a way to penalize the patient if they do not comply? We need to be mindful of this when creating incentives. Gary Olson (Intertrust) asked how much trust is enough. Do you need hardware, or is software sufficient? Cost is a problem. Wolman replied that hardware is coming, independent of medical apps. As for trust, you want to protect yourself not only from users but from malware. The final question by the Chair was, Is runtime integrity enough? ARM is more flexible than TPM with runtime integrity.

POLICY FOR HEALTH RECORDS

Summarized by Joseph Ayo Akinyele (jakinye3@jhu.edu)

- ***Practical Health Information Exchange using a Personally Controlled Health Record***
  Ben Adida, Isaac S. Kohane, and Kenneth D. Mandl, Children's Hospital Boston and Harvard Medical School

Ben Adida said that PCHRs represent a paradigm shift, with medical records controlled by the patient as opposed to the Nationwide Health Information Network (NHIN) model, which allows access to records via a Web portal. In addition, patients visiting different specialists for various purposes means that records must be aggregated in one location (the PCHR). With PCHRs, data can be aggregated from a variety of sources, including from implantable medical devices such as pacemakers and defibrillators. Patients can annotate their records and share selectively with their physicians. In this model, patients determine, through the PCHR, who gets access to their data, and clinics or hospitals connect to the PCHR to access the patient's records; in the current, provider-centric NHIN model, the focus is on provider-to-provider data sharing, and patients have to independently give each provider access to their records.

Adida argued that Health Information Exchange (HIE) can be mediated by the PCHR and that once data is shared with the physicians, patients are mainly concerned with who else may have access. But if patients are given tools to annotate, update, and share their data, this could create a very powerful health record system. He concluded with comments on the future of the PCHR concept, involving using email addresses to locate health records and PCHR format standardization across healthcare providers.

Avi Rubin (Johns Hopkins) commented that despite the common belief that patients should have control over their records, most doctors mistrust records received from patients. Adida replied that the idea of patients having control has evolved because healthcare is fragmented today. Hospitals rely on out-of-band mechanisms to share records with other hospitals. With PCHRs, patients can now take their records from one doctor to the next. However, safeguards must be in place so that patients do not unwittingly share data. One audience member asked how much thought has been put into the ecosystem of patients controlling their records. For example, in the Indivo PHR system, when considering records for children, parents have more access to their children's PHRs than to their own. Further, any sensitive data is not included in the PHR, because of the difficulty in managing that data.

- ***Technology Companies Are Best Positioned to Offer Health Record Trusts***
  Shirley Gaw and Umesh Shankar, Google

Umesh Shankar discussed the notion of a health record trust as an independent archive of patients' medical data in which patients ultimately have control over how their information is released. These trusts guarantee that data from any time period can be retrievable without loss of information. For instance, a patient with a chronic disease may want to see the progression of her disease over time, but if the practice or clinic goes out of business, the data could be difficult, if not impossible, to retrieve.

A service that can meet demands for high availability, data integrity, and provenance is achieved best by technology companies. Technology companies are more diverse and do a better job than government-led IT in handling large-scale projects. Most large-scale IT projects in fact do and should fail, but the government wastes millions of dollars on projects that end up not working. If ten tech companies compete on an IT project, perhaps three provide a good solution, making the odds of a working solution much better than solely with the government. EMR vendors have a lot of experience managing medical data, but usually only for a single hospital or HMO. The biggest challenge is the aggregation of data from different sources, and EMR vendors are not built to support such integration with other vendors.

Tech companies are prepared to work on a problem of providing record trusts on a large scale that requires high availability, integrity, and redundancy. Shankar pointed out that people expect Google services to run all the time, and when those services are unavailable, Google is embarrassed. This is how it should be for health records. However, tech companies cannot solve this problem alone. They need government and EMR vendor collaboration to establish public-key infrastructures for trusts and to define interoperability standards between institutions. These are some of the issues that tech companies should not solve in an ad hoc fashion.

One audience member asked if patients are to trust tech companies with their data and whether the incentives are aligned with the patient's privacy. What is the business model for Google Health? Shankar replied that Google does not make money from providing health services to patients or from securing their data. Although Google Health does not conform to HIPAA regulations, Google's privacy guidelines have the patient's interests in mind. Another audience member asked whether placing all the trust in a tech company creates a failure and availability risk. Why not consider an open federated model for managing record trusts? Shankar agreed that the records should be fetched from different providers, but argued that the records must still reside in a central repository.

- ***Policy Management for E-Health Records***
  Maritza Johnson and Steven M. Bellovin, Columbia University

Johnson began by explaining that EHRs are records created and maintained by institutions such as hospitals, and patients may or may not have access to the information. This notion of health records is different from PCHRs, which are maintained by patients. Existing access-control EHR systems allow access to all patient health records, based on successful authentication to the EHR system. User access (including by nurses, doctors, etc.) is audited by the system, and patients must monitor their own records for unauthorized accesses. An exception to this rule is the EHRs of celebrities, professional athletes, and chemotherapy patients admitted at the hospital. Because these types of patients are high-profile, strict access controls are enforced.

New mechanisms are needed to support and control EHR-sharing between hospitals. Currently, ad hoc out-of-band mechanisms such as email, fax, or mail are used to share EHRs. Johnson argued that an adequate architecture that supports access policies must be developed, and she questioned who will manage the access policies and with what mechanism. So far, the focus has been on the adoption of electronic records, not how they will be shared, how access is controlled, or even what those access policies will be.

In the current literature there are two kinds of approaches to EHRs.Human-centered approaches focus on the interactions doctors have with EHRs over paper-based charts in day-to-day activities. Computer scientists focus on the architecture for EHRs to support sharing EHRs. Johnson discussed two possible types of access control: preventive and audit-based. Preventive (similar to file-based) access determines access policies a priori; audit-based relaxes preventive policies for emergency situations. Finally, usable policy tools are needed to handle the difficult task of creating and managing fine-grained access policies for EHRs.

- ***Dr. Jekyll or Mr. Hyde: Information Security in the Ecosystem of Healthcare***
  Joseph Cooley and Sean W. Smith, Dartmouth College

Sara Sinclair, speaking for Joseph Cooley, said that policymakers mandate that medical data should be protected in a particular way, but deployed mechanisms do not match the policy or align with daily practice. Once these mechanisms are put in place, clinicians work around the mechanisms when they prevent them from getting their work done.

To achieve usable security from a healthcare provider and patient perspective, the authors propose retrieving user feedback. Acquiring feedback is a proven approach to understanding issues between a system and its users. This same approach is proposed to help improve the ecosystem of the healthcare environment. The authors argue for a practical approach which includes spending time with users, performing observations with users and a system, and retrieving system logs to elicit feedback. The authors' goal is to equip clinicians, policymakers, and developers with information to be able to implement such mechanisms.

The authors argue that to be worthwhile the feedback process should be easy and painless. Users should not suffer negative repercussions for providing feedback. For instance, if a clinician shares a password in order to get her job done, then she may be subject to certain penalties by the hospital. In addition, the process should reward the users such that they are motivated to help improve and build trust in the system. If closed loop feedback is provided and it is possible for users to inform the system, users will have greater trust in the system.

Avi Rubin asked whether the role for technologists is to develop solutions and leave decisions to policymakers or to develop solutions that influence decisions one way or another. It is impossible to design a one-size-fits-all system that satisfies technology and policy requirements. However, technologists should not blindly design systems based on preconceived needs of a system. Technologists need to collaborate with users, usability experts, social scientists, and clinicians to build a system that satisfies both requirements.

- ***Privacy Challenges in Patient-centric Health Information Systems***
  Anupam Datta, Carnegie Mellon University; Nipun Dave and John Mitchell, Stanford University; Helen Nissenbaum, New York University; Divya Sharma, Carnegie Mellon University

Helen Nissenbaum and Anupam Datta presented this workshop paper on the privacy challenges in personal health record (PHR) systems. Nissenbaum questioned what the rules or policies should be that govern the inflow and outflow of information in PHRs and how to formalize these rules and enforce them in the PHR systems. PHR systems such as Google Health and Microsoft HealthVault provide aggregation of data from diverse sources, offer patient control, and allow for customization according to the patient's needs. For example, these systems can determine a patient's risk for diabetes simply by analyzing their PHR. With PHR systems, healthcare providers can now extract all sorts of interesting data from anonymized PHRs such as for advertising or for public health purposes.

Nissenbaum argued that the notion that patients have full control over their PHR contradicts and is incompatible with the idea of practitioners using the patient's PHR as a basis for medical care. Doctors and clinicians are concerned with the integrity of patient data and usually prefer that the patient data come from their colleagues. Nissenbaum asked what model patient health records should follow: a patient portfolio model (i.e., patient controlled), a credit-report model (i.e., institutionally managed records), or a trust-based model (i.e., third-party managed records). Because each model offers different levels of patient control, the model selected must promote the values and purposes in the context of providing medical care.

Datta then discussed the challenges of representing policies and enforcing those policies using traditional access control mechanisms. He referenced their previous research that analyzed the HIPAA requirements and created a system to formalize those requirements in logic. He argued that such requirements cannot be enforced using traditional access control, due to interpretations of the HIPAA rules. For example, the HIPAA rules use terms such as "belief" or "trust" that are subject to various interpretations. The authors proposed a hybrid approach which incorporates proactive access control and auditing to enforce the HIPAA rules on PHRs.

An audience member asked whether data integrity based on the source of the information is considered in PHR models. For example, a doctor could add an incorrect diagnosis into a patient's records, for a variety of reasons. Nissenbaum replied by referring to the different models of health records she discussed during her talk that offer options for patients. The issue of data integrity of records is controversial, as the model chosen for the health records will dictate how information is controlled.

DEVICES

Summarized by Aarathi Prasad (aarathi@cs.dartmouth.edu)

- ***Security That Is Meant to Be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices***
  Stuart Schechter, Microsoft Research

Pacemakers and implantable cardiac defibrillators are increasingly becoming wireless. It has been shown that unauthenticated commands can change the device state. An obvious solution is to add authentication and check if the commands are from an authorized party. But how do we distribute this key? This issue can be solved if the key could be something you know, you have, or you are, where the "you" implies the emergency health care provider or the patient. These can also be interpreted as what you forgot, what you lost, or what you used to be! Something that you know can't be given to all HPs, especially if the patient is unconscious. Something you have could be an object that you possess, but if you lose it or forget to carry it with you, who gets access? An alternative to this is authentication by proximity. Something you are implies that the key could be a biometric; but this might be difficult, especially if the device is implanted. Medical tattoos can be placed next to the scar that marks where the device has been implanted. It should be in human readable form, in case the tattoo reader fails. This key can be generated by the patient's device. The tattoos could be ultraviolet for privacy, since other tattoos might be visible. When their clothes are off, patients can hide the tattoos using sunscreen.

- ***Privacy Challenges for Wireless Medical Devices***
  Brent Lagesse, Oak Ridge National Laboratory

Device usage can leak information such as conditions, patient actions, or device type or model. Adversaries can determine what the patient is doing by profiling using communication patterns. So if an adversary knows the protocol used, he can determine who among a crowd has a particular device implanted. Adversaries can launch spoofing, replay, and denial of service attacks or, knowing that a patient has a certain condition, physical attacks. A patient could also be subject to discrimination by an employer or insurance company. Several approaches have been taken to protect privacy—encrypt the data (traffic patterns might still leak information), mask communication so that you will be in the set of possible sets of insulin pumps (k-anonymity), and mixes (pass the information to all other devices that the patient is carrying such that it is possible to hide what devices are being used).

New approaches are being studied to reduce attacks, remote to physical, to provide practical privacy (by changing cyber to physical attacks) and to prevent wide-range scanning. Keep in mind that as a researcher, you need to take a minimalistic approach—sensors don't have to be general-purpose computers. The device should use common protocols; if only one device is using a strange protocol, it is easy to identify.

- ***Insulin Pump System Security***
  Nathanael Paul, CSIIR, Oak Ridge National Lab; David C. Klonoff, Diabetes Research Institute, Mills-Peninsula Health Services

Medical devices can communicate with patients, caregivers, etc. There are different components to this system that interact with the device and with each other. An example of a remote-control device is a glucometer which tells patient about blood glucose level. This glucometer could be recording continuously. A smartphone can be used to control a glucometer remotely and can also act as a data recording tool. As a monitoring tool, the smartphone can calculate how much insulin the patient needs, store this data, and use it to record data from the patient. As a controlling tool, it can issue several commands.

Physicians are increasingly using mobile devices to control or monitor patient condition. But worms can spread from phone to phone through Bluetooth and we need to determine how this will affect patients.

- ***Is Bluetooth the Right Technology for mHealth?***
  Shrirang Mare, Dartmouth College; David Kotz, Dartmouth College and ISTS

A communication technology for medical devices should be: (1) secure—it should authenticate transactions and ensure that the data is correct; (2) private—encryption does not provide enough privacy protection for patients; (3) reliable—the device should be able to resist interference; (4) scalable. The *E*0 cipher was used to provide security, though it was not secure enough. JW was used for those devices without I/O. Privacy became an issue, since headers of the data packets contained MAC information, which could be used to identify devices and link all data transactions. Reliability was achieved through Bluetooth's hopping pattern and channels were reduced from 79 to 40. But how will Bluetooth piconet interfere with other Bluetooth technologies?

There are alternatives to Bluetooth. The Sly-Fi protocol encrypts headers and provides unlinkability. We could use the human body as a communication channel, which is more secure and private. Galvanic transfer involves attaching electrodes to the skin and sending electricity through the human body. A 2 mbps throughput is achieved. Another option is body-coupled communication, which achieves less throughput but is power efficient, but is this safe? There are other issues as well.

- ***On Usable Authentication for Wireless Body Area Networks***
  Cory Cornelius, Dartmouth College; David Kotz, Dartmouth College and ISTS

If we want systems to be used, we should make them usable, so that the patient shouldn't have to do anything. Body area networks are a bunch of devices that send data to a gateway. Data can either be sent to a cloud service or be stored on a mobile phone. Devices such as Fitbit and Nike plus are available in the market now. We need to provide usable and secure authentication so that doctors can be confident that data is coming from the actual patient. The problem being tackled is a weak version of this, where the cell phone or gateway is trying to determine if all sensors are on the same person. The strong version of this problem confirms that all sensors are on the actual patient. This authentication is necessary in a scenario where an elderly couple might accidentally swap sensors. A solution to this problem is wireless localization. Even though the body might attenuate signals, we can still detect if the sensors are within some bodily distance.

In the Q&A the authors were asked what prompted their research—had there been any such attacks? They answered that some attacks might not leave evidence behind, and, in order to protect their business, manufacturers might not reveal that attacks had occurred. If an attack does happen, it might be difficult to patch; hence it is better to prevent attacks. It is also important to anticipate attack scenarios, in order to identify the important security metrics. The switch from wired to wireless has exposed the devices to imminent attacks. But wireless does help treatments. We need to consider battery life too. Wireless technologies drain batteries, and unauthorized commands can launch a DoS attack on the device by draining the battery. You can't replace batteries on implantable devices easily. The patient can lie about the data, so that could be an attack too.

How do you evaluate proposals and next steps? With a user feedback form. Why are medical tattoos better than biometrics? Using biometrics, you are not authenticating the health care provider. Biometrics should not be changing and hard to read—for example, a heartbeat would change in a dying patient. The patient will recognize that his privacy is being violated when someone tries to access the tattoo, unlike a retina or fingerprint scan. If someone asks to check the area on the body near the scar, the patient will realize that the person has no need to do so.

SHARING DATA

Summarized by Tamara Denning (tdenning@cs.washington.edu)

- ***A Risk Management Framework for Health Care Data Anonymization***
  Tyrone Grandison, IBM Services Research; Murat Kantarcioglu, University of Texas at Dallas

The goal of this research is to share data sets for research in an anonymized way; the ideal result would be to anonymize data sets so that they are protected from all re-identification attacks. This work takes a slightly different approach from other research in this area by embracing a more practical approach: not 100% guaranteed privacy, but providing a user instead with information about the amount of risk that is left.

The risk management framework for health care data anonymization incorporates: (1) the chance of re-identification of sensitive data; (2) the repercussions of data reidentification; and (3) the utility of sharing the data set in question.

The researchers propose that the parameters of the risk model can be estimated using publicly available data. The risk management framework must also incorporate a way to tune anonymization based upon risk estimates (and feedback).

- ***On Resolving the Privacy Debate in Deidentified Neuroimages***
  Nakeisha L. Schimke, Mary Kuehler, and John Hale, University of Tulsa

The topic of this research is finding a way to deidentify neuroimages such as CT, MRI, and PET scans. These scans are images with high spatial resolution that includes facial data. Personally identifying information (PII) can be stripped from the image's metadata, but there is a chance that a person may be identifiable based upon the facial data in the image.

One approach is to remove all content from the image except for the brain tissue; however, this can result in the loss of some brain tissue imagery, and there is no standard for this kind of deidentification process. As a result, neuroimages using different deidentification processes may not be comparable in research studies.

The researchers are currently experimenting with different reidentification techniques in order to study whether it is feasible to reidentify visually deidentified neuroimages. Based upon their findings, they may also investigate possible mitigation techniques.

- ***Securing Medical Research Data with a Rights Management System***
  Mohammad Jafari, Reihaneh Safavi-Naini, and Chad Saunders, University of Calgary; Nicholas Paul Sheppard, Queensland University of Technology

The motivation behind this research is to be able to share data for research while simultaneously respecting patients' privacy. Current approaches include anonymizing data sets by adding noise, which can result in losing relevant data, and using access control policies.

The researchers propose using DRM mechanisms in order to control access to medical records. Specifically, they are addressing "bench-to-bedside" medical research, where clinical information is repurposed for medical research. The authors suggest an approach where data is always encrypted and a trusted agent examines the data and a license in order to reveal decrypted data as allowed by the license.

The authors released a 2009 technical report describing a Sharepoint implementation of such a system where data is presented in DRM-protected Excel files. In future work they hope to refine access roles, handle data from multiple sources, and extend their system to operate in the cloud.

Questions for the panel of presenters included the nature of PII: specifically, where does PII end? If you bring in enough contextual information, almost anything can become PII. One workshop participant suggested that rules should be attached to pieces of medical information that define whether or not the information is PII given the context.

A question regarding the risk management framework was how the risk can be boiled down to a scalar number, when the risk of reidentification might be distributed across the members of a population. One proposed approach was to have adaptive fuzzing, where unique individuals are overgeneralized (fuzzed) and individuals closer to the norm are undergeneralized. This led to the question of how one can assign a uniqueness score to an individual based upon the fields of the medical record.

In terms of adding noise to data sets, concerns were expressed that the noise can affect downstream science. In addition, medical researchers in general dislike working with fuzzed medical records. To further complicate matters, the anonymized records do not generally contain metadata about the anonymization techniques used to add noise to the data.

More general concerns were expressed that the security community may not completely understand the domain-specific problems related to working with medical records. Additionally, a workshop participant suggested that patients and study participants do not have an accurate or complete understanding of what it means to have their records anonymized or of the various degrees of privacy different anonymization techniques can offer.

APPROACHES FOR HEALTH RECORDS

Summarized by Aarathi Prasad (aarathi@cs.dartmouth.edu)

- ***Beefing Up a Health-Data Ecosystem: Struggles and Successes from Microsoft HealthVault***
  Jim O'Leary, Microsoft Health Solutions Group and University of Washington

O'Leary discussed the common problems faced by the HealthVault team and how they were handled. First, he talked about authentication. Security provided by HealthVault is "weak" because the credentials used to log in to HealthVault are shared with "lesser integrity systems" such as email, calendar, and Xbox live accounts. HealthVault depends on third-party providers, such as LiveId and OpenId, that support authentication protocols. It includes dependencies in systems, but providing these options gives redundancy. Authorization is at two levels—a user wants to share his health information with another user or with an application. This presents another struggle, since users want granularity. They want to control what data is going where and to be able to track it throughout the system. But this produces usability issues.

Then O'Leary talked about the ecosystem security model. Microsoft has to depend on its partners. When faced with a blue screen, end users might blame Windows, but it might be due to some third-party error. The same issue happens in HealthVault when a partner loses data—the blame is on HealthVault. He briefly mentioned the shared data problem of multiple people sharing data from multiple platforms, which introduces more trust relationships and attacks. Solutions to the attacks are presented as security tips in a public white paper.

- ***Using the Wave Protocol to Represent Individuals' Health Records***
  Shirley Gaw and Umesh Shankar, Google

Shankar said that attribution is important in health records. In the latest Google Health UI, a mouse-over a particular data point on a graph from a lab test will tell you where the point of data came from. How do you preserve attribution over time and in aggregated data? Dr. Dre sends his diagnosis to Shankar's PHR from his EMR, saying Shankar broke his ankle and tore his Achilles tendon. After two months, his ankle has healed. Shankar updates his record, adds an end date. Hence the real diagnosis done by Dr. Dre is gone due to the change done over time.

Or suppose there was an error, accidental or deliberate. The local copy is gone when you delete something. How do you update the central server? When the doctor tries to synchronize the data with Shankar's updates, how does the doctor know what to take from or send to Shankar's PHR? A "diff" will not help, since a deletion occurred. There should be a common notion of the state of a patient's records. This can allow for bi-directional updates. Also, a history should be maintained, not just the current state. Wave protocol can be used for this purpose (http://www.waveprotocol.org/).

- ***EBAM: Experience-Based Access Management for Healthcare***
  Carl Gunter, University of Illinois at Urbana-Champaign; David Liebovitz, Northwestern University; Bradley Malin, Vanderbilt University

Carl Gunter explained that identity and access management are crucial enterprise functions in health care organizations (HCOs), but insufficient attention is given to the process of access control. What is the fundamental problem? Accountability versus enforced control: HCOs give access to everyone, assuming they will use it properly. Professional ethics are set up by the government and this is too difficult to set up as enforced control. Access logs are raw and factual and should be converted into information that can be understood in a manner that we desire. EBAM takes into account what happens in the system and feeds it back in, so that over time the model would evolve into something close to ideal.

The enforced-control model generates the access logs, which can be compared to the ideal model. The access logs combined with the ideal model give you good knowledge of what you want in your organization, and though them the enforced control model can evolve. The EBAM approach involves generating models based on audit events and attributes. These are used to create workflows and group health providers into social networks. Rules and actions are developed after analyzing the results.

Experience-based systems have been used for a long time; successful ones include spam filters and intrusion detection. This technique can be used only in applications that tolerate false positives and negatives. There is a strong demand to catch violations in access control and there is a debate over what technologies should be used. There is also the challenge of health information exchanges between organizations.

- ***Fine-grained Sharing of Health Records using XSPA Profile for XACML—An Extended Abstract***
  A. Al-Faresi, B. Yu, K. Moidu, and A. Stavrou, George Mason University; D. Wijesekera, National Institute of Standards and Technology and George Mason University; A. Singhal, National Institute of Standards and Technology

How can we collect the different actors, patient's health information, and other parts of the record, such as psychological notes, into one model? asked Wijesekera. To what extent has XSPA captured all these scenarios? HITECH implies that the patient should have delegation rights. On the other hand, PHI can be disclosed without an individual's authorization for certain national priority purposes. Health records contain different views for the patient and the healthcare provider. When the healthcare provider needs access to some information, he sends the request to the patient, without knowing whether the data was actually derived from those records that he had access to. Some changes are required in the XSPA model in order to fulfill its central purpose.

- ***An Anonymous Health Care System***
  Melissa Chase and Kristin Lauter, Microsoft Research

Melissa Chase pointed out that privacy is a huge concern in healthcare, so we should be careful to reveal information only when necessary. Doctors, nurses, insurance companies, pharmacies, etc., need to see patients' health records, but not necessarily all the information that they contain. So a health record system should reveal as little as possible, while allowing the consumers to access the required information.

One technique is to use Anonymous Credentials or Minimal Disclosure Tokens, which ensures that the service cannot identify the user. An example scenario involves user Alice, who gets a policy token when she registers with an insurance company. Her doctor uses Alice's policy token for some transactions. When the doctor bills the insurance company, he uses an anonymized token for the procedure. The insurance company learns that some patient had some procedure done. Similarly, the doctor can send an anonymized token for a prescription to the pharmacy and a prescription token to both the pharmacy and the patient. The pharmacy can send an anonymized token for the prescription to the insurance company as well. This ensures that only required information is shared with others. The anonymous policy token needs to contain only the information that the recipient requires.

The limitations of the system are not technical. The take-home message is that we should be thinking about what information should be revealed and reveal only what is necessary.

Many issues were brought up in the ensuing discussion. There could be other factors, not just bias, that could become barriers to adopting the techniques. For example, insurance companies would want patients to buy medicines from their authorized pharmacies. Could the authentication methods in HealthVault be used by real patients in real-world circumstances? HealthVault targets all kind of people. What about patients who are brought into trauma care or who are unconscious, when we don't know who the patient is? We can design the system to be open and support situations as they happen.

What about people lying when they update their records? We need accurate provenance of data. It is hard to encode trust in the data, but you can trust the data as long as you have accurate provenance. Data other than time-series data can be difficult to visualize, but technologies like Wave can display the flow of information. We should also understand that the user interface is different for different consumers and needs to be integrated.

Even lawyers have different interpretations of health policies. Implementing these policies into code is a non-terminating problem. Pharmacies need the patient's name and prescription, so would presenting an anonymized token be sufficient? Pharmacies don't need your name; they can authenticate you if the barcode you present matches the barcode on the prescription. But rules could change in the real world if the patient forgets to bring the barcode with her or when the pharmacist looks at the medicine and understands what the patient's medical condition is.

The system could function very well if we determine what information needs to come together to perform the function we need. Note that we might not be able to understand who needs what from the raw information that we get. Consider the digital cash argument, where you could perform transactions without giving away too much information. How is it different in healthcare just because you deal with medical information and insurance companies? Those are similar but we have to be more careful, because a failure in the system could prove fatal.

When coming up with technologies, should you try to envision environments outside of North America? During floods in Pakistan, the government provided aid only if you provided your ID card. It would be interesting to develop technologies to work with antagonistic consumers.

Insurance companies need to know how a patient is doing. How can they assess risks and charge premiums when a patient's health data is anonymized? We know that they need information about everybody, but is it their right to have all the information they want? Chase discussed the purpose and use limitation in her talk. What are some potential applications in research settings? It is difficult to guarantee that the data you give out is used only for a given purpose. But it is possible to prove that a particular statement that you claim to be true is true, rather than giving out data and trying to protect it from being used elsewhere, which is a hard problem.

How do you see primary care physicians using such technologies when they have no IT staff? People will trust technologies that allow them to partition health information and protect it. Doctors view the role of PHRs as supplemental, equivalent to clipboards. They can take data in the PHRs and do their diagnosis. Patients can do lots of stuff with the data as well. PHRs will be adopted slowly, one step at a time. As a first step, we can reduce redundant procedures and tests—for example, when you redo a test with another doctor because you can't transfer the fact that test was done earlier.

Central healthcare repositories are not possible in the US, since we don't have the technology to manage access control. If PHRs are starting to fill with information collected from glucometers or insulin pumps, how does the patient know whether to believe the data? We need to look at higher-level abstracted data, rather than looking at the raw data. HealthVault digitally signs data before uploading it. But the processing power of some medical devices is not ready for encryption to support the provenance claims. So you could still attack between the device and client PC, unless you are timing the data on the device itself. It is hard to determine what is enough: is it good enough for the client application to sign the data? You have no option but to trust the outcome of the device, unless the device is broken. The other issue is how you get data into PHR—issues such as, is it my glucometer or not? There are good techniques to authenticate devices that have no I/P or O/P.

Information from medical devices has to be summarized. Also, you can't have a machine diagnose like a physician. If we dump raw data, no one is going to look at it. EHRs are crucial not to just repeat tests but to do tests. Health providers have not seen any patients who use PHRs, even though they have treated students and other technologically advanced patients. Another bit of information that could be captured by PHRs would be a list of a patient's medications, which patients never remember; so it would be good to have bi-directional contact with pharmacies. Adoption of PHRs is slow since there are no central repositories to get information from. We need to make deals with organizations to get data flowing. Also, there are no computers that patients could use in a doctor's office. Adoption will happen gradually with time and education. PHRs are at an early adoption phase. The most practical thing happening now are HIEs. PHRs have been left behind so far.