# Making mobile health effective and secure

December 18 2015

Credit: AI-generated image (disclaimer)

With Internet-connected medical technology and digitized health records on the rise, cybersecurity is a growing concern for patients and hospitals alike. One research team is taking a holistic approach to strengthening the medical system's security—from the computer networks that support hospitals, to the cloud, to the smart phone in your pocket.

David Kotz, a professor of computer science at Dartmouth College,

leads a National Science Foundation (NSF)-funded project, titled "Trustworthy Health and Wellness" (THaW.org) that aims to protect patients and preserve the confidentiality of medical data as records move from paper to electronic form.

"Mobile medical applications offer tremendous opportunities to improve quality and access to care, reduce costs and improve individual wellness and public health," Kotz says. "However, these new technologies, whether in the form of software for smartphones or specialized devices to be worn, carried or applied as needed, may also pose risks if they are not designed or configured with security and privacy in mind."

For example, a patient's insulin pump may accept dosage instructions from unauthorized smartphones that have been infected with malicious software, or a patient's fertility-tracking app could expose itself to nearby strangers by probing for a Bluetooth device to connect with.

The THaW team conducts research related to mobile and cloud technology for health and wellness applications. That portfolio includes authentication and privacy tools to protect health records, methods to secure small-scale clinical networks and efforts to reduce malicious activity in hospitals. The team is also training the next generation of computer scientists by involving undergraduate and high school students in research and by developing an exchange program for its postdoctoral fellows and research students.

"In complex environments having to do with health, wellness and medicine, there are a lot of moving parts involving devices, software, wireless and wired communications, and other dimensions, which are rich in challenges for security, privacy and safety," says NSF program officer Sol Greenspan. This project, he says, "brings together expertise and resources to work on these challenges."

Supported by a $10-million, five-year grant from NSF's Secure and Trustworthy Cyberspace (SaTC) program, the Frontier-scale project includes experts in computer science, business, behavioral health, health policy and healthcare information technology from Dartmouth College, Johns Hopkins University, the University of Illinois Urbana-Champaign (UIUC), the University of Michigan and Vanderbilt University.

"This project tackles many of the fundamental computer science research challenges to providing trustworthy information systems for health and wellness, as sensitive information and health-related tasks are increasingly pushed into mobile devices and cloud-based services," Kotz says.

## App Insecurity

Mobile Health (mHealth) apps, particularly those in app stores for iOS and Android, are increasingly handling sensitive data for both medical professionals and patients. However, these applications lie outside of regulatory protection such as HIPAA, an act passed by Congress in 1996 that mandates industry-wide standards for health care information and requires a baseline of privacy and security protections appropriate for sensitive medical data.

David Kotz and Shrirang Mare are experimenting with a BRACE prototype. The device pictured on the wrist is a third-party commercial product called "Shimmer" that they use for prototyping the idea. Credit: Eli Burakian, Dartmouth College

THaW researchers led by Klara Nahrstedt at UIUC conducted three studies of the mHealth apps in Google Play to determine how common apps handle medical data. They found a variety of vulnerabilities that a malicious party could exploit to gain access to sensitive data. Perhaps more significantly, they found that many apps send sensitive information over the Internet in ways that are fundamentally insecure.

Of the 22 randomly selected top mHealth apps they studied that send sensitive information over the Internet, they found 81 percent used third-

party storage and hosting services, such as Amazon's cloud services, and 63 percent sent the data in an unencrypted form, leaving them vulnerable to theft.

Both of these practices would be problematic under HIPAA, suggesting that the increased use of mHealth apps could lead to less secure treatment of health data—unless mHealth vendors improve the way they communicate and store data.

"These issues need attention and are not easily fixable because they require extra effort and security expertise from developers and computational capabilities from platforms," the researchers concluded. "Steps should be made to encourage mHealth app vendors to assure encrypted network links for communications and the use of third-party storage only when adequate security and privacy guarantees are obtained."

The team presented its results at the American Medical Informatics Association Symposium in Washington, D.C., in November 2014.

## Improving Health IT Security at Hospitals

This lack of security is not limited to mHealth apps. The researchers found critical vulnerabilities in some health care environments as well, like hospitals, where workstations used by clinicians can be susceptible to unwarranted access.

Hospital workstations allow doctors to enter information about patients efficiently, without having to transcribe notes or return to their offices. But user authentication at those terminals requires time and effort from clinicians—they have to log in, then remember to log out.

Because of these inconveniences, doctors sometimes do not log out,

leaving computers unsecured and open to use by other parties.

The BRACE (Bilateral Recurring Authentication Conducted Effortlessly) project addresses this challenge by developing a user-friendly authentication mechanism that blends seamlessly into the clinicians' workflow.

Dartmouth graduate student Shrirang Mare developed a potential wearable solution. When a user is equipped with a device such as a smart watch or fitness band, a terminal can monitor wrist movements to know who's logged in, and when that person is finished.

"The smartwatch monitors the continued presence of a user on a terminal when the user is interacting with it and can detect if someone else starts using the terminal," Mare says. "This allows the system to secure the user's session by logging out the user when they are not near the machine or when someone else tries to use terminal."

The researchers are now developing a usable authentication method that would allow users to log into their terminals with simple actions—such as wiggling a mouse or tapping a key a few times—that are quick, familiar and easy. They are also exploring techniques for usable authentication and automatic de-authentication for smartphones. An early part of this work was published in 2014.

Kotz notes that mobile health technologies have incredible potential, but he is concerned that insufficient attention to their security could hinder their adoption and lead to the theft of personal data or worse.

Fortunately, "THaW research is identifying gaps in security and providing practical security solutions," Kotz says. "We are developing novel methods for security and privacy, so we can help usher in an era of effective and secure mHealth solutions."

**More information:** Security Concerns in Android mHealth Apps. seclab.illinois.edu/wp-content … /2014/08/HeNGN14.pdf

Provided by National Science Foundation