Security with the wave of a wand

March 1 2016

Dartmouth College Professor David Kotz demonstrates a commercial prototype of Wanda imparting information such as the network name and password of a Wi-Fi access point onto a blood pressure monitor. Credit: Dartmouth College

Increasingly, health care is moving out of the doctor's office and into the

home, allowing greater patient freedom and monitoring, but also giving rise to new security risks.

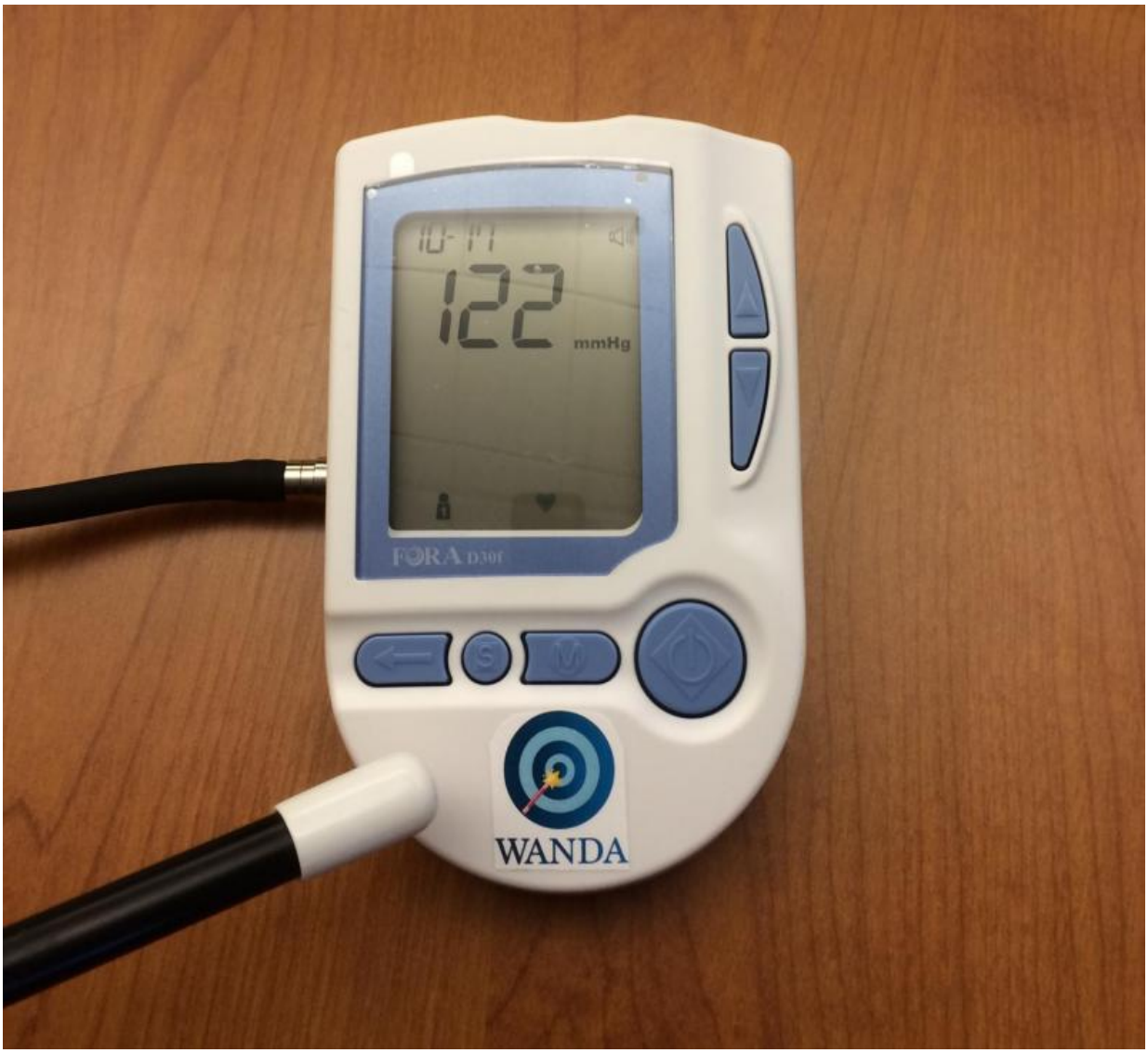
One of the main challenges facing home health technology design is the public's inability to set up a secure network in their home and keep it operational. This can lead to compromised or stolen data, or even potentially hacked devices, such as heart rate monitors or dialysis machines.

To address this problem, researchers from Dartmouth College have developed a digital "magic wand" to improve home health care and to prevent hackers from stealing one's personal data.

The system, called Wanda, makes it easy for people to add a new device to their Wi-Fi network at home (or in a clinic), even if they don't have professional IT support staff to configure, track and update the medical devices.

The researchers will present a paper on the wand-based cybersecurity configurations at the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Computer Communications (INFOCOM) in San Francisco in April.

The research is part of a project funded by the National Science Foundation (NSF), titled "Trustworthy Health and Wellness" (THaW.org) and led by Dartmouth computer science professor David Kotz. The project aims to protect patients and preserve the confidentiality of medical data.



Wanda is a small hardware device that has two antennas separated by one-half wavelength and uses radio strength as a communication channel. It makes it easy for people to add a new device to their home (or clinic) Wi-Fi network: they simply pull the wand from a USB port on the Wi-Fi access point, carry it close to the new device and point it at the device. Within a few seconds, the wand securely beams the secret Wi-Fi network information to the device. The same method can be used to transfer any information from the wand to the new device without anyone nearby capturing the secrets or tampering with the information. Credit: Dartmouth College

The THaW team conducts research related to mobile and cloud technology for health and wellness applications, including efforts to secure small-scale clinical networks and to reduce malicious activity in hospitals.

Supported by a $10 million, five-year grant from NSF, the project includes experts in computer science, business, behavioral health, health policy and health care information technology from Dartmouth, Johns Hopkins University, the University of Illinois at Urbana-Champaign (UIUC), the University of Michigan and Vanderbilt University.

As part of ThaW, graduate student Tim Pierson developed a system where an individual can simply pull a small wand from a USB port on a Wi-Fi access point and point it at a new device at close range. Within a few seconds, the wand securely beams the secret Wi-Fi network information to the device, making it secure and operational.

Dartmouth computer scientist David Kotz leads a team that conducts NSF-funded research in the secure use of mobile and cloud technology for health and wellness applications. Credit: Eli Burakian, Dartmouth College

One can use the same method to transfer any information from the wand to the new device without anyone nearby capturing private data or tampering with the information.

"People love this new approach to connecting devices to Wi-Fi," says Pierson. "So many of our volunteer testers remark on the frustration they've encountered in configuring wireless devices at home and ask when they can take our 'wand' home."

There are three basic operations involved. First, Wanda configures a

device to join the wireless local-area network. Second, it partners that device with others nearby, so they can work together. And third, it configures the device so it can connect to the relevant individual or organizational account in the cloud.

In addition to Wanda, the Trustworthy Health and Wellness team conducts research related to mobile and cloud technology for health and wellness applications and experiments with new mobile health devices, like the BRACE prototype (above) that prevents unwarranted access to hospital workstations. Credit: Dartmouth College

Wanda—a small piece of hardware with two antennas that uses radio strength as a communication channel—accomplishes all of these tasks

without the need for outside assistance.

"We anticipate our Wanda technology being useful in a wide variety of applications, not just health care, and for a wide range of device management tasks, not just Wi-Fi network configuration," Kotz says.

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

Fortunately, THaW researchers are identifying gaps in security and providing practical security solutions, says Kotz.

"We are developing novel methods for security and privacy so we can help usher in an era of effective and secure mobile health solutions," he says.

More information: Timothy J. Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Wanda: securely introducing mobile devices. In IEEE International Conference on Computer Communications (INFOCOM), April, 2016. Accepted for publication. www.cs.dartmouth.edu/~dfk/pape … s/pierson-wanda.html

Provided by National Science Foundation

Citation: Security with the wave of a wand (2016, March 1) retrieved 18 April 2024 from https://phys.org/news/2016-03-wand.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.