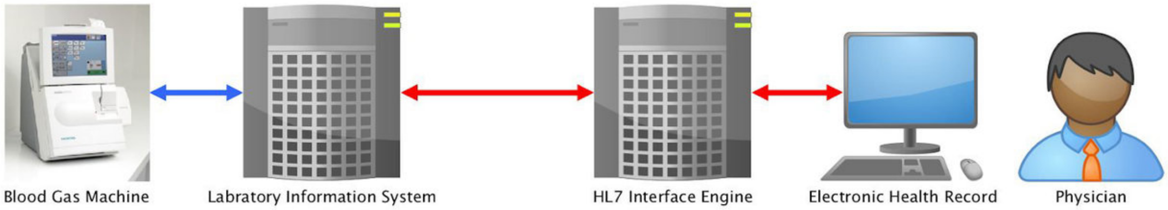
How unsecured, obsolete medical record systems and medical devices put patient lives at risk

August 29 2018, by Ioana Patringenaru



Credit: University of California - San Diego

A team of physicians and computer scientists at the University of California has shown that it is easy to modify medical test results remotely by attacking the connection between hospital laboratory devices and medical record systems.

These types of attacks might be more likely used against high-profile targets, such as heads of state and celebrities, than against the general public. But they could also be used by a nation-state to cripple the

United States' medical infrastructure.

The researchers from UC San Diego and UC Davis detailed their findings Aug. 9 at the Black Hat 2018 conference in Las Vegas, where they staged a demonstration of the attack. Dubbed Pestilence, the attack is solely proof-of-concept and will not be released to the general public. While the vulnerabilities the researchers exploited are not new, this is the first time that a research team has shown how they could be exploited to compromise patient health.

These vulnerabilities arise from the standards used to transfer patient data within hospital networks, known as the Health Level Seven standards, or HL7. Essentially the language that allows all devices and systems in a medical facility to communicate, HL7 was developed in the 1970s and has remained untouched by many of the cybersecurity advances made in the last four decades.

Implementation of the standards on aging medical equipment by personnel with little or no cybersecurity training has led to untold amounts of patient data circulating in an unsecure fashion. Specifically, the data are transmitted as unencrypted plain text on networks that do not require any passwords or other forms of authentication.

Data hacking in hospitals has been in the news in recent years. But researchers want to draw attention to how that data, once compromised, could be manipulated. "Healthcare is distinct from other sectors in that the manipulation of critical infrastructure has the potential to directly impact human life, whether through direct manipulation of devices themselves or through the networks which connect them," the researchers write in a white paper released in conjunction with their Black Hat demonstration.

The vulnerabilities and methodologies used to create the Pestilence tool have been previously published. The innovation here is combining computer science know-how and clinicians' knowledge to exploit weaknesses in the HL7 standard to negatively impact the patient care process.

The team includes Dr. Christian Dameff, an emergency physician and clinical informatics fellow, and Maxwell Bland, a master's student in computer science, both at UC San Diego, and Dr. Jeffrey Tully, an anesthesiology resident at the UC Davis Medical Center. Physicians need to be able to trust that their data are accurate, Tully said. "As a physician, I aim to educate my colleagues that the implicit trust we place in the technologies and infrastructure we use to care for our patients may be misplaced, and that an awareness of and vigilance for these threat models is critical for the practice of medicine in the 21st century," he said.

Securing data against manipulation is imperative. "We are talking about this because we are trying to secure healthcare devices and infrastructure before medical systems experience a major failure," Dameff said. "We need to fix this now."

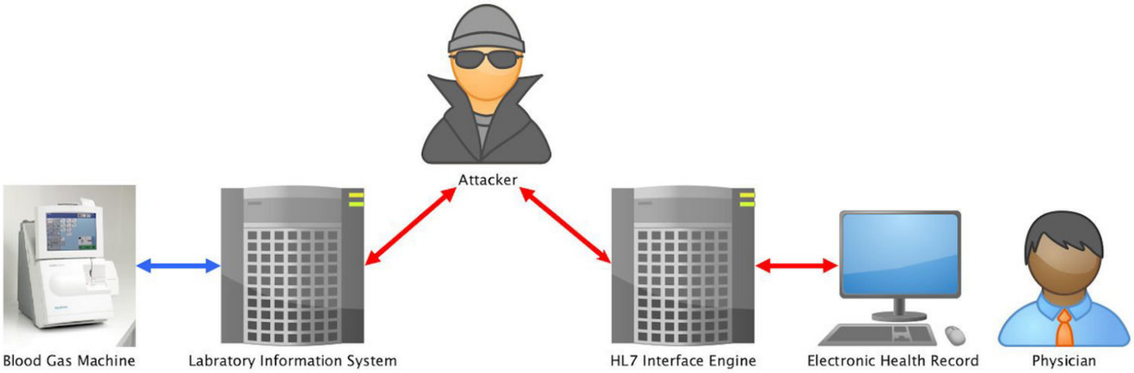
Researchers outline countermeasures medical systems can take to protect themselves against these types of attack.

The Pestilence tool

Researchers used what's called a "man in the middle attack," where a computer inserts itself between the laboratory machine and the medical records system. Bland, the UC San Diego computer science graduate student, automated the attack so it could tackle large amounts of data remotely. Researchers did not infiltrate an existing hospital system, of course. Instead, they built a testbed comprised of medical laboratory testing devices, computers and servers. This allowed the team to run tests, such as blood and urine analysis, intercept the test results, change them and then send the modified information to a medical records system.

Researchers took normal blood test results and modified them to make it look like the patient was suffering from diabetic ketoacidosis, or DKA, a severe complication of diabetes. This diagnosis would cause physicians to prescribe an insulin drip, which in a healthy patient could lead to a coma, or even death.

Researchers also modified normal blood test results to look like the patient had extremely low potassium. Treatment with a potassium IV on a healthy patient would cause a heart attack, which would likely be fatal.



Researchers used a "man in the middle attack" to intercept and modify data transmitted from a laboratory information sysetm to an electronic medical record system. Credit: University of California - San Diego

Countermeasures

The researchers detail a number of steps that hospitals and government agencies can take to protect medical infrastructure in their Black Hat white paper.

Hospitals need to improve their security practices. Specifically, medical record systems and medical devices need to be password-protected and secured behind a firewall. Each device and system on the network needs to be restricted to communicating with only one server, to limit hackers' opportunities to penetrate inside hospital networks. This is called "network segmenting" and is the best way to protect medical infrastructure, said Bland, the computer science graduate student at the Jacobs School of Engineering at UC San Diego.

Researchers also would like to raise awareness of a new standard that could replace HL7: the Fast Healthcare Interoperability Resource, or FHIR, would allow for encrypted communications inside hospital networks.

Hospital IT staff need to be made aware of cybersecurity issues and trained to put in place defenses against potential attacks, researchers said. For example, IT personnel need to know how to configure networks and servers to support encryption. Researchers point a 2017 report from a Health and Human Services task force stating that 80 percent of hospital IT personnel are not trained in cybersecurity.

In addition, cybersecurity needs to become part of the FDA approval process for healthcare devices, the researchers said. Manufacturers should be encouraged to adopt the newest and most secure operating systems. For example, today, many medical devices still run on Windows XP, an operating system that was released in 2001 and is no longer supported by Microsoft—meaning that vulnerabilities are not fixed. These devices can't be easily upgraded as they would need to be taken offline, which would compromise patient care. In addition, some devices are too told to be upgraded.

"Working together, we are able to raise awareness of security vulnerabilities that have the potential to impact patient care and then develop solutions to remediate them," UC Davis' Tully said.

Provided by University of California - San Diego

Citation: How unsecured, obsolete medical record systems and medical devices put patient lives at risk (2018, August 29) retrieved 30 April 2024 from https://techxplore.com/news/2018-08-unsecured-obsolete-medical-devices-patient.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.