UAB COLLEGE OF ARTS AND SCIENCES

UAB CAS Interdisciplinary Innovation Forum

An Interdisciplinary Approach Towards Securing Biomedical Devices

PI: Dr. Ragib Hasan (CIS)
Co-PI: Dr. Darrell Burke (SHP)

Interdisciplinary Team

- **PI**: Dr. Ragib Hasan, Assistant Professor, CIS, Director, UAB SECRETLab

- **Co-PI**: Dr. Darrell E. Burke, Associate Professor, School of Health Professionals

- **Graduate Student**: Shahid Noor, CIS
- **UAB HSIS Contact**: Donald G Fast, Director UAB Health Systems Information Systems

Good old days (of “dumb” medical devices) …

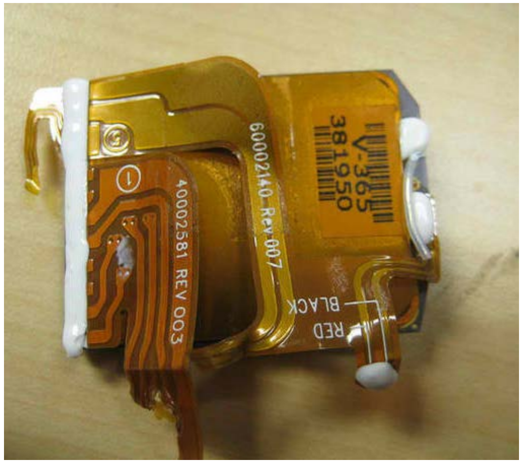
- Medical devices of yesteryears were **not “smart”**, and could be configured/controlled only via a direct interface

- To get data from or send commands to a device, healthcare providers had to be in physical proximity of the patient

Pacemaker, circa 1951

Problem: New medical devices are more connected, yet more vulnerable

Implantable Devices now boast wireless data and control interfaces



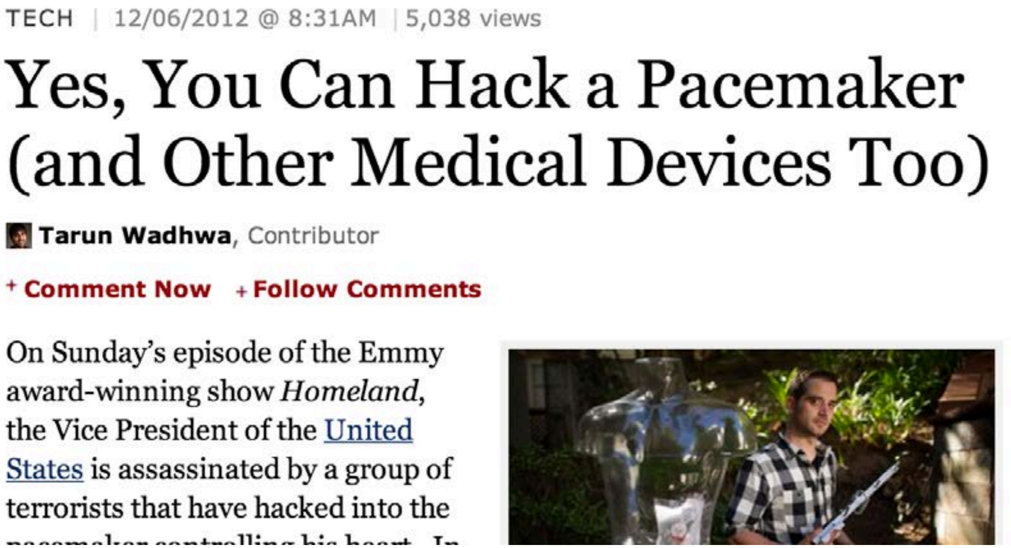
A pacemaker with wireless interface

A wireless insulin pump system

Monitors/insulin pumps are increasingly connected via wireless

All of which have been hacked!!

A movie plot threat? It used to be, but now its REAL



TECH | 12/06/2012 @ 8:31AM | 5,038 views

Yes, You Can Hack a Pacemaker (and Other Medical Devices Too)

Tarun Wadhwa, Contributor

+ Comment Now + Follow Comments

On Sunday's episode of the Emmy award-winning show *Homeland*, the Vice President of the United States is assassinated by a group of terrorists that have hacked into the pacemaker controlling his heart. In

Forbes, December 2012

"(a researcher) showed how he'd reverse-engineered a pacemaker and could deliver an 830-volt shock to a person's device from 50 feet away – which he likened to an anonymous assassination."

Bloomberg, February 2012

" has discovered a way to scan a public space from up to 300 feet away, find vulnerable pumps … and force them to dispense fatal insulin doses. :

TECH BLOG

Daily dose of culture, clashes, and trends.

Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device

Problem: Attacks can come from **anywhere**, even from **insiders**

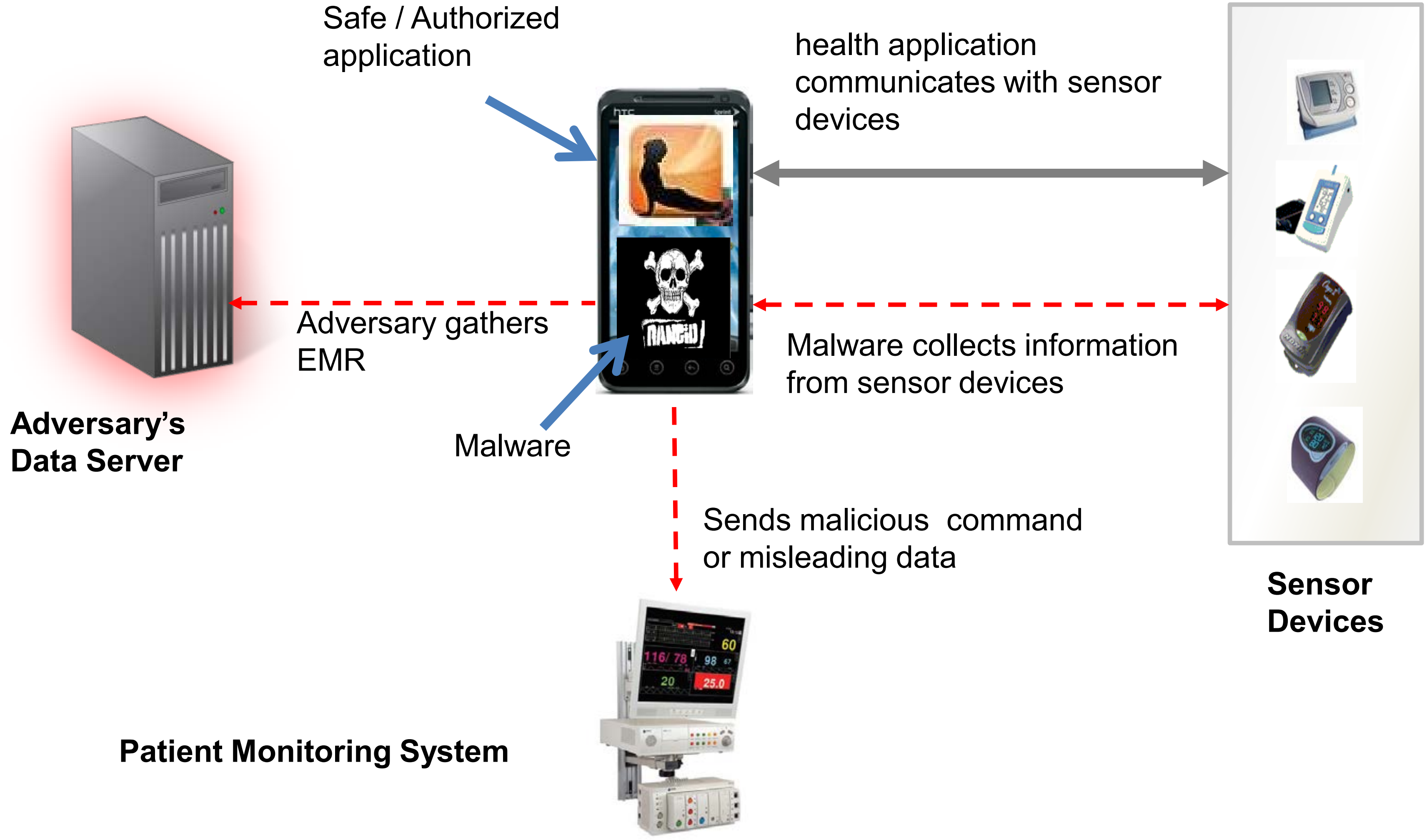
- Even if a hospital network is isolated from outsiders, malicious insiders can still attack it

- Many workplaces use the Bring Your Own Device (**BYOD**) model

- Doctors and healthcare providers have smart phones already connected to the network

- Malware infecting such phones do not have to break into the network – they are already in!!

Example: Threat from an infected mobile device inside a hospital network



Safe / Authorized application

health application communicates with sensor devices

Adversary gathers EMR

Malware collects information from sensor devices

Adversary's Data Server

Malware

Sends malicious command or misleading data

Sensor Devices

Patient Monitoring System

Typical hospital rooms have dozens of devices/monitors with wireless interfaces

Smart monitors talk to medical record systems

Smart pumps/devices can be controlled remotely

Most newer devices have Wifi or Bluetooth capability

All of which are subject to potentially devastating drive-by attacks from mobile devices belonging to doctors, patients, or even visitors

Our Goal: Identify Vulnerabilities and Hospital Environments against attacks

- **Identify** and categorize **vulnerabilities** and **threats** to medical devices and hospital environments, in particular from mobile devices

- **Develop** an **automated security analysis tool** for biomedical devices and healthcare infrastructure

- **Perform** a **case study** in which we will evaluate the security of real-life biomedical devices and equipment used at the UAB Hospital;

- Eventually, **Create** **potential solutions** and defenses against such attacks.

Approach

- Examine the network topologies and typical practices in hospital environments to identify vulnerable attack points/devices

- Determine attack vectors and identify potential attack scenarios

- Create a set of tools and best practices for securing devices and hospital environments

Progress to date:

- Analysis of Vulnerabilities and creation of a threat model [**done**]
- Identifying a path for analysis [**done**]
- Feasibility study of attacks on mobile devices and networks in a test setting [**mostly done**]
- Field study in UAB HSIS Lab environment [**ongoing**]
- Tests in actual UAB hospital environment [**todo**]

Publications

Shams Zawoad and Ragib Hasan,
“**The Enemy Within: The Emerging Threats to Healthcare from Malicious Mobile Devices**”,
in Proceedings of the 3rd International Conference on Wireless Mobile Communication and Healthcare (MobiHealth), Paris, France, November 2012.

Future Funding Opportunities

- NSF Secure and Trustworthy Cyberspace (SaTC)
  - Planned submission in October ‘13
- NSF Smart and Connected Health (SCH)
  - Planned submission in May ‘13

Thank you

For more information, please check out the **UAB SECRETLab** web page

http://secret.cis.uab.edu