Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security

Balancing Safety and Security

Tamara Denning\textsuperscript{1}, Tadayoshi Kohno\textsuperscript{1}, Kevin Fu\textsuperscript{2}

\textsuperscript{1}University of Washington \hspace{1cm} \textsuperscript{2}University of Massachusetts at Amherst

http://www.secure-medicine.org
Implantable Medical Devices (IMDs)

- Pacemakers, Implantable Cardioverter Defibrillators (ICDs), Drug Pumps, Neurostimulators
- Life-Supporting/Quality of Life
- Devices Have Wireless Capabilities
Wireless ICD Attacks

- The People:
  - University of Washington (Dan Halperin, Tadayoshi Kohno)
  - University of Massachusetts Amherst
  - Harvard Medical School

- The Hardware:
  - GNU Radio Software, $0
  - USRP Board, $700
  - Daughterboards, Antennas: $100
  - Software Radio
What Could They Do?

- Obtain serial number, patient name, diagnosis
- Turn off therapies
- Induce cardiac fibrillation

Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses [Halperin], Oakland ‘08
Heparin Contamination May Have Been Deliberate, F.D.A. Says

By GARDINER HARRIS

WASHINGTON — Federal drug regulators believe that a contaminant detected in a crucial blood thinner that has caused 81 deaths was added deliberately, something the Food and Drug Administration has only hinted at previously.

“F.D.A.’s working hypothesis is that this was intentional contamination, but this is not yet proven,” Dr. Janet Woodcock, director of the Food and Drug Administration’s drug center, told the House Subcommittee on Oversight and Investigations in written testimony given Tuesday.

A third of the material in some batches of the thinner heparin were contaminants, “and it does strain one’s credulity to suggest that might have been done accidentally,” Dr. Woodcock said.
Malicious Computer-Based Attacks

Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month

Houston, TX, November 19, 2007 --(PR.com)-- Internet hooligans launched a malicious attack on Coping With Epilepsy (CWE), an internet web site that serves as a peer support network for people with epilepsy, last Saturday. The perpetrators flooded CWE with hateful messages, images of hardcore pornography and, worst of all, animated images with rapidly flashing colors in an attempt to induce seizures in the photosensitive members (and guests) of the site.

The attack lasted several hours as CWE moderators, members, and guests tried to remove the offensive content as fast as it was being posted. The attack ended only when CWE administrators arrived and locked down the site.

“I was able to trace back the source of the attack to a hand full of sites where the perpetrators were instigating the event,” said Bernard Erdt, CWE Administrator. “It was just a bunch of immature people delighting in their attempts to cause pain to others. Unfortunately, this time they tried to hurt people who passed away just two weeks ago from a seizure. SUDER (Sudden Unexpected Death of Epilepsy) is a serious concern.”

“Since the attack, CWE has implemented modifications to our system,” said Erdt. “This was the first time CWE has been targeted in this manner due to the site’s popularity. We’re working to ensure that there won’t be a repeat of this incident.”

Ironically, the attack occurred during November, which is National Epilepsy Awareness Month.

About CWE

Coping With Epilepsy is a peer support forum for people including medical professionals.

Hackers Assault Epilepsy Patients via Computer

Internet grievers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

“We are seeing people affected,” says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. “It’s fortunately only a handful. It’s possible that people are just not reporting yet -- people affected by it may not be coming back to the forum so fast.”

The incident, possibly the first computer attack to inflict physical harm on the victims, began Saturday, March 22, when attackers used a script to post hundreds of messages embedded with flashing animated gifs.

The attackers turned to a more effective tactic on Sunday, injecting JavaScript into some posts that redirected users’ browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.
Current Security

- IMD does not keep list of authorized programmers

- How about keeping a list and only allowing authorized programmers?
Goals of IMD Security

Y + Y = Y

Y + N = Y

Y + Y = Y
Goals of IMD Security
Insufficient Approaches

- Case-by-Case Access Credentials
- User Alert
- Require Close Proximity
Insufficient Approaches

- Case-by-Case Access Credentials
- User Alert
- Require Close Proximity
Insufficient Approaches

- Case-by-Case Access Credentials
- User Alert
- Require Close Proximity
What about encryption with a carried passkey?

+ IMDpassword1 + + = Y

+ No + + = N

+ IMDpassword1 + + = Y
What about encryption with a carried passkey?
New Approach

What if we REMOVE something to gain access?

*Communication Cloaker*
How it works

N
Y
= =

Y
= =

Y
= =

Tamara Denning, University of Washington, Affiliates 2008
**Communication Cloaker**

- **Present**
  - Allows Pre-Approved Programmers (common case)
  - Blocks Unauthorized Programmers (adversarial case)

- **Absent**
  - Fails open…Allows All Programmers!
Challenges

• How to handle limited resources on IMD?

• How to protect against DoS attacks?

• What if the emergency staff can’t locate the Cloaker?
Interesting Research Landscape!

Safety (open access)
- Patient Usability

High Impact

Security (closed access)
- IMD Response Time
- Storage Constraints

Auditability

Psychological Effects

Battery Life
Value Sensitive Design

- Methodology to Incorporate Human Values into Design

- What Values?
  - Privacy
  - Sustainability
  - Aesthetics
  - Etc.

- Stakeholders
  - Direct
  - Indirect
What do patients care about?

- Self-image?
- Privacy?
- Autonomy?
- Psychological Impact?

What do physicians care about?

- Safety?
- Security?
- Accountability?
- Ease of maintenance?

What about: Patients’ families, device manufacturers, hospitals
Conclusion

- Exciting and important research area!
- Cloaker is one design
- VSD may help find others
- Questions?