Absence Makes the Heart Grow Fonder:

New Directions for Implantable Medical Device Security

Balancing **Safety** and **Security**

Tamara Denning[1], Tadayoshi Kohno[1], Kevin Fu[2]

[1]University of Washington [2]University of Massachusetts at Amherst

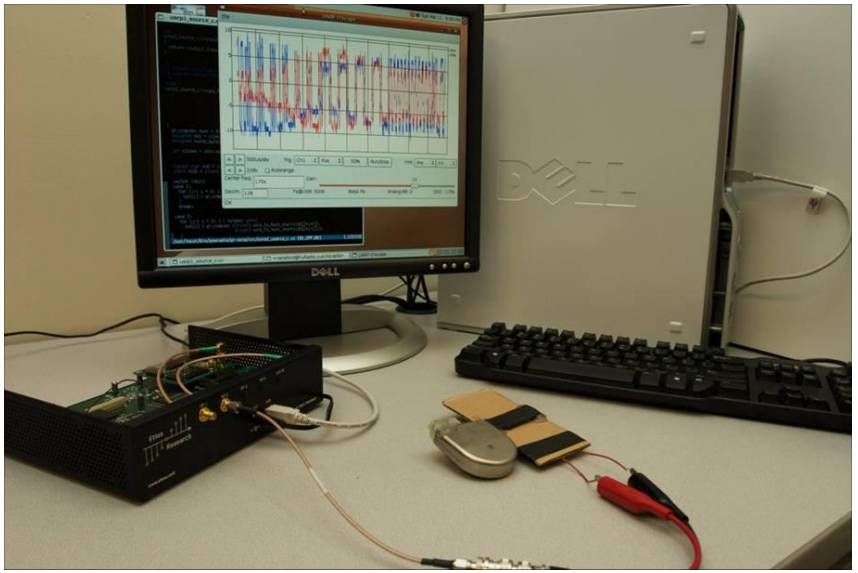
http://www.secure-medicine.org

Implantable Medical Devices (IMDs)

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

Wireless ICD Attacks

- 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

Why Security? Malicious Attacks

The New York Times nytimes.com Young @ Heart

April 30, 2008

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

PRESS RELEASE

Receive press releases from coping-with-epilepsy.com: By Email RSS Feeds: XML MY YAHOO!

Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month

Hooligans attack epilepsy support forum in an attempt to induc

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

The attack lasted several hours as CWE moderators, ma
them photosensitive themselves, battled to remove the offe
content as fast as it was being posted. The attack ended
CWE administrators arrived and locked down the site.

"I was able to trace back the source of the attack to a hanc
sites where the perpetrators were instigating the event,"
Bernard Ertl, CWE Administrator. "It was just a bunch of
immature people delighting in their attempts to cause pe
them. Unfortunately, this time they tried to hurt people.
passed away just two weeks ago from a seizure. SUDEP (S
serious concern."

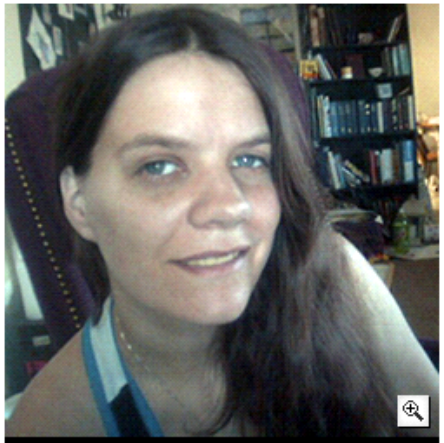
"Since the attack, CWE has implemented modifications to d
"This was the first time CWE has been targeted in this m
popularity of the site. We're working to ensure that there wi

Ironically, the attack occurred during November, which is Na

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

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08 | 8:00 PM



RyAnne Fultz, 33, says she suffered her worst epileptic attack in a year after she clicked on the wrong post at a forum run by the nonprofit Epilepsy Foundation.
Photo courtesy RyAnne Fultz

Internet griefers 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.

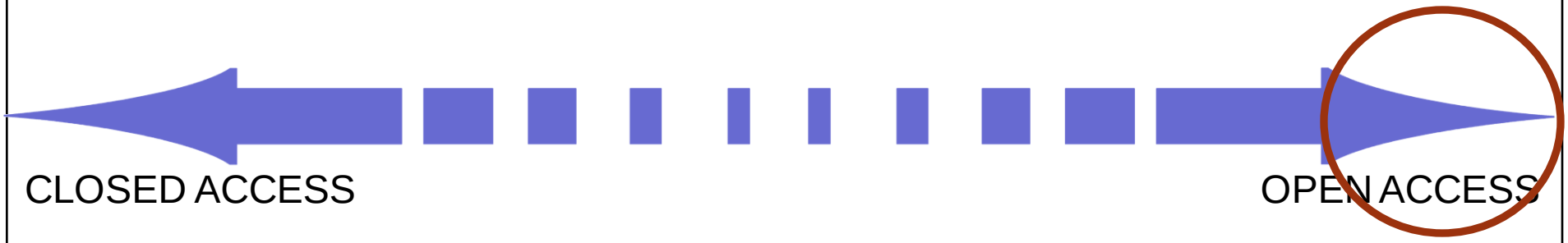
"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. "It's fortunately only a handful. It's possible that people are just not reporting yet -- people affected by it may not be coming back to the forum so fast."

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

N

Y

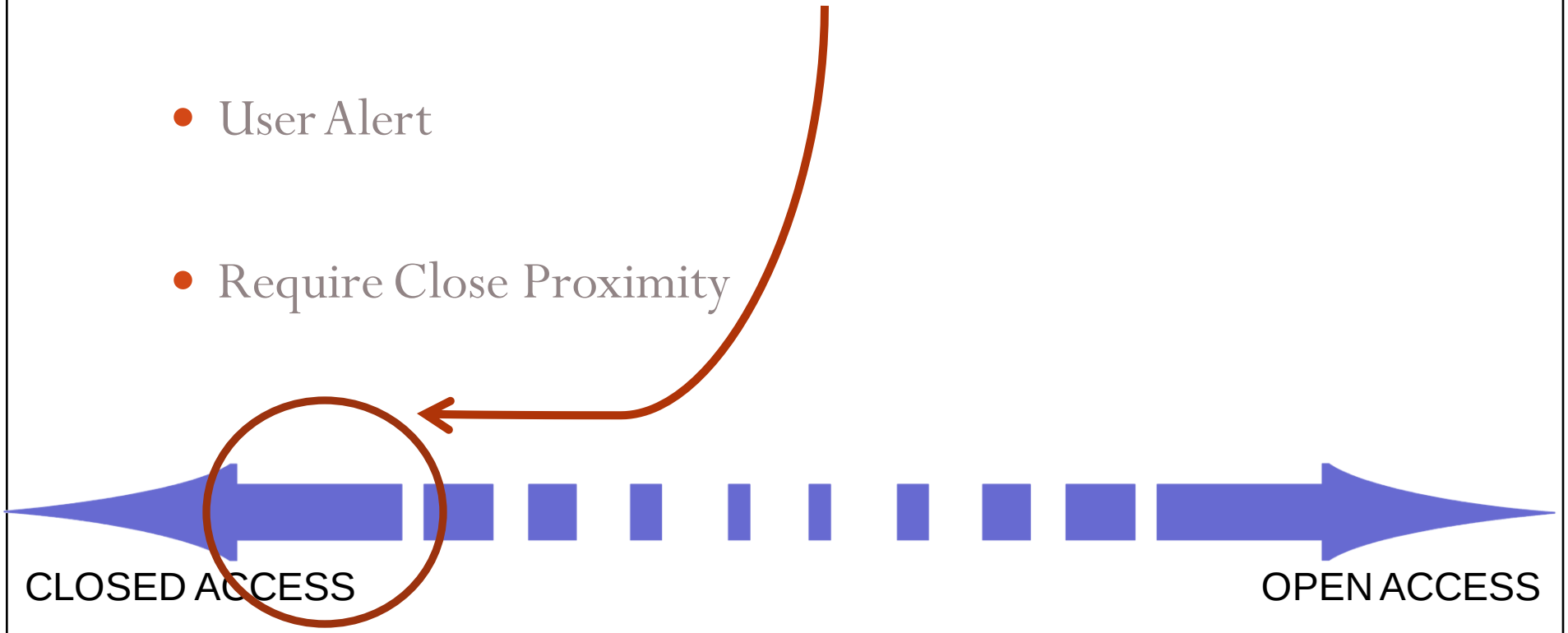
Tensions of IMD Security

- Safety in the *Common Case*
  - Timely access anywhere, anytime
- Security in the *Adversarial Case*
  - Protect from unauthorized access

CLOSED ACCESS OPEN ACCESS

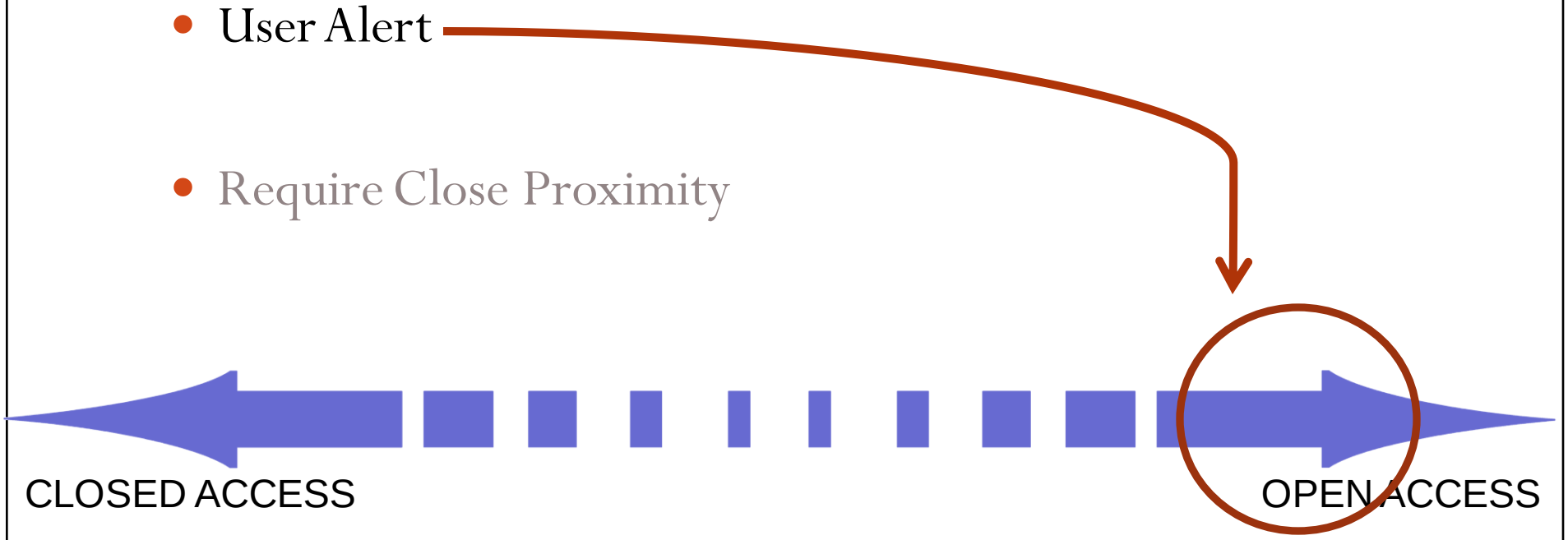
Insufficient Approaches

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



Insufficient Approaches

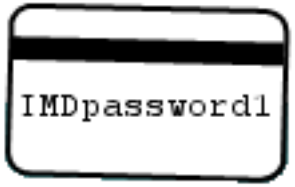
- Case-by-Case Access Credentials
- User Alert
- Require Close Proximity

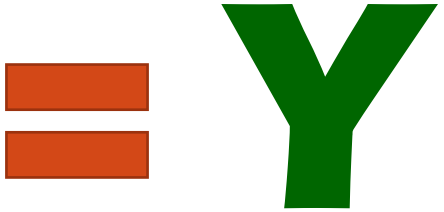


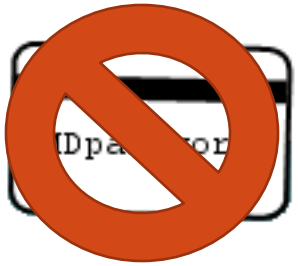
Insufficient Approaches

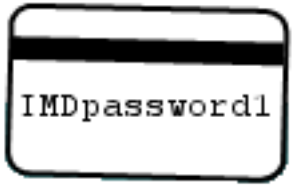
- Case-by-Case Access Credentials
- User Alert
- Require Close Proximity

What about encryption with a carried passkey?

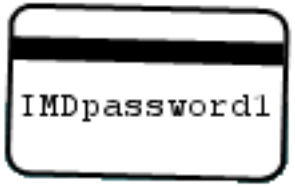




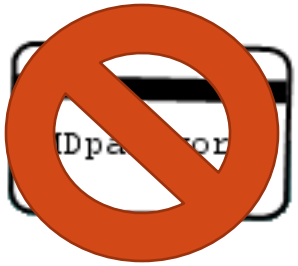




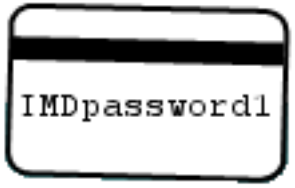
What about encryption with a carried passkey?

Y


N

Y



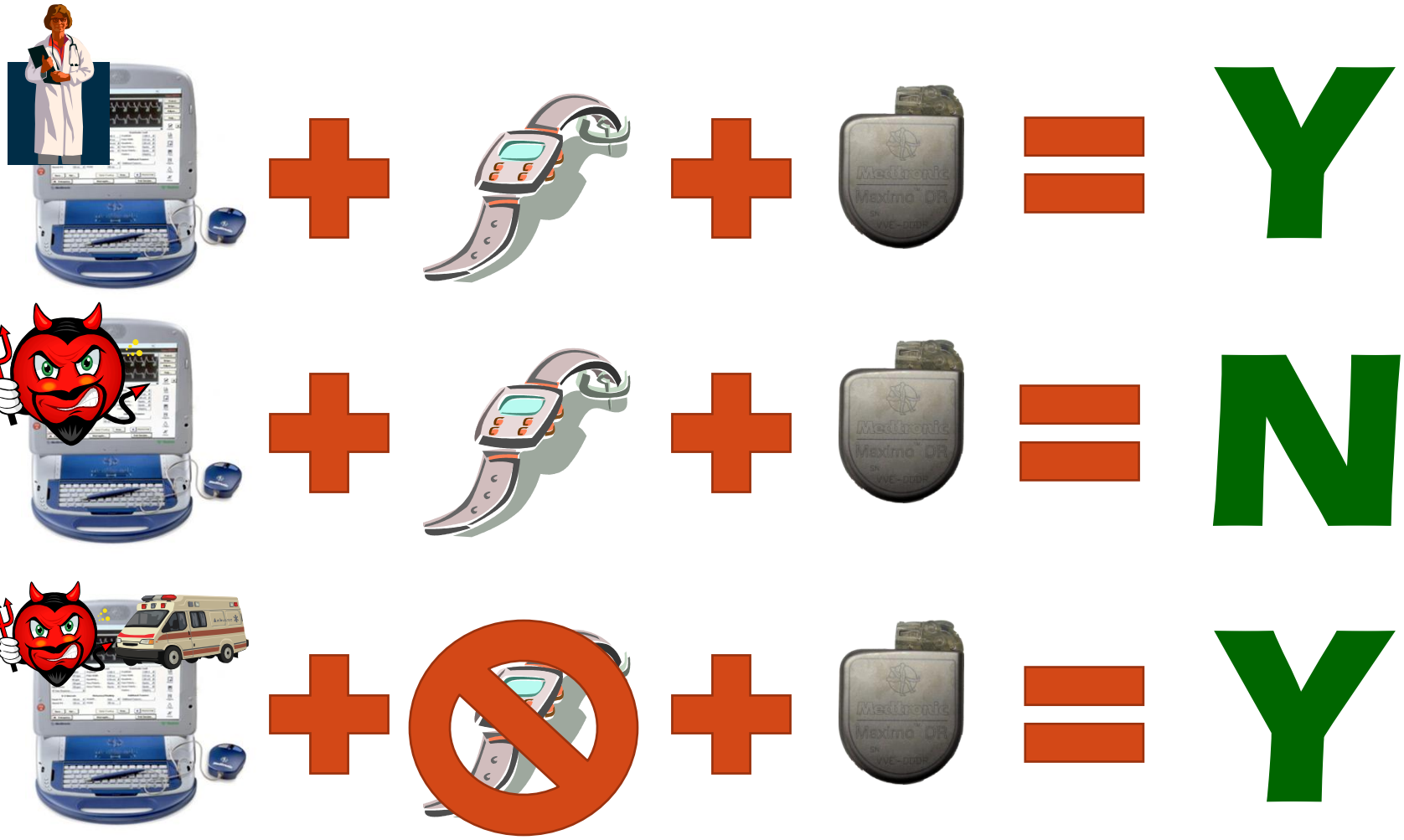
N

New Approach

What if we REMOVE something to gain access?

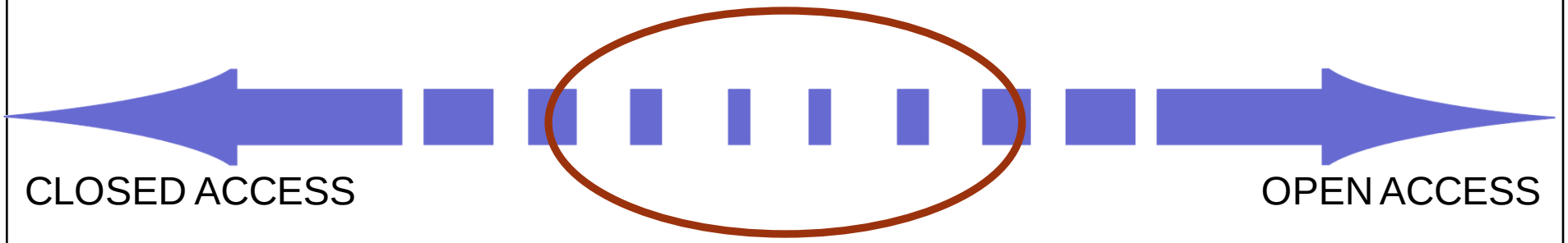
Communication Cloaker

How it works



Communication Cloaker

- Present
  - Allows Pre-Approved Programmers (common case)
  - Blocks Unauthorized Programmers (adversarial case)
- Absent
  - Fails open…Allows All Programmers!



Assumptions

- IMD Power is Limited – Use Cheap Cryptography
- Cloaker Can be Recharged – Use Heavier Cryptography
- IMD and Cloaker are Paired Long-term

Challenges

- How to handle IMD-Programmer communications?
- How the IMD "knows" the Cloaker's presence?
- What if the emergency staff can't locate the Cloaker?

Challenges…Possible Answers

- How to handle IMD-Programmer communications?
  - ? Hand off symmetric key pair
  - ? Proxy
- How the IMD "knows" the Cloaker's presence?
  - ? IMD listens and queries oracle
  - ? Keep-alives
- What if the emergency staff can't locate the Cloaker?
  - Pulse sensor

Preliminary Simulation

- 14 Java classes
- TCP sockets
- Inputs alter system
  - Selective DoS, jamming all wireless
- Manageable code size

Module Type	Code Size
Cloaker	179
IMD	115
Programmer	44
Other	294

Code Function	Code Size
I/O	124
Configuration	72
Communication	436

Summary

- New Approach to IMD Security

- Further Investigations:
  - Passively-powered transceivers (WISPs)
  - Patient must wear Cloaker
  - Psychological Impact
  - What if the patient's wrist is trapped in a car?

Interesting Research Landscape!

Auditability

Safety (open access)

Psychological Effects

High Impact

Patient Usability

Security (closed access)

Storage Constraints

IMD Response Time

Battery Life