CS 598 - Computer Security in the Physical World:

Project Submission #1 & "Pacemakers and Implantable Cardiac Defibrillators…"

Professor Adam Bates

Fall 2016

Oct 4th Deliverable

Choose one of your project choices and prepare the following:

- Abstract
- Background
- Related Work

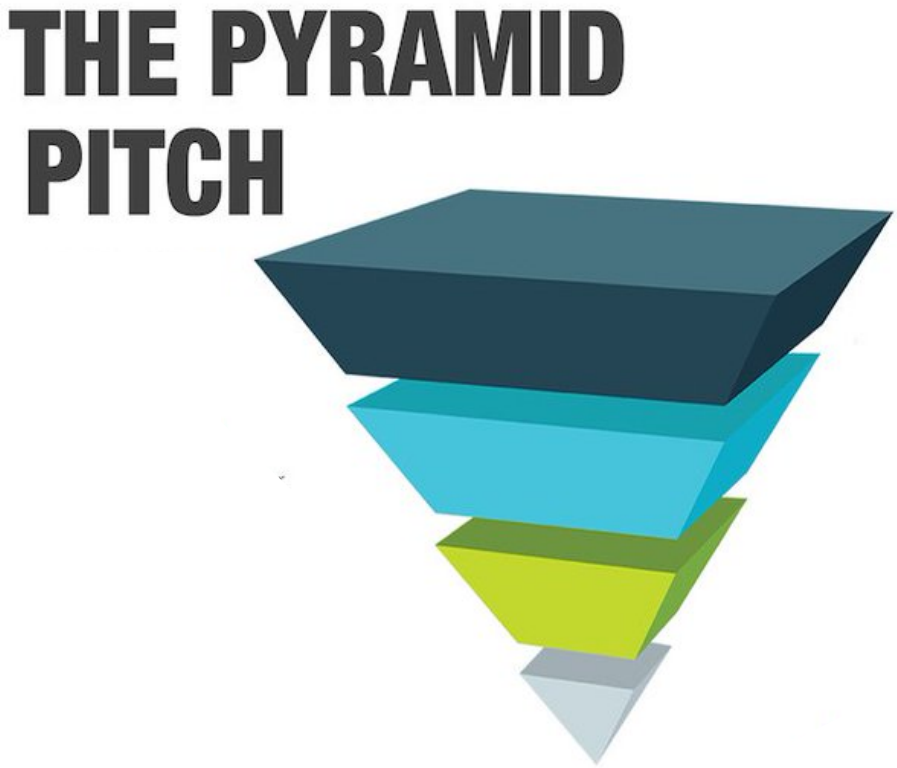
Format: LaTeX Two Column ACM

Submission: Email me (include [cs598] in subject line)

How to Abstract

- One (maybe two) paragraphs
- The "Elevator Pitch" of your paper, should cover:

1. Area
2. Problem
3. Solution
4. Methodology
5. Results
6. Takeaway



Why start with BG/RW?

1. Be smart and conduct a literature survey so that you can understand the space before committing to a research direction.

2. Easiest part of the paper to write. Once they're 'locked in' there is no need to change them, so it's best to get them out of the way.

How to Background

- What knowledge does a reviewer need to possess before they can evaluate your work?
- Concept-driven, not paper-driven
- Specifications, RFCs, Schematics, Workflows
- Citation Density: Low - Medium
- Examples:
  - AccessPrint -> HW Descriptions, Mechanical Imperfections, HW Fingerprints
  - (Special Agent) Johnny -> Extensive P25 Overview
  - USBFILTER -> USB Architecture Overview, Real World Deployment and Ubiquity, In-the-Wild Attacks

How to RelWork

- Goals:
  - Demonstrate understanding of area
  - Distill prior work into easily understood taxonomy
  - Identify gaps in the literature, differentiate your idea
  - Appease your reviewers by citing their work
- Citation Density: High
- Requirement for your submission: 30 citations
  - Quantity != Quality, but it's a start

RelWork Examples

- USBFILTER -> "Modern operating systems implicitly approve all interfaces on any device that has been physically attached to the host. Due to this, a wide range of attacks have been built on USB including malware and data exfiltration on removable storage [15, 34, 46], tampered device firmware [27, 7], and unauthorized devices [1]."
- Do You Hear…? -> "Hardware based fingerprinting approaches rely on some static source of idiosyncrasies. It has been shown that network devices tends to have constant clock skews [53] and researchers have been able to exploit these clock skews to distinguish devices through TCP and ICMP timestamps [46]. However, clock skew rate is highly dependent on the experimental environment [67]. Researchers have also extensively looked at fingerprinting the unique transient characteristics of radio transmitters (also known as RF fingerprinting). RF fingerprinting has been shown as a means of enhancing wireless authentication [49, 55]."

RelWork Examples 2

- Cap off citation dumps with commentary that differentiates your work or identifies gaps in literature:
  - Boxed Out -> "Our work is an improvement over the state of the art because we can reliably detect simboxed calls using features inherent to simboxing at the time of the call, thus making simboxing unprofitable."
  - Mo(bile) Money -> "… prior work does not investigate the security guarantees and the severe consequences of smart phone application compromise in branchless banking systems."

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel

Oakland'08

Characteristics of IMDs

- Physical access is… messy.
- Wireless access: Medical Implant Communication (MICS) radio band, telemetry data broadcasts
- *Extremely* Resource Constrained, non-rechargeable battery needs to remain charged for O(years).
- Sensors and actuators directly inform and/or issue life-or-death medical treatments.

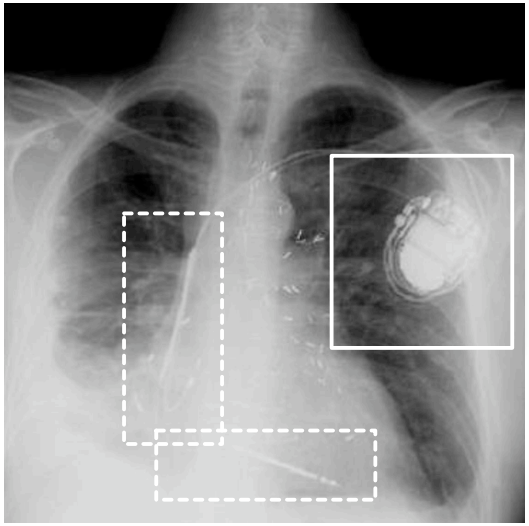
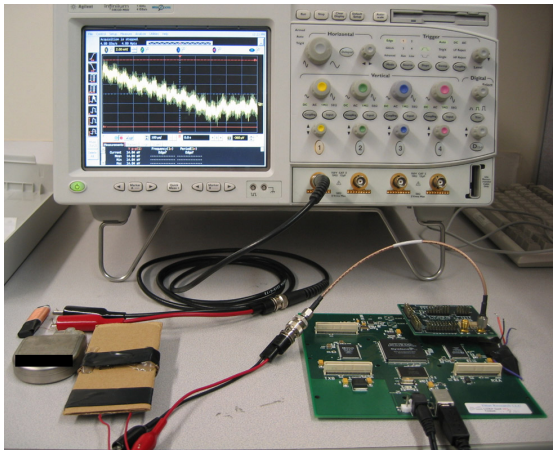


Fig. 1. Chest xray image of an implanted ICD (top right, near shoulder, solid outline) and electrical leads connected to heart chambers (center of rib cage, dotted outline).

This is not a screen grab but an embedded PDF #ProBall

Passive Adversary



- Black Box Methodology:
  1. RE Layer 1 bits w/ oscilloscope
  2. Eavesdrop on protocol with software-defined radio
  3. Did not perform full RE of protocol, just gripped for cribs
- Results:
  - No transport secrecy: eavesdropping revealed patient PII (e.g., name, DOB, medical ID)
  - Household magnet prompts broadcast of telemetry data (e.g., heart rate), confirmed with chosen plaintext attack.

This is not a screen grab but an embedded PDF #ProBall

Active Adversary

- Methodology:
  - Naïve replay attacks at close range
  - Magnet was not required to send control messages to the ICD
- Example results:
  - Device Fingerprinting (ICD TX's its metadata)
  - Disclose patient data and telemetry data
  - Modify patient name, ICD clock, therapy settings
  - Trigger test mode that induces fibrillation

Defenses: Goals

- "Traditional approaches could introduce new hazards to patient safety," e.g., botched key mgmt, power drain.
- Security Goals:
  1. Prevent/Deter insider attacks (also outsider)
  2. Security solution must draw "zero power"
  3. "Effortless" patient detection of security-sensitive events as they occur

Defenses: Overview

1. 0-power notification: piezo-element harvests induced RF energy to beep during security-sensitive events

   Evaluation: Bacon-based

2. 0-power authentication: harvest RF energy to perform cryptographically authenticate external programmer

3. Sensible Key Exchange: Vibration-based key distribution

Ethical MedSec Research

- Disclosure:
  - Traditional: Notify companies of vuln's in advance
  - Occasional: Omit technical details to avoid how-to
- Trigger-Avoiding: Paper does not describe attack scenarios (Threat Model / Motivation is dialed down).
- Solutions-based: Possible defenses against attacks are immediately presented (Discard L.P.U.-based approach)

Practicality of Defense

What were your thoughts on the practicality of these defenses?

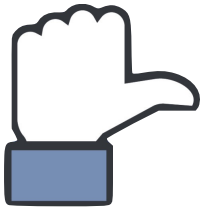
Zero-Power Notification

Zero-Power Authentication

Sensible Key Exchange

Practicality of Defense

What were your thoughts on the practicality of these defenses?



Zero-Power Notification

Zero-Power Authentication

Sensible Key Exchange

Medical Security Tipping Point

SECURITY

Motivation: Money
Approach: Fail Closed

$$Cost_S(Lawsuit) = ???$$
$$P_S(Lawsuit) = ???$$

MEDICAL

Motivation: Money
Approach: Fail Open

$$Cost_M(Lawsuit) = \$\$\$$$
$$P_M(Lawsuit) = \text{yes}$$

Classic security guarantees will only become relevant to the medical space if and when:

$$Cost_S(Lawsuit) * P_S(Lawsuit) \approx Cost_M(Lawsuit) * P_M(Lawsuit)$$

Any other beef?

Any other thoughts or criticisms?

Any other beef?

Any other thoughts or criticisms?

- Takes lots of "shortcuts"
  - "Lazy" Attack Methodology
  - "Lazy" Defense Methodology
- Pictures of meat bags