Heart-to-Heart (H2H): Authentication for Implanted Medical Devices

M. Rostami  A. Juels  F. Koushanfar
Rice Univ.  RSA Laboratories  Rice Univ.
A pacemaker is a small device that's placed in the chest or abdomen to help control abnormal heart rhythms.
A **neurostimulator** is a surgically placed device which delivers mild electrical signals and causes a tingling sensation in the area of your chronic pain.
• 25 million people in U.S. alone fitted with IMDs

• Example: Transcranial Direct Current Stimulation (tDCS)
  • Improves cognitive performance
  • (May also prevent migraines)
IMD access is too hard
• E.g., Patient collapses on sidewalk
• EMTs arrive and try to read diagnostics / reprogram IMD
• They can’t get access…
• (They can’t remember their first pets’ names)

IMD access is too easy
• Landmark attack by Halperin et al. in 2008 (UMass, UW, BI)
• Expose IMDs to unauthorized wireless access and physically harm patients
Overview

- Introduction
- Related work
- Model and approach
  - Model construction
  - Authentication process
  - Programmer–IMD pairing protocol
- Implementation
- Conclusion and future work
Related work

- Conventional password / device key?
  - 2010 U.S. Dept. of HHS report: medical errors may be third leading cause of death
  - Password or key-based access to IMDs would be a key-distribution nightmare

- Ultraviolet Micropigmentation Tattoos [S10]
  - Clever and probably workable
  - May not meet patient acceptance, may be hard to find, lacerations?

- Distance-bounding [RCH-BC09]
  - Nice approach
  - Power considerations, hardware modification, various attacks

- Wearing a shield or jammer around the neck [GHRK+11]
  - Can violate FCC rules, inconvenient

- Transmitting key via Piezo device [HH-BRC+08]
Challenges:

- Demonstrate EGG is suitable PV for authentication
  - Truly random
  - Touch-to-access avoid reading cardiac rhythms
  - Cryptographic pairing protocol

- Tight computational and power constraints.
  - Long-lived device
  - Limited memory and computational resources

Contribution:

- Using real world ECG measurements and quantify the extractable entropy in ECG signals.

- Present a novel, lightweight, noise-tolerant cryptographic scheme.

- Describe a full implementation of H2H.
• Two devices:
  • IMD
  • Programmer

• Access-control policy: *Touch-to-access*

• Protocol in H2H
  1. Programmer sensor touches patient’s body
  2. IMD reads PV $A$
  3. Programmer reads PV $B$
  4. Devices check that $A \approx B$
Overview

- Introduction
- Related work
- Model and approach
  - Model construction
  - Authentication process
  - Programmer–IMD pairing protocol
- Implementation
- Conclusion and future work
ECG model

- EKG measures electrical activity in body, reflecting activity of heart
- R peak is the most prominent EKG feature
- We examine R-R interval (heart-beat duration)
ECG model

- R-R interval is also called the inter-pulse interval (IPI)
- Underlying processes have well-studied chaotic nature
- IPI is a good source of entropy (used in previous work)
Overview

- Introduction
- Related work
- Model and approach
  - Model construction
  - Authentication process
  - Programmer–IMD pairing protocol
- Implementation
- Conclusion and future work
They analyze some standard EKG databases (MIT-BIH, PTB, and MGH/MF)

- IPIs are normalized, quantized, and Gray-coded, yielding 8-bit value

- Use NIST suite of statistical tests to dataset.

<table>
<thead>
<tr>
<th>NIST test</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Runs</td>
<td>0.311310</td>
</tr>
<tr>
<td>Rank</td>
<td>0.879647</td>
</tr>
<tr>
<td>Longest runs</td>
<td>0.185359</td>
</tr>
<tr>
<td>Frequency</td>
<td>0.011830</td>
</tr>
<tr>
<td>Universal test</td>
<td>0.013223</td>
</tr>
<tr>
<td>Approximate entropy test</td>
<td>0.464725</td>
</tr>
<tr>
<td>FFT test</td>
<td>0.131301</td>
</tr>
<tr>
<td>Linear complexity</td>
<td>0.612269</td>
</tr>
</tbody>
</table>
Take humming distance between IMD & Programmer as surrogate

Error rate varies considerably across quantized bits:
- The lower the significance of the bit, the higher its error rate and entropy

<table>
<thead>
<tr>
<th>Bit</th>
<th>Entropy</th>
<th>Error rate</th>
<th>Denoted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 (MSB)</td>
<td>0.27</td>
<td>0.001</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.80</td>
<td>0.003</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0.90</td>
<td>0.004</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.98</td>
<td>0.006</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0.009</td>
<td>$x_4$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0.018</td>
<td>$x_3$</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0.039</td>
<td>$x_2$</td>
</tr>
<tr>
<td>1 (LSB)</td>
<td>1</td>
<td>0.080</td>
<td>$x_1$</td>
</tr>
</tbody>
</table>
Challenge 1: How to compare $A$ and $B$?

- IMD should only give access to Programmer if $A \approx B$
- But how close should $A$ and $B$ be?
- Previous schemes just look at Hamming distance between $A$ and $B$
- But the error rates are non-uniform across bits
- This naïve approach throws away entropy!
Neyman-Pearson Lemma:

- Let $P(u)$ be probability adversary (no skin contact) makes guess $u$ for true PV
- Let $Q(u)$ be probability valid Programmer/IMD yields $u$ for true PV
- There exists an threshold $T$ such that an optimal classifier accepts a reading $u$ as valid if

\[
\log \left( \frac{P(u)}{Q(u)} \right) > T
\]

- Calculate $T$ according to the false negative rate
Why Neyman-Pearson Lemma:

- Maximum acceptable false negative rate lead to the minimum false positive rate as follows.
- Conveniently, bits $x_1x_2x_3x_4$ are unbiased and independent.
Do we really get touch-to-access policy?

- Is skin contact by Programmer required to read IPIs clearly?

- Photoplethysmography (PPG)
  - Subtle changes in skin color due to heart
  - Their experiments show it isn’t a viable attack
Overview

- Introduction
- Related work
- Model and approach
  - Model construction
  - Authentication process
  - Programmer–IMD pairing protocol
- Implementation
- Conclusion and future work
Challenge 2: How to compare A and B securely

- **Idea 1**: Have Programmer send B to the IMD and compare A and B on IMD
  - An adversary can intercept and replay B
  - How to compare A and B without exposing them on unauthenticated channel?

- **Ideal 2**: Use a Password-Based Key Agreement (PAKE) protocol
  - PAKEs require $A=B$, and we have $A \approx B$
  - General secure function evaluation too expensive for embedded devices

What we need is a *fuzzy* PAKE
Challenge 2: How to compare A and B securely

- **Solution 1**: Entropy source changes continuously, so A and B treatable as one-time secrets
  - Expose A and B at end of protocol
  - Use commit / decommit approach

- **Solution 2**: Bootstrap protocol with unauthenticated secure channel SecChannel
H2H pairing protocol

IMD

SecChannel (TLS) \( \rightarrow \) s

Programmer

Read A

\( C_A \leftarrow \text{Commit}(A,w_A;s) \)

Read B

\( C_B \leftarrow \text{Commit}(B,w_B;s) \)

\( A \approx B \) ???

A \approx B ???
IMPLEMENTATION
Implementation

- An ECG analog A/D front end
- A leopard Gecko EFM-32 microcontroller
- A wireless sensor modem
Implementation

- **Design objective 1**: Minimal power consumption on IMD
  - SecChannel: Low exponent RSA-based TLS (\(e = 2^{16}+1\)) with IMD as client

- **Design objective 2**: Stronger security than ordinary 8-digit (e.g., SecurID) authentication token
  - Read \(n = 15\) IPIs (11 to 15 secs.)
    - FAR, FRR < \(3 \times 10^{-9}\)

- **Design objective 3**: No hardware modification to existing IMDs
IMD authentication is an important and interesting problem at physical / logical security boundary

H2H offers touch-to-access authentication policy using ECG and does not require hardware modification to existing IMDs.

H2H devised a novel cryptographic device pairing protocol which exploits ECG randomness to secure against active attacks.

Implement a device in an ARM Cortex-M3 microcontroller.
QUESTION
More detailed security analysis
  • Remove idealized SecChannel?

Using H2H with other PVs
  • EEG? EMG?

Sensing attacks against touch-to-access?
Thank You!