Security and Privacy for Health Care Applications

Yih-Chun Hu
University of Illinois at Urbana-Champaign

May 17, 2013
Story Time

“Who is the adversary?”

- NSFNet
- The power grid

Maps provided by geni.org and jojoyek.blogspot.com
“Honest but Curious”

- Suppose that information providers run protocols correctly, but try to infer health information

Explore flu trends - United States

We've found that certain search terms are good indicators of flu activity. Google Flu Trends uses aggregated Google search data to estimate flu activity. Learn more »
Less Honest, Equally Curious

China's APT-12, The Entity That May Be Behind The New York Times Website Blockage

By Michelle FlorCruz | January 31 2013 2:51 PM

The New York Times has had a rough year with China. After publishing an article about the secret wealth of Chinese Premier Wen Jiabao, the New York Times website was blocked in mainland China and on the country's social media. Following that, one of the paper's Beijing-based correspondents, Chris Buckley, was given a difficult time obtaining a press visa and had to temporarily leave the country. Now, the Times found out it has been persistently attacked by Chinese hackers for the past four months.

DDoS attack boots Kyrgyzstan from net

Russian bears blamed

By Dan Goodin • Get more from this author
Posted in Security, 28th January 2009 19:57 GMT

The central Asian republic of Kyrgyzstan was effectively knocked offline for more than a week by a Russian cybermilitia that continues to flood the country's internet providers with crippling data attacks, a security expert said.

Facebook, Twitter boot WikiLeaks supporters after Visa attack

Group that shut down MasterCard.com and PayPal forces Visa offline with a denial-of-service attack as part of its Operation Payback campaign.

A hacker group that calls itself "Anonymous" says it took the Visa Web site down today in retaliation for the credit card company suspending payments to the web site.

http://isitup.org/www.visa.com IT'S DOWN! KEEP FIRING!!! #DDOS

40M credit cards hacked

Breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards.
July 27, 2009: 6:16 PM EDT
By Jeanne Sahadi, CNN/Money senior writer

NEW YORK (CNN/Money) - Over 40 million card accounts were exposed to potential fraud due to a security breach that occurred at a third-party processor of payment card transactions, MasterCard International said last Friday.
Sharing a Secret on a Body

• Prior researchers propose using electrocardiogram (ECG) to share a secret
  – Poon et al., “A Novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health,” IEEE Communications Magazine 2006
  – Bao et al., “Using the timing information of heartbeats as an entity identifier to secure body sensor network,” IEEE Transactions on Information Technology in Biomedicine 2008
  – Venkatasubramanian et al., “EKG-based key agreement in body sensor networks,” IEEE INFOCOM 2008
  – Xu et al., “IMDGuard: securing implantable medical devices with the external wearable guardian,” IEEE INFOCOM 2011

• They generally assume ideal ECG measurement, evaluations use hospital-provided data
Suboptimal ECG Measurement

- Isopotential lines represent locations of equal electrical potential.
- Any sensing along a line has zero information.
- In areas where the lines are sparse, sensors will gain little information.
Fundamental Problems

- Physiological value measurements are not robust to the sensor deployment location
- Outsiders can use other technology to remotely measure ECG and compromise physiological value-based secret sharing
- Existing techniques for remote measurement include using images

Instant Heart Rate & CardioGraph on iTunes App Store
External Measurement

• Hemoglobin carries oxygen in your blood. Oxygen-saturated hemoglobin and oxygen-depleted hemoglobin absorb different spectra.

• Since $O_2$ saturation varies with the cardiac cycle, images can give pulse timing information.

[Poh et al., Non-contact, automated cardiac pulse measurements using video imaging and blind source separation, Optics Express, 2010]

Image credit: SarekOfVulcan, Wikipedia
Our Exploration

- We sought to explore the problem of same-body detection:
  - Practicality of using ECG signals for secret sharing (ECG experiment)
  - Developed a novel approach for secret sharing using the body as a channel
  - Modeled the body channel to determine the rate at which we can share secrets

[Chang et al., Body Area Network Security: Robust Key Establishment Using Human Body Channel, HealthSec 2012]
ECG Experiment

- Correlation coefficient ($\rho$) for a quantitative measurement of similarity between ideal (I) and other locations
- The measurements are sensitive to electrode orientation; we only show the maximum correlation (the minimum is 0)
- Measurements are time synchronized due to low autocorrelation ($\rho=0.0394$)
- Designated target sensor locations that emulate predicted BAN use (see diagram on the right)
### ECG Experiment Result

#### Distance vs. ρ

<table>
<thead>
<tr>
<th>Distance</th>
<th>ρ</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>0.9139</td>
</tr>
<tr>
<td>5</td>
<td>0.8473</td>
</tr>
<tr>
<td>1</td>
<td>0.7709</td>
</tr>
</tbody>
</table>

#### Distance vs. ρ for B

<table>
<thead>
<tr>
<th>Distance</th>
<th>ρ</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>0.3442</td>
</tr>
<tr>
<td>5</td>
<td>0.3047</td>
</tr>
<tr>
<td>1</td>
<td>0.1003</td>
</tr>
</tbody>
</table>

#### Distance vs. ρ for A

<table>
<thead>
<tr>
<th>Distance</th>
<th>ρ</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>0.0992</td>
</tr>
<tr>
<td>5</td>
<td>0.0371</td>
</tr>
<tr>
<td>1</td>
<td>0.0155</td>
</tr>
</tbody>
</table>

#### Distance vs. ρ for N

<table>
<thead>
<tr>
<th>Distance</th>
<th>ρ</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>0.0782</td>
</tr>
<tr>
<td>5</td>
<td>0.0362</td>
</tr>
<tr>
<td>1</td>
<td>0.0123</td>
</tr>
</tbody>
</table>

(Distance in cm)
Our Approach

• Our scheme replaces the body physiological values with an artificial electrical signal

• We directly attach an information-carrying electrical signal to the body around the torso
  – Safe at low voltages; used for pain treatment
  – Use voltage below the nerve action potential

• Treat the body as a communications channel between a common sender and a group of receivers

Image from Yeza, Wikipedia article on TENS
Evaluating the Human Body Channel

• Ideal approach: acquire a TENS unit, attach it to a subject, measure the signal at the TENS unit and at our pre-determined body locations

• Unfortunately, TENS units are only available by prescription in the United States

• Alternative approach: characterize the channel:
  – Measure the signal attenuation in heterogeneous and homogenous meat
  – Measure the noise level in a human body
  – Use $C \leq B \log_2 (1+S/N)$ [Shannon, 1948] as our metric
Human Body Channel Model

- Additive noise channel model

\[ S' = h \cdot S + n \]

- \( S \) is the transmitted signal,
- \( S' \) is the distorted and received signal,
- \( h \) is channel amplitude,
- \( n \) is noise

Patl Homogeneous Meat Experiment
Heterogeneous Meat Experiment

where \( d \) is distance and \( \alpha, \gamma \) some constants
Channel Measurements

• We place a voltage potential across two points of our sample
  – Modulated every 500ms, to carry data
• We place two electrodes at various points to measure the attenuation and reception probability
• Bit error rates:
  – 0% error rate at almost every region
  – Except one that had mean error rate of 0.16%

The tissue is not alive
(noise is much less than in living tissue)
Amplitude vs Distance

- Data (homogenous)
- Data (heterogeneous)
- Fit (homogenous)

Normalized Peak-to-Peak Voltage (V)

Distance (cm)

- 57% less
- 23x more

h

h_{worst \ case}
Noise Variance ($\sigma^2$) Measurement

$\sigma^2 = 124.3$
$\sigma^2 = 142.4$
$\sigma^2 = 35.74$
$\sigma^2 = 358.3$
$\sigma^2 = 239.5$
$\sigma^2 = 116.6$

($\sigma^2$ in $\mu V^2$)
## Capacity of Our Scheme

<table>
<thead>
<tr>
<th>d (cm)</th>
<th>SNR (dB)</th>
<th>R (bits/hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>-36.80</td>
<td>5.429</td>
</tr>
<tr>
<td>20</td>
<td>-44.74</td>
<td>0.871</td>
</tr>
<tr>
<td>80</td>
<td>-47.43</td>
<td>0.469</td>
</tr>
<tr>
<td>40</td>
<td>-46.34</td>
<td>0.603</td>
</tr>
<tr>
<td>100</td>
<td>-42.51</td>
<td>1.458</td>
</tr>
<tr>
<td>50</td>
<td>-44.29</td>
<td>0.966</td>
</tr>
</tbody>
</table>

\((d\text{ in cm, SNR in dB, } R\text{ in bits per hour})\)
Application to Body Area Networks

- Shannon capacity > 11 secure bits per day with maximally conservative assumptions
  - Transmit 10 symbols/second * 7200 seconds
- BAN applications are characterized by high-risk, low-occurrence events
- Secret updates are necessary only when the population of nodes changes
- Our scheme requires minimal hardware (two electrodes, ADC, and DAC) and is power-efficient, making it suitable for BAN applications
Questions?