RFID Privacy: from Transportation Payment Systems to Implantable Medical Devices

Wayne Burleson

University of Massachusetts Amherst
burleson@ecs.umass.edu

AMD Research Boston
wayne.burleson@amd.com

This material is based upon work supported by: the Armstrong Fund for Science; the National Science Foundation under Grants No. 831244, 0923313 and 0964641; Cooperative Agreement No. 90TR0003/01 from the Department of Health and Human Services; two NSF Graduate Research Fellowships; and a Sloan Research Fellowship. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of DHHS or NSF.
Prof. Wayne Burleson, burleson@ecs.umass.edu

• At UMass Amherst since 1990.
• VLSI Researcher/Designer/Consultant
• Teaching: VLSI Design, Embedded Systems, Security Engineering
• Research: VLSI Circuits
  – Low-power and Side-channels (NSF)
  – Interconnects, Clocking and Interfaces (SRC, NSF and Intel)
  – On-Chip Sensors (NSF, SRC)
  – SRAM (Intel, NSF)
  – Hardware Security: TRNG, PUF, Trojans (NSF, SRC)
  – Soft-error detection and resilience (Sharp, NSF, Intel)
  – Thermal Sensing and Management (SRC, AMD)
• Research: VLSI Architecture, DSP, Arithmetic, Systems
  – Adaptive SOC (NSF)
  – On-chip Monitor NOC (SRC)
  – Video, 3D Graphics, DSP(NSF)
  – Crypto, Embedded Security (NSF, CISCO, Crypto Research)
• Systems Engineering: Weather Radar, Transportation Payment, RFID, IMD
AMD Research

~50 researchers spread among Boston, Austin, Sunnyvale, Seattle, Ft. Collins, Toronto, Beijing, Bangalore, Paris ...

Exascale Computing initiative (DoE supercomputing in 2020)
- CPU/GPU/APU Architectures
- Supercomputing Workloads
- Low-Power Design

Exploring Low-Power Frontiers (low-power everywhere)
- Networks on Chip
- Reliability
- Thermal Issues and Power Delivery
- Post-CMOS

Technology Transfer
- Tight interaction with product groups (Cores, GPU, SoCs, Software...)
- Publications in top venues (ISCA, Micro, ISSCC, ISLPED, DAC, Supercomputing)
- Patents

Jobs! internship, co-op, post-doc opportunities.
Outline

- Privacy is Hot!
- RFID Privacy in the last 7 years
- Two exciting apps:
  - Transportation Payments
  - Implantable Medical Devices
- The Future
Abstract

- Although RFID has been widely known for its impact on supply chain and inventory management, two of the most exciting applications from a privacy perspective are in: 1) transportation payment systems and 2) implantable medical devices.

- This talk presents recent research in both areas, drawing parallels but making important distinctions between the two applications. Both projects involve broad international collaborations due to the large number of technical disciplines involved, as well as varying legal and societal dimensions across different cultures.

- Transportation payment systems have the ability to divulge user location and hence travel habits. However, they also facilitate sophisticated dynamic fare schemes and optimization of the transportation system.

- Implantable medical devices contain extremely private information about personal health and habits, as well as enabling tracking and other privacy concerns. However, the ability to wirelessly access implanted devices provides enormous health and cost benefits.

- Both topics raise interesting cross-disciplinary issues in
Some notable dates in privacy

- 1953 European Convention on Human Rights, Article 8,
- 1982 Chaum: Anonymous email, E-cash
- 1990 Privacy International, PGP
- 1997 Diffie and Landau: Privacy on the Line (wiretapping)
- 1998 k-anonymity
- 1999 Sun’s McNealy: “You have zero privacy anyway. Get over it.”
- 2000 First PETS workshop (Berkeley)
- 2002 Tor
- 2003 Benetton: RFID privacy
- 2004 E-passports, mix-zones
- 2005 First RFIDSec (Graz)
- 2006 Differential privacy
- 2007 EZ-pass subpoenas, TJ Maxx data breach
- 2008 Bitcoins, Implantable Medical Device vulnerabilities
- 2009 Facebook – privacy changes
- 2010 Privacy by Design
- 2011 Wikileaks, Apple: iphone locations
- 2012 Google: shares history
- 2013 US Supreme Court allows DNA collection
- 2013 NSA: Snowden
Privacy in many academic fields

Why I find Privacy more interesting than Security

- **Subtle threat model**
  - Privacy metric is often a result of a very complex attack
  - Not yet conceived use of data
  - No boogie man

- **Economics**
  - what will people pay for privacy?

- **Human and social issues**
  - Different cultures, ethics, opinions

For each weakness, why was privacy compromised?
- Security
- Convenience
- Social
- Marketing
- Research

For each solution, why was privacy preserved?
- Anti-government
- Tax avoidance
- Contraband
- Principles

“Instead of ‘getting over it’, citizens need to demand clear rules on privacy, security, and confidentiality.” (Manes)
RFID Security and Privacy: A Research Survey

Ari Juels

Invited Paper

Abstract—This paper surveys recent technical research on the problems of privacy and security for radio frequency identification (RFID).

RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next several years—and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While

1) Unique identification: A barcode indicates the type of object on which it is printed, e.g., “this is a 100 g bar of ABC brand 70% chocolate.” An RFID tag goes a step further. It emits a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate, e.g., that “this is 100 g bar of ABC brand 70% chocolate, serial no. 897 348 738.” The unique identifiers in RFID tags can act as pointers to a database entries containing rich transaction histories for individual items.

Recommended reading!
RFID Privacy concerns… (what has changed since 2007?)

RFID tags will soon be everywhere…

Replacement hip
medical part #3568ac

Wig
model #4456
(cheap polyester)

Das Kapital and
Communist-party
handbook

500 Euros
in wallet
Serial numbers:
597387,389473…

30 items
of lingerie

Can they support privacy-preserving protocols?

Ari Juels, RSA Labs, 2007
Implantable Medical Device

Wireless IMD access reduces hospital visits by 40% and cost per visit by $1800

[Journal of the American College of Cardiology, 2011]
# Comparing RFID Security/Privacy issues

<table>
<thead>
<tr>
<th></th>
<th><strong>Transportation payment systems</strong></th>
<th><strong>Implantable medical devices</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>• very low cost,</td>
<td>• expensive,</td>
</tr>
<tr>
<td></td>
<td>• disposable</td>
<td>• (but some disposable applications)</td>
</tr>
<tr>
<td><strong>User model</strong></td>
<td>• time-aware,</td>
<td>• latency-tolerant</td>
</tr>
<tr>
<td></td>
<td>• broad spectrum of population</td>
<td>• may have multiple devices / health issues</td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td>• user identity,</td>
<td>• user identity,</td>
</tr>
<tr>
<td></td>
<td>• location,</td>
<td>• life-critical</td>
</tr>
<tr>
<td></td>
<td>• habits</td>
<td>• health</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• genomics, proteomics,...</td>
</tr>
<tr>
<td><strong>Threat model</strong></td>
<td>• tracking,</td>
<td>• tracking,</td>
</tr>
<tr>
<td></td>
<td>• marketing</td>
<td>• insurance fraud,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• discrimination</td>
</tr>
</tbody>
</table>
Multi-disciplinary teams

- **Transportation Payment Systems – “Pay as you Go”**
  - UMass ECE – Security Engineering and VLSI
  - UMass Transportation – Transportation financing, user acceptance,
  - UMass CS - Wisp/Moo, Security Engineering
  - Brown - Crypto, E-cash
  - UMass Dartmouth – Transportation design and optimization
  - MBTA, - Data-sets, Real-world issues
  - EPFL CS – Location Privacy
  - KUL – ECC Engine

- **Implantable Medical Devices**
  - UMass ECE and CS – Security Engineering, IMDs
  - EPFL EE – Bio-sensors and prototyping
  - Bochum – Security Implementation (KECCAK)
  - MIT – Secure Communications
  - SHARPS – IMD Security, Privacy Ethics, Health Records
  - SPIMD book: Clemson, Metarini, Princeton, U. Michigan, Shanghai
Multi-disciplinary teams

- Transportation Payment Systems – “Pay as you Go”
  - UMass Transportation – M. Skelly, M. Plotnikov, J. Collura
  - UMass CS - A. Molina-Markham, K. Fu
  - Brown - F. Baltsami, A. Lysyanskaya
  - UMass Dartmouth – M. Zarrillo
  - MBTA, - S. Pepin
  - EPFL CS – R. Shokri, J-P. Hubaux
  - KUL – I. Verbauwhede

- Implantable Medical Devices
  - UMass ECE and CS – S. Clark, B. Ransford, W. Burleson, K. Fu
  - EPFL EE – S. Carrara, S. Ghoreishizadeh, A. Pullini, J. Olivo, G. DeMicheli
  - Bochum – T. Yalcin, C. Paar
  - MIT – S. Gollakata, D. Katabi,…
  - SHARPS – H. Nissenbaum, D. Kotz, C. Gunter …
  - SPIMD book: A. Guiseppi-Elie, Q. Tan, N. Jha, …
Public Transportation Payments

Why Electronic Payments

• Throughput and convenience
• Reduced revenue collection cost
• Variable and Dynamic pricing
• Collection of meaningful data
Riders are willing to offer some information for a reduced fare!

**Students**

- Green = Bus line 1000
- Red = Bus line 1100
- Blue = Bus line 1300

**Seniors**

- Uses of Data?:
  - Advertising
  - Services
  - Security/Safety

The dataset contains 10,805,791 transactions and 682 routes and stops over a 2 week period.
Privacy Utility Tradeoffs

Privacy Preservation vs Data Utility

- User residence
- User income
- User politics
- User education-level
- User vehicle ownership
- ...

Ability to predict user choice of public vs. private transportation (Skelley and Collura, 2013)
Public Transportation Payments

Hacking the T: MBTA sues to keep MIT students from telling how they cracked the CharlieCard

Hackers Crack London Tube’s Ticketing System But agencies call T’s new Charlie Card an invasion of privacy

By Mac Danilowicz

When T riders fear, commuters hate

The new agency is tracking passengers with a Clipper Card. The new card, which started on SMT

The technology is designed to cut down on fare evasion, but some riders, cut do not

A hearing is public for the high-tech system.

Filed Under
E-cash

withdrawal

Bank

spending

deposit

Chaum, 1982
Brands, 1992
E-cash

Blind signature

Double Spending

Double Spending reveals User’s ID!!!
E-cash in Public Transport

Different Denominations

Modular Payment Systems

Encoding of attributes

Offline Verification

Age

Postal Code

Wheelchair access

Price Reduced

6/10/14 Coin expiration
Which E-cash scheme?

• What we want:
  • Offline
  • Provable security
  • Efficient
  • Encoding of attributes

• Brands’ untraceable offline cash scheme [Bra93]
  • Most efficient during spending phase
  • Blind signature not proven secure [BL12]

• Abe’s scheme [Abe01]
  • Security proof, while only little less efficient
  • No encoding of attributes

  ➢ Anonymous Credentials Light [ACL12]
    • Based on Abe
    • Allows the encoding of attributes and has security proof

Brands’ Scheme on RFID Tag

<table>
<thead>
<tr>
<th>Withdrawal</th>
<th>Spending</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 Exponentiations</td>
<td>0 Exponentiations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cycle Count</th>
<th>Execution time @16 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brands’ withdrawing one coin</td>
<td>69 120 181</td>
<td>4.32 s</td>
</tr>
<tr>
<td>Brands’ spending one coin</td>
<td>35 052</td>
<td>0.0022 s</td>
</tr>
</tbody>
</table>

NFC-smartphone e-cash implementation

Execution time for withdrawing one coin on BlackBerry Bold 9900

Execution time for spending one coin on BlackBerry Bold 9900

All times in milli-seconds

## Storage Estimations

<table>
<thead>
<tr>
<th>Scheme</th>
<th>User device (in bytes per coin)</th>
<th>Terminal (in bytes per coin)</th>
<th>Database (in bytes per coin)</th>
<th>Database (in GB per year*)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Without Attributes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brands</td>
<td>284</td>
<td>284</td>
<td>103</td>
<td>44.8</td>
</tr>
<tr>
<td>Abe</td>
<td>227</td>
<td>248</td>
<td>183</td>
<td>79.6</td>
</tr>
<tr>
<td><strong>With 2 Attributes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brands</td>
<td>326</td>
<td>326</td>
<td>145</td>
<td>63.0</td>
</tr>
<tr>
<td>ACL</td>
<td>389</td>
<td>248</td>
<td>183</td>
<td>79.6</td>
</tr>
</tbody>
</table>

* Assuming ridership of 1.28 million passengers per day [MBTA13].

[MBTA13] MBTA ScoreCard 2013 March [Feb’13 Data].
http://www.mbta.com/uploadedfiles/About_the_T/Score_Card/ScoreCard2013
P4R: Prepayments with Refunds

P4R: Security/Privacy issues

• Features
  • Allows distance-based pricing (e.g. even where exit is not known at time of boarding)
  • Allows dynamic variable pricing (e.g. reduced fares on overcrowded buses, delayed trains, etc.)

• Transportation authority security
  • User cannot forge tickets
  • User cannot receive refunds that exceed the overall deposit for tickets minus the overall fare of trips

• User security
  • A passive adversary cannot steal tickets or refunds from a user

• User privacy
  • Adversary cannot differentiate between all possible trip sequences leading to the same total refund amount

• Open Problem: How can user prove they paid (to police on train) without revealing identity?
Implantable and Wearable Medical Devices

- **Bio-Medical**
  - EEG Electroencephalography
  - ECG Electrocardiogram
  - EMG Electromyography (muscular)
  - Blood pressure
  - Blood SpO2
  - Blood pH
  - Glucose sensor
  - Respiration
  - Temperature
  - Fall detection
  - Ocular/cochlear prosthesis
  - Digestive tract tracking
  - Digestive tract imaging

- **Sports performance**
  - Distance
  - Speed
  - Posture (Body Position)
  - Sports training aid

- **Cyber-human interfaces**

Images courtesy CSEM, Switzerland
Security and Privacy in Implantable Medical Devices

1. IMD’s are an increasingly important technology
   • Leveraging many recent technologies in Nano/Bio/Info
   • Possible solutions to major societal problems
     • Clinical
     • Research
   • Many types of IMDs (see taxonomy coming up)

2. Security and Privacy increasingly relevant in modern society
   • Fundamental human rights
   • Quality of life, Related to safety/health
   • Acceptance of new technologies

Combining 1. and 2., IMD Security and Privacy involves:
   • Protecting human life, health and well-being
   • Protecting health information and record privacy
   • Engineering Challenges!
IMD Examples

- **Existing**
  - Glucose sensor and insulin pump
  - Pacemaker/defibrillator
  - Neuro-stimulator
  - Cochlear implant

- **Emerging**
  - Ingestible “smart-pills”
  - Drug delivery
  - Sub-cutaneous biosensor
  - Brain implant
  - Deep cardiac implant
  - Smart Orthodontia
  - Glaucoma sensors and ocular implants

- **Futuristic**
  - Body 2.0 - Continuous Monitoring of the Human Body
  - Bio-reactors
  - Cyber-human Interfaces
Personalized Therapies with multiple IMDs

The Development of new Implantable Medical Devices is a key-factor for succeeding in Personalized therapy.

S. Carrara, EPFL, Nanotera
**Smart pills**

*Raisin*, a digestible, ingestible microchip, can be put into medicines and food. Chip is activated and powered by stomach acids and can transmit to an external receiver from within the body! Useful for tracking existence and location of drugs, nutrients, etc.

“...there’s more silicon in a banana...” - Proteus CTO

Proteus Biomedical
Axes for a taxonomy of IMDs

- Physical location/depth, procedure, lifetime,
- Sensing/Actuating functions, (sense, deliver drugs or stimulus, grow tissue!)
- Computational capabilities (ops/sec, ops/joule,...)
- Data storage (volatile, non-volatile)
- Communication: bandwidth, up-link, down-link, inter-device? Positioning system (IPS), distance to reader, noise
- Energy requirements, (memory, communication, computation,) powering, harvesting, storage, (battery or capacitive)?
- Vulnerabilities. Security functions (access control, authentication, encryption)
- Reliability and Failure modes
Power/Energy Challenges

- Remote powered systems (RFID) limited to 10’s of microwatts
- Near field powering improves this to milliwatts
- Current energy harvesting systems similarly limited...

- Small batteries typically store several 1000 Joules.
- Over several years of operation, this translates to 10’s of microwatts

- Batteries are still large and heavy
- Rechargeable batteries dissipate heat and have safety concerns
- Non-rechargeable batteries require surgery for replacement

- Brain implants can not incur more than 1 degree temperature gradient without safety concerns
Security Goals for IMD Design

- Incorporate security **early**.
- **Encrypt** sensitive traffic.
- **Authenticate** third-party devices.
- Use well-studied cryptographic building blocks.
- Do not rely on **security through obscurity**.
- Use industry-standard **source-code analysis**.
- Develop a realistic **threat model**.

Threat model – Understand your adversary!

- **Motives:**
  - Violence
  - Identity Theft
  - Insurance fraud
  - Counterfeit devices
  - Discrimination
  - Privacy

- **Resources:**
  - Individual
  - Organization
  - Nation-state...

- **Attack vectors:**
  - Wireless interfaces (eavesdropping, jamming, man-in-middle)
  - Data/control from unauthenticated sources
  - Data retention in discarded devices
Privacy threat taxonomy

- D. Kotz, (Dartmouth)  
**A threat taxonomy for mHealth privacy**, NetHealth 2011

---

### TABLE I

**PRIVACY-RELATED THREATS IN mHEALTH SYSTEMS**

<table>
<thead>
<tr>
<th>Threats: mis-use of patient identities</th>
</tr>
</thead>
<tbody>
<tr>
<td>patients</td>
</tr>
<tr>
<td>patients</td>
</tr>
<tr>
<td>patients</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unauthorized access to PHI or PHR</th>
</tr>
</thead>
<tbody>
<tr>
<td>patients</td>
</tr>
<tr>
<td>patients</td>
</tr>
<tr>
<td>patients</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unauthorized disclosure of PII and PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>data at rest, in the PHR:</td>
</tr>
<tr>
<td>patients</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>insiders</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
<tr>
<td>data at rest, in the mobile devices:</td>
</tr>
<tr>
<td>patients</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
<tr>
<td>data in transit:</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
<tr>
<td>outsiders</td>
</tr>
</tbody>
</table>
Lightweight Cryptography for Bio-sensors

**Hummingbird Stream Cipher**

**AES Block Cipher**

Glucose sensor

Ocular implant

---


Secure Platform for Bio-sensing (Umass, EPFL, Bochum)

• Applications
  • Disposable Diagnostic
    • Low-cost, infectious disease detection (malaria, HIV, dengue, cholera)
  • DNA
  • Implantable Device
    • Sub-cutaneous multi-function sensor (drugs, antibodies)
    • Glucose/Lactate in Trauma victims

• Security Technology
  • KECCAK (Authenticated Encryption)
  • PUF for low-cost ID and Challenge-Response
  • TRNG for crypto-primitive

Images: Disposable Diagnostic: Gentag.com, Sub-cutaneous Implant: LSI, EPFL, NanoTera 2-element biochip: CBBB, Clemson University
Mobile – patch – implant

Patch to Sensor communication:
- (Very) Low data-rates
- Implanted
  - hard to lose/steal/tamper!
- Short range
- Known orientation

S. Carrara, EPFL, Nanotera
Authenticated Encryption: Resource-Efficient Schemes

- Hummingbird-2 authenticated encryption algorithm
  - Very compact – as low as 2.2K GE!
  - The fastest version requires 4 cycles/word

- ALE – Authenticated Lightweight Encryption
  - AES-based scheme – Only 4 rounds used
  - Authentication part of encryption process
  - Not TOO light and not too fast (high-latency in AES rounds)

- Sponge-based authenticated encryption (SHA-3 - KECCAK)
  - Introduced after the “birth” of sponge functions
  - Uses the same sponge permutation for both encryption and authentication
Sponge Functions

- Introduced during the SHA-3 competition with KECCAK
  - Permutation-based
  - Variable input length – pushed into the state during “absorbing” phase
  - Arbitrary output – extracted from the state during “squeezing” phase
KECCAK

Pseudo-code of KECCAK-f

\texttt{KECCAK-f}[b](A)

\begin{itemize}
  \item \texttt{for} \texttt{i} \texttt{in} 0 \ldots n_r - 1
  \item \texttt{A} = \texttt{Round}[b](A, RC[i])
  \item \texttt{return A}
\end{itemize}

\texttt{Round}[b](A, RC)

\begin{itemize}
  \item $0$ step:
    \begin{align*}
      C[x] &= A[x, 0] \oplus A[x, 1] \oplus A[x, 2] \oplus A[x, 3] \oplus A[x, 4], \forall x \text{ in } 0 \ldots 4 \\
      D[x] &= C[x - 1] \oplus \text{ROT}(C[x + 1], 1), \forall x \text{ in } 0 \ldots 4 \\
      A[x, y] &= A[x, y] \oplus D[x], \forall (x, y) \text{ in } (0 \ldots 4, 0 \ldots 4)
    \end{align*}
  \item $\rho$ and $\pi$ steps:
    \begin{align*}
      B[y, 2x + 3y] &= \text{ROT}(A[x, y], r[x, y]), \forall (x, y) \text{ in } (0 \ldots 4, 0 \ldots 4)
    \end{align*}
  \item $\chi$ step:
    \begin{align*}
      A[x, y] &= B[x, y] \oplus (\text{NOT}B[x + 1, y] \text{AND}B[x + 2, y]), \forall (x, y) \text{ in } (0 \ldots 4, 0 \ldots 4)
    \end{align*}
  \item $\chi$ step:
    \begin{align*}
      A[0, 0] &= A[0, 0] \oplus RC
    \end{align*}
  \item return \texttt{A}
\end{itemize}

- Permutation function $f$:

\begin{align*}
  q &\rightarrow r & p &\rightarrow c &\rightarrow i
\end{align*}

- State organized as a $5 \times 5$ matrix of $2l$-bits ($l=64$)
- $r=1088$, $c=512$
KECCAK Permutation Steps

- **θ Step:**
  ![θ Step Diagram]

- **π Step:**
  ![π Step Diagram]

- **ρ Step:**
  ![ρ Step Diagram]

- **χ Step:**
  ![χ Step Diagram]
Permutation-based Authenticated Encryption: SpongeWrap

- Key added onto the zero initial state
  - Followed by absorption of additional authentication data (AAD) into the state
- Each new plaintext is XORed with the internal state to generate a new ciphertext (similar to counter mode of operation)
  - Also absorbed into the internal state
- Message digest (with desired length) squeezed from internal state
Permutation-based Authenticated Encryption: DuplexSponge

- Based on SpongeWrap – run in duplex mode
  - Requires a unique IV – fragile, but considerably more secure
  - Number of duplex rounds as low as “1” – extremely low latency → high data rates
Implementation Aspects

- Keccak-100 selected
- 93-bits of security: 100-4(data rate)-3(padding and parity)
- 320 cycles for initial key processing, 80 cycles per 16 bits of data
- Only 1550 GE for the authenticated encryption core
- 2280 GE including interface wrapper
- < 7 µW @500 KHz
Implantable bio-sensor

3mm x 5mm

Prototype mixed-signal IC 180nm, sensor circuitry, I/O, crypto

Open Problem: Key distribution in IMDs? PUFs? DNA?

S. Carrara, G. DeMicheli, EPFL, Nanotera

S. Ghoreishizadeh, EPFL, A. Pullini, EPFL, T. Yalcin, Bochum, W. Burleson, UMass
Protecting existing IMDs

- Gollakota et al (MIT, UMASS), They Can Hear Your Heartbeats: Non-Invasive Security for Implanted Medical Devices, SIGCOMM 2011 (Best Paper)
External “protector devices”

- Sorber et al (Dartmouth), An Amulet for trustworthy wearable mHealth, *HotMobile 2012*
Design Tension Challenges

Security/Privacy goals

- Authorization (personal, role-based, IMD selection)
- Availability
- Device software and settings
- Device-existence privacy
- Device-type privacy
- Specific-device ID privacy
- Measurement and Log Privacy
- Bearer privacy
- Data integrity

Safety/Utility goals

- Data access
- Data accuracy
- Device identification
- Configurability
- Updatable software
- Multi-device coordination
- Auditable
- Resource efficient

Design for Medical is different!

“Medical marches to a different cadence than most of the electronics industry. Design cycles can stretch from three to five years and cost $10-15 million, thanks to the lengthy regulatory process. The product lifecycles can also extend over a 20 year time span.”

*Boston Scientific*

- What is the role of FDA and other regulators?
  - FDA currently regulates safety, but not security
Describes problems of security and privacy in implantable medical devices and proposes solutions
Includes basic abstractions of cryptographic services and primitives such as public key cryptography, block ciphers and digital signatures
Provides state-of-the-art research of interest to a multidisciplinary audience in electrical, computer and bio-engineering, computer networks and cryptography and medical and health sciences

Content Level » Professional/practitioner
Related subjects » Biomedical Engineering - Circuits & Systems - Security and Cryptology
Table of contents
SHARPS is a multi-institutional and multidisciplinary research project, supported by the Office of the National Coordinator for Health Information Technology, aimed at reducing security and privacy barriers to the effective use of health information technology. The project is organized around three major healthcare environments:

- **Electronic Health Records (EHR)**
- **Health Information Exchange (HIE)**
- **Telemedicine (TEL)**

A multidisciplinary team of computer security, medical, and social science experts is developing security and privacy policies and technology tools to support electronic use and exchange of health information.

UIUC, Stanford, Berkeley, Dartmouth, CMU, JHU, Vanderbilt, NYU, Harvard/BethIsrael, Northwestern, UWash, UMass
The Future

• Pay as you *
  • Consume
  • Dispose,…
• Human++
• Future Platforms
  • Other remotely powered devices
  • Harvested power
• Future Privacy Threats
  • Side-channels
  • Big-data
Trends in VLSI Research

- **Driving Applications**
  - Microprocessors
  - DSP
  - Video
  - Wireless
  - Hand-sets
  - Smart Cards
  - Sensor Networks
  - RFID
  - Internet of Things
  - ...

- **Design Challenges**
  - Area
  - Performance
  - Complexity
  - Test/Yield
  - Power
  - Flexibility
  - Reliability
  - Process
  - Voltage
  - Temperature
  - Security/Privacy

1970’s
1980’s
1990’s
2000’s
2010’s
Conclusions

- RFID takes many forms
  - If humans carry RFID in or on their person, privacy issues arise
  - Solutions vary depending on requirements
    - Algorithm
    - Implementation
- Much work to be done
  - Cyber-physical and cyber-human systems
  - Many exciting new applications
  - Many possible new threats
- Internet of Things – Privacy of Things?

Thank you for your attention!
And your questions!
Backup/Q&A slides
Bio-sensors for hemorrhaging trauma victims

Implantable biosensor for monitoring lactate and glucose levels. Funded by the US Department of Defense.

Developing a temporary implantable dual sensing element biochip with wireless transmission capabilities.

Applications in mass triage scenarios such as battlefields and natural disaster sites provide a means for medical personnel to make life saving decisions.

**Low-cost, short life-time, rapid deployment, life-saving**

Future applications in diabetes care, transplant organ health, and intensive care.

A. Guiseppe-Elie, C3B, Clemson University (USA)
Thoughts on: Privacy-preserving transportation payments

- **E-cash plus attributes** allow users to opt-in to possible tracking and receive a discount on their fare. Other transportation payment solutions require users to trust infrastructure, black-box, obfuscation methods, etc. to varying degrees to ensure their privacy.

- **Users can choose to play a game or not.** If they play the game, they can trade off privacy for lower fares. Similarly, the transportation operators can play by offering reasonable discounts in order to incentivize users to give up some privacy in order to give up some information to allow operators to optimize their services. They can gain additional revenue by targeting advertising.

- **E-cash needs to become a culturally trusted anonymous payment** (as regular cash is today). Attributes will be a bit like Cookies where most users will opt-in and accept them for the convenience and reduced fares that they allow, but some users (e.g. Stallman, et al.) can stay anonymous. Various levels of privacy vs. convenience/economy can be provided. These levels may vary depending on culture, law and education of users. See: *Contextual privacy* by H. Nissenbaum, 2012.

- **Location-Privacy is hard for the general population to understand** since the vulnerability is defined by ever-improving tracking algorithms. Some users may wish to learn about these vulnerabilities, calculate risks and play the game, but others should be able to opt out and rest assured that their privacy is not being compromised. (Somewhat analogous to playing the stock market vs. staying in a less risky investment with one's savings).

Collaborations with A. Lysyanskaya, Brown University, and J.-P. Hubaux, EPFL
Security and Privacy Design Issues

- System Requirements
  - Sensor/Actuator Functionality, Software updates
  - Communications: Data-rate (>100kbps), Range/Channel (BAN)
  - Protocol Design: Asymmetric channel, (Active RFID)

- Design Constraints
  - Power (battery-powered, harvested, or remote-powered device)
  - Size, Bio-compatibility, calibration
  - Long life-time, little maintenance, reliability

- Security Analysis
  - Assets: Human health and well-being, personal and health data
  - Threats: Device cloning and counterfeiting, Eavesdropping, Physical Layer Detection and Identification,

- Security Primitives
  - Public and private key crypto, block and stream ciphers, TRNG, PUF
  - Secure radios, Distance-bounding protocols, etc.
Global cross-disciplinary efforts needed!

Speakers:
• K. Fu Umass Amherst, USA
• S. Capkun, ETHZ, CH
• S. Carrara, EPFL, CH
• J. Huiskens, IMEC, NL
• A. Sadeghi, Darmstadt, DE
• I. Brown, Oxford, GB
• F. Valgimigli, Metarini, IT
• A. Guiseppi-Elie, Clemson, USA
• S. Khayat, UFM, Iran
• Q. Tan, Shanghai, China

Panel: How real and urgent are the security/privacy threats for IMDs? Which IMDs?

Springer Book underway, to appear early 2013

http://si.epfl.ch/SPIMD
Prototyping Security and Privacy Solutions

- Why?
- HW vs. SW

- How?
  - Moo
  - Biosensor
  - Umass 32nm
Security Attacks: Theory vs. Practice

- Bribe an employee
- Factor 1024-bit RSA key
- Reverse engineer the security chip
- Try DPA and glitching
- Test for a known software bug

Hacker's perspective: Factoring is irrelevant
Theoretical perspective: Factoring is hard

Source: Paul Kocher, DAC'04
Smart Card
DuplexSponge Operation

• Length/key/nonce loading phase – upon start the core loads initialization data into registers (includes padding)
• Initialization – key/nonce hashed to generate secret internal state ($n_{init}$ rounds)
• Header absorption – Header data padded, loaded and processed (absorbed into the internal state) in blocks ($n_{absorb}$ rounds per block)
• Data absorption – Data words (plaintext or ciphertext) padded, loaded, added onto the secret state → encryption/decryption and update of internal state (also $n_{absorb}$ rounds per block)
• Tag extraction – Core is run with “zero,” input data → Updated internal state bits extracted as tag ($n_{squeeze}$ rounds per block)
Security Goals for IMD Design

- Incorporate security **early**.
- **Encrypt** sensitive traffic.
- **Authenticate** third-party devices.
- Use well-studied cryptographic building blocks.
- Do not rely on **security through obscurity**.
- Use industry-standard source-code analysis.
- Develop a realistic **threat model**.
Why is Hardware Security interesting for RFID and Ubiquitous Computing nodes?

- **Very cost-sensitive**, high-volume, justifies large design effort
- **Very low-power/energy** budget
- Low-level of complexity and efficiency requirements warrant full-custom design
  - Mostly hardware rather than software implementation
  - Very little memory ($10^2 - 10^5$ bits), some is non-volatile
- **Soft real-time** performance requirements
- Side-channel leakage and tamper attacks require careful circuit designs
- **Mixed-signal design** due to unusual wireless communications and energy harvesting approach
- Application/Algorithm/Architecture/Circuit co-design, crossing traditional layers of abstraction
Integrated Payment Systems for Transportation

Q: How to Finance Crumbling Transportation Infrastructure?
A: User Pay-as-you-Go Fees with Electronic Payment Systems...

- Payment smart cards being deployed without adequate security or privacy considerations (January 2008 breaks of Translink and Mifare)

- Open road tolling being deployed in Texas, New Jersey and Florida with security and privacy vulnerabilities

- How to gather user behavior for system optimization without compromising privacy? (w/ Brown, TUDarmstadt)

- Partial anonymization using e-cash schemes needs lightweight elliptic curve engine (w/ Bochum, Leuven)

- First UMass Workshop on Integrated Payment Systems for Transportation, Boston, Feb. 2009, 40 participants from industry, government and academics

- Working with MBTA, Mass Highways, E-Zpass, RSA, MIT, Volpe Center, to assess vulnerabilities and develop both short-term and long-term solutions
Security Choice: Authenticated Encryption

- Best of both worlds
  - Combines encryption and authentication in a single scheme
  - Very well analyzed = several schemes
  - Even standardized – CCM, GCM, OCB, EAX, etc...

- Existing schemes
  - An encryption and a hash function running in parallel → Expensive – requires both primitives
  - As a block cipher mode of operation → The same encryption primitive used for both purposes – cheap but slow