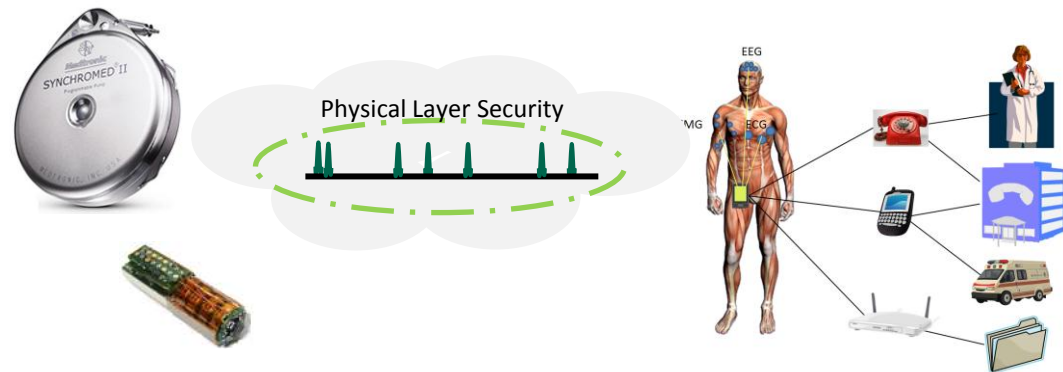


Design Challenges for Secure Implantable Medical Devices

Wayne Burleson
Department of Electrical and
Computer Engineering

Shane Clark, Ben Ransford, Kevin Fu,
Department of Computer Science

University of Massachusetts Amherst
burleson@ecs.umass.edu



Implantable and Wearable Medical Devices

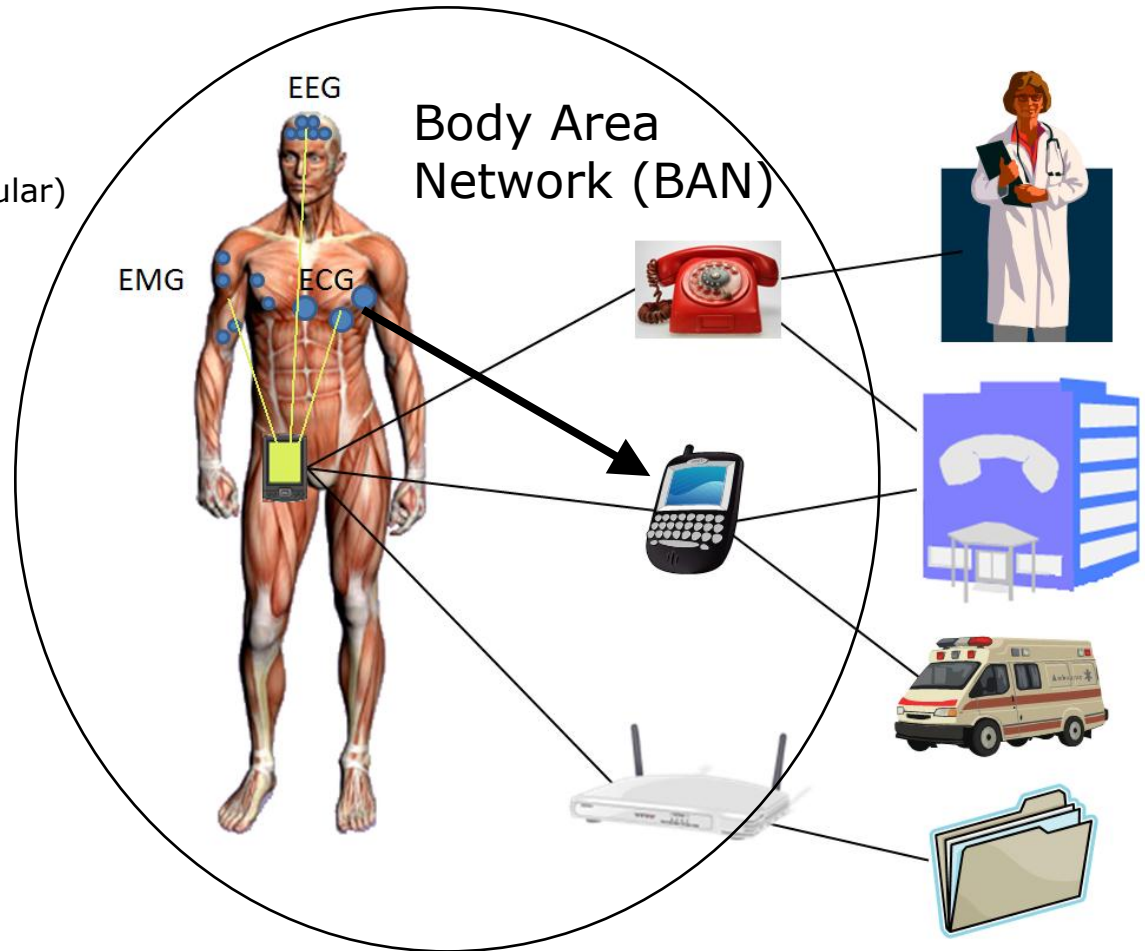
- **Bio-Medical**

- 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**



Security and Privacy in Implantable Medical Devices

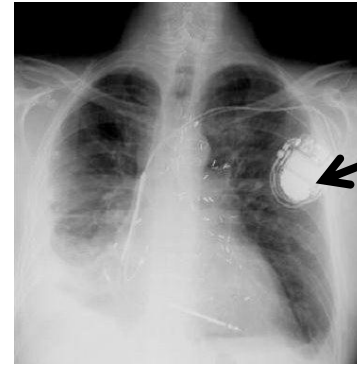
1. IMD's are an increasingly important technology
 - Leveraging many recent technologies in Nano/Bio/Info
 - Possible solutions to major societal problems
 - Clinical
 - Research
 - Many types of IMDs (see taxonomy coming up)
2. Security and Privacy increasingly relevant in modern society
 - Fundamental human rights
 - Quality of life, Related to safety/health
 - Acceptance of new technologies

Combining 1. and 2., IMD Security and Privacy involves:

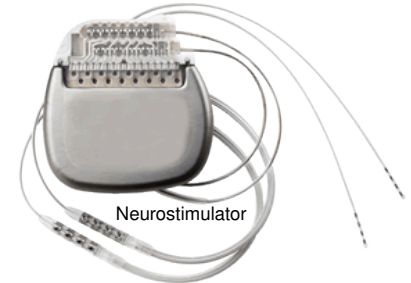
- *Protecting human life, health and well-being*
- *Protecting health information and record privacy*
- *Engineering Challenges!*

IMD Examples

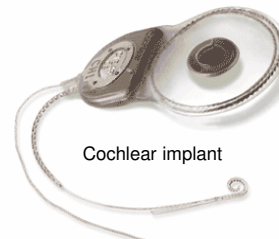
- Existing
 - Glucose sensor and insulin pump
 - Pacemaker/defibrillator
 - Neuro-stimulator
 - Cochlear implant
- Emerging
 - Ingestible “smart-pills”
 - Drug delivery
 - Sub-cutaneous biosensor
 - Brain implant
 - Deep cardiac implant
 - Smart Orthodontia
 - Glaucoma sensors and ocular implants
- Futuristic
 - Body 2.0 - Continuous Monitoring of the Human Body
 - Bio-reactors
 - Cyber-human Interfaces



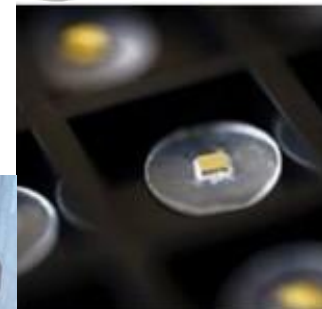
Pacemaker - Medtronic



Neurostimulator



Cochlear implant



Smart pill - Proteus biomedical



Subcutaneous biosensor – EPFL-Nanotera



concept illustration from [yankodesign](http://yankodesign.com)

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

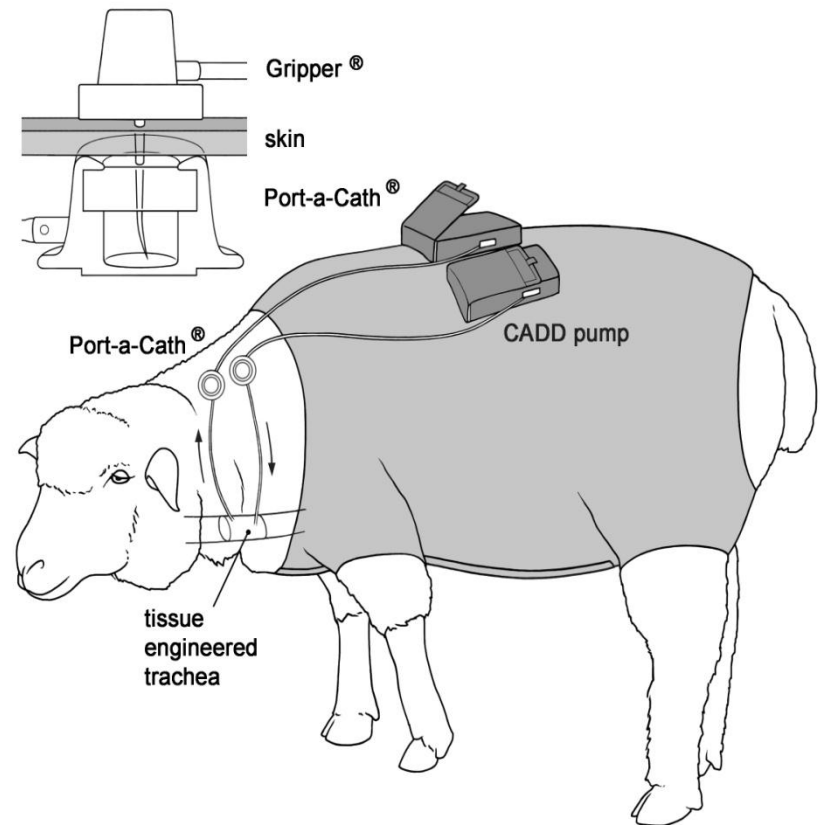
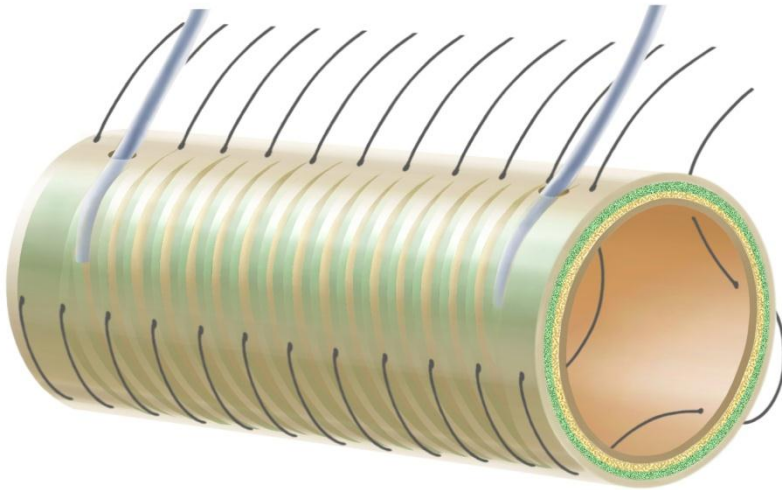


Ingestible Raisin microchip

Futuristic IMDs: Bio-reactor grows tissue in-vivo

Concept

- Organ prosthesis (e.g. stem-cell based) connected to an extra-corporeal perfusion system



Qiang Tan MD., Prof. Qingquan Luo, Prof. Walter Weder
Shanghai Lung Tumor Clinical Center, Shanghai Chest Hospital
Clinic of Thoracic Surgery, University Hospital Zurich

Axes for a taxonomy of IMDs

- Physical location/depth, procedure, lifetime,
- Sensing/Actuating functions, (sense, deliver drugs or stimulus, grow tissue!)
- Computational capabilities
- Data storage
- 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

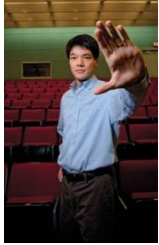
Security Goals for IMD Design

- 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

Pacemakers, Defibrillators (UM Amherst, Harvard, Beth Israel)



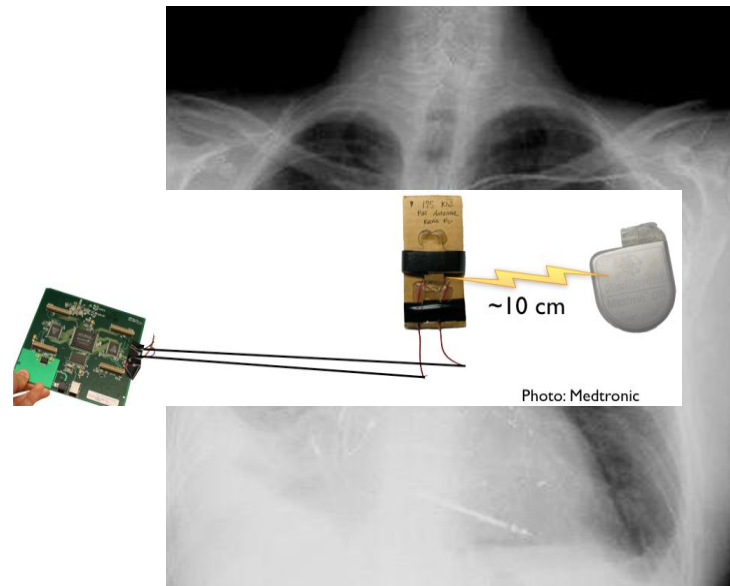
TR 35

- Many medical devices rely on wireless connectivity for remote monitoring, remote therapies and software updates.
- Recent research identified several attacks and defenses for implantable cardiac defibrillators
 - Wireless communications were *unencrypted and unauthenticated*
 - Leading to several *lethal* vulnerabilities
- Extensions to numerous other emerging implantable devices



March 12, 2008

Heart-Device Hacking Risks Seen



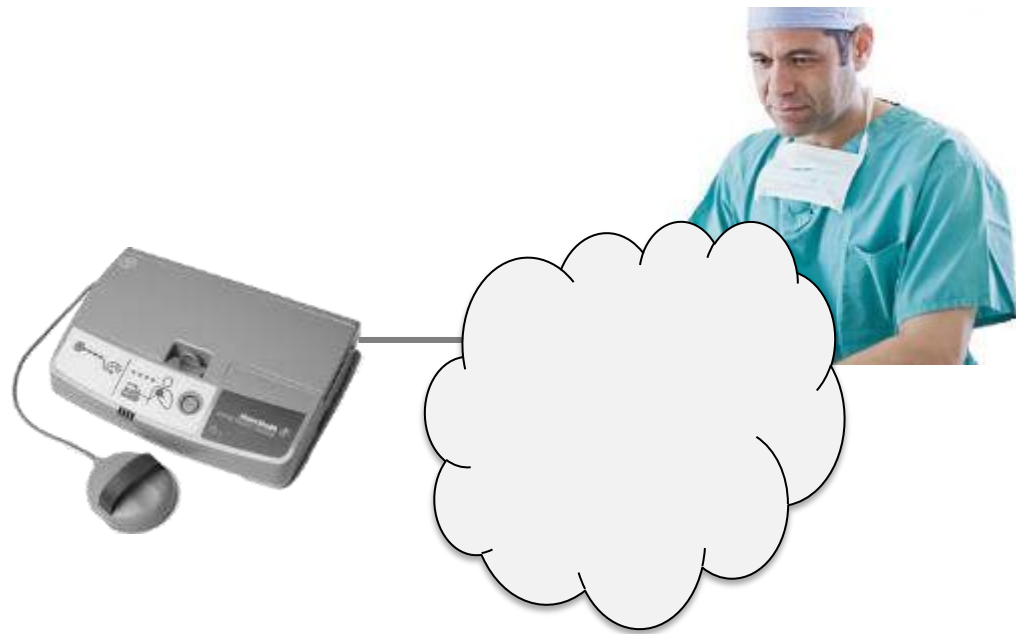
Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses.

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

In Proceedings of the 29th Annual IEEE Symposium on Security and Privacy, May 2008. **Best Paper Award**

Benefits of Wireless

- Easier communication with implant
- Remote monitoring



Benefits of Wireless

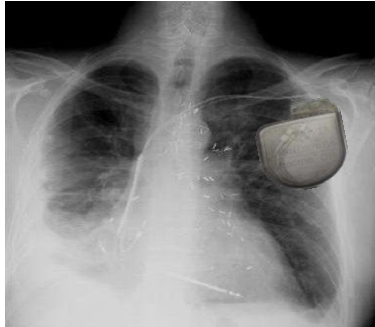
- Easier communication with implant
- Remote monitoring
 - Reduces hospital visits by 40% and cost per visit by \$1800

[Journal of the American College of Cardiology, 2011]

What about security?

Security Attacks

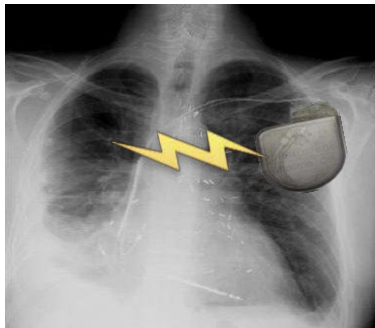
1) Passive attack: Eavesdrop on private data



Patient
diagnosis, vital
signs



2) Active attack: Send unauthorized commands



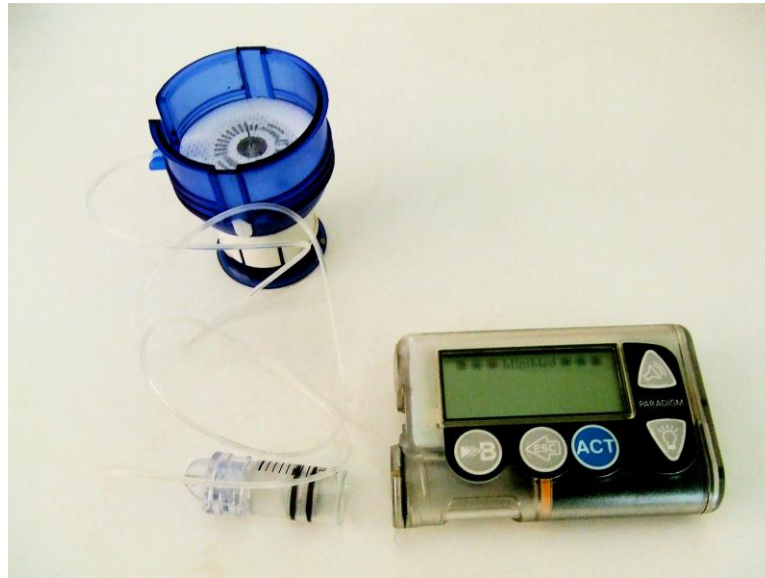
Turn off therapies,
deliver electric
shock



[Halperin'08] demonstrated attacks using software radios

Insulin Pump Systems

- Patient-controlled open-loop systems used to monitor and stabilize glucose levels.
- Several researchers have highlighted security and privacy risks in insulin pump systems.
 - Wireless forgery of insulin readings
 - Wireless administration and potentially fatal over-dosage.



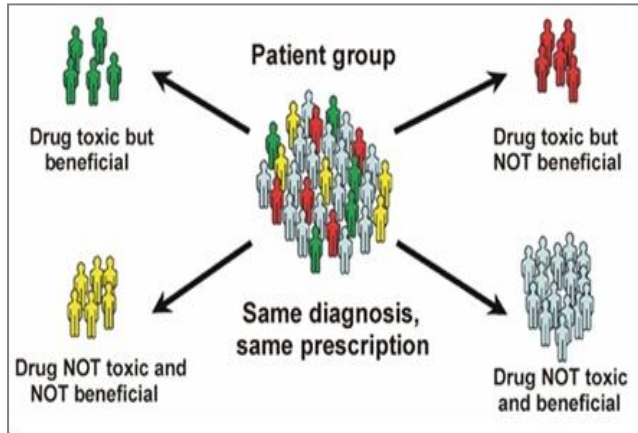
C. Li, A. Raghunathan, and N. K. Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In Proceedings of the 13th IEEE International Conference on e-Health Networking, Applications, and Services, Healthcom '11, June 2011.

N. Paul, T. Kohno, and D. C. Klonoff. A review of the security of insulin pump infusion systems. Journal of Diabetes Science and Technology, 5(6):1557–1562, November 2011.

Cross-cutting Concerns

- When and how to apply encryption
 - Authentication and Key management
 - Lightweight ciphers (stream and block)
 - Physical layer security
 - Appropriate failure modes
- Novel approaches to authentication
 - Ultrasonic distance-bounding
 - Auxiliary “helper” devices
 - PUFs
- Cyber-human systems
 - Human on both ends of the system
 - Controlling
 - Sensing
 - Humans in the loop

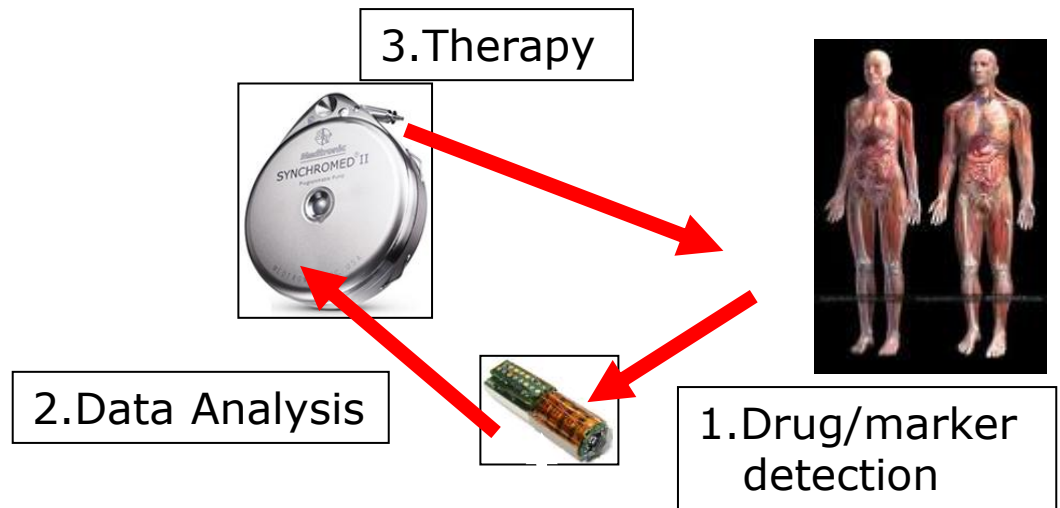
Personalized Therapies with multiple IMDs



Therapeutic area	Rate of efficacy with standard drug treatment
Cancer (all types)	25%
Alzheimer's disease	30%
Incontinence	40%
Hepatitis C	47%
Osteoporosis	48%
Rheumatoid arthritis	50%
Migraine (prophylaxis)	50%
Migraine (acute)	52%
Diabetes	57%
Asthma	60%
Cardiac arrhythmias	60%
Schizophrenia	60%
Depression	62%


For depression, the data apply specifically to the drug class known as selective serotonin reuptake inhibitors.

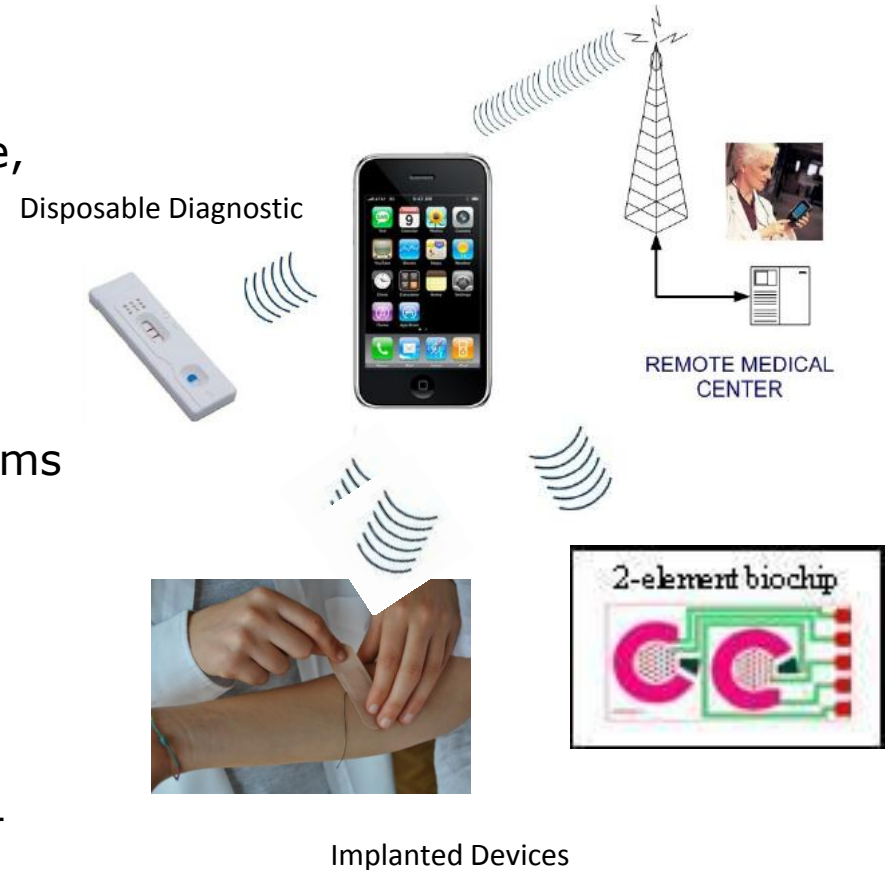
Source: Brian D. Sobot, Margo Hoehn-Chiodo, and Jeffrey Huff, "On-site Applications of Pharmacogenetics," Trends in Molecular Medicine (May 2001).



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

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 
 - NFC Cell Phone
 - EPC Class 1, Gen 2 protocol
 - PRESENT Block Cipher (Encryption, Signing, Authentication)
 - PUF for low-cost ID and Challenge-Response



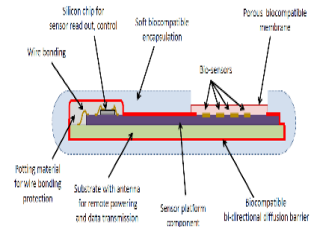
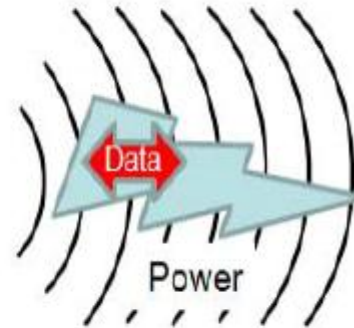
Images: Disposable Diagnostic: Gentag.com,
Sub-cutaneous Implant: LSI, EPFL, NanoTera
2-element biochip: CBBB, Clemson University

Mobile – patch – implant

Bluetooth

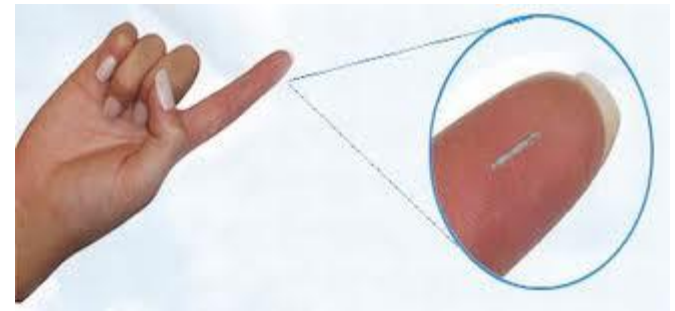


RFID/NFC



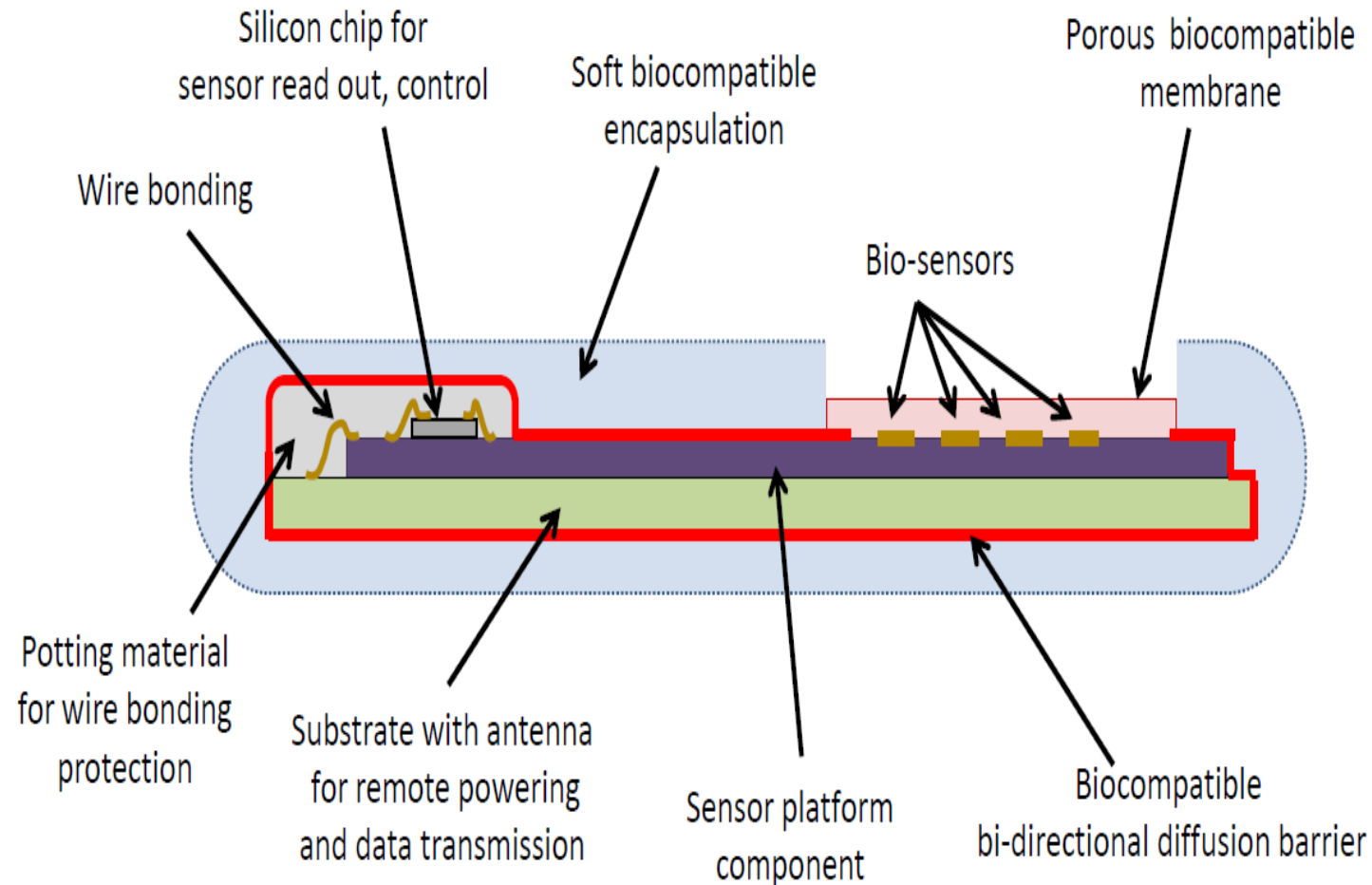
Patch to Sensor communication:

- (Very) Low data-rates
- Implanted
 - hard to lose!
- Short range
- Known orientation



Implantable bio-sensor

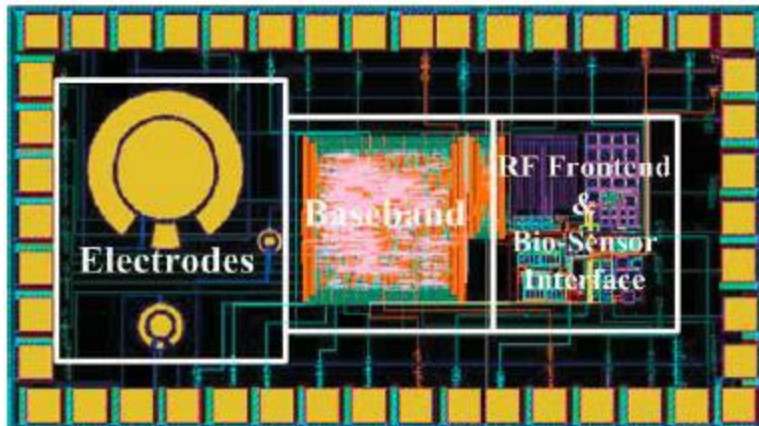
1mm x 3mm



Lightweight Cryptography for Bio-sensors

Hummingbird Stream Cipher

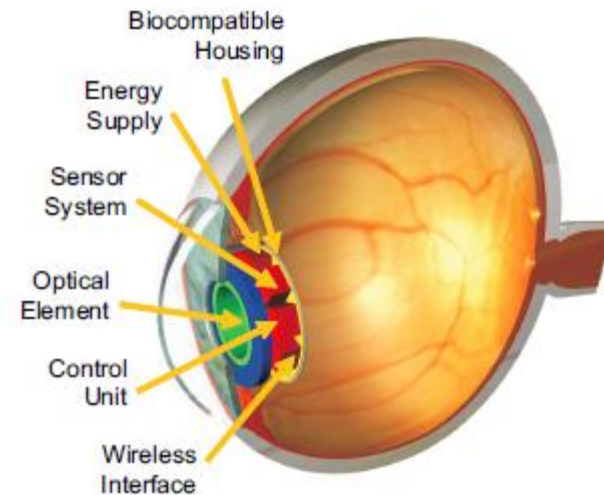
Glucose sensor



S. Guan, J. Gu, Z. Shen, J. Wang, Y. Huang, and A. Mason.
A wireless powered implantable bio-sensor tag system-on-chip for continuous glucose monitoring.
BioCAS 2011.

AES Block Cipher

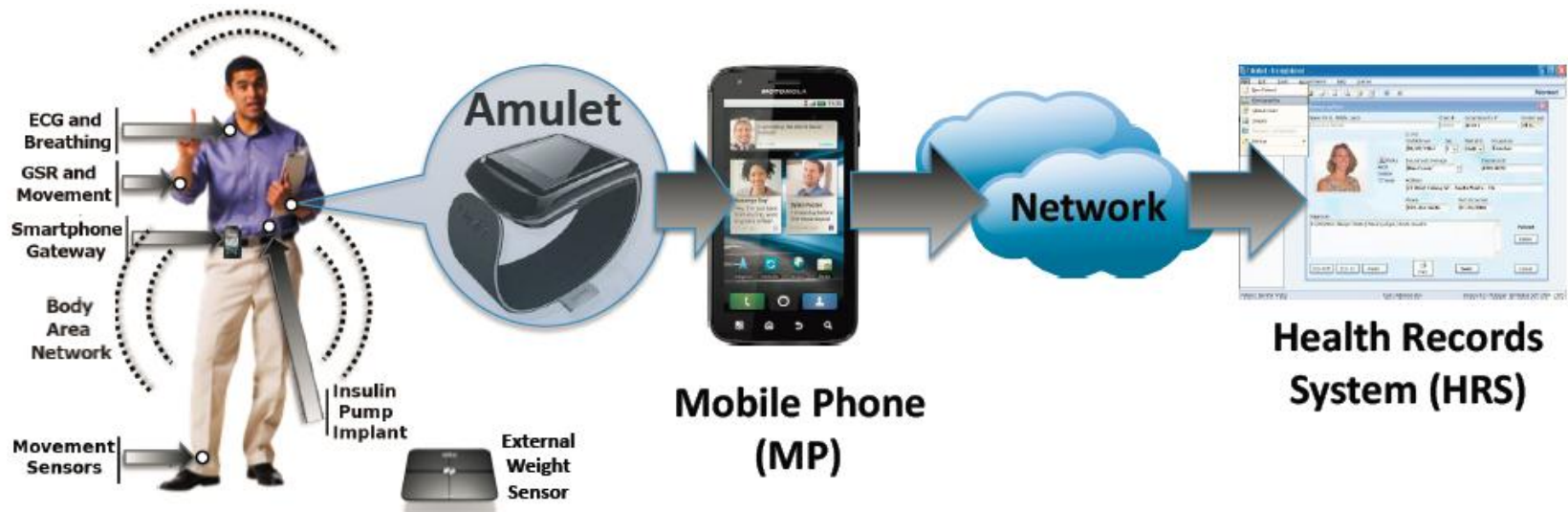
Ocular implant



C. Beck, D. Masny, W. Geiselmann, and G. Bretthauer.
Block cipher based security for severely resource-constrained implantable medical devices. International Symposium on Applied Sciences in Biomedical and Communication Technologies, ISABEL 2011.

External “protector devices”

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



Protecting existing IMDs

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

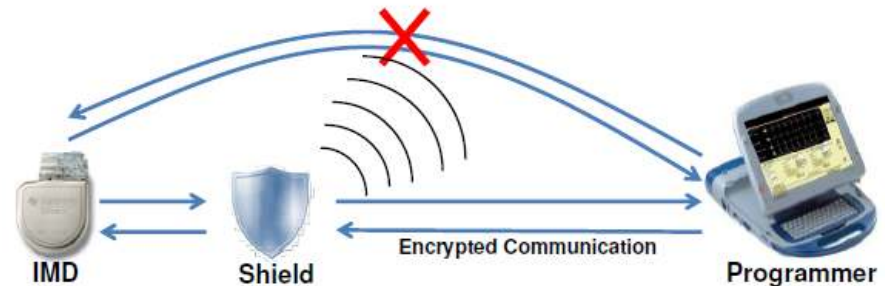


Figure 1—Protecting an IMD without modifying it: The shield jams any direct communication with the IMD. An authorized programmer communicates with the IMD only through the shield, with which it establishes a secure channel.

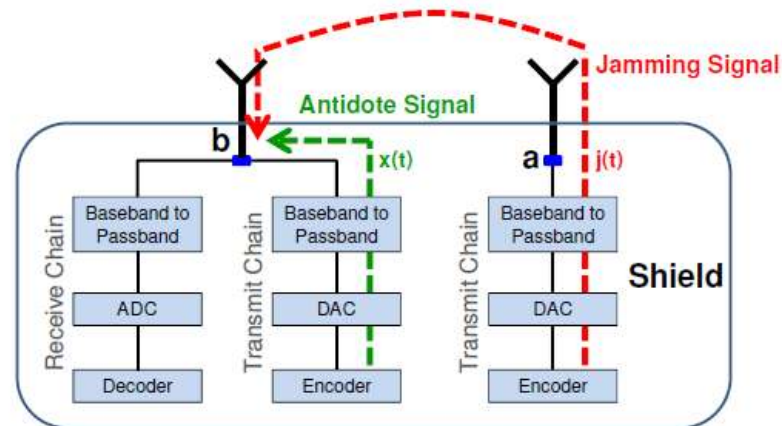
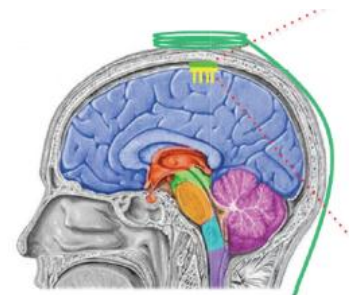


Figure 2—The jammer-cum-receiver design uses two antennas: a jamming antenna that transmits the jamming signal, and a receive antenna. The receive antenna is connected to both a transmit and receive chain. The antidote signal is transmitted from the transmit chain to cancel out the jamming signal in the receive chain.

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



[Courtesy: Subbu Venkatraman]

Design Tension Challenges

Safety/Utility goals

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

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

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

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>



(co-located with IEEE ISMICT in nearby Montreux, Switzerland, www.ismict2011.org)

in the USA...



SHARPS

Strategic Healthcare IT Advanced Research Projects on Security

sharps.org

- 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

Conclusions

- Implantable Medical Devices have unique challenges in Security and Privacy
 - Critical assets
 - Resource constraints (power/energy, size)
 - Hard to maintain
 - Long lifetime
 - Human factors
 - Security/Safety tradeoffs
- But solutions can leverage unique aspects of IMDs
 - Proximity, in-body location
 - Data-rates
 - Threat models
- Need to work with IMD designers and users
- Much work to be done
 - Cyber-physical and cyber-human systems
 - Many exciting new IMDs
 - Many possible new threats

Backup/Q&A slides

Threat taxonomy

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

TABLE I
PRIVACY-RELATED THREATS IN MHEALTH SYSTEMS

Identity threats: mis-use of patient identities

patients	leave PHR credentials on public computer (identity loss)
patients	share passwords with outsiders (identity sharing)
patients	reveal passwords to outsiders (social-engineering attack)
insiders	mis-use identities to obtain reimbursement (insurance fraud) [12]
insiders	mis-use identities to obtain medical services (identity theft) [13]
outsiders	mis-use identities to obtain medical services (identity theft) [13]
outsiders	re-identifying PHI in de-identified data sets [14]
outsiders	observe patient identity or location from communications

Access threats: unauthorized access to PHI or PHR

patients	consent preferences, as expressed, do not match those desired
patients	intentional (or unintentional) access beyond authorized limit
patients	mistaken modifications, because of over-privilege or inadequate controls
insiders	mistaken modifications, because of over-privilege or inadequate controls [15]
insiders	intentional unauthorized access, for curiosity or malice [15], [16]
insiders	intentional modifications, to obtain reimbursement (insurance fraud) [12]
outsiders	intentional unauthorized access, for curiosity or malice [17]
outsiders	intentional modifications, for fraud or malice [17]

Disclosure threats: unauthorized disclosure of PII and PHI

data at rest, in the PHR:

patients	inadvertent disclosure due to malware or file-sharing tools [13]
insiders	inadvertent disclosure due to malware or file-sharing tools [13]
insiders	inadvertent disclosure due to sharing passwords [15]
insiders	intentional disclosure, for profit or malice [16]
outsiders	intentional disclosure, for profit or malice [16]

data at rest, in the mobile devices:

patients	loss of MN or SN exposes PHI, keys, SN types, sensing tasks
outsiders	theft of MN or SN exposes PHI, keys, SN types, sensing tasks

data in transit:

outsiders	eavesdrop on SN-MN, MN-PHR, PHR-PHR, PHR-client; traffic analysis and/or content decryption [18, for example]
outsiders	observe presence and type of sensors on patient [19]

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.



Ingestible Raisin microchip

"...there's more silicon in a banana..." - Proteus CTO

Bio-sensors for hemorrhaging trauma victims

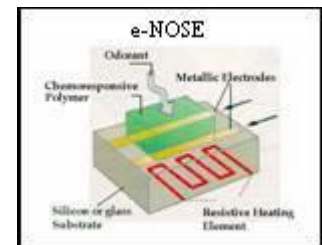
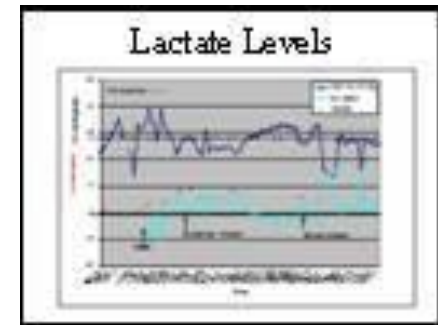
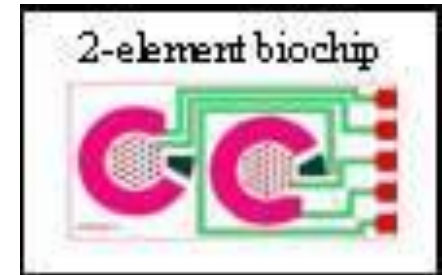
Implantable biosensor for monitoring lactate and glucose levels. Funded by the US Department of Defense

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.



Security and Privacy Design Issues

- System Requirements
 - Sensor/Actuator Functionality, Software updates
 - Communications: Data-rate ($>100\text{kbps}$), 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.

