Welcome!

- To Switzerland
- To Lausanne
- To EPFL
- To SPIMD

- Thanks to
  - Nano-Tera
  - EPFL,
  - Anil Leblebici
  - Christina Govoni

Why Switzerland?

- Innovation
  - Ranking in world
  - Ranking in Europe
- Health Technology industry
- Medical Device industry
- Government investment
  - NanoTera
  - Other

Why now?

- 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. Jon Knight, Boston Scientific

Schedule - morning

9:00 – **Welcome!, Giovanni De Micheli, *Professor and Director, Institute of Electrical Engineering, Integrated Systems Centre, Swiss Federal Institute of Technology, Lausanne, Switzerland***

9:05 **- Overview of the Challenges in Security and Privacy for Implantable Medical Devices, Wayne Burleson, *University of Massachusetts, Amherst, MA, USA***

9:15 **Session 1: Overviews**

- **From IMD to Cloud!, Ahmad-Reza Sadeghi, *Technical University Darmstadt, Germany***
- **New Concepts in Remotely-Powered Telemetry of the Human Metabolism, Sandro Carrara, *Swiss Federal Institute of Technology, Lausanne, Switzerland***

10:15 ***Break***

10:30 **Session 2: Bio-medical Technology**

- **Overview of the Commercially Successful Implantable Glucose Sensors: Key Features and Requirements for Performance, Safety and Reliability, Francesco Valgimigli, *A. Menarini Diagnostics, Italy***
- **An Implantable Biochip to Influence Patient Outcomes Following Trauma-induced Hemorrhage, Anthony Guiseppi-Elie, *Clemson University, Clemson, SC, USA***
- **Principles and Advantages of "In vivo Bioreactor" in Tissue Engineered Trachea Reconstruction, Qiang Tan, *Shanghai Chest Hospital, China***

Schedule - afternoon

12:00 ***Lunch***

12:45 **Session 3: Privacy Policy**

- **Privacy by Design, Ian Brown, *University of Oxford University, United Kingdom***

13:15 **Session 4: Vulnerabilities and Solutions**

- **Trustworthy Medical Device Software, Kevin Fu, *University of Massachusetts, Amherst, MA, USA***
- **Towards Ultra Light-weight Solutions for IMD Security, Saied Hosseini-Khayat, *Ferdowsi University of Mashhad (FUM), Iran***
- **On Secure Access to Medical Implants, Srdjan Capkun, *Swiss Federal Institute of Technology, Zurich, Switzerland***
- **Challenges in Applying Physical Unclonable Functions as a Basis for Security in Body Area Networked Devices, Jos Huisken, *IMEC-NL, Eindhoven, Netherlands***

15:15 ***Break***

15:30 **Panel Discussion**

- **How Real and Urgent are Security/Privacy Threats to IMDs?**

16:30 - **Conclusions and Next Steps, - Wayne Burleson and Sandro Carrara**

17:00 ***Adjourn***

SPIMD

Motivations - Why are we here?

Objectives - What should we accomplish?

Motivations

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)
2. Security and Privacy increasingly relevant in modern society
   - Fundamental human rights
   - Quality of life
   - Acceptance of new technologies

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

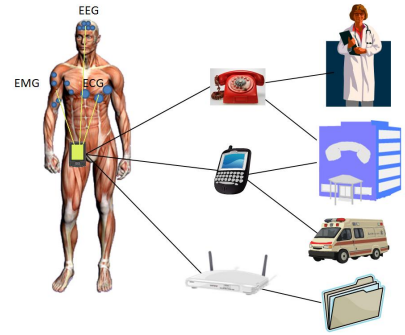
Objectives

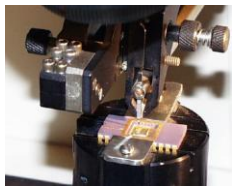
- Cross-disciplinary exposure
  - Learn about the other fields
  - Learn the language
  - Learn the techniques
  - What are the impressive problems that have been solved?
  - What are the open problems?
  - What is similar? What is different?
  - What abstractions/metaphors are useful?
- What are the key multi-disciplinary challenges?
- How real, urgent and practical are these challenges?
- What next steps can we take?

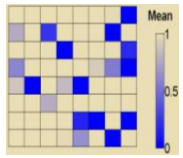
UMassAmherst

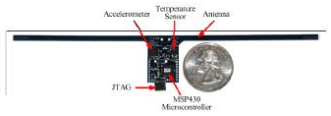
Challenges in Security and Privacy Implantable Medical Devices

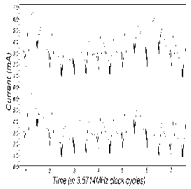
Prof. Wayne Burleson
Department of Electrical and Computer Engineering
University of Massachusetts Amherst
burleson@ecs.umass.edu
(visiting EPFL 2010-2011)











Challenges and Solutions

- IMD security and privacy introduces challenging design problems due to the unique combination of resource constrained computation (size, cost and most importantly energy), and the critical assets of personal safety and health information.
- A systematic approach will be developed for analyzing these systems engineering problems by considering vulnerabilities and defenses across multiple levels.
- A taxonomy of IMDs will be presented based on their physical location, energy requirements, bandwidth, sensing/actuating functions, and vulnerabilities.

Implantable Medical Devices (Kevin Fu, UMass)

- 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*
  - Power depletion attacks
- Extensions to numerous other emerging implantable devices

WSJ.com THE WALL STREET JOURNAL. ONLINE

March 12, 2008

Heart-Device Hacking Risks Seen

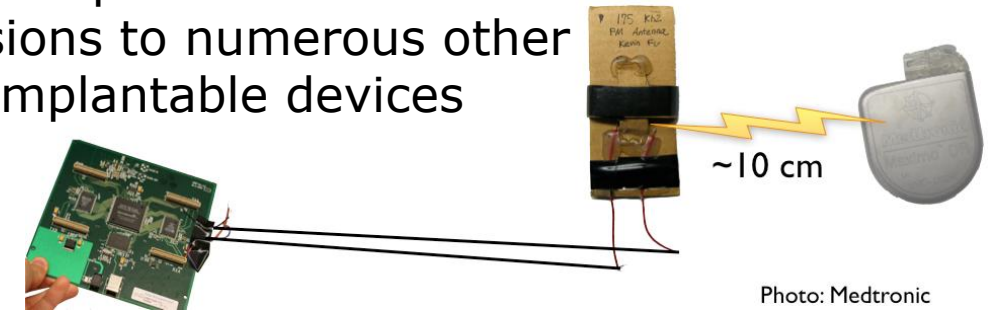


Photo: Medtronic

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. **Outstanding Paper Award**

Design Goals in IMDs

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

From D. Halperin et al, "Security and Privacy for Implantable Medical Devices", IEEE Pervasive Computing, 2008

Axes for a taxonomy of IMDs

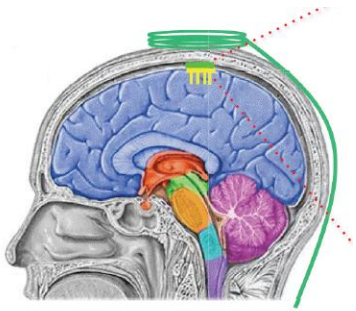
- Physical location, procedure, lifetime, depth
- Energy requirements, (memory, communication, computation,) powereing, harvesting, storage, (battery or capacitive)?
- Computational capabilities
- Data storage
- Communication: bandwidth, up-link, down-link, inter-device? Positioning system (IPS), distance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

Some examples:

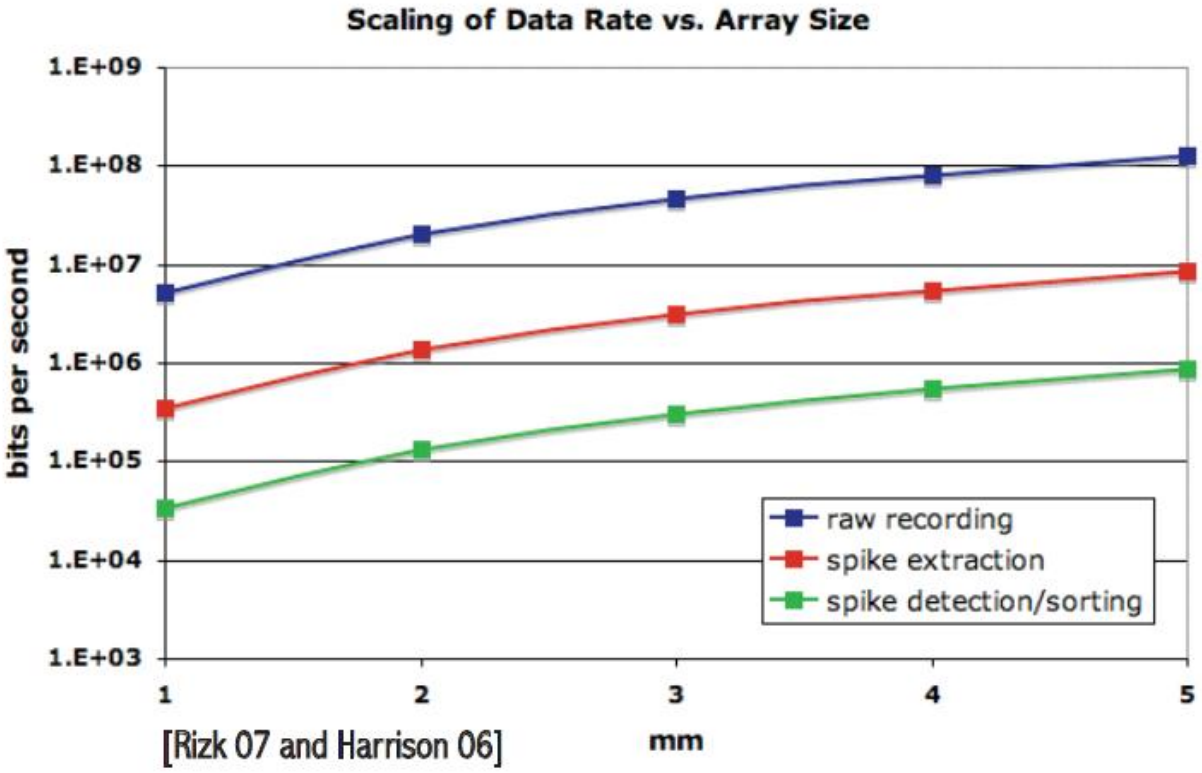
- Existing
  - Glucose sensor
  - Pacemaker/defibrillator
- Emerging
  - Brain implant
  - Injestable "smart-pills"
  - Deep cardiac implant
  - Drug delivery
  - Cochlear
- Futuristic
  - Bio-reactors

Increasing data rates in IMDs

Example:
Brain Implant,
Berkeley Wireless
Research Center



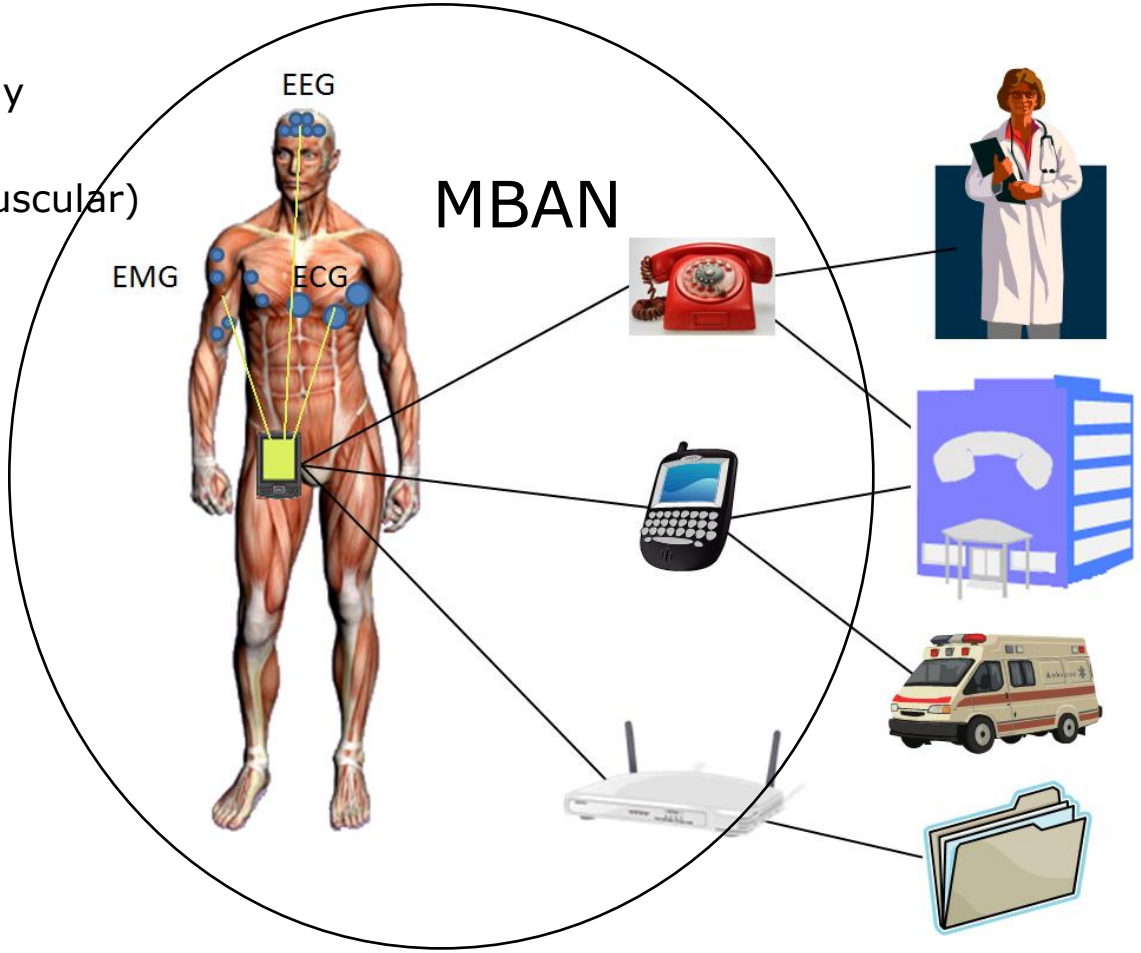
[Courtesy: Subbu Venkatraman]



[Rizk 07 and Harrison 06]

Wearable Medical BAN applications

- **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



Images courtesy CSEM , 2009

A Taxonomy of IMDs

- Physical Location
- Physical Size
- Procedure for Insertion
- Cost
- Lifetime
- Energy source
- Sensors
- Actuators
- Programmability
- Security Analysis
  - Assets/Motives
  - Vulnerabilities
  - Defenses

Medtech on display in Anaheim

- **2/10/2011 1:07 AM EST**
- ANAHEIM, Calif. – The annual MD&M West show here, one of the world's largest medical electronics events, gathers a cross section of the medical electronics industry and much more. This year it included DesignMed, a new engineering conference located a few floors above the massive exhibition floor.

  A handful of semiconductor companies exhibited the latest in medical devices using their silicon. We invite you to take a virtual walk through their demos which provide a window on the future of a medtech sector in its transition to digital, network technology.

The systems ranged from implantable devices to hospital patient monitors and consumer fitness devices such as the Omron Body Mass Index (BMI) meter demonstrated by a Texas Instruments spokeswoman (below). The device takes weight, height and age information and automatically calculates body fat percentage and BMI based on readings through sensors in the handle.

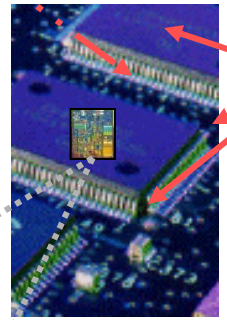
- **Headset reads brain waves**
- **Implant cools back pain**
- **8-bitter drives disposable pump**
- **Bluetooth clip on reads vitals**
- **Wired clip carries Freescale chip**
- **A call to design innovation**
- **Clocking progress in weight loss**
- **Keeping an eye on elders**
- **ADI drives beat of heart monitor**
- **Patient monitor gets graphical**
- **FDA decodes software regs**

Threat Models in IMDs? Still uncharted…

Remote attacks

Worm, virus, Trojan

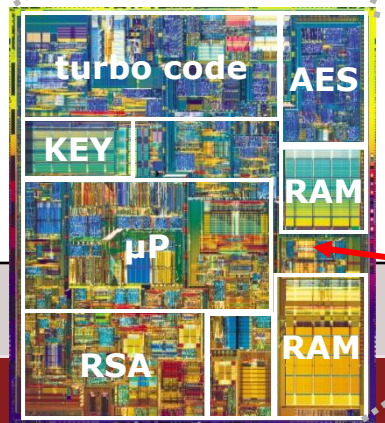
Proximity-based
Passive Hardware attacks
Power or EM analysis



Reversible active
proximity-based attacks

Fault injection

Eavesdropping



Irreversible
hardware attacks

Tampering

Threat Model

Resources\ Adversary	Passive	Active	Coordinated	Insider
Conventional equipment (off-the-shelf)			Relay attack (e.g. Capkun)	
Specialized Equipment (custom, costly, possibly illegal)	Special antennas and receivers, key search engines (e.g. COPOCABANA)	Non-FCC compliant RFID readers (e.g. Pappu, Juels)		Design information, Key storage,

From D. Halperin et al, "Security and Privacy for Implantable Medical Devices", IEEE Pervasive Computing, 2008

Motives of the Adversary?

- Privacy
  - Health privacy
    - Steve Jobs' health…
    - Kim Jong Il's health…
  - Insurance fraud or mis-use
- Security
  - Employment discrimination

Data in IMDs

- Rates
- Precision
- Dimensionality
- Local storage/buffering?
- Programmability
- Calibration
- Test

Panel

- Question: **How realistic are the security and privacy threats of IMDs? How urgent are these concerns?**
- Format:
  - Each panelist will present 2-3 minute position statement
  - Questions from audience, moderator and panel

- Some questions:
  - What is the role of FDA and other regulators?
  - "Courage is the ability to distinguish between real and perceived threats", Socrates c. 600 BC
  - "Only the paranoid survive", A. Grove, Intel

Topics

- Power/area/cost budget for security? Nano-watts
- Privacy is social science… Learn to live with risks
- High expectations for IMDs.
- Risk: Known unknowns and unknown unknowns
- Privacy apathy…
- US Patriot Act…
- Employment discrimination based on health
- Security and privacy design from the beginning
- Trade-offs!
- Security specifications/requirements (quantitative?)
- Surgeons manage risk. But still worry…
- Future IMDs may have different tradeoffs. S&P may matter more
- Many different IMDs. Exposure to threats (comm.) Impact of threats.
- Should certain people have different IMD security/safety tradeoffs
- Security-awareness of IMD manufacturers?

Next Steps

- Special sessions
  - IEEE BioCAS
  - CMOSET Whistler
- Book
  - Springer (C. Glazer)
- Funding
  - NSF (w/ Intl. partners)
  - European (w/ N. American and Chinese partners)