



Workshop on Security and Privacy in Implantable Medical Devices

1 April 2011, EPFL Conference room: ELA 2, Lausanne, Switzerland

Co-organizers:

Wayne Burleson, *University of Massachusetts Amherst, MA, USA*; Visiting Professor EPFL 2010-2011

Sandro Carrara, *EPFL, Lausanne, Switzerland*

Implantable Medical Devices are increasingly being used to solve a wide variety of medical and research challenges. However, they introduce potential vulnerabilities to adversaries that can result in life-threatening situations as well as compromises of privacy. This workshop brings together researchers and advocates from a range of perspectives to present recent research and experiences in this domain.

Implantable Medical Devices (IMDs) allow an unprecedented view into the human body as well as the ability to deliver life-saving therapies. However, the fact that they operate remotely from the direct care of a physician presents unique concerns as well as capabilities. Examples of IMDs range from pacemakers and defibrillators, to artificial organs and joints, to brain implants, to drug delivery systems and many types of bio-sensors. Many implanted medical devices now include microelectronics, sensors and wireless interfaces to the outside world. Some devices can even be re-programmed by over the Internet.

The audience for this workshop is a diverse combination of researchers and practitioners in the areas of Computer Science, Electrical and Computer Engineering, Bio-Engineering, Medical and Health Sciences as well as Legal and Ethical scholars.

Panel Discussion:

Moderator: Wayne Burleson, *EPFL and University of Massachusetts Amherst, USA*

How realistic are the security and privacy threats of IMDs? How urgent are these concerns? One could argue that the technologies are still very young and an overemphasis on security/privacy issues is premature. However, this can be countered by numerous examples of systems that were deployed without adequate security/privacy analysis and are now suffering. In particular, the life-critical aspects of IMDs and the highly sensitive nature of medical privacy requires us to think about these problems differently than similar electronic systems for e-voting (Diebold), personal finance (Paypal), transportation payments (Myfare), social networks (Facebook) or digital entertainment media (DMCA).

For more information please see: <http://si.epfl.ch/SPIMD>

This workshop is sponsored by nano-tera.ch.

Workshop schedule:

- 8:30 **Registration & Greeting**
- 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*
- 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**