

Thomas S. Heydt-Benjamin

Contact Information

530 E86th St #3C
NYC, NY 10028, USA

+1 (914) 744-7934
tshb@acm.org
<http://cryptocracy.net>

Research Interests

Privacy, security, and identity management in both traditional and pervasive contexts. Implantable medical devices. Biometry.

Education

2008 – 2010 **ETH Zurich (Swiss Federal Institute of Technology)**
Ph. D. Studies; ABD

2007 – 2009 **IBM Research Zurich Research Laboratory**
Pre-Doctoral Research

2004 – 2007 **University of Massachusetts Amherst**
M.S. in Computer Science
Thesis topic: Cloning resistant anonymous credentials

2003 – 2004 **Columbia University**
Continuing education in computer science

1996 – 2000 **Yale University**
B.S. In Computer Science

1990 – 1996 **Riverdale Country School**
Graduated Cum Laude, and later returned to teach.

Awards

IEEE Security and Privacy Best Paper Award for: *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*

Peer Reviewed Publications

Preliminary Thoughts on Privacy Supporting Binding of Biometrics to Credentials

Jan Camenisch, Thomas S. Heydt-Benjamin

Hot Topics in Privacy Enhancing Technology (HotPETs 2010)

2010, Berlin, Germany

Proximity-based Access Control for Implantable Medical Devices

Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S. Heydt-Benjamin and Srdjan Capkun

16th ACM Conference on Computer and Communications Security (CCS)

2009, Chicago, USA

Accountable Privacy Supporting Services

Jan Camenisch, Thomas Gross, Thomas S. Heydt-Benjamin

Journal of Identity in the Information Society, 2009, Springer

Physical-layer Identification of RFID Devices

Boris Danev, Thomas S. Heydt-Benjamin, Srdjan Capkun

Usenix Security

2009, San Diego, USA

Rethinking Accountable Privacy Supporting Services <i>Jan Camenisch, Thomas Gross, Thomas S. Heydt-Benjamin</i>	ACM Digital Identity Management 2008, Fairfax, VA, USA
Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses <i>Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel M.D.</i>	Winner: Best Paper Award IEEE Security and Privacy (Oakland) 2008, Oakland, CA, USA
Security and Privacy for Implantable Medical Devices <i>Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, William H. Maisel M.D.</i>	IEEE Pervasive Computing 2008, IEEE
Vulnerabilities in First-Generation RFID-enabled Credit Cards <i>Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare</i>	Financial Cryptography and Data Security 2007 Scarborough, Trinidad/Tobago
Nonesuch: A Mix Network with Sender Unobservability <i>Thomas S. Heydt-Benjamin, Andrei Serjantov, and Benessa Defend</i>	Workshop for Privacy in Electronic Society 2006 Alexandria, VA, USA
Privacy for Public Transit <i>Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu</i>	Privacy Enhancing Technologies 2006 Cambridge University, England

Professional Experience

For details of professional background please see my resume: <http://cryptocracy.net/resume.html>

ETH Zurich (The Swiss Federal Institute of Technology) Research Assistant	2008 – 2010
IBM Research Zurich Pre-doctoral researcher for the Cryptography and Security group	2008 – 2009
IBM Research Zurich Intern for the Cryptography and Security group	2007
University of Massachusetts Amherst Research Assistant	2004 – 2007
Columbia University Volunteer Research Assistant	2003 – 2004
Riverdale Country School Department of Computer Science and Technology Responsibilities included teaching, system and school administration, curriculum development and planning, large scale technology infrastructure planning and implementation.	2000 – 2004

Panels and Invited Talks

Panel: *Personal and Professional Privacy* EuroDIG, Geneva, Switzerland, Sept 2009

Invited talk: <i>Wireless Security and Physical Layer Identification</i>	KU Leuven, Belgium, Feb 2009
Invited talk: <i>The world goes wireless: A paradigm shift still not fully realized</i>	RWTH Aachen, Germany, Feb 2009
Invited talk: <i>Anonymous Credentials in Electronic ID</i>	Advanced Applications for Electric Identity Cards (ADAPID) Leuven, Belgium, July 2008
Invited talk: <i>Privacy Supporting Identity Systems - Theory Meets Practice</i>	The International Conference on Java Technology (Jazoon) Zurich, Switzerland, June 2008
Invited talk: <i>Privacy and Identity Management</i>	Secure Vehicular Communications EPFL, Lausanne, Switzerland, Feb 2008
Panel: <i>Ethics in Privacy Research</i> Thomas S. Heydt-Benjamin (Proposer and Moderator), Panelists: Caspar Bowden, George Danezis (co-proposer), Steven Murdoch, Andreas Pfitzmann, Gene Tsudik	Privacy Enhancing Technologies Symposium Ottawa, CA, 2007

Program Committee Memberships

Security and Privacy in Medical and Home-Care Systems (An ACM CCS Affiliated Workshop)	2009, 2010
Hot Topics in Privacy Enhancing Technologies (PC co-chair)	2008, 2009
Privacy Enhancing Technologies Symposium (2010 Rump Session Chair)	2008 – 2010
Workshop for Privacy in Electronic Society Private Information Management session chair in 2007	2006, 2007, 2010

Other Peer Review

Journal of Computer Security	2010
Communications of the ACM (CACM)	2010
Database and Expert Systems Applications (DEXA)	2010
IEEE International Conference on Information, Communications and Signal Processing (ICICS)	2009
IEEE INFOCOM	2006, 2009, 2010
IEEE Transactions on Dependable and Secure Computing	2009
International Conference on Networked Sensing Systems (INSS)	2009
IEEE SECON	2009

IEEE Transactions on Dependable and Secure Computing (TDSC)	2008
Journal of Computer Science	2008
ACM Transactions on Information and System Security (TISSEC)	2008
IEEE Symposium on Reliable Distributed Systems (SRDS)	2008
IEEE Symposium on Security and Privacy (Oakland)	2006 - 2008
Financial Cryptography and Data Security	2008
IEEE Transactions on Dependable and Secure Computing	2008
IEEE Transactions on Software Engineering	2007
Network and Distributed System Security Symposium	2006 - 2007
ACM Communications and Computer Security (CCS)	2007
Workshop on RFID Security (RFIDsec)	2007
International Conference on Applied Cryptography and Network Security	2007
IFIP SEC	2007
Workshop on Privacy Enhancing Technologies	2005

Other Committees and Service

Academic Standards and Curriculum Committee of the Graduate School (ASCC)	2004 – 2006
UMASS Graduate Council: the advisory and oversight committee of the graduate school	2004 – 2006
Faculty Senate Ad Hoc Committee on Student Information Systems (ACSIS)	2004 – 2006
UMASS Graduate Student Senate; elected representative of the computer science department	2004 – 2006
Yale University Departmental Student Advisory Committee; elected representative	1999 – 2000

Selected Media Coverage

“A Heart Device Is Found Vulnerable to Hacker Attacks”	The New York Times, March 12 2008
“Heart-Device Hacking Risks Seen”	The Wall Street Journal, March 12 2008
Guest on National Public Radio's Leonard Lopate show to discuss privacy for public transportation	40 minute interview, March 9, 2007
“Security researcher shows just how easy it is to steal personal data from RFID-bearing credit cards”	live interview on Fox news, December 2006
“‘Smart’ cards are quick, but are they safe?”	NBC's Today Show, October 26, 2006

“No-Swipe Credit Cards Could Make ID Theft Easier”	ABC's Good Morning America, October 24, 2006
“Researchers See Privacy Pitfalls in No-Swipe Credit Cards”	The New York Times, October 23, 2006

Popular Science and Public Service

Schweizerische Gesellschaft für Mechatronische Kunst (SGMK) Active (teaching) member	2009
Ontario Information and Privacy Commissioner's office: RFID and electronic drivers' license related subjects.	2008
Consumer Reports: advice on and explanation of RFID related subjects.	2008

Teaching and Advising

Honors diploma thesis advisor: Timur Alperovich and Shane Clark research in embedded device security and privacy.	2007
Research mentor: Russel Silva on topics in embedded device security and privacy.	2006
Teaching Associate (Instructor) cs197c: The C++ Programming Language	2005
Teaching Assistant cs445: Information Systems	2005
Teaching Associate (Instructor): The Unix Programming Environment	2005
AB level Advanced Placement Computer Science: A two semester course of my own design covering most of the ACM CS1 & CS2 curriculum, preparing students for the College Board AP exam.	2000 – 2004
Introduction to Technology for Grade Nine / Ten: A one semester course covering technology literacy topics and simple programming. In the 2003-2004 school year, I was the curriculum coordinator, coordinating three teachers with 5 sections.	2000 – 2004
Introduction to Technology for Grade Seven	2000 – 2002

Memberships

International Association for Cryptologic Research (IACR)
 International Financial Cryptography Association (IFCA)
 Institute of Electrical and Electronics Engineers (IEEE)
 Association for Computing Machinery (ACM)

Personal

Captain Emeritus of UMASS Tae Kwon Do, 10 year volunteer EMT in the South Bronx