Thomas S. Benjamin
Curriculum Vitae

Contact Information

32 West Street Apt. 3N
Cold Spring, NY 10516

+1 (917) 744-7934
tomb@cryptocracy.net
http://cryptocracy.net

Research Interests

Computer security and privacy, implantable medical devices, RFID, biometrics

Education

2008 – 2010 ETH Zurich (Swiss Federal Institute of Technology)
Doctoral Research (ABD)
Thesis topic: Security and Privacy of Embedded Devices

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

Awards

2008 IEEE Security and Privacy Best Paper Award for: *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*

Peer Reviewed Publications

Towards Practical Identification of HF RFID Devices
Boris Danev (ETH Zurich), Srdjan Capkun (ETH Zurich), Ramya Jayaram Masti (ETH Zurich), Thomas S. Benjamin (Cryptocracy LLC)

ACM Transactions on Information and System Security (TISSEC), 2012

Preliminary Thoughts on Privacy Supporting Binding of Biometrics to Credentials
Jan Camenisch (IBM Research), Thomas Gross (IBM Research), Thomas S. Heydt-Benjamin (IBM Research)

Hot Topics in Privacy Enhancing Technology (HotPETs)
2010, Berlin, Germany

Proximity-based Access Control for Implantable Medical Devices
Kasper Bonne Rasmussen (ETH Zurich), Claude Castelluccia (INRIA), Thomas S. Heydt-Benjamin (ETH Zurich) and Srdjan Capkun (ETH Zurich)

ACM Conference on Computer and Communications Security (CCS) 2009, Chicago, USA

Accountable Privacy Supporting Services
Jan Camenisch (IBM Research), Thomas Gross (IBM Research), Thomas S. Heydt-Benjamin (IBM Research)

Journal of Identity in the Information Society, 2009, Springer

Physical-layer Identification of RFID Devices
Boris Danev (ETH Zurich), Thomas S. Heydt-Benjamin (IBM Research), Srdjan Capkun (ETH Zurich)

Usenix Security
2009, San Diego, USA

Rethinking Accountable Privacy Supporting Services
Jan Camenisch (IBM Research), Thomas Gross (IBM Research), Thomas S. Heydt-Benjamin (IBM Research)

ACM Digital Identity Management
2008, Fairfax, VA, USA

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses
Daniel Halperin (University of Washington), Thomas S. Heydt-Benjamin (UMASS Amherst), Benjamin Ransford (UMASS Amherst), Shane S. Clark (UMASS Amherst), Benessa Defend (UMASS Amherst), Will Morgan (UMASS Amherst), Kevin Fu (UMASS Amherst), Tadayoshi Kohno (University of Washington), and William H. Maisel M.D. (BIDMC and Harvard Medical School)

Winner: Best Paper Award
IEEE Security and Privacy (Oakland)
2008, Oakland, CA, USA

Security and Privacy for Implantable Medical Devices
Daniel Halperin (University of Washington), Thomas S. Heydt-Benjamin (UMASS Amherst), Kevin Fu (UMASS Amherst), Tadayoshi Kohno (University of Washington), William H. Maisel M.D. (BIDMC and Harvard Medical School)

IEEE Pervasive Computing
2008, IEEE

Vulnerabilities in First-Generation RFID-enabled Credit Cards
Thomas S. Heydt-Benjamin (UMASS Amherst), Daniel V. Bailey (RSA Labs), Kevin Fu (UMASS Amherst), Ari Juels (RSA Labs), and Tom O'Hare (Innealta)

Financial Cryptography and Data Security 2007 Scarborough, Trinidad/Tobago

Nonesuch: A Mix Network with Sender Unobservability
Thomas S. Heydt-Benjamin (UMASS Amherst), Andrei Serjantov (The Freehaven Project), and Benessa Defend (UMASS Amherst)

Workshop for Privacy in Electronic Society 2006 Alexandria, VA, USA

Privacy for Public Transit
Thomas S. Heydt-Benjamin (UMASS Amherst), Hee-Jin Chae (UMASS Amherst), Benessa Defend (UMASS Amherst), and Kevin Fu (UMASS Amherst)

Privacy Enhancing Technologies
2006 Cambridge University, England

Technical papers and patents

Efficient Tight Interval Proofs with Camenisch-Gross Encoding.
Camenisch J, Gross T, Heydt-Benjamin TS

IBM Research Report RZ3800, IBM Research Division, Zurich, Switzerland. 2011

Cryptographic Proofs In Data Processing Systems *Camenisch J, Gross T, Heydt-Benjamin TS*	**US Patent**: US8527777B2 Grant Date: 2013-09-03
Cryptographic Encoding and Decoding of Secret Data *Camenisch J, Gross T, Heydt-Benjamin TS*	**US Patent** No.: US8744077B2 Grant Date: 2014-06-03
Cryptographic Protocols of the Identity Mixer Library *Patrik Bichsel, Carl Binding, Jan Camenisch, Thomas Gross, Tom Heydt-Benjamin, Dieter Sommer, and Greg Zaverucha*	**IBM Research Report** RZ3730, IBM Research Division, Zurich Switzerland, March 2009.
RFID Payment Card Vulnerabilities *Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare*	**UMASS Amherst Technical Report**, 2006

Professional Experience

Applied Communication Sciences (dba Vencore Labs) Senior Research Scientist	2017 – Present
Cryptocracy LLC Member	2016 – 2017
TPIPR CTO	2013 – 2016
Aquavit Pharmaceuticals VP Technology	2012 – 2013
Cryptocracy LLC Member	2011 – 2012
The Tor Project Research Scientist	2010 – 2011
ETH Zurich (The Swiss Federal Institute of Technology) Research Assistant	2008 – 2010
IBM Research Zurich Predoctoral 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 Research Assistant	2003 – 2004

Riverdale Country School 2000 – 2004
Teacher, Administrative staff member.

Panels and Invited Talks

Panel: *Personal and Professional Privacy*	EuroDIG, Geneva, Switzerland, Sept 2009
Invited talk: *Wireless Security and Physical Layer Identification*	KU Leuven, Belgium, Feb 2009
Invited talk: *The world goes wireless: A paradigm shift still not fully realized*	RWTH Aachen, Germany, Feb 2009
Invited talk: *Anonymous Credentials in Electronic ID*	Advanced Applications for Electronic Identity Cards (ADAPID) Leuven, Belgium, July 2008
Invited talk: *Privacy Supporting Identity Systems—Theory Meets Practice*	The International Conference on Java Technology (Jazoon) Zurich, Switzerland, June 2008
Invited talk: *Privacy and Identity Management*	Secure Vehicular Communications EPFL, Lausanne, Switzerland, Feb 2008
Panel: *Ethics in Privacy Research* 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

Privacy Enhancing Technologies Symposium	2008 – 2012
Workshop for Privacy in Electronic Society (An ACM CCS Affiliated Workshop)	2006, 2007, 2010
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

University Committees and Service

Academic Standards and Curriculum Committee of the Graduate School	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	2004 – 2006
UMASS Graduate Student Senate; elected representative of the computer science department	2004 – 2006

Selected Media Coverage

Interview on "dark net" and anonymity technology	Telemundo PR October 22nd 2015
Interview on credit card security	Fox News September 29 2015
“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	NPR, 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

Ontario Information and Privacy Commissioner's office: RFID and electronic driver’s license related subjects.	2008
Consumer Reports: advice on and explanation of RFID related subjects.	2008

Selected Teaching and Advising

GSoC Google Mentor: "Blocking-resistant Transport Evaluation Framework", Student: Brandon Wiley	2011
Honors diploma thesis advisor: Embedded Device Security and Privacy. Students: Timur Alperovich and Shane Clark	2007
Research mentor: Embedded Device Security and Privacy. Student: Russel Silva	2006
Teaching Associate (Instructor) cs197c: The C++ Programming Language	2005
Teaching Assistant cs445: Information Systems	2005
Teaching Associate (Instructor): The Unix Programming Environment	2005

Invited Peer Review

IEEE Transactions on Dependable and Secure Computing	2008, 2009, 2011
Journal of Computer Security	2010, 2011
Computers & Security	2011
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
International Conference on Networked Sensing Systems (INSS)	2009
IEEE SECON	2009
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

Memberships

Mensa, Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), ARRL - AA2TB

07/08/2017