Pitney Bowes' Conference on Information Security & Information Communication

Thursday June 28th, 2007

Location: Auditorium
Pitney Bowes World Headquarters
1 Elmcroft Road
Stamford, CT

Schedule

8:00 – 8:15 Welcome & Continental breakfast

****

8:15 – 8:30 **Morning Opening:** Leon Pintsov (Pitney Bowes; Leon.Pintsov@pb.com)

8:30 – 9:15
Speaker: Alfred Menezes (University of Waterloo, Canada; ajmeneze@uwaterloo.ca)

Title: Pitfalls in proving the security of key agreement protocols

Abstract: It has been 31 years since Diffie and Hellman first proposed their famous key agreement protocol. However, researchers are still debating about what the *correct* notion of security should be for such protocols. In this talk, I will give some examples that illustrate the subtlety and difficulty of capturing all conceivable realistic attacks in security models for key agreement protocols.

Bio: Alfred Menezes is a professor of mathematics at the University of Waterloo, in Ontario, Canada, where he also serves as managing director of the Centre for Applied Cryptographic Research. His research interests are in elliptic curve cryptography, key agreement protocols, provable security, and algorithmic number theory. He is co-author of the "Handbook of Applied Cryptography" and "Guide to Elliptic Curve Cryptography". Alfred has also worked as an independent consultant on projects involving protocol design, security analysis, standardization, patent strategy and litigation.

9:15-10:00
Speaker: Min Wu (University of Maryland, ECE Dept.; minwu@umiacs.umd.edu)

Title: Multimedia Forensics: Where Sherlock Holmes Meets Signal Processing

Abstract: Every technology has its time: in the past decades, we have witnessed advances in communication and networking infrastructure, followed by the development of multimedia compression and coding standards, and then the demands of content search and retrieval. This path of technological evolution has naturally led to an unsolved critical issue, that is, information assurance and forensics. Multimedia forensics reconstructs what has happened to the content to answer who has done what, when and how. It is an emerging new field seeing its horizon rising via the interdisciplinary interactions of signal processing, cryptology, communication and information theory, game theory, and the psychology of

human visual and auditory perception.
In this talk, three exemplary multimedia forensic cases will be illustrated to highlight the excitement of Sherlock Holmes in the 21st century when examining evidences for multimedia documents and devices via the tools of signal processing. These forensic studies can provide useful evidence to help answer a number of questions arising from law enforcement, intelligence operation, journalism, and technology intellectual property protection. For example, can it be determined whether one company's new product infringes an existing patent by its competitor? How did a terrorist group make a propaganda video aired in the Middle East? By what brand and model of A/V equipment? Was there any editing or alteration done to a digital photo reporting a potential piece of breaking news? To whom was it distributed and where was it from? Who was the source leaking a classified picture?

New technologies of traitor tracing forensics, device forensics, and content forensics developed by the University of Maryland research teams will be presented in the talk.

Bio: Dr. Min Wu received the B.E. degree in electrical engineering and the B.A. degree in economics from Tsinghua University, Beijing, China, in 1996, and the Ph.D. degree in electrical engineering from Princeton University in 2001. Since 2001, she has been with the department of electrical and computer engineering and the Institute of Advanced Computer Studies at the University of Maryland, College Park, where she is currently an associate professor. Dr. Wu leads the Media and Security Team (MAST) at University of Maryland, with research interests on information security and forensics, multimedia signal processing, and multimedia communications.
Drs. Liu and Wu are co-authors of *Multimedia Fingerprinting Forensics for Traitor Tracing,* EURASIP Book Series on Signal Processing and Communication, 2005. Dr. Wu co-authored *Multimedia Data Hiding*, Springer-Verlag, 2003, and holds five U.S. patents.

She is an associate editor of the IEEE *Signal Processing Letters* and an area editor of the IEEE *Signal Processing Magazine*. She is a member of the IEEE technical committees on Image and Multi-dimensional Signal Processing, on Multimedia Signal Processing, and on Multimedia Systems and Applications. She received a National Science Foundation CAREER award in 2002, a University of Maryland George Corcoran Education Award in 2003, an MIT Technology Review's TR100 Young Innovator Award in 2004, and an Office of Naval Research Young Investigator Award in 2005. She is a co-recipient of the 2004 EURASIP Best Paper Award and the 2005 IEEE Signal Processing Society Best Paper Award. For more information, see Dr. Wu's webpage at www.ece.umd.edu/~minwu.

****

10:00-10:15 **Coffee break**

10:15-11:00
Speaker: Michael Sipser (MIT, Mathematics Dept.; Sipser@math.mit.edu)

Title: Beyond Computation: the P versus NP problem

Abstract: In a remarkable 1956 letter, the great logician Kurt Godel asked the famous mathematician and computer pioneer John von Neumann whether certain computational problems could be solved without resorting to brute force search. In so doing, he foreshadowed the P versus NP problem, one of the great unanswered questions of contemporary mathematics and theoretical computer science. A solution to this problem would reveal the theoretical limitations of computer power for solving puzzles, cracking codes, proving theorems, and optimizing many practical tasks. We'll discuss all this and more...

Bio: Michael Sipser is a Professor of Applied Mathematics at MIT and Head of the Mathematics Department. He received his Ph.D. from the University of California/Berkeley in 1979 under the

supervision of Manuel Blum and came to MIT shortly thereafter. Sipser is recognized for his work on complexity theory, automata and language theory, and algorithms. He is the author of the widely used textbook, Introduction to the Theory of Computation. His published research spans several areas, including efficient error correcting codes, combinatorial algorithms, interactive proof systems, quantum computation, and establishing the inherent computational difficulty of problems.

11:00-11:45
Speaker: Norbert Lutkenhaus (IQC, Waterloo, Canada; nlutkenhaus@iqc.ca)

Title: Quantum Key Distributions in Networks

Abstract: Quantum Key Distribution uses quantum mechanics and authenticated public channels to distribute secret keys to two communication parties. This talk will summarize the basic ideas of QKD and the problems and opportunities arising, including composability, initialization and rate/distances performance. In the second part of the talk, special attention will be given to the new aspects that arise once QKD is performed not only in point-to-point connections, but in optical networks.

Bio: Norbert Lütkenhaus obtained a Masters in Physics with a Thesis in General Relativity (LMU Munich, 1993) and then switched fields to Quantum Optics and Quantum Information. In his PhD thesis (U. Strathclyde, Glasgow, UK, 1996) he already worked on security of QKD. During postdoc positions in Innsbruck and Helsinki he continued in his work to narrow the gap between theory and experiments in QKD by moving theory closer to the experiments. A milestone in that program has been the adaptation (with H. Inamori and D. Mayers) of Mayers' unconditional security proof of QKD to the then available experimental implementations using weak laser pulses instead of abstract single-photon sources. After that, he joined MagiQ Technologies in New York to initialize the project leading to today's commercially available QKD devices. In 2001 he turned back to academia starting his own research group in Erlangen, Germany. The group moved in 2006 to the Institute of Quantum Computing at the University of Waterloo, Canada.

****
11:45-1:00: **Lunch**
****

1:00-1:15 **Afternoon Opening:** Joseph Wall (Pitney Bowes; Joseph.Wall@pb.com)

1:15-1:45
Speaker: Thad Hall (University of Utah, Dept. of Political Science; thadhall@gmail.com)

Title: The Internet Revolution: How Europe is Leaving America Behind

Abstract: Although the United States is at the cutting edge of technology, since 2000, Internet voting in the United States has stagnated as the debates over electronic voting and election fraud complicate the electoral process. However, the concerns of about electronic voting in America has not stopped experimentation with Internet voting. In fact, interest in and experiments with Internet voting is exploding in Europe and Asia. Since 2000, Internet voting pilots have occurred in Switzerland, the United Kingdom, and other nations in Europe. In Estonia, Internet voting has become a normal channel for voting, alongside early voting and in-person election day voting.

Using data from Estonia and the United Kingdom, I illustrate how innovation with Internet voting is expanding internationally and how such systems are affecting the electoral process. In a report for the Council of Europe, we find that there is a marked growth in Internet voting in Estonia and a shift in general toward convenience voting. I also consider how internet voting is likely to move forward in the United States and how such policy changes should be considered using risk analysis.

Bio: Thad E. Hall is Assistant Professor of Political Science and a research fellow at the Institute of Public and International Affairs at the University of Utah. He is an internationally recognized expert on election reform and administration who has written several books and articles on election participation, voting fraud, voting technology, and public policy and administration. These books include *Point, Click, and Vote: The Future of Internet Voting* and the forthcoming books *Electronic Elections* and *Understanding, Detecting, and Preventing Election Fraud.*

He has conducted research for the Department of Defense, the Election Assistance Commission, Carnegie Corporation of New York, the IBM Center for the Business of Government and is currently part of a research team studying Internet voting in Estonia for the Council of Europe. His BA is from Oglethorpe University, and he holds and MPA from Georgia State University and a Ph.D. in political science from the University of Georgia.

1:45-2:15
Speaker: Michael Epstein (Phillips; Michael.Epstein@philips.com)

Title: Digital Rights Management (DRM) Interoperability

Abstract: Digital Rights Management or DRM is a system which securely connects complex rights (or permissions) to digital content. Most often this content is music or video but DRM can also be applied to medical or business records. The very flexibility of DRM makes it difficult to transfer content from one such system to another since each system has a specific rights language and uses distinct technical measures. This talk will discuss the legal and technical difficulties of DRM interoperability as well as some possible solutions for this dilemma.

Bio: Michael Epstein is a Manager of Technology and Standards at Philips Electronics Intellectual Property Division. Michael has been working for Philips Electronics for more than 20 years. Michael currently tracks US based copy protection standards efforts such as the Copy Protection Technical Working Group (CPTWG). Recently Michael Co-Chaired the Analog Redistribution Discussion Group (ARDG) and participated in the Broadcast Protection Discussion Group (BPDG) both of which were sub-groups of CPTWG.

Prior to joining the Intellectual Property Division Michael was a senior member of the research staff at the Philips corporate research laboratory in Briarcliff Manor, NY. Over his tenure as a researcher Michael has automated factories, designed microprocessors, supercomputers and HDTV prototypes. Michael led the Philips US-based security team to develop “CDSafe” and other innovative copy protection technologies, which enable the proliferation of *legal* digital music distribution as part of the SDMI process.

Over his tenure as research scientist Michael has received 24 issued patents and has filed more that 60 patent applications.

Michael holds a Bachelor of Science degree in electrical engineering from M.I.T and a Master of Science degree in electrical engineering from Columbia University.

2:15-2:45
Speaker: Robert Cordery (Pitney Bowes; Robert.Cordery@pb.com)

Title: The envelope code

Abstract: The surface of a mail piece is paper communication channel among the various parties that handle the mail. The envelope includes a multitude of symbols with different design criteria, purposes, messages and histories. The printing systems (transmitters) produce the various symbols under different,

often difficult conditions at several pieces per second. Postal equipment processes the mail at ten pieces per second and must take actions based on the messages contained on the envelope. The symbols include an interesting collection of redundant information including error correction codes, error detection codes, and cryptographic authentication. This presentation will describe the properties and purposes of several of the symbols found on the paper channel.

Bio: Robert Cordery, as a Principal Fellow in the Secure Systems Group at Pitney Bowes, has played a key role in the evolution of cryptographically secured postage evidencing. Robert's other research interests include formal methods for protocol analysis, graphic security, printed watermarks, bar code grading and modeling ink-paper interactions.

****

2:45-3:00: Coffee break

3:00-3:30
Speaker: Ramesh Karri (Polytechnic University, Brooklyn; rkarri@duke.poly.edu)

Title: Towards Securing Hardware Designs

Abstract: A 2005 Defense Science Board Task Force paper highlighted new and important security risks that are incurred when defense-related semiconductor components are fabricated in offshore foundries. Because intellectual property and military secrets are intrinsically incorporated into the design of integrated circuits, they are vulnerable to exposure during the “hand-off” process between trusted design teams and commercial fabrication facilities. Rogue elements may insert malicious circuits that compromise or deliberately degrade components at some point during their life cycle. Furthermore, intellectual property may be compromised by reverse engineering of manufactured designs, post-silicon monitoring and analysis of power signatures, or by timing and other side channel activity.

New devices must be capable of safe and scalable production in “untrusted” commercial foundries, obfuscate the function and the mission of the device such that adversarial misuse is minimized or impossible and incorporate tamper-proof and radiation-hardened-by-design techniques. In this talk, we will describe SECUREFABRIC, a distributed reconfigurable infrastructure that may be inserted into a design and configured in a secure fashion at run time so as to obfuscate various parts of a design including controllers and data paths.

Bio: Ramesh Karri received his MS in Computer Engineering and a PhD in Computer Science from the University of California, San Diego in 1992 and 1993 respectively. Ramesh Karri has pioneered computer aided design of Fault Tolerant VLSI Systems as part of his Ph.D. dissertation and is a recognized expert in fault-tolerant VLSI Design. He has advised Masters and Ph.D. dissertations in this area. More recently, he has developed design methods and methodologies for Trusted Integrated Circuits Design.

Ramesh Karri has several publications in the areas Design and Test of Trusted Integrated Circuits Design (eeweb.poly.edu/karri/rameshkarri/, eeweb.poly.edu/karri/encryption), CAD of fault-tolerant VLSI Systems, Low power design, High Level Synthesis and Design for Reliability of Deep Submicron VLSI. He was the recipient of an NSF CAREER award. He has served on the DARPA Information Sciences and Technology Study on Trusted Integrated Circuits. This study is identifying and defining the Design, CAD and Test related problems and solutions to Trusted Integrated Circuits.

During 1993-98 he was an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Massachusetts at Amherst. During 1997-98 he was member of technical staff at Bell Labs, Lucent technologies. There he initiated the research and development effort in on-line built-in self test of VLSICs. Since August 1998 he is an Associate Professor of Electrical Engineering at Polytechnic University, Brooklyn, NY. His research interests include Design for Trust, CAD for Trust, CAD for Fault-

Tolerance, Re-configurable computing and Hardware-Software Co-Design. He was the recipient of an NSF CAREER award and an Alexander Von Humboldt Fellow at the University of Potsdam, Germany. He is member of IEEE and Chair of the IEEE Task Force on Nanoarchitectures. He has served on several program committees including IEEE Workshop on Fault Diagnosis and Tolerance of Crypto Systems (2004, 2005, 2006). He is the founding chair of the IEEE workshop on nano architectures (2005, 2006, 2007).

3:30-4:00
Speaker: Darrel Hankerson (Auburn University; hankedr@auburn.edu)

Title: Implementation of pairing-based protocols based on supersingular elliptic curves

Abstract: Fast arithmetic for characteristic three finite fields is desirable in pairing-based cryptography because there is an associated family of elliptic curves with embedding degree 6. We develop structure results for Gaussian normal bases that significantly speed multiplication, and compare with methods for polynomial bases. Finally, we compare the speed of encryption and decryption for the Boneh-Franklin and Sakai-Kasahara identity-based encryption schemes at the 128-bit security level, in the case where supersingular elliptic curves with embedding degrees 2, 4, and 6 are employed.
This work is joint with Omran Ahmadi and Alfred Menezes.

Bio: Darrel Hankerson received an M.Sc. in mathematics and computer science from Mankato State University (Minnesota) in 1982, and a Ph.D. in mathematics from the University of Nebraska-Lincoln in 1986. Since then he has been a professor of mathematics at Auburn University.

Darrel is co-author of two undergraduate textbooks, "Introduction to Information Theory and Data Compression" and "Coding Theory and Cryptography". Along with Alfred Menezes and Scott Vanstone, he is a co-author of the recent Springer "Guide to Elliptic Curve Cryptography".

Although his graduate work was in differential equations, he now works primarily in cryptography. Much of this work has focused on efficiency issues for methods based on elliptic curves. He has been a frequent visitor to the University of Waterloo and its Centre for Applied Cryptographic Research.

4:00-4:30
Speaker: Lisa Yin (PB Consultant; yiqun@alum.mit.edu)

Title: Hash Functions and Hash-Based Security Protocols

Abstract: Cryptographic hash function is an important building block in almost all security applications. It is a necessary component in digital signatures. Besides, it is also used in various security protocols such as message authentication, random number generation, secure mail, and electronic payment. In the past few years, there have been major advances in the cryptanalysis of hash functions, and several widely used hash standards have been broken. A nature question is how these attacks affect the security of hash-based protocols. In this talk, we will first examine several hash-based protocols and identify properties of the hash function that are necessaryto ensure the security of upper-layer protocols. We will then present new collision attacks on the X.509 digital certificates and key-recovery attacks on the HMAC authentication protocol. These results show that the strength of a security protocol can be greatly weakened by the insecurity of the underlying hash function.

Bio: Dr. Yin is an independent security consultant based in Connecticut. She has over fifteen years of research and industry experience in cryptography and security. She held positions as director of security technologies at NTT Labs in California, senior scientist at RSA Labs, and visiting researcher at Princeton University. She received her Ph.D. in Applied Mathematics from MIT in 1994.

****