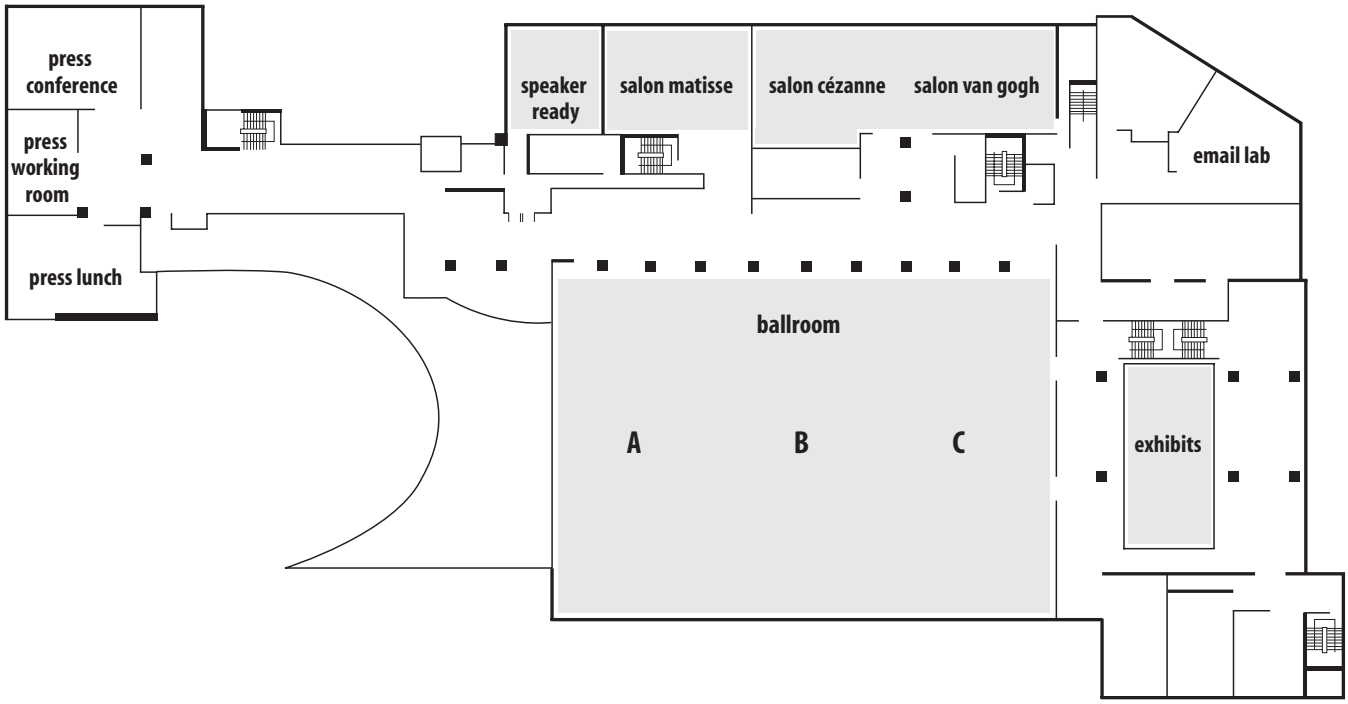
	monday, 10. april	tuesday, 11. april	wednesday, 12. april	thursday, 13. april
AM		**General Sessions** 9:00 am-12:30 pm **Expo** open 10:00 am-8:00 pm	**General Sessions** 8:00 am-12:30 pm **Expo** open 10:00 am-6:00 pm	**Class Tracks** 8:00 am-11:00 am
PM	**(optional) Tutorials** 2:00 pm-6:00 pm	**Class Tracks** 2:00 pm-6:15 pm	**Class Tracks** 2:00 pm-6:15 pm	**Closing Sessions** 11:15 am-1:15 pm
EVENING	**Welcome Reception** 6:00 pm-8:00 pm	**Expo Reception** 6:00 pm-8:00 pm (Expo Open)	**Gala** 7:00 pm-11:00 pm	



monday, 10. april

Monday Tutorials. The RSA Conference has traditionally been the gathering of industry insiders – but as the applications of security technologies have broadened, so have our audiences. To make sure that you get the most out of the Conference, we are pleased to offer special Monday Tutorials.

The Tutorials are designed to help professionals who are new to crypto and security technologies get a fundamental understanding of concepts that will be discussed during the week. The Tutorials are also a useful "refresher course," reinforcing the basics in preparation for more advanced classes.

TUTORIALS

	CRYPTOGRAPHY BASICS TUTORIAL Salon Van Gogh	ENTERPRISE SECURITY BASICS TUTORIAL Salon Matisse	PKCS BASICS TUTORIAL Salon Cézanne
2:00 pm	**Crypto 101: Intro to Cryptographic Concepts** Steve Burnett, *RSA Security Inc.*	**Enterprise Security 101: Intro to Public Key Infrastructure** Andrew Nash, *RSA Security Inc.*	**PKCS 101: Introduction to the Public Key Cryptography Standards** Jakob Jonsson, *RSA Laboratories Europe*
3:00 pm	**Crypto 201: Advanced Cryptographic Concepts** Steve Burnett, *RSA Security Inc.*	**Enterprise Security 201: Advanced PKI** Andrew Nash, *RSA Security Inc.*	**PKCS 102: An ASN.1 Primer** Magnus Nyström, *RSA Laboratories*
4:00 pm	**Crypto 202: Overview of Security Protocols** Dr. Jay McCauley, *RSA Security Inc.*	**Enterprise Security 202: Authentication Options for PKI** Andy Kemshall, *RSA Security Inc. United Kingdom*	**PKCS 201: Cryptographic Techniques and Message Formats** Jakob Jonsson, *RSA Security Inc.*
5:00 pm	**Crypto 301: Practical Implementations of Cryptography** Dr. Jay McCauley, *RSA Security Inc.*	**Enterprise Security 301: Making Applications PKI-Ready** Bronislav Kavsan, *RSA Security Inc.*	**PKCS 202: Cryptographic Tokens and Data** Magnus Nyström, *RSA Laboratories*

Welcome Reception 6:00 pm to 8:00 pm Salon Sapporo/Marco Polo

tuesday, 11. april

MORNING

KEYNOTE AND GENERAL SESSIONS Ballroom

9:00 am	**Welcome** Jim Bidzos, *RSA Security Inc.*
9:15 am	**E-security Strategies for the New Millennium** Scott Schnell, *RSA Security Inc.*
10:30 am	**Cryptographers' Panel** Burt Kaliski, *RSA Laboratories;* Walter Fumy, *Siemens AG;* Claus P. Schnorr, *J.W. Goethe University Frankfurt;* Dr. David Naccache, *Gemplus, France;* Dr. Kaisa Nyberg, *Nokia Finland*
11:30 am	**Whose Risk Is It Anyway?** Dr. Charles Palmer, *IBM*

AFTERNOON

	2:00 pm	3:00 pm	4:15 pm	5:15 pm
CRYPTOGRAPHERS' TRACK Ballroom C	**Key Generation with Implicit Key Recovery** Nicko van Someren, *nCipher Corporation Ltd.*	**FIPS 140-2 and Common Criteria Certification** John Hines, *Netscape/Sun Alliance;* John Morris, *Corsec Security, Inc.;* Ray Snouffer, *NIST;* Dr. Sean W. Smith, *IBM T.J. Watson Research Center*	**WAP's WTLS Protocol – Lessons Learnt** Magnus Nyström, *RSA Laboratories*	**The Advanced Encryption Standard: Development and Status** Ray Snouffer, *NIST*
DEVELOPERS' TRACK Ballroom A	**Certificate Considerations in Wireless Environments** Dr. Warwick Ford, *VeriSign Inc.*	**Utilizing Secure Hardware** Joan Dyer, *IBM*	**Digitally Signed XML: A New Internet Standard** Barbara Fox, *Microsoft*	**Passwords: Beyond the Terminal Interaction Model** Niklas Frykholm, *RSA Laboratories*
IMPLEMENTERS' TRACK Ballroom B	**Wireless Payment Solutions** Marcus Berglund, *Parallel Consulting Group AB*	**Implementing a Wireless PKI to Secure Financial and Healthcare Applications** Michael Crerar, *Diversinet Corporation*	**Windows 2000 Authentication: Under the Hood** Jan De Clercq, *Compaq Computer EMEA BV*	**Requirements for a Card Management Infrastructrure** Laurent Den Hollander, *Gemplus*
NEW PRODUCTS TRACK Salon Cézanne/Van Gogh	**IPlanet Certificate Management System 4.2** John Hines, *Netscape/Sun Alliance*	**Network Security Beyond Firewalls and VPN's** Tomas Olovsson, *AppGate*	**Super Scalable Server-Based S/MIME for the Enterprise** Blake Ramsdell, *Tumbleweed Communications*	**Building an Enterprise PKI** Bob Pratt, *VeriSign Inc.*
RSA PRODUCTS TRACK Salon Matisse	**RSA BSAFE® SSL-C In-Depth** Tim Hudson, *RSA Security Inc.*	**Encryption for Worldwide Markets: Developing Applications with RSA BSAFE® Crypto** Steve Burnett, *RSA Security Inc.*	**PKI Case Study: Enabling Secure Inter-Company Collaboration** Lina Liberti, *RSA Security Inc.*	**Enabling PKI with the RSA BSAFE® Cert Tools** Marina Milshtein, *RSA Security Inc.*

Expo Reception 6:00 pm to 8:00 pm Foyer Ballsaal

wednesday, 12. april

MORNING

KEYNOTE AND GENERAL SESSIONS Ballroom

8:00 am — **VeriSign Keynote**
Dr. Warwick Ford, *VeriSign* Inc.

9:00 am — **More Machines Than People**
Professor Peter Cochrane, *BT Laboratories*

10:30 am — **Privacy and Security Challenges in an Era of Non-Stop, Continuously Available Computing**
Andrew Dixon, *Compaq Computer EMEA BV*

11:30 am — **Security in Electronic Communication – The EU Approach**
Richard Schlechter, *European Commision*

Optional Lunch Hour Session

12:30 pm — **PKI Forum Member Companies: PKI Interoperability*** This session will be held in the Salon Matisse.
Seating is limited to 80 people.

AFTERNOON

	2:00 pm	3:00 pm	4:15 pm	5:15 pm
CRYPTOGRAPHERS' TRACK Ballroom C	**Proofs of Knowledge of Discrete Logarithms and Applications** Marc Girault, *France Telecom/CNET*	**Fast Monte-Carlo Primality Evidence Shown in the Dark** Dr. Wenbo Mao, *Hewlett-Packard Laboratories*	**Why Hyperelliptic Curves Might Be More Secure than Elliptic Curves** Detlef Huehnlein, *Secunet AG*	**Privacy and Security of Public Databases** Dr. Susanne Wetzel, *Lucent Technologies – Bell Laboratories*
DEVELOPERS' TRACK Ballroom A	**Time Stamping Services – Motivation and Basic Techniques** Roland Mueller, *TUVIT, Inc.*	**Why Europe Hesitates to Buy American Electronic Stamps** Detlef Huehnlein, *Secunet AG*	**Cryptography and Biometrics in Banking** Vashek Matyás Jr. , *Ubilab; UBS AG*	**IPsec, A General Solution for Securing the Internet** Tatu Ylönen, *SSH Communications Security Ltd.*
IMPLEMENTERS' TRACK Ballroom B	**Nordic Standardization Moves to Interesting Implementations** May-Lis Farnes, *SEIS*	**Do-it-Yourself Certification Authorities: The Legal Toolkit** Samoera Jacobs, *GlobalSign*	**Deploying S/MIME in the Enterprise** Blake Ramsdell, *Tumbleweed Communications*	**Certificate Based Access Control Mechanisms for the Web** Scott Shorter, *CygnaCom Solutions*
NEW PRODUCTS TRACK Salon Cézanne/Van Gogh	**Lock up Your Keys! The nCipher Key Management Tool** Alex van Someren, *nCipher Corporation Ltd*	**Taking Care of the 'I' in PKI: Managed PKI Services** Peter Forret, *GlobalSign*	**Extraordinary Extranets: Effectively Teaming VPN's and PKI** Melanie Ciosek Francis, *CyberTrust Solutions* John Summers, *GTE Internetworking*	**End to End Security and Trust** Sam Asseer, *LCI Technology Group*
RSA PRODUCTS TRACK Salon Matisse	**RSA Keon® Agent Software Developer Kit** Per Eliasson, *RSA Security Inc.*	**RSA Keon® Single Sign-On Software Developer Kit (SSO)** Per Eliasson, *RSA Security Inc.*	**RSA SecurID® in a Wireless Environment** Göran Walles, *RSA Security Sweden*	**RSA SecurID® for Web Applications** Norbert Olbrich, *RSA Security Germany*

Cryptographers' Gala 7:00 pm to 11:00 pm Löwenbräukeller *(Coaches will depart from the Hiltons München Park and City from 6:45 pm-7:30 pm)*

thursday, 13. april

MORNING

	8:00 am	9:00 am	10:00 am
CRYPTOGRAPHERS' TRACK Ballroom C	**Further Lessons in Protocol Design: Unknown Key-Share Attacks and the MQV Key Agreement Protocol** Burt Kaliski, *RSA Laboratories*	**How to Puzzle an Attacker** Dr. Ari Juels, *RSA Laboratories*	**High Speed RSA Hardware Implemented in Dynamic True Single Phase Clocked Logic** Johann Groszschaedl, *Graz University of Technology*
DEVELOPERS' TRACK Ballroom A	**Replacing the Smart Card PIN: Fingerprint Matching on 8-bit Smart Cards** Anthony Russo, *Veridicom, Inc.*	**Crypto Policy and Technological Development for Global Markets** Ian Walker, *Entrust Technologies*	***Special Presentation Threats and Lies: Hacker, Viruses and Spys*** Dr. Christian Fill, InformationWeek
IMPLEMENTERS' TRACK Ballroom B	**What to Look at in a Practical PKI** Dominic Storey, *RSA Security*	**Case Study: Italy Moving Business into the Digital Age with a National CA** Trevor Thomas, *CyberTrust;* Mr. Vinetti, *SIA*	**Xcert Gold Sponsor Lecture** Kevin Bocek, *Xcert International Inc.*
NEW PRODUCTS TRACK Salon Cézanne/Van Gogh	**How To Safely Integrate Your Back-Office To The Web: An Intro to Air Gap Technology** Yair Tsoran, *Whale Communications*	**MAILguardian Enterprise: The Ultimate Enterprise E-Mail Security Solution** Raviv Karnieli, *Vanguard Security Technologies Ltd.*	**Open Source and Security Software** Terry A. Smith, *Intel Corporation;* Guest Speaker, *Trustworks TBA;* Guest Speaker, *Checkpoint TBA*
RSA PRODUCTS TRACK Salon Matisse	**RSA SecurID® in a Managed Service Environment** Jonathan Smith, *RSA Security United Kingdom*	**RSA SecurID®: A Critical Component of Your PKI** Ted Kamionek, *RSA Security Inc.*	**Professional Services: Providing Solutions with Services** Fabien Séheux, *RSA Security United Kingdom*

KEYNOTE AND CLOSING SESSIONS Ballroom

11:15 am — **Securing Electronic Business**
Roger Farnsworth, *Cisco Systems*

12:15 pm — **From Cellular Phone to Personal Trusted Device**
Ilkka Raiskinen, *Nokia Mobile Phones, Finland*

parties & receptions

monday, 10. april

Welcome Reception
6:00 pm to 8:00 pm
Salon Sapporo/Marco Polo – 15th Floor

tuesday, 11. april

Expo Reception
6:00 pm to 8:00 pm
Foyer Ballsaal

wednesday, 12. april

Cryptographers' Gala
7:00 pm to 11:00 pm Löwenbräukeller
Coaches will depart from the Hilton's München Park and City from 6:45 pm-7:30 pm

cryptography basics tutorial

2:00 pm **Crypto 101: Intro to Cryptographic Concepts**
Steve Burnett, *RSA Security Inc.*

The importance of cryptography as a foundation for e-commerce has transformed what was once an obscure discipline into an essential part of the working knowledge of every IT professional. This session explains the key concepts of modern cryptography, including high-level descriptions of public key, symmetric key, message digests, digital envelopes, digital signatures, and digital certificates.

With degrees in math from Grinnell College in Iowa and the Claremont Graduate School in California, **Steve Burnett** has spent most of his professional career converting math into computer programs, first at Intergraph Corp. and presently with RSA Security. A frequent speaker at industry conferences, Mr. Burnett is the lead engineer for RSA's BSAFE® Crypto-C and Crypto-J products – general purpose cryptography software development kits in C and Java.

3:00 pm **Crypto 201: Advanced Cryptographic Concepts**
Steve Burnett, *RSA Security Inc.*

In order for IT professionals to make well-informed decisions about which encryption technologies to apply to various e-business applications, it is important to have a working understanding of the strengths and weaknesses of the various algorithms within each family of cryptography. This session presents more technical (algorithmic-level) descriptions of block ciphers, stream ciphers, RSA, DSA, Diffie-Hellman, and Elliptic Curve algorithms, and provides an update on the development of a new AES standard.

4:00 pm **Crypto 202: Overview of Security Protocols**
Dr. Jay McCauley, *RSA Security Inc.*

Like diplomats from different countries, the myriad heterogeneous systems that make up the global Internet need a set of standard protocols, which enable interoperable security on the Internet, represent another crucial set of technologies that support e-commerce. This session describes the most important security protocols for today's market, including SSL, S/MIME, IPSec, and SET.

Dr. Edwin J. McCauley (Jay) is the Director of BSAFE® Development at RSA Security, Inc. Prior to RSA, Dr. McCauley worked for SGI in a number of different OS and communications product development and marketing positions. He managed the development of Trusted IRIX/CMW, SGI's B1 secure level secure operating system, and it's formal evaluation by the US National Computer Security Center. He received his Ph.D. in Computer and Information Science from Ohio State University where his dissertation dealt with database security.

5:00 pm **Crypto 301: Practical Implementations of Cryptography**
Dr. Jay McCauley, *RSA Security Inc.*

Cryptographic technologies are only useful when they are actually implemented and deployed in meaningful e-business applications. This session provides a high-level over-view of the various toolkits available to software developers for implementing cryptographic security in their products using C and Java, and includes a few simple live examples using RSA's BSAFE® products.

enterprise security basics tutorial

2:00 pm **Enterprise Security 101: Intro to Public Key Infrastructure**
Andrew Nash, *RSA Security Inc.*

Public Key Infrastructure is widely believed to be the crucial enabling technology for large-scale, secure e-commerce. For many organizations, PKI will soon constitute the core of their Internet security infrastructure. For IT professionals with no previous knowledge of PKI, this session provides a high-level description of a PKI's essential components, how PKIs function, and how PKIs can effectively co-exist and interoperate.

Andrew Nash is Director of PKI Standards and Technologies at RSA Security. Mr. Nash joined RSA in March of 1997. He was one of the architects for the Keon® Advanced PKI product line, and is co-chair of the PKI Forum Technical Working Group. Mr. Nash was a Technical Director for a Digital Equipment Corporation engineering group in Australia that dealt with migrating technologies such as Alta Vista Search, Network Computers and Micro Cash Payment systems from Digital's research labs into product development. His background is in Networking protocols and development of Unix Kernel code.

3:00 pm **Enterprise Security 201: Advanced PKI**
Andrew Nash, *RSA Security Inc.*

Building on the Intro to Public Key Infrastructure provided by Enterprise Security 101, this session describes in greater detail the solutions to some of the practical issues involved in the deployment and operation of secure e-business applications using PKI technologies. Specifically addressed is the management of keys and digital certificates throughout their entire life cycle, including registration, certification, distribution, protection of the private key by the end-user, update, backup and recovery, revocation, and certificate validation.

4:00 pm **Enterprise Security 202: Authentication Options for PKI**
Andy Kemshall, *RSA Security Inc. United Kingdom*

Analogous to a passport, public key certificates are digital documents that attest to the binding of a specific public key to a specific individual. It is important to understand, however, the risks and limitations of software-based certificates. This session describes the many options for strong, standards-based authentication for PKI-based applications, including the use of certificates in conjunction with tokens, smart cards, virtual smart cards, and biometrics.

Mr. Kemshall is the EMEA Technical Manager for RSA, he has worked for RSA for 5 years and been in the IT industry for over 15 years. He has been involved with PKI and Keon® for the past 3 years.

5:00 pm **Enterprise Security 301: Making Applications PKI-Ready**
Bronislav Kavsan, *RSA Security Inc.*

Organizations have come to realize the value of protecting and controlling access to their mission-critical data and back-end applications based on a common security infrastructure. Not all applications are natively PKI-aware. However, this session describes the pros and cons of several methods – including toolkits, agent technology, and Web-based front-ends – to PKI-enable existing applications, and provides insights into how various application segments are evolving to take advantage of PKI.

Bronislav Kavsan is a Vice President of Engineering at RSA Security where he leads the Advanced PKI engineering organization. This organization is responsible for implementing the Keon® family of PKI products. Prior to joining RSA in 2000, Mr. Kavsan was a Senior Systems Architect at IRE, an engineering firm specializing in developing VPN products. At IRE he lead various Network Security projects, including Public Key Security Systems and IPSec Client. Previously, Mr. Kavsan was a Technical Manager at AT&T/Lucent Bell Laboratories, where for almost 15 years he led various engineering projects in Data Communications Protocols, such as OSI and TMN for SONET/SDH networks.

pkcs basics tutorial

2:00 pm **PKCS 101: Introduction to the Public Key Cryptography Standards**
Jakob Jonsson, *RSA Laboratories Europe*

First published in 1991, the PKCS series has been widely referenced and implemented by developers of public-key technology. The PKCS documents address many aspects of PKI, from cryptographic algorithms to message formats to tokens and storage. This session provides a general overview of the PKCS series, its major deployments, and its role in standards development.

Jakob Jonsson joined RSA Laboratories in the fall of 1999 and is part of the research staff. Before he started working for RSA, he received a licentiate degree in mathematics, which requires two years of post-graduate studies and includes a written thesis. He is particularly interested in mathematical aspects of cryptography.

3:00 pm **PKCS 102: An ASN.1 Primer**
Magnus Nyström, *RSA Laboratories*

Originally developed for specifying OSI standards, ASN.1 Abstract Syntax Notation One is the underlying specification language of the PKCS documents, as well as, many PKI technologies. This session gives an overview of the language, as well as, several of the encoding rules for representing values as strings, including the Basic Encoding Rules (BER), Distinguished Encoding Rules (DER), and Packet Encoding Rules (PER).

Magnus Nyström joined RSA Laboratories in 1998. His research interests include smart cards, security architectures and cryptographic protocols. He received his M.S. from the University of Uppsala, Sweden in 1990 and has been working in the field since then. In 1996, he joined the Swedish company DynaSoft, later acquired by Security Dynamics Inc., where he held a position as an Engineering Manager with responsibility for implementations of Public Key Technology.

4:00 pm **PKCS 201: Cryptographic Techniques and Message Formats**
Jakob Jonsson, *RSA Security Inc.*

Many of today's PKI standards and proposed standards are derived in some way from the four PKCS documents related to cryptographic techniques and message formats. PKCS #1: RSA Cryptography Standard, specifies encryption and signature schemes based on the RSA algorithm, and has been incorporated in the SSL and S/MIME protocols; most certificates are signed with the algorithm specified in PKCS #1. PKCS #5: Password-Based Cryptography, gives general constructions for encrypting private keys and other data with passwords. PKCS #7: Cryptographic Message Syntax, specifies formats for signed and encrypted messages, and is the basis for the S/MIME and SET protocols. And PKCS #10: Certification Request Syntax, is an option in the PKIX Certificate Management Protocols (CMP). This session will give an overview of those four documents, as well as, their relationship to the industry standards that include them.

5:00 pm **PKCS 202: Cryptographic Tokens and Data**
Magnus Nyström, *RSA Laboratories*

Perhaps the most significant impact of the PKCS series has been in areas beyond the algorithms, relating to the storage and exchange of cryptographic data and implementation of cryptographic modules. This session will describe the three PKCS documents of this class. PKCS #11, also known as Cryptoki, is a cryptographic programming interface for smart cards and other cryptographic tokens. Technology – and algorithm – independent, it supports many different token types from Fortezza cards to RSA smart cards to software tokens. PKCS #12 was defined for the exchange of cryptographic data such as keys and certificates between PKI components. PKCS #15, aimed to support PKCS #11 implementations (but not dependent on PKCS #11) as well as to replace PKCS #12, provides a flexible and general way of representing stored cryptographic data, whether in a smart card or on a desktop. PKCS #15 is also the basis for several electronic ID standards projects.

9:00 am **Welcome**
Jim Bidzos, *RSA Security Inc.*

The conference will open with a special presentation and a "not to be missed" entrance from Jim Bidzos. Join us for Jim's grand opening and the security year in review.

Jim Bidzos was President of RSA Security for over twelve years, and has recently assumed the mantle of Vice Chairman of the Board. Under his leadership, RSA Security has become the worldwide de facto standard for encryption, being included in such products as Lotus Notes, Novell Netware, Netscape Navigator, Intuit's Quicken, and Microsoft Windows 95. There are close to a half billion copies of RSA software in use today, making RSA the most widely distributed code on earth.

9:15 am **E-security Strategies for the New Millennium**
Scott Schnell, *RSA Security Inc.*

E-security has become a vital component of nearly every company's strategy as they are driven by the rush to e-business. Yet yesterday's security policies and practices are at risk in this new environment. Companies must use e-security as a strategic asset for both enablement and control. Join RSA Security's Scott Schnell to examine the trends driving the use of e-security and effective strategies for building a secure e-business.

Scott Schnell is senior vice president of marketing for RSA Security, where he directs the global marketing and communications efforts for the company. Mr. Schnell joined RSA as a vice president of marketing in 1996, where he was responsible for building the marketing organization and developing the company's long-term strategy. His vision and strategy was recently realized with the relaunch of the company and its new PKI product line in September 1999, elevating RSA Security's position as a leader in e-business security and becoming one of the world's preeminent software companies. Previously, Mr. Schnell spent 15 years in product and strategic marketing positions at Apple, Photonics and McKinsey and Company.

10:30 am **Cryptographers' Panel**
Burt Kaliski, *RSA Laboratories;* Walter Fumy, *Siemens AG;* Claus P. Schnorr, *J.W. Goethe University Frankfurt;* Dr. David Naccache, *Gemplus, France;* Dr. Kaisa Nyberg, *Nokia Finland*

A perennial favorite. Join us for a traditional RSA Conference cryptographers' round table and learn what is on the security horizon.

Dr. Burt Kaliski received B.S., M.S., and Ph.D. degrees in computer science from MIT in 1984, 1987, and 1988 respectively. In 1989, he joined RSA Security and since 1991 has been chief scientist of RSA Laboratories. Dr. Kaliski has served as general chair of CRYPTO '91, program chair of CRYPTO '97, and chair of the IEEE P1363 working group.
Dr. Walter Fumy is Vice President of Trusted Networks & Applications at Siemens AG where his work ranges from cryptographic research to security consulting. He is actively involved in the standardization ranges from cryptographic research to security consulting. He is actively involved in the standardization of cryptographic techniques, serves as vice-chairman of ETSI TC Security, and is chairman of ISO/IEC JTC 1/SC 27 "IT Security Techniques."
Dr. Kaisa Nyberg's career in Cryptography spans over more than ten years. She has written a number of scientific papers on digital signatures and design of block ciphers, and acted as editor for international standards on digital signatures. She chaired the program committee of EUROCRYPT'98 and has served in several other scientific committees. In 1998 she joined Nokia and is now responsible for cryptographic techniques in cellular security and related mobile applications.
Dr. David Naccache is the director of Gemplus' cryptography and security department (40 researchers). His current research interests are public key cryptography, tamper-resistance and Java security.
Before his current job he was with Philips TRT where he worked on various smart card projects and with Thomson Multimedia, where he was involved in the design of Pay-TV decoders and smart cards.

11:30 am **Whose Risk Is It Anyway?**
Dr. Charles Palmer, *IBM*

Security and privacy are regularly cited as the top issues on the minds of e-business leaders and their customers. Both of these issues can be expressed as risk management challenges. E-businesses must clearly identify what to protect and what it is worth. This information guides the definition of policies and the selection of tools to effectively mitigate those risks. This presentation will describe risk management best practices for businesses on the Internet.

Dr. Palmer manages the Network Security and Cryptography department at IBM's Thomas J. Watson Research Center. His teams work in the areas of cryptography research, internet security technologies, Java security, and the Global Security Analysis lab, which he helped found in 1995. The GSA lab – also known as the "ethical hackers" – represents IBM's center of expertise in the areas of applied computer and network security research and development. Dr. Palmer frequently speaks on the topics of computer and network security at conferences around the world. He has also been an adjunct professor of computer science at Polytechnic University since 1993.

c cryptographers' track
d developers' track
i implementers' track
p new products track
r RSA products track
5 high
technical level
1 low

c 5

Key Generation with Implicit Key Recovery

Nicko van Someren, *nCipher Corporation Ltd.*

Research papers published by Dr. Nicko van Someren and Prof. Adi Shamir show a set of theoretical attacks which indicate that storing cryptographic keys in software might not be as secure as many designers had previously thought. In this presentation, the ways in which these and other theoretical attacks can be turned into practical attacks which can be used by criminals to compromise real systems will be discussed. Systems that are particularly vulnerable will be revealed to show that in practice a great many systems which rely on Public Key Infrastructure are in a state of 'clear and present danger.' As well as talking about the ease of implementation of these attacks, a live demonstration of some of the possible attacks in action will be presented. A simple web server script, running without any special privileges, which can extract the private keys from a running web server will be presented. After demonstrating the ease of this type of attack, different ways in which people can protect systems against any attack in this class will discussed. This will be a discussion of the issues surrounding hardware key storage and several prevention methods which can close the door to an attacker. Ultimately, practice hardware security modules are the only reliable solution to the key storage problem.

Nicko van Someren is Chief Technical Officer and a co-founder of nCipher. Nicko has almost 20 years of experience in cryptography, software and hardware product development, and academic research. He holds a doctorate and first class degree in Computer Science from Trinity College, Cambridge, England. He maintains contacts in the academic community, particularly with the Computer Laboratory at Cambridge University, and recently co-authored a research paper on key hiding which attracted worldwide press attention.

d 5

Certificate Considerations in Wireless Environments

Dr. Warwick Ford, *VeriSign Inc.*

The security of wireless Internet applications depends upon digital certificates and PKI in much the same way as wired Internet applications. This presentation addresses these types of issues, and also looks more generally at how the design of PKI for wireless environments can benefit from past experiences with PKI for the wired Internet.

Dr. Warwick Ford is Chief Technology Officer at VeriSign, Inc., the provider of Internet trust services for e-commerce, enterprises, and the public. Dr. Ford is a recognized authority on the application of public-key technology, and led the development of digital certificate standards in ISO and the Internet community. He is co-author of the 1997 Prentice Hall book "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption."

i 3

Wireless Payment Solutions

Marcus Berglund, *Parallel Consulting Group AB*

Within two years, more than 50 percent of all terminals connected to the Internet will be cellular phones or mobile terminals. The potential for creating new applications and services are enormous. The key for functionality is secure and user-friendly Internet payment methods. This presentation gives an overview over existing payment methods and if they can be used in a wireless environment. Examples of applications and services are games, IP-telephony and multimedia. Relevant questions are: – Is it possible to use current payment standards? – Is the functionality in today's wireless terminals, like SMS, SAT and WAP 1.1, enough for creating secure payments? – Is there a need for a wire-less PKI? The conclusion is that new payment methods are required. Jalda™ is proposed as a candidate for an open standard for Internet payments, including wireless Internet payments. The idea is simple but powerful. It is based on signed contracts and ticks, which makes it suitable for all kinds of payments, including session based micro-payments and macro-payments. Ticks is an imaginary currency which is translated to the local currency.

Marcus Berglund received a B.S. in mathematics and a Ph. lic. in numerical analysis from the University of Stockholm. His creditials include Parallel Consulting Group AB; design and implementation of Certificate Management System at iD2; winner of the well respected Grand Prize at the European IT Prize awards 1998 (www-it-prize.org); Design and implementation of smart card support and card reader support. From 1996 to 1997 Mr. Berglund was a consultant at the Swedish Defense, where he focused on design and modification of DCE's security protocols for defense crypto hardware like smart cards and encryption boards. He was also involved with ITSEC, security target review of middleware for Swedish defense. From 1997 to 1998 he was a consultant at Ericsson, Hewlett-Packard Telecommuncations AB. Today he is the chief designer of security solutions and architecture for Ericsson's Internet Payment System (Jalda ™, see www.jalda.com).

p 3

IPlanet Certificate Management System 4.2

John Hines, *Netscape/Sun Alliance*

Sun/Netscape Alliance will present the architecture of its IPlanet Certificate Management System 4.2 product. Technical details of the product will be presented along with possible deployment scenarios. Details about interoperability with a variety of client, servers, VPN, CA, toolkit and hardware vendors will also be presented.

John Hines is the engineering manager for Certificate Management System and Security Tools. He is also responsible for Netscape's FIPS 140-1 validation efforts, and various other security analysis tasks at Netscape. Prior to Netscape, he was an MTS at AT&T Bell Laboratories where he worked on a number of security related products and services.

r 5

RSA BSAFE® SSL-C In-Depth

Tim Hudson, *RSA Security Inc.*

Developers of secure applications need to know how to implement SSL properly in their software. Servers can be designed to handle multiple connections in a number of fashions. This talk covers the issues surrounding implementing SSL-C to fit your needs. Topics will cover writing basic clients and servers, and C-specific issues, such as socket programming.

Tim Hudson has been involved in the field of network and system security for the last 15 years, starting with his initial exposure to networked Unix systems in 1984. Since graduating with a B.Sc. (Hons) from the University of Queensland, he has worked on network protocol implementations, system security analysis, large-scale commercial distributed transaction processing systems, high-end performance analysis and tuning in Unix environments, and cross-platform portability environments. He has extensive experience in the application of security architectures to real-world problems. Since 1995, he has been deeply involved in applying and adapting SSL to a wide range of problems on a wide range of platforms. He is also the author of all the initial SSL applications provided along with SSLeay. As Technical Director of Development for RSA Australia, he continues to direct the development of RSA BSAFE® SSL-C (and other RSA Australia products) to solve the real security problems facing today's application developers.

FIPS 140-2 and Common Criteria Certification

c 4

John Hines, *Netscape/Sun Alliance;* John Morris, *Corsec Security, Inc.;*
Ray Snouffer, *NIST;* Dr. Sean W. Smith, *IBM T.J. Watson Research Center*

FIPS 140-2 has become the de facto standard for cryptographic conformance in the U.S., Canada, and the financial community. Worldwide acceptance of FIPS 140-2 and ANSI X9.66 is growing. However, Common Criteria (CC) evaluations hold international recognition. Join a panel of FIPS 140-2 experts to discuss international cryptographic certification and evaluation of FIPS 140-2 in a CC protection profile. John Morris, the former manager of FIPS 140-2 certification laboratory will moderate this in-depth analysis of the CC and FIPS 140-2 certification process, documentation requirements, and strategies for streamlining product design, documentation, and certification. Panelists will share realworld FIPS 140 and CC cetification experiences from leading security companies, and respond to audience questions with candid discussion of certification strategies, costs, and times.

John Morris is President and founder of Corsec Security. Mr. Morris is the former manager of a NVLAP accredited FIPS 140-1 testing laboratory, and holds degrees in Electrical Engineering, Telecommunications and Computers.
John Hines is the Engineering Manager for Netscape's Certificate Management System product and Security Tools. Mr. Hines is also responsible for Netscape's FIPS 140-1 validation efforts, and various other security analysis tasks at Netscape. Prior to Netscape, Mr. Hines was an MTS at AT&T Bell Laboratories where he worked on a number of security related products and services.
Ray Snouffer began his career with the Defense Information Systems Agency (DISA) serving in a variety of roles including senior mathematician, lead software developer, and Project Officer for the Strategic Defense Analysis Project. He was National Program Manager for U.S. Government's Key Escrow program at NIST. Since January 1997, Mr. Snouffer has served as the Program Manager for the Cryptographic Module Validation Program.
Dr. Sean Smith, after studying math at Princeton and CS at Carnegie-Mellon, worked at Los Alamos National Laboratory doing security research and vulner-ability analysis. Joining IBM Watson in 1996, he led the software component of the security architecture, development, and FIPS 140-1 Level 4 validation work for the IBM 4758 secure co-processor.

Utilizing Secure Hardware

d 4

Joan Dyer, *IBM*

This talk will discuss how to use secure hardware to provide security for distributed e-commerce solutions. The new world of e-commerce can extend business access via kiosks, webservers and on-site contractors. However, this extended access increases exposure to attack, which cryptography can address if it works – but cryptography only works if secrets remain uncompromised and algorithms remain unmodified. Incorporating elements of secure hardware into the distributed e-commerce system can provide these properties. Design, engineering, and assessment issues for a spectrum of example problems and hardware will be addressed.

Joan Dyer joined IBM Research after an academic career in pure mathematics. She is involved with software design and implementation, currently with the Secure Systems and Smart cards group based at Hawthorne, New York.

Implementing a Wireless PKI to Secure Financial and Healthcare Applications

i 3

Michael Crerar, *Diversinet Corporation*

1999 has seen many deployments of Enterprise PKI's to provide robust, cryptographically strong user authentication and non-repudiation and facilitate the growth of electronic commerce over the Internet. Some analysts are predicting that by 2004, more than half the devices accessing the Internet will be mobile phones or PDA's. However, current wireless networks have very low bandwidth and users must pay for each byte of data broadcast. The devices themselves are limited by battery consumption, display capabilities, memory and computational ability. The Enterprise PKI's that have been deployed on land-line networks are not practical for wireless networks. We have implemented a wireless PKI on the RIM 950 Interactive Pager to provide secure mobile-to-mobile messaging. The main focus of this talk will be to discuss Diversinet's wireless PKI and e-commerce pilot with BellSouth Wireless Data, First Call and other financial service providers to demonstrate the potential of this new market. To overcome the constraints of the wireless environment, an architecture has been developed to efficiently utilize scarce resources. The PKI deployment uses short certificates and efficient transaction-based protocols to fetch and validate certificates and deal with the problem of registering and identifying users and devices. A method has been developed to securely distribute and update root level certificates on devices called Root Certificate Rollover. The recent work in WAP is helping to promote interoperability between the wireless world and the Internet world. A gateway is typically necessary to translate between the two environments. Important design considerations to achieve this interoperability will also be discussed.

Michael Crerar holds a Master's in Cryptography from the University of Waterloo. He is involved in security architecture, PKI and cryptography standards such as WAP, ANSI X9 and SECG. Prior to joining Diversinet in 1998, he held positions with Citibank and IBM's Footprint Software Division.

Network Security Beyond Firewalls and VPN's

p 3

Tomas Olovsson, *AppGate*

A great deal of companies and organizations rely on firewalls and VPN solutions to protect their most valuable data information. However, these security solutions do not provide control over who can access which applications at what time. Moreover, they are very cumbersome to administrate. There are, however, products and techniques that can segment your network as well as give each user an individual VPN, from the user to one or more applications in a secure network. This presentation will introduce techniques and products, based on RSA authentications product, that are able to give you a fine-grained access control, high scalability and does not require you to modify any of your existing applications.

Mr. Olovsson holds a Ph.D. in Computer Security and is CTO of AppGate AB. Before joining AppGate, Mr. Olovsson has held positions as system developer, development manager and business area manager for companies in US and Europe.

Encryption for Worldwide Markets: Developing Applications with RSA BSAFE® Crypto

r 4

Steve Burnett, *RSA Security Inc.*

This presentation will show how developers can use the RSA BSAFE® Crypto software development kits to implement cryptographic constructs in their applications. It will demonstrate the general BSAFE® Crypto model and provide examples of implementation. Also discussed are various security issues and how to address them with BSAFE® Crypto software development kits.

After graduating with degrees in math from Grinnell College in Iowa and The Claremont Graduate School in California, **Steve Burnett** has spent most of his career converting math into computer programs, first at Intergraph Corporation and now with RSA Security. He is currently the lead engineer for RSA BSAFE® Crypto-C and Crypto-J.

c cryptographers' track
d developers' track
i implementers' track
p new products track
r RSA products track
5 high
technical level
1 low

c 4 WAP's WTLS Protocol – Lessons Learnt

Magnus Nyström, *RSA Laboratories*

The Wireless Transport Layer Security Specification defines WAP's main security protocol, WTLS. WTLS is closely modeled after its Internet counterpart, TLS, and this talk will present WTLS and compare it with TLS. Further, a selection of potential attacks against WTLS, not applicable to TLS, will be discussed. The talk will conclude with a discussion of protocol design lessons to be learnt.

Magnus Nyström joined RSA Laboratories in 1998. His research interests include smart cards, security architectures and cryptographic protocols. He received his M.S. from the University of Uppsala, Sweden in 1990 and has been working in the field since then. In 1996, he joined the Swedish company DynaSoft, later acquired by Security Dynamics Inc., where he held a position as an Engineering Manager with responsibility for implementations of Public Key Technology.

d 4 Digitally Signed XML: A New Internet Standard

Barbara Fox, *Microsoft*

The PKIX (509) Internet standard profile for public key certificates and certificate revocation lists (RFC 2459) is complete, but hot on its heels is a whole new approach to the syntax and semantics of digital signatures on the Internet. What's different about XML signatures isn't as straightforward as a new cryptographic algorithm. The XML Digital Signature Specification, a product of a joint W3C-IETF working group, describes the standard mechanism for signing documents, transactions, and other resources on the Internet and its target is any developer creating applications for the web. The most noticeable differences with this new breed of signatures are format and encoding. XML tags are human-readable and the XML signature syntax leverages the web by using pointers (URI's, XPointers, and XSL for example) to associate a digital signature with its components such as algorithms and objects. More important, the underlying design philosophy is that a signature is simply a statement about another type of statement. The signature statement itself is expressed in XML, which makes it lightweight enough for wireless web-connected devices like pagers. So, does this new format obsolete the PKCS, CMS, and PKIX standards? No, but we can expect these digital signature types to co-exist and interoperate. This talk will focus on the requirements, syntax, and progress of the emerging Internet XML digital signature standard and assess its impact on developers and users of web applications.

Barbara Fox is Security Architect at Microsoft where she is currently responsible for the architecture of next generation web security. Her past projects included Internet Explorer, Java, and most recently, the Windows 2000 public key infrastructure. Ms. Fox holds Masters degrees in Computer Science and Business.

i 3 Windows 2000 Authentication: Under the Hood

Jan De Clercq, *Compaq Computer EMEA BV*

This session focuses on one of the core operating system security services of Windows 2000: Authentication. Without a solid and trustworthy authentication mechanism network operating system security becomes completely unreliable and in a certain sense even worthless. Windows 2000 implements the IETF standard Kerberos as its new default authentication protocol. The primary focus of this talk is Kerberos. The purpose of the session is however not just to give a thorough understanding of the basic protocol; it also addresses key concepts such as the Windows 2000 authentication architecture, the link between authentication and authorization, cross-domain operation and last but not least Kerberos authentication interoperability.

Jan De Clercq is a Compaq consultant working in the APPLIED Microsoft Technology Group. He's focusing on E-Commerce security (PKI) and security on top of MS platforms. He participates in the security seminars of the COSIC department at the Katholieke Universiteit Leuven (KUL), has written several white papers on Windows 2000 security, is writing articles for Windows NT Magazine, and has been a speaker at Microsoft conferences.

p 3 Super Scalable Server-Based S/MIME for the Enterprise

Blake Ramsdell, *Tumbleweed Communications*

The Worldtalk WorldSecure/Mail product pioneered server-based S/MIME three years ago. The new, super-scalable version will include server-based plaintext access for policy enforcement, as well as automated certificate lookup.

Mr. Ramsdell is the chief cryptographer of Tumbleweed. Mr. Ramsdell is one of the creators of the original S/MIME specification, and is a co-author and editor of the IETF S/MIME RFCs. Prior to his joining Tumbleweed, Mr. Ramsdell was the CTO of Worldtalk Corporation which was acquired by Tumbleweed in November of 1999. In addition to cryptography, Mr. Ramsdell's technical background includes significant work in groupware, electronic messaging and Internet technologies.

r 2 PKI Case Study: Enabling Secure Inter-Company Collaboration

Lina Liberti, *RSA Security Inc.*

By utilizing powerful ERP software, companies can seize the opportunity to harness the power of the ubiquitous, low-cost Internet backbone – but only if they can ensure that the security of their information systems and relationships are not compromised. This session presents a real life case study of how one corporation used PKI technology to provide secure access to corporate networks and applications to attain the increased productivity gains they sought.

Lina Liberti is a Director of Product Marketing at RSA Security Inc. in Bedford, MA. Ms. Liberti is responsible for the product direction and marketing for RSA Keon® Advanced PKI, RSA's suite of products, which help companies simplify and optimize their use of public key infrastructure (PKI) by extending digital certificates across organizations and applications. Ms. Liberti has spent the past 10 years in the high-tech security industry in product marketing positions at companies such as MEMCO and Mergent International. At MEMCO, Ms. Liberti was responsible for the product direction and marketing for MEMCO's single sign-on and security administration product suite. At RSA Security, she is a frequent presenter to industry analysts, the press and customers regarding the company's products.

c 3 The Advanced Encryption Standard: Development and Status

Ray Snouffer, *NIST*

For over twenty years, NIST's Data Encryption Standard (DES) has been the U.S. Federal Government's standard for encrypting unclassified information. In addition, it has gained wide acceptance in the private sector and is found in countless Internet and banking applications. The DES algorithm has evolved from a U.S. Government algorithm into one that is used globally. Consequently, in the spirit of DES's success, NIST's goal in the Advanced Encryption Standard (AES) development effort is to specify an algorithm that will 1) have a usable lifetime of at least thirty years, 2) be available royalty-free worldwide, and 3) be used extensively throughout the U.S. Government and private sectors. In January 1997, NIST announced its intention to develop a Federal Information Processing Standard (FIPS) for the AES. The culmination of this multi-year, multistage effort will be a FIPS specifying an Advanced Encryption Algorithm (AEA) – an unclassified, symmetric, block-cipher algorithm accommodating multiple key sizes. NIST and the public have completed their first round of evaluation of the fifteen candidate algorithms for security, efficiency, and other properties. At the time of RSA Conference 2000 Europe, the five finalist algorithms will be undergoing their second round of evaluation and analysis by NIST and the global cryptographic community. The purpose of this presentation is to articulate the status of NIST's AES development effort. This presentation will include: a description of the overall AES development effort; discussion of the second round of analysis (Round 2), including significant Round 2 issues; and future plans for the AES and related standards.

Ray Snouffer began his career with the Defense Information Systems Agency (DISA) serving in a variety of roles including senior mathematician, lead software developer, and Project Officer for the Strategic Defense Analysis Project. He was National Program Manager for U.S. Government's Key Escrow program at NIST. Since January 1997, Mr. Snouffer has served as the Program Manager for the Cryptographic Module Validation Program.

d 3 Passwords: Beyond the Terminal Interaction Model

Niklas Frykholm, *RSA Laboratories*

Passwords originated as a means of identifying terminal users to mainframes. It is still the most common identification method, even on systems that are not well suited for the terminal interaction model. For example, on hand held and embedded systems keyboard entry is awkward or impossible. Furthermore, the increase in processing speed and a widely spread knowledge of password selection psychology has made password cracking programs a harsh reality. By taking advantage of the new possibilities for representing and entering passwords offered by graphical display and interaction devices, we can hope to achieve two things: to facilitate password entry on keyboardless devices and to develop password schemes which are better adapted to the particulars of the human memory system. Graphical password systems can be divided into two classes based on the two actions possible with a mouse/stylus: click and drag. Some of the members of each class will be analyzed with respect to security, memorability and ease of use to see how they compare with traditional password systems. How to make a password system tolerant to small user input errors without compromising security and the advantages offered by such "fuzzy passwords" will also be discussed. Finally, this talk will present an implementation of the most promising system on a Palm computer. It will be demonstrated how the addition of memory cues can facilitate recall and demonstrate that computer generated passwords of 50 bits or more are within the reach of this system.

Niklas Frykholm is a Computer Science student at the University of Umeå, Sweden. He has written his master thesis in collaboration with RSA Laboratories in Stockholm, Sweden.

i 3 Requirements for a Card Management Infrastructrure

Laurent Den Hollander, *Gemplus*

In the ever more complex and distributed environments of modern enterprise information systems, the smart card appears as a secure and mobile intelligent token to represent and assist the end user whenever (s)he needs to interact with the IS: physical access to premises, logical access to information resources, secured remote communications. The management of smart cards as a new, full fledged component, of the information system requires specific professional tools closely integrated with the existing infrastructure: HR databases, PKI, OS and application accounts management, physical access systems. This presentation will identify the major requirements and propose an architectural framework to facilitate the deployment and management of smart card enabled security in the enterprise: The Card Management Infrastructure (CMI).

Laurent Den Hollander is a corporate staff scientist of Gemplus' Software division. With a strong background in systems analysis, requirements analysis and knowledge engineering he is dedicated to the design of added value card centric architectures in IT and mobile communications systems.

p 4 Building an Enterprise PKI

Bob Pratt, *VeriSign Inc.*

There are many important issues to consider when designing and deploying a Public Key Infrastructure, whether its for internal use at a company, to enable an extranet application, to secure your corporate e-mail, or all of these and more. This presentation will discuss the most important of these issues, and give you pointers on how you can best evaluate each of the key issues, both from a technology and cost point of view. This presentation will also introduce you to VeriSign's suite of Go Secure! applications for BtoB Web access and secure messaging, and for VPN's.

Bob Pratt is a Product Manager at VeriSign Inc., the leading provider of Internet authentication services. In this capacity, he is responsible for VeriSign's customized certificate products and services. These are targeted at customers who need the best authentication for their intranet and Internet applications, but who also need customized data and authorization processes. Prior to joining VeriSign, Mr. Pratt was the Product Line Manager for Management and Administration products at Novell, Inc. He was responsible for ManageWise, LANalyzer for Windows, NW Admin, software distribution, and all of Novell's other management and administration applications. Before joining Novell, Mr. Pratt was a software designer for Tandem Computers.

r 4 Enabling PKI with the RSA BSAFE® Cert Tools

Marina Milshtein, *RSA Security Inc.*

This presentation will show how developers can use RSA BSAFE® Cert tools Public Key Infrastructure to enable their applications. It will demonstrate the general BSAFE® Cert tools model and examples how to use Cert-C and Cert-J products. It will walk through the basics of creating CertRequests and submitting it to Certificate Authority (CA). It will show how to parse, create and sign certificates. This presentation will show how to use different Service providers: Policy Service Provider for chain validation, Database Service Provider for Key Pair Storage/Retrieval, and Certificate Storage/Retrieval.

Marina Milshtein works as a software engineer on the RSA BSAFE® Cert-J product. She received a B.S. in Computer Science from Hebrew University in Jerusalem, Israel and a M.S. in Computer Science from University of Pittsburgh.

8:00 am **VeriSign Keynote**
Dr. Warwick Ford, *VeriSign* Inc.

It's clear that trust and security will be fundamental pillars of any enterprise's push into e-commerce transactions and communications. But in the fast-evolving Internet economy, how can enterprises balance the need for absolute data protection and privacy against the increasing pressure to put every business process online.

Dr. Warwick Ford is Chief Technology Officer at VeriSign, Inc., the provider of Internet trust services for e-commerce, enterprises, and the public. Dr. Ford is a recognized authority on the application of public-key technology, and led the development of digital certificate standards in ISO and the Internet community. He is co-author of the 1997 Prentice Hall book "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption."

9:00 am **More Machines Than People**
Professor Peter Cochrane, *BT Laboratories*

Our world was dominated by atoms, but is now dominated by bits. Already we have electronic cameras on every street corner, in every parking lot, and in every store. Wear a mobile phone or use your credit card and the system knows where you are, and as chips and radio systems are embedded into everything we own we will be tracked, watched and recorded. Should we be worried?

Peter Cochrane was Head of BT Research from 1993-99, in 1999 he was appointed Chief Technologist. A graduate of Trent Polytechnic and Essex University, he is currently the Collier Chair for The Public Understanding of Science & Technology at The University of Bristol. He is a Fellow of the IEE, IEEE, Royal Academy of Engineering, and a Member of the New York Academy of Sciences. He has published and lectured widely on technology and the implications of IT.

10:30 am **Privacy and Security Challenges in an Era of Non-Stop, Continuously Available Computing**
Andrew Dixon, *Compaq Computer EMEA BV*

Increasingly, companies rely upon continuously available and massively scalable systems. In a Non-Stop Computing environment, information must be available, accessible, end-to-end secured and trusted. Conducting business securely in a 7x24x365 world presents a new set of challenges and concerns around traditional areas of privacy and information access.

11:30 am **Security in Electronic Communication – The EU Approach**
Richard Schlechter, *European Commision – Directorate Information Society*

The European Commission's security policy approach is based on a pragmatic distinction between authentication (electronic signatures) and security related issues (encryption). At this stage, the Commission will work towards facilitating the Intra-community shipment of so-called Dual Use goods as well as check that the measures implemented at Member State level do not create undue obstacles to the Internal Market.

Richard Schlechter is an attorney with the European Commission Directorate General, working on policy planning and information security strategy. He is a member of the United Nations Working Group on International Trade Law (UNCITRAL), as well as a Member of the OECD – Working Group on Information Security and Privacy (WISP). His specialities include the European Directive on "A Community Framework for Electronic Signatures" and encryption policy.

12:30 pm **PKI Forum: PKI Interoperability***
Optional Lunch Hour Session

The objectives of this open session are to provide new PKI Forum members and all interested RSA Conference attendees with an opportunity to learn more about the mission of the PKI Forum, discuss the initial priorities of the PKI Forum Technical Working Group, and provide an opportunity to provide input/priorities to the work list. The PKI Forum is an international, not-for-profit, multi-vendor alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI) and PKI-based products and services. The PKI Forum advocates industry cooperation and market aware-ness to enable organizations to understand and exploit the value of PKI in their e-business applications.

* This session will be held in the Salon Matisse. Seating is limited to 80 people.

c 4

Proofs of Knowledge of Discrete Logarithms and Applications

Marc Girault, *France Telecom/CNET*

Proofs of knowledge of a discrete logarithm have become in recent years a central tool in the design of many cryptographic protocols. Authentication, electronic cash, group signatures, verifiable encryption are just some examples of areas in which this tool appears to be crucial. This talk provides a unified presentation of many such proofs of knowledge known to date, stating their security properties and their performances. It also presents refinements of the basic proofs and gives some quite recent examples of applications, including very fast authentication, verifiable encryption of RSA keys, proof of RSA bits and fair protocols.

Marc Girault has been working in theoretical and applied cryptography for fifteen years, for The French Post and France Telecom. He presented a Ph.D. thesis in 1991 and has directed Ph.D. students for six years. Dr. Girault has published about twenty scientific papers on cryptology and security; and filed as many patents.

d 5

Time Stamping Services – Motivation and Basic Techniques

Roland Mueller, *TUVIT, Inc.*

Time plays an important role in any transaction, especially if initiated on the Internet. Digital time stamping is a basic technique for achieving proofs of timeliness (i.e. of the existence of an object at a specific point in time). Over the past years, a number of cryptographic time stamping methods have been proposed. This talk motivates the need for secure time stamping, presents different approaches to time stamping and discusses their requirements (e.g., a reliable and protected time source) and the services and entities involved. It discusses various techniques of how time parameters can be tied to electronic information thus allowing determining prior to which point in time this data existed. It also introduces services required to renew a time stamp and validate it and gives an overview on standards and standardization activities in the area. As time stamping different models of trust between the entities involved are possible; therefore protocols are introduced that rely on linking mechanisms for issued time stamps, either locally linked or in a distributed way. While some protocols require extensive interaction between affected entities, others only need certification of time from a trusted source. In this case, the source can simply provide a signed statement that the object existed and was presented for signature at the indicated time.

i 1

Nordic Standardization Moves to Interesting Implementations

May-Lis Farnes, *SEIS*

The SEIS, Secured Electronic Information in Society, work has contributed to the building of a necessary infrastructure of security based on PKI, which enables electronic commerce on the Internet to grow. SEIS began with work on technical standardization and the work continues on related policy and legislative questions. SEIS work has had an impact on implementations in all of the Nordic Countries and contributed to both the European and International standardization work. Because of this early initiative, several applications and implementations have been established in the Nordic Countries.

May-Lis Farnes, president of SEIS Sweden, earned her Master of Science, Computer Science, degree from the University of Oslo, Norway. After which she joined ITT/Alcatel, Belgium and Norway as a Research Engineer. From 1990-1995 Ms. Farnes was a System Developer/Project Leader at CAPGemeni, Germany and Norway. Ms. Farnes has served as Head of System Development (Department of Billing) and Product managment: Internet, Electronic Identification, Electronic Commerce for Telia, Sweden.

p 2

Lock up Your Keys! The nCipher Key Management Tool

Alex van Someren, *nCipher Corporation Ltd*

Digital signatures and data encryption involving math-intensive calculations and highly sensitive cryptographic keys have become the principal enabler of secure electronic transactions. The highest quality solutions to performance-crippling computational overhead as well as unacceptable risk from key vulnerability are hardware-based: e.g. the nFast cryptographic accelerators for performance, and nFast/KM hardware key storage devices for security. The nCipher KMtool, running on a UNIX or Windows host system, brings total life cycle management of secure cryptographic key to leadership nFast cryptographic accelerators using smart cards. Cryptographic operations are off-loaded from the host server to the nFast hardware device containing the sensitive keys, which never appear "in the clear" outside the nFast device. An intuitive user interface reduces the perceived complexity of key management tasks without compromising on security or the special attention paid to minimizing possible human error in key handling. Public/private key pairs for a variety of applications (including Netscape, Microsoft IIS, Apache or other PKCS#11-compliant applications) can be generated on the nFast/KM module using a unique hardware-based true random number generator (TRNG). Alternatively, keys previously generated can also be imported to the nFast module or smart cards for enhanced storage security. Support for "key splitting" and "key sharing" delivers the highest private key security while flexible "access control list" management of key properties supports, but does not dictate, your application's security policy. Finally, key destruction is managed with the KMtool application in a rigorous fashion, ensuring that all copies of keys can be tracked and destroyed. The KMtool is designed with FIPS 140-1 guidelines built in from the ground up.

Alex van Someren, president and CEO of nCipher, has over fourteen years of entrepreneurial success in the global computer industry. He has successfully managed the establishment of several businesses, the development of numerous software and hardware products, and supervised the hiring and smooth growth of sales, marketing and technical teams. His areas of professional accomplishment include over £3m in sales of products from within self-financed organizations, the securing of corporate finance for start-up businesses and oversight of the growth of several companies into self-sustaining enterprises. His is also the author of several books on the applications of computers and microprocessor. He is currently supervising production and global deployment of nCipher's state-of-the-art cryptographic products for electronic commerce.

r 4

RSA Keon® Agent Software Developer Kit

Per Eliasson, *RSA Security Inc.*

RSA Keon® Agent software is used to provide security solutions for client-server based applications. The agents offers features such as strong user authentication and line encryption, centralized access control and centralized audit logs. The RSA Keon® Agents are "plug-in" solutions which can be installed at existing application environments, without modifications of the original application installations. The Keon® Agent SDK is a toolkit, which allows developers to develop their own agents for inhouse – or 3rd party developed applications. This presentation describes the architecture of Keon® Agents, and how agents may be implemented using the Keon® Agent SDK.

Per Eliasson is a Software Engineer at RSA Security in Uppsala, Sweden. Mr. Eliasson has been with the company for almost two years, mainly working with development of the RSA Keon® Agent SDK.

c cryptographers' track
d developers' track
i implementers' track
p new products track
r RSA products track
5 high
technical level
1 low

c 5 Fast Monte-Carlo Primality Evidence Shown in the Dark

Dr. Wenbo Mao, *Hewlett-Packard Laboratories*

Proof of primality "in the dark" means to show that a number is a prime without disclosing it. A fast proof can provide an efficient key-certification service in that a cryptographic key is strong and trustworthy. We construct a fast in-the-dark proof scheme for the demonstration of Monte-Carlo evidence that a number n is the product of two odd primes of roughly equal size. The length of a proof amounts to $k\log_2n$ bits where k is a security parameter which controls the error probability of the proof under 2^{-k}. With n of 1024 bits and $k = 40$ for a 1-in-a-trillion odds of error, the length of a proof is around 5 kilobytes which is short enough for being included inside a key certificate.

Dr. Wenbo Mao received his B.Sc. degree in Mathematics from the University of Fudan, Shanghai, China and his Ph.D. degree in Computer Science from the University of Strathclyde, Glasgow, UK. In 1994 he joined Hewlett-Packard Laboratories, Bristol. His research interest include computer security and cryptography. He has served in the program committees of several security conferences including the ACM Conference on Computer and Communications Security, the IEEE Symposium on Security and Privacy and the IEEE Computer Security Foundations Workshop.

d 2 Why Europe Hesitates to Buy American Electronic Stamps

Detlef Huehnlein, *Secunet AG*

As e-mail clearly will not supersede conventional mail in the future it is necessary to integrate mechanisms for electronic franking in the standard office communication environment. Therefore the U.S. Postal Service started the Information Based Indica Program (IBIP) to issue "electronic stamps" involving digital signatures, to prevent forging of stamps. However it seems that European postal services hesitate in adopting the American program, because it seems to introduce an unreasonable overhead due to the verification of (asymmetric) digital signatures in the verification step which has to be performed for billions of stamps. Recent developments will be discussed, as well as an introduction to an alternative approach based on symmetric algorithms which is more suitable for large scale deployment.

Dipl. Inform. Detlef Huehnlein, is working for SECUNET AG as senior consultant for cryptography, electronic payment, electronic banking and smart card technology. Prior to his employment at SECUNET, Frankfurt/Eschborn, he graduated in computer science at FH Wuerzburg, worked for the information security research group of Siemens AG, Munich and the security technology research group in the institute for telecooperation technique of GMD, Darmstadt. He has been actively involved in the IETF/CAT working group, the preparation of the DIN-SigG-smart card-specification and the organization of IT-Security conferences like VIS'99 and CQRE. Besides these activities he is a member of the cryptography and number theory research group at Darmstadt University of Technology, lead by Prof. J. Buchmann, where he is currently preparing his Ph.D. thesis "Cryptosystems based on quadratic orders." He (co-) authored more than 15 papers for journals and conferences. For example he recently had contributions to NDSS'98, Euro-crypt'98, ICISC'98, SAC'99, Asiacrypt'99, CQRE'99 and PKC2000.

i 4 Do-it-Yourself Certification Authorities: The Legal Toolkit

Samoera Jacobs, *GlobalSign*

Digital signatures are widely seen as the staple of electronic commerce. This article draws from the hands-on experience of GlobalSign as a provider of PKI products and services in helping companies build their own PKI's in-house and beyond. This presentation provides answers to questions like: Legal elements and steps for a successful PKI operation contracts needed to operate a CA, managing liability, organizational and technical procedures, your CA and the consumers, your CA and data protection. This presentation is essential to management and counsels involved in deploying corporate PKIs.

After her law degree with specialization in intellectual property rights and computer law, **Samoera Jacobs** obtained a Master in Social and Cultural Anthropology at the KU Leuven. Before she was at Belgium Online responsible for the legal implementation of the Internet Project and for the contracts with subscribers and providers. At GlobalSign she heads the department of Legal Practices and Procedures.

p 3 Taking Care of the 'I' in PKI: Managed PKI Services

Peter Forret, *GlobalSign*

Setting up a PKI project is not a simple task. GlobalSign has a track-record in outsourced PKI solutions, and will talk about the project definition, PKI components, integration and compatibility issues. Some recent projects will be highlighted and the integration with some of the GlobalSign Ready products will be commented.

Peter Forret, Vice-President, is responsible for PKI-infrastructures and GlobalSign's products. As a civil engineer in computer sciences, he is an expert in security technology, biometrics and telecom. Before GlobalSign, he worked for Sopres Marketing and Keyware Technologies.

r 4 RSA Keon® Single Sign-On Software Developer Kit (SSO)

Per Eliasson, *RSA Security Inc.*

In many cases, application software allows for automation of the login procedure on the client side. However, storing passwords in scripts on the client is not secure. The Keon® SSO Software Deveopler Kit is a tool to create secure solutions where the username/password is sent to the client at login, to be forwarded to the application server.

Per Eliasson is a Software Engineer at RSA Security in Uppsala, Sweden. Mr. Eliasson has been with the company for almost two years, mainly working with development of the RSA Keon® Agent SDK.

c 4

Why Hyperelliptic Curves Might Be More Secure than Elliptic Curves

Detlef Huehnlein, *Secunet AG*

As all known attacks against special classes of Elliptic Curves have a straightforward generalization to Hyperelliptic Curves and there is an algorithm to compute DL's in Hyperelliptic Curves which is subexponential for large genera, one is tempted to conclude that Elliptic Curves are inherently at least as secure as hyperelliptic curves. However, Lenstra has shown that Elliptic Curves E are isomorphic to a module M over its endomorphism ring, and this result fails to hold for curves of higher genus. If there would be a CONSTRUCTIVE map E -> M, then one could obviously reduce the DLP in E to the DLP in M. It will be shown that the latter problem can be solved in polynomial time and investigate approaches to obtain the desired constructive map. It should be stressed that, at present, our approach does NOT imply any new weak class of Elliptic Curves.

Dipl. Inform. Detlef Huehnlein, is working for SECUNET AG as senior consultant for cryptography, electronic payment, electronic banking and smart card technology. Prior to his employment at SECUNET, Frankfurt/Eschborn, he graduated in computer science at FH Wuerzburg, worked for the information security research group of Siemens AG, Munich and the security technology research group in the institute for telecooperation technique of GMD, Darmstadt. He has been actively involved in the IETF/CAT working group, the preparation of the DIN-SigG-smart card-specification and the organization of IT-Security conferences like VIS'99 and CQRE. Besides these activities he is a member of the cryptography and number theory research group at Darmstadt University of Technology, lead by Prof. J. Buchmann, where he is currently preparing his Ph.D. thesis "Cryptosystems based on quadratic orders." He (co-) authored more than 15 papers for journals and conferences. For example he recently had contributions to NDSS'98, Euro-crypt'98, ICISC'98, SAC'99, Asiacrypt'99, CQRE'99 and PKC2000.

d 3

Cryptography and Biometrics in Banking

Vashek Matyás Jr., *Ubilab; UBS AG*

This talk focuses on the cryptographic issues relevant to the deployment of various biometric authentication techniques. Various scenarios for deployment of biometrics within the banking environment will be discussed and some of the critical issues of such applications where there is a potential to use cryptographic tools/techniques to resolve these issues will be examined. There will be a review of various biometric technologies with the aim of identifying which biometrics are most appropriate for various banking applications, both for the use inside the bank and for interacting with customers. Biometrics have had virtually no impact on the banking sector; however, things have been changing in the last few years. A comparative overview of various technologies is provided and their features are discussed with respect to their potential use in various environments within a bank. Also, the critical issues within some of the foreseen scenarios for deploying biometrics in a bank will be identified. Last, there will be a discussion to detail some of the ways cryptographic tools and techni-ques could be helpful to resolve these issues.

Dr. Vashek Matyás Jr. is a researcher with Ubilab, UBS AG. His research interests relate to applied cryptography and security. He was with the Cambridge University Computer Lab in 1996-98 and he holds assistant professorship at the Masaryk University, Czech Republic.

i 4

Deploying S/MIME in the Enterprise

Blake Ramsdell, *Tumbleweed Communications*

There are many factors to consider when deploying S/MIME in the enterprise. This presentation will explain what components are available, how they can be combined to effect a corporate S/MIME strategy, and how they can be incrementally deployed for minimal disruption.

Mr. Ramsdell is the chief cryptographer of Tumbleweed. Mr. Ramsdell is one of the creators of the original S/MIME specification, and is a co-author and editor of the IETF S/MIME RFCs. Prior to his joining Tumbleweed, Mr. Ramsdell was the CTO of Worldtalk Corporation which was acquired by Tumbleweed in November of 1999. In addition to cryptography, Mr. Ramsdell's technical background includes significant work in groupware, electronic messaging and Internet technologies.

p 3

Extraordinary Extranets: Effectively Teaming VPN's and PKI

Melanie Ciosek Francis, *CyberTrust*
John Summers, *GTE Internetworking*

The market for securing electronic communications has shown vast improvements in 1999. Many organizations are now moving away from pilot implementations and are now deploying several different technologies that work in concert to make their extranets secure. Some customers have chosen to initially implement a Virtual Private Network (VPN), which allows remote locations to securely communicate while veraging their existing Local Area Network (LAN). Other organizations have chosen to first implement a secure solution based on Public Key Infrastructure (PKI), thereby taking advantage of the benefits of authentication, encryption and signing. Regardless of which technology a customer initially chooses, they quickly learn that deploying VPN's and PKI leads to maximum advantage. This presentation will highlight some of the situations GTE and CyberTrust have encountered during 1999 and will give examples of when the use of VPN's, PKI, or both are optimal.

Melanie Ciosek Francis, CyberTrust PKI Product Marketing Manager, has worked in the PKI industry since 1996 and regularly addresses large audiences at trade shows, seminars and customer events to present the latest advances in cryptography as well as other technical and market issues of PKI.
John Summers is the Senior Product Manager for GTE Internetworking's VPN Advantage group, and is known for his skill in presenting VPN technology. Mr. Summers has a wealth of technical knowledge on the intricacies of VPN implementations and is regularly called upon to address large and small audiences on this topic.

r 3

RSA SecurID® in a Wireless Environment

Göran Walles, *RSA Security Sweden*

Authenticating users accessing networks and applications via the Internet is critical. Two-factor authentication solutions; however, must go beyond the browser and VPN client. Learn how the award-winning RSA SecurID® extends to the wireless environment, providing authentication for wireless sessions, as well as the convenience of running RSA SecurID® from the wireless device for use with traditional computing devices.

Göran Walles is working as a Systems Engineer at RSA Security, Nordic Region. He is responsible for presales technical advisory, providing the expertise to customers as well as partners. Göran has 10 years of experience within the field of data communications and access solutions. Prior to his joining RSA Security in 1999, Göran worked at 3Com. He was responsible for access products and the Carrier market from a technical perspective.

c cryptographers' track
d developers' track
i implementers' track
p new products track
r RSA products track
5 high
technical level
1 low

c 4

Privacy and Security of Public Databases

Dr. Susanne Wetzel, *Lucent Technologies – Bell Laboratories*

This presentation proposes a technique for access control that incorporates biometric information into the user's credentials. Specifically, this technique generates cryptographic keys from static or non-static biometrics which can then be used for protecting records in a database. Our approach effectively hides information about which of a user's features are relevant to generating her keys, even from an adversary that captures all metadata used by the access control system. At the same time, it employs novel techniques that impose an additional work factor on the adversary who attempts to exhaustively search the key space. This scheme is very attractive for use in practice. Unlike other biometric authentication procedures our approach is unintrusive. This scheme initially is as secure as traditional access control schemes and then gradually strengthens the cryptographic key using biometric information. For example, techniques can be used to improve password-based authentication by strengthening a user's password using habitual patterns and typing behavior. More specifically, applying secret-sharing techniques we disperse a cryptographic secret over a table, and then use both the password characters and the user's typing patterns when typing the password to recon-struct the key (i.e., in a login attempt, the login program uses the user's password to decrypt a table, and typing behavior to select elements from the table). The login program will fail to reconstruct the cryptographic key if either something other than the user's password is entered in the password field or if the user's typing patterns significantly differ from the typing patterns displayed in previous successful logins to the account.

Dr. Susanne Wetzel is a member of the Secure Systems Research Department at Bell Laboratories, Lucent Technologies, Murray Hill (USA). She received her Ph.D. in computer science from Saarland University (Germany) in 1998. Dr. Wetzel's research interests include various aspects in cryptography (secret sharing, visual cryptography, distributed computing) and algorithmic number theory.

d 3

IPsec, A General Solution for Securing the Internet

Tatu Ylönen, *SSH Communications Security Ltd.*

Cryptography is the only viable method in securing the network traffic on the Internet without losing flexibility. Four basic services offered are: Confidentiality; only authorized parties get access to the information, Integrity; the information remains untampered, Authentication; the parties and the origins of communication can be authenticated, Non-Repudiation, cheating on contracts impossible. Many applications using cryptography have emerged. The most common of them include e-mail encryption, file encryption, authentication, electronic money, and traffic encryption in different layers with IPsec, SSL, SHTTP, SSH, etc. IPsec (Internet Protocol Security) is a breakthrough in these technologies. It is a general solution to the security problem protecting all Internet traffic. SSH's IPSEC Express™ is a market leading software family that enables IPsec (Internet Protocol Security), IKE (Internet Key Exchange), and X.509 certificate management system solutions. With the Internet, organizations can be connected very flexibly with low cost increasing network uptime and geographical coverage. It offers over 90% reductions of time in building connections between offices, commuters, etc, and over 60% reductions in communication costs. Also, general trends like, the enormous increase in private use of the Internet, the integration of tele-phony and the Internet, the use of the Internet for critical business applications, transactions of monetary value, e-commerce, and standardization work show an expected explosion of the Internet technology.

Tatu Ylönen is the founder of SSH Communications Security and chairman and CTO. He is also the inventor of Secure Shell protocol, the de facto standard for secure remote connections over the Internet. He is a Licentiate of Computer Sciences, a member of ICSA, IEEE, ACM and IETF, and author of several technical articles.

i 3

Certificate Based Access Control Mechanisms for the Web

Scott Shorter, *CygnaCom Solutions*

This talk examines the state of the art in certificate based access control, including the use of attribute certificates for authorization, role- and rule-based access control procedures, access control granularity, and the different delivery methods for getting the authorization information to the web server. Attribute certificates decouple access control from authentication, permitting the authorizing authority to be diff-erent from the authentication authority, and allowing authorization information to be updated more frequently than authentication information. This approach requires a trusted method for linking attribute certificates to authentication certificates, and some approaches for performing this linking will be presented. Role- or rule-based access control enables a more sophisticated access control method than the more common methods of allowing access to users with certificates issued by a certain set of CAs, or restricting access by subject distinguished name. These methods also allow easier distribution of security policy than access control lists (ACL's). The granularity of access control for web purposes could be at the level of a web site, a directory, a web page, or even objects on a web page. The different granularity levels impose various requirements on the access control methodology, and this is discussed in the paper. Delivery methods for authorization information depend on whether attribute certificates are used, but include transmission from the client during the SSL handshake, obtaining the information from a directory, or obtaining a freshly issued attribute certificate from an authorizing authority.

Scott Shorter is manager of PKI consulting services for CygnaCom Solutions, Inc. His responsibilities include software development, technical consulting, and certification practice statement development.

p 1

End to End Security and Trust

Sam Asseer, *LCI Technology Group*

Electronic commerce is rapidly becoming the way the world conducts business. As more transactions are carried out over open electronic networks such as the Internet, it becomes necessary to verify the identity of business partners. Enhanced encryption technology offers a heightened level of security that provides trust and confidence in various online transactions.

r 3

RSA SecurID® Authentication for Web Applications

Norbert Olbrich, *RSA Security Germany*

In this session, it will be discussed how RSA SecurID® will enable organizations to capitalize on e-business opportunities. Topics include the need to know whom you are doing electronic business with, the strength of a zero-footprint, portable authentication solution, and how RSA SecurID® can be used to reinforce your organization's corporate identity with your customers and business partners.

Since 1996, **Norbert Olbrich,** a mechanical engineer, has been responsible for all technical matters of the RSA Security GmbH. He is Pre-Sales Manager for Germany, Austria and Switzerland, and a frequent keynote speaker at conferences and associations. He also worked for Dynatech Inc., an American hardware producer for communications technologies. Mr. Olbrich started his IT-career in 1990 with a German systems integrator where he was responsible for CAD development and network technologies, as well as external training.

c 4

Further Lessons in Protocol Design: Unknown Key-Share Attacks and the MQV Key Agreement Protocol

Burt Kaliski, *RSA Laboratories*

During the development of the IEEE P1363 standard in 1998, the MQV key agreement protocol, one of the techniques in the draft standard, was shown to be vulnerable to an unknown key-share attack. Though the attack's practical impact on security is minimal – a key confirmation step, which is a standard feature in many protocol specifications, easily prevents it – the attack is noteworthy in the principles it illustrates about protocol design. In particular, it serves as a reminder of three important lessons. First, minor "efficiency improvements" can significantly alter the security properties of a protocol. Second, protocol analysis must consider potential interactions with all parties, not just those that are normally on-line. Finally, attacks must be assessed in terms of system requirements, not just in isolation.

Burt Kaliski received B.S., M.S., and Ph.D. degrees in computer science from MIT in 1984, 1987, and 1988 respectively. In 1989 he joined RSA Security and since 1991 has been chief scientist of RSA Laboratories. Dr. Kaliski has served as general chair of CRYPTO '91, program chair of CRYPTO '97, and chair of the IEEE P1363 working group.

d 3

Replacing the Smart Card PIN: Fingerprint Matching on 8-bit Smart Cards

Anthony Russo, *Veridicom, Inc.*

The enormous potential of e-commerce will only be reached with the proper balance of security, privacy, and customer convenience. Recent advances in biometric technology can be employed together with those cards to boost all three of these aspects. In Europe, and increasingly in the U.S., smart cards are playing an important role in e-commerce, and this is driving demand for higher security smart cards. It is well known that biometrics can increase security by linking a smart card to the card's owner, much the same way a PIN is intended to do. But PINs can be stolen rather easily, so on the surface it seems like a good idea to replace or supplement the PIN with a biometric, especially since biometrics are usually easy to use and reliable. The problem that arises when trying to replace a PIN with a biometric, however, is that the private biometric data stored on the card must be sent to a host computer to be verified. Therefore, the card must be unlocked before the user can be authenticated, a design flaw that would circumvent most of the security benefits inherent in smart cards. Furthermore, even if a PIN is still used to unlock the card prior to user verification, the biometric data becomes publically readable once the card is unlocked with the PIN. Therefore it is vulnerable to attack and arguably adds little to the overall security of the system. In addition, such a system may violate European privacy laws. Recent algorithm developments have led to the first high-performance fingerprint matching engine feasible force use on a card with an 8-bit processor. This talk will describe the algorithmic advancements at a high level, and describe in moderate detail a prototype system Veridicom has implemented with a smart card partner that can serve as a basis for future products.

Anthony P. Russo is a co-founder of Veridicom, Inc. and currently serves as its Distinguished Staff Technologist after a one-year period as Software Director. He is a fingerprint and pattern recognition expert who designed and developed the verification algorithms of Veridicom's fingerprint analysis software. His work in this field began in 1985 with his Master's thesis, in which he created a set of efficient image-processing algorithms for fingerprint analysis. Since that time, he has developed fingerprint systems for Bell Labs and invented a novel neural network architecture for fingerprint classification. Mr. Russo earned a B.S.E.E. from Columbia University in New York City and an M.S.E.E. from Rensselaer Polytechnic Institute in Troy, New York. From 1985 until joining Veridicom in 1997, he worked for Bell Laboratories. In 1994, he became a Distinguished Member of Technical Staff at Bell Labs. His broad problem solving skills have resulted in a diverse portfolio of 8 patents granted or pending.

i 2

What to Look at in a Practical PKI

Dominic Storey, *RSA Security United Kingdom*

What are the practical issues in implementing PKI's? What requirements do modern businesses make on using PKI, such as user mobility and international considerations? This presentation, designed for business people, outlines key criteria in choosing PKI products and the "gotchas" that may exist for the unwary purchaser.

Dominic Storey is Technical Director for Europe, Middle East & Africa. Dominic articulates RSA strategy to customers, analysts, press and partners as well as running a research team looking into new areas of eBusiness requiring security.

p 3

How To Safely Integrate Your Back-Office To The Web: An Intro to Air Gap Technology

Yair Tsoran, *Whale Communications*

In today's burgeoning e-business economy, maintaining a secure back office is vital to the success of a company's e-business function. A new security technology is emerging called Air Gap that protects a company's internal networks by physically disconnecting commerce servers and internal databases. This presentation will demonstrate this unique technology, while discussing the key benefits for the e-business marketplace.

Yair Tsoran, Technology Director at Whale Communications, has worked actively for more than ten years in the fields of computer networking and information security. Prior to Whale, Mr. Tsoran worked at Compaq as a software and communications product manager. In this position, he coordinated two Special Users Groups (SIG) in Communications SIG and Information Security. Previously, Mr. Tsoran worked at Digital Equipment Corporation, as a Senior Consultant in Data networking, Information security, Windows NT and Internet, among other positions. He served in the Israeli Navy as a programmer and then as a system engineer. Mr. Tsoran holds a B.S. in Physics and Computer Science from Bar-Ilan University.

r 3

RSA SecurID® in a Managed Service Environment

Jonathan Smith, *RSA Security United Kingdom*

Corporations worldwide are increasingly opting to outsource the management of their VPN, RAS and Web application infrastructures. This session will address how this trend is significantly impacting corporate security, strengthening the need for authentication and encryption, and how RSA SecurID® and its partners are meeting these challenges.

Johnathan Smith is a UK pre-sales technical consultant for RSA Security, working in the fields of PKI and Authentication technologies. He has 12 years of experience in IT for companies like ICI, Zeneca, and RSA. He has been instrumental in architecting many ISP based authentication solutions.

c cryptographers' track
d developers' track
i implementers' track
p new products track
r RSA products track
5 high
technical level
1 low

c 3

How to Puzzle an Attacker

Dr. Ari Juels, *RSA Laboratories*

A series of recent research results from RSA Laboratories exploring the deployment of puzzles to achieve a range of different security goals will be discussed. A puzzle is a small cryptographically based problem whose solution requires a moderate level of computational effort, typically on the order of a couple of seconds on a workstation. First, it will be shown how puzzles can serve as a means of defending against denial-of-service attacks involving saturation of resource intensive server protocols such as SSL. The efficacy of this method depends on the computational resources available to the attacker, rather than on information specific to the attacker. This proposal offers an advantage over most common solutions, which fail when an attacker is capable of achieving anonymity. There are at present new efficiency enhancements to our previously proposed version of this protocol. These describe how puzzles may be used as a means of distributing large computational tasks in a manner that preserves privacy. As an example, consider MicroMint, a micropayment scheme devised by Rivest and Shamir in which the task of minting requires expensive, special-purpose hardware. By use of puzzles, this minting operation can be distributed among a large collection of untrusted entities, eliminating the need for a single, fast computing device. A presentation of some back-of-the-envelope calculations will demonstrate the financial viability of this proposal.

Dr. Ari Juels is a senior research scientist at RSA Laboratories. His interests span a number of areas of cryptology, including financial security protocols, biometrics, random number generation, and the theory of cryptography.

d 3

Crypto Policy and Technological Development for Global Markets

Ian Walker, *Entrust Technologies*

Policies related to the use of cryptography by several governments, most notably the United States, have had a significant impact on how this technology gets developed and deployed globally. This presentation will evaluate the impact of the regulations, and look at some innovative solutions that have been developed to deliver full strength cryptography and stay within the framework of the regulations. Recent changes to these regulations and possible next steps will also be discussed.

Ian Walker is Entrust Technologies' EMEA Technical Director. With over 25 years experience in the IT industry, Ian has concentrated for the last 6 years on the rapidly expanding area of Information Security and Public Key Infrastructure (PKI). Prior to joining Entrust, he was involved in product management at EDS. He went on to manage EDS' initial PKI product capability project. This developed into the first digital e-commerce solution in the UK to use PKI technology and demonstrated inter-company workflow between Microsoft, Novell and Digital products – using Entrust/PKI. Ian also has experience in the banking industry and worked on one of the first UK Automatic Teller Machine projects.

i 5

Case Study: Italy Moving Business into the Digital Age with a National CA

Trevor Thomas, *CyberTrust;* Mr. Vinetti, *SIA*

As business and governments move into the digital age, secure legally binding electronic transactions have become a critical issue. This case study presents how Italy used Certificate Authority technology to take the lead in supporting secure electronic transactions for its business and financial communities. The Italian government appointed Societa Interbancaria per l'Automazione (SIA), IT provider of the Italian financial community, to authorize all organizations, agencies and individuals who use digital certificates to secure transactions over the Internet. CyberTrust and Hewlett Packard worked with SIA to develop a nationwide certificate authority (CA) solution that meets all security measures required by Italian law and ensures that transactions remain private and that audit trails verify transactions that took place. All Italian banks and financial institutions, including the Stock Exchange, will use the CA solution. The presentation will discuss how the CA solution was integrated into SIA's digital time stamping services and how it supports multiple variations of certificate content, format and security in a single system.

p 1

MAILguardian Enterprise: The Ultimate Enterprise E-Mail Security Solution

Raviv Karnieli, *Vanguard Security Technologies Ltd.*

E-mail is the most popular Internet application used today within enterprises, however it is not used expansively for e-business, due to the lack of good reliable security solutions. While several e-mail encryption solutions exist today, they are not implemented by enterprises. The reason is that all of the existing solutions either put the security responsibility on the end users or provide only partial solutions via servers or gateways. Vanguard Security Technologies released the first e-mail security solution that provides enterprises with a comprehensive solution. MAILguardian Enterprise combines the following three features: end to end e-mail security, total transparency to end users and a central, policy based, management station. This presentation discusses the market's needs, MAILguardian Enterprise features, benefits, procedures and algorithms.

Mr. Raviv Karnieli holds a BA degree in Mathematics and Computer Science from Bar-Ilan University in Ramat Gan, Israel. He has over 25 years experience developing software including 12 years as a software engineer in the Israeli air force and as Director and senior managing partner in a privately owned software and systems company. Mr. Karnieli has acquired a great deal of experience in defining, developing, and implementing software systems, and leading development teams. In 1997 he founded Vanguard Security Technologies and serves as its CTO since.

r 1

RSA SecurID®, A Critical Component of Your PKI

Ted Kamionek, *RSA Security Inc.*

The integrity of a public key infrastructure (PKI) relies on the protection of the private key of each individual user. It is critical that only the rightful owner of the private key can gain access to it. This session will review the alternative ways that RSA SecurID® can provide the level of strong authentication and non-repudiation required for mission-critical e-business applications.

Ted Kamionek joined RSA Security in 1998 with more than 7 years of experience working in the high technology field in software development, product management and marketing. As a frequent speaker at industry conferences such as CardTech SecurTech, Internet World and The Wharton School of Economics Technology Forum, Ted is currently responsible for the current and future smart card related products from RSA Security – one of the largest PKI and e-security product companies in the world. Prior to joining RSA Security, Ted was Director of Marketing at Firefly Network (acquired by Microsoft in 1998), a provider of Internet software solutions for personalization and user profiling. Before joining Firefly, Ted was a consultant to companies such as Motorola, MCI, 3DO and Packard Bell Electronics. Ted earned a BA from Tufts University.

c 4

High Speed RSA Hardware Implemented in Dynamic True Single Phase Clocked Logic

Johann Groszschaedl, *Graz University of Technology*

The speed of RSA based crypto systems is primarily determined by the efficient implementation of the long integer modular arithmetic. This presentation covers basic concepts and design considerations for high speed RSA hardware on several levels, including algorithmic issues, long integer multiplier architecture and VLSI circuit technique.

i 2

Xcert Gold Sponsor Lecture

Kevin Bocek, *Xcert International, Inc.*

This talk will highlight Xcert's PKI deployments in Europe while providing an in-depth overview of successfully implementing an award-winning PKI.

Senior Systems Engineer and Regional European Manager of Xcert International, Inc., **Kevin Bocek,** has spent the last two years working closely with their European partners in Stuttgart, Germany and London, England. Mr. Bocek has developed distributed connectivity and security applications using Java and has expanded his expertise to directory and database technologies on the Internet.

p 2

Open Source and Security Software

Terry A. Smith, *Intel Corporation; Guest Speaker, Trustworks TBA; Guest Speaker, Checkpoint TBA*

Top Security Companies discuss strategies for implementing heterogeneous, multi-vendor public key infrastructures that "work." You'll learn what is compatible and, more importantly, what is not at the eminently practical expert panel.

Terry A. Smith is the Marketing Manager for the Security Technology Lab at Intel Corporation. He helps forge the strategic direction of STL, and also develops and implements STL's marketing strategies. STL focuses on the creation of leading edge, industry-enabling security technologies, which include Intel's Common Data Security Architecture (CDSA) Initiative.

r 2

Professional Services: Providing Solutions with Services

Fabien Séheux, *RSA Security United Kingdom*

The RSA Keon® PKI family is briefly introduced to demonstrate the breadth of product type in a PKI environment. This will encompass the distinct roles of the Keon® Certificate Server, Keon® Security Server, Keon® Desktop, Keon® Application Agent and the available PKI toolkits (such as BSAFE® CERT-C, SSL-C etc). Throughout the presentation, attention will be drawn to the value of consulting services which are useful to successfully implementing PKI solutions, such as those provided by the RSA Professional Services Organization. Experienced Consultants should deliver business and technical expertise and on-going support to their customers who see the benefit in working closely with their partners and suppliers.

Fabien Séheux is working with RSA Security Inc. as a Senior Consultant within EMEA Professional Services. He has been involved in PKI deployments, e-commerce and Unix access control projects all over Europe. He has been previously working as a Pre-Sales Consultant for Southern Europe, Middle East and Africa, actively promoting PKI, authentication and application access control.

d

*Special Presentation**
Threats and Lies: Hacker, Viruses and Spys

Dr. Christian Fill, *InformationWeek*

Overall, security breaches are slightly more widespread compared to 1998, but the culprit is viruses rather than hacking or various forms of espionage or code breaking. Nevertheless, there is a distinct increase in downtime this year at sites which have had security breaches, including viruses. While security policies and anti-virus strategies seem to be an industry standard the survey shows that encryption is not yet an overall top issue. If the company is engaged in some form of encryption, there is a higher percentage of data traffic encrypted by larger companies worldwide rather than smaller ones. The 1999 Global Information Security Survey, fielded by PricewaterhouseCoopers LLP, is an editorial research product of InformationWeek magazine and its affiliates in Europe, South America and Asia. The 1999 study was collected by mail and on the World Wide Web, and was completed by 2,700 security professionals spanning 49 flags and five languages (English, French, German, Portuguese and Spanish).

Dr. Christian Fill, Executive Editor, InformationWeek Germany, he studied engineering in Munich and started his career in journalism as a freelancer at several German technology and science magazines. He covers IT-security and management topics for InformationWeek.

** will be held in Ballroom A*

11:15 am **Securing Electronic Business**
Roger Farnsworth, *Cisco Systems*

As the Internet moves toward true ubiquity, the issue of privacy for those who utilize its life-changing services, becomes more compelling, and yet more complex. Issues such as bandwidth and reach, seamless convergence of data, voice, video, and changing national policies, all determine the viability and ubiquity of the Internet – and yet along with those catalysts of change, must be the assurance of security of personal and corporate privacy. Find out what one of the industry's leading visionaries has to say about networking's next challenge.

Roger Farnsworth is responsible for managing the marketing of security technologies used to enable global Internet solutions. Mr. Farnsworth's group develops the Cisco technologies which are used to provide solutions for perimeter security, identity, privacy and encryption, secure remote access, and virtual private networking. He has been working in the networking and communications industry since 1980. Before joining Cisco, Mr. Farnsworth was National Field Marketing Manager for Network Systems Corporation.

12:15 pm **From Cellular Phone to Personal Trusted Device**
Ilkka Raiskinen, *Nokia Mobile Phones, Finland*

Mr. Raiskinen will evaluate the role of cellular phones in the secure transaction business. He will discuss the market situation today and key drivers; What are the key enabling technologies; What applications will drive the development; What are the implications on the current value chains; and an Industry outlook for the future.

Ilkka Raiskinen is currently Vice President, Mobile Applications and Services at Nokia Mobile Phones. He has been working on Wireless Internet since the introduction of GSM.