
RSA® Conference 2001
April 8-12 • Moscone Center • San Francisco

Pioneer 10 was the first spacecraft to leave the solar system, and is currently the most remote object made by man... over seven billion miles from Earth. Heading towards the constellation Taurus, it will take Pioneer two million years to cross the gulf between the stars. But should some alien traveler encounter Pioneer along the way, it bears a greeting card from humanity - with a return address: this map, showing the position of our solar system relative to 14 prominent pulsars and the center of the Milky Way Galaxy.

The detection of a communication of extraterrestrial origin would be one of the greatest events in human history. Yet, paradoxically, the very differences that would make any subsequent transfer of knowledge so valuable would almost certainly impede it. How could we possibly decipher a message from beings whose very modes of consciousness might be completely unlike our own?

Ever since Frank Drake first aimed his 85-foot radio telescope at Tau Ceti on April 8, 1960, the science of cryptology has played an important role in the formulation of strategies for interpreting such a message. And hopefully, someday - our talents can be applied to help compose the response.

Join more than 200 industry vendors and 10,000 decision-makers from business, government, academia, Wall Street, and the media at the industry's premier data security and cryptography event. The annual U.S. RSA Conference delivers keynote presentations from industry leaders and international policy makers, plus over 200 individual break-out sessions on topics ranging from the latest in cutting-edge cryptographic research to the most current implementations of enterprise security and secure electronic commerce.

RSA security inc. presents

RSA® Conference 2001

April 8-12 • Moscone Center • San Francisco

P.01

RSA SECURITY

RSA Security Inc., The Most Trusted Name in e-Security™, helps organizations build secure, trusted foundations for e-Business through its RSA SecurID® two-factor authentication, RSA BSAFE® encryption and RSA Keon® digital certificate management systems. With more than a half billion RSA BSAFE-enabled applications in use worldwide, more than six million RSA SecurID users and almost 20 years of industry experience, RSA Security has the proven leadership and innovative technology to address the changing security needs of e-Business and bring trust to the new, online economy. RSA Security can be reached at www.rsasecurity.com.

sponsors

without the support of several major sponsors, the annual RSA conference would be impossible. Please join us in showing support for our partners:

COMPAQ

COMPUTER ASSOCIATES
Software superior by design.

EDS

HEWLETT PACKARD

intel

Microsoft

nCIPHER

RSA SECURITY

VeriSign

Any possible extraterrestrial signal will have to be sifted out from an almost unimaginable morass of background noise and earthly sources.

overview

The RSA Conference consists of four main components: General Sessions, Expo, Tutorials and Class Tracks. The General Sessions bring everyone together for special keynote addresses, expert panels and discussions of general interest. This year's Expo – the largest security expo ever staged – will feature over 181,000 square feet of exhibit space with more than 200 vendors demonstrating the very latest e-Security products.

Optional Sunday tutorials and immersion training sessions will provide the basics of crypto technology, enterprise security and network security development techniques. Last but not least, thirteen simultaneous Class Tracks – presented in the state-of-the-art Metreon theatre complex attached to Moscone Center – will feature a wide variety of workshops, seminars and talks. This year's Conference offers an expanded catalog of over 200 classes, tracked as follows:

	SUN 04:08	MON 04:09	TUE 04:10	WED 04:11	THU 04:12
MORNING		Class Tracks	Class Tracks Expo Open	Class Tracks Expo Open	Class Tracks
AFTERNOON	Tutorials	General Sessions	General Sessions Expo Open	General Sessions Expo Closes	General Sessions
EVENING	Welcome Reception	Expo Reception		nCipher Gala	

class tracks

Analysts' Track	Topics of interest to industry analysts, public interest groups, lawmakers and the media.
Cryptographers' Track	Presentation of the latest developments in the science of cryptography for mathematicians, academics and researchers.
Developers' Track	Classes for developers building security-enabled solutions.
Law and Policy Track	Topics of interest to 'hacktivists,' privacy and civil-rights activists, policy-makers, lawyers, lawmakers and public-interest groups.
Freedom and Privacy Track	Sessions for privacy and civil rights activists, policy-makers and academics.
Government Track	Topics of interest to the public sector and the industries that serve it: federal, state and local contractors and government employees.
Hackers and Threats Track	Talks focusing on network forensics, hacks, attacks and countermeasures.
Implementers' Track	Case studies and practical advice for the IS professional implementing security solutions in the enterprise.
Industry Track	Industry-specific case studies and solutions, focusing on Finance, Telecom/Wireless, Healthcare/Biotech and ASPs.
New Products A Track	Demonstrations and product pitches featuring the latest crypto-enabled and e-Security products.
New Products B Track	More demonstrations and product pitches featuring the latest crypto-enabled and e-Security products.
RSA Products Track	Immersion workshops for security professionals working with RSA Security products.
Standards Track	Discussions covering domestic and international standards efforts in security and e-Commerce.

social events

You know what they say about "all work and no play"... a jam-packed day at the RSA conference can be hard on the neurons, so we understand the importance of a little relaxation. The conference offers several opportunities for you to enjoy yourself and network with your colleagues. So join us for a refreshment and perhaps a bite to eat at one of the events listed below.

RSA SECURITY

sunday: welcome reception and early check-in

Check-in to the Conference, get your badge and retrieve your materials on Sunday evening, and avoid the crowds and long lines of Monday morning...then join us for a special welcome reception hosted by your friends at RSA Security Inc.

A maze of sights and sounds, mirrors and movement, bubbling cauldrons and scary good times - and you're the one making it happen with every move you make. Based on award-winning author Maurice Sendak's "Where The Wild Things Are," you'll find that adventure lurks behind every tree, every forest and every cave with goblins, flying birds, howling creatures and interactive entertainment. We promise plenty of food and drink, music, and a great chance to network before the schedule really heats up.

Where the Wild Things Are, Metreon – A Sony Entertainment Center.
Early Check-in: Sunday 12pm - 8pm, Moscone Center North Lobby
Welcome Reception: 6pm - 8pm, Metreon Terrace

monday night: expo reception

Monday night the exhibit hall opens for a private showing, just for Full-Conference attendees. Here's where you get a sneak preview of the products and demonstrations at the largest computer security exhibition ever staged, before the hall opens to the crowds and general public Tuesday morning. Of course, cocktails and appetizers will be served to sustain you on your long trips up and down the aisles.

Moscone Center North – Hall D & E
Monday Night, 6pm - 8pm

nCIPHER™

wednesday: nCipher cryptographers' gala

Dress up, step out and join us at what WIRED magazine called "one of the Last Great Parties of the computer industry." First-rate entertainment, champagne and food by one of the best caterers in the country. The annual Cryptographers' Gala is truly an event not to be missed. Open to all Full-Conference attendees, speakers and registered press.

California Academy of Sciences
Wednesday Night, 7pm - 11pm
Business formal attire is suggested.

Eyewitness accounts of unidentified flying objects are sometimes corroborated by anomalous, seemingly "impossible" radar tracks at local air traffic control centers.

sunday tutorials

The RSA Conference has traditionally been the gathering of industry insiders – however, as the applications of security technologies have broadened, so have our audiences. To make sure that everyone gets the most out of the Conference, we are pleased to offer special Sunday Tutorials. They will help professionals who are new to crypto and security technologies get off on the right foot. They can also serve as useful refresher courses, laying the foundation for the more advanced classes you will attend at the Conference later in the week. At $395, you won't find a better educational value anywhere else. So, join us a day early, and brush up on the basics!

Space is limited to the first 500 registrants: sign up for the Sunday tutorials now by calling 1.800.340.3010 toll free (in the U.S. or Canada) or +1.415.544.9300.

enterprise security basics tutorials

sunday02:00pm
Authentication Options
Bill Duane, RSA Security Inc.
When is a password good enough? When are digital certificates required? When do smart cards make sense? This session provides an objective description of the many options currently available for user authentication, including time-synchronous tokens and the use of digital certificates in conjunction with tokens, smart cards, virtual smart cards and biometrics.

sunday03:00pm
PKI Primer
Bruce Leary, RSA Security Inc.
For IT professionals with no previous knowledge of Public Key Infrastructure (PKI), this session provides a high-level description of a PKI's essential components, how PKIs function, and how PKIs can effectively coexist and interoperate. Also addressed is the management of keys and digital certificates, including registration, certification, distribution and protection of the private key.

sunday04:00pm
PKI-Enabling Applications
Andrew Nash, RSA Security Inc.
Organizations have come to realize the value of protecting and controlling access to their mission-critical data and backend applications based on a common security infrastructure such as PKI. This session describes several methods including developer toolkits, agent technology, Web-based front ends, and other middleware approaches to PKI-enable existing applications.

sunday05:00pm
PKI ROI
Derek Brink, RSA Security Inc.
The business case for security must increasingly show not only how it mitigates risk, but also how it reduces costs or increases top line revenues. This session describes a return on investment (ROI) framework for PKI implementations with an emphasis on the "R" from the perspective of several specific industry segments, including financial, manufacturing, and healthcare.

developer security basics tutorials

sunday02:00pm
e-Security 101
Steve Burnett, RSA Security Inc.
Learn how basic e-Security technologies – modern day cryptography and application independent security protocols – are working together to provide secure e-Commerce transactions. Participants will be instructed through the maze of public and secret key cryptography to understand when to use protocols, like SSL, IPSec, and WTLS with the appropriate ciphers like the fast RC4 symmetric cipher.

sunday03:00pm
e-Commerce Security in Action!
Stephen Paine, RSA Security Inc.
Cryptography is great for security and number theorists, but sometimes difficult to implement in e-Commerce applications. Find the answers to the many implementation questions that are plaguing e-Commerce security like how to optimize performance, achieve client side authentication and learn how protocols like SSL are being used today on the Internet to do this and much more.

sunday04:00pm
Wireless e-Commerce Security in Action
Mike Vergara, RSA Security Inc.
Your wallet just became digital. And, actually it's in your phone. How will millions of wireless users who now have Internet-enabled wireless devices interact with your e-Commerce site? How will you achieve end-to-end security in today's wireless architectures? Find out how protocols like SSL, WTLS, and IPSec are being used in wireless devices to allow secure e-Commerce transactions.

sunday05:00pm
How Secure is Secure?
Blake Dournaee, Kim Getgen, Nino Marino; RSA Security Inc.
Security is about staying one step ahead of the "hackers, crackers, spies and thieves." There are implementation issues, security policies, and economic forces at work, which either protect customers' digital assets or put these assets at risk. This panel will cover the hard facts to make decisions about the amount of security needed for e-Commerce sites based on economic and technical issues.

Tuition for the tutorials is $395. Please note: tutorials are open to full-Conference attendees only.

keynotes and general sessions

monday02:00pm

Welcome

Jim Bidzos, Vice Chairman, RSA Security Inc.

Jim Bidzos was President of RSA Data Security for 12 years and currently serves as Vice Chairman of the Board. Under his leadership, RSA has become the worldwide de facto standard for encryption.

A warm welcome to you from Jim Bidzos, Vice Chairman of the Board, 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, the security year in review and the RSA Awards for excellence in security.

monday02:45pm

Economics of Internet Time

Dr. Paul Erdman

Noted author and economist, Paul Erdman is a former commercial bank CEO and author of thirteen books. He is a regular contributor to publications such as The New York Times, the Washington Post and the London Financial Times.

While the technology engine driving business growth and productivity may be running out of steam, its impact on the world's economy promises to have lasting impact on California, the nation and the world. Economist and author Paul Erdman will review the fundamental social and business changes brought about by the Internet economy, and what this will mean in the next decade.

monday03:30pm

Authenticity in e-Business

Scott Schnell, Sr VP of Marketing, RSA Security Inc.

Mr. Schnell directs the global marketing and communications efforts for RSA Security. He is responsible for building the marketing organization and developing the company's long term strategy.

E-commerce, m-Commerce, and outsourcing are placing greater demands on the expanding network for authenticity of people, devices and transactions in the wired and wireless worlds. Mr. Schnell looks at authenticity on the Internet and the use of certificates to bind digital identities to devices and transactions in 2001 and beyond.

monday04:30pm

Cryptographers' Panel

Peter Neumann, SRI International; Burton S. Kaliski Jr, RSA Laboratories; Ron Rivest, MIT Laboratory for Computer Science; Whitfield Diffie, Sun Microsystems; Adi Shamir, Weizmann Institute; Paul Kocher, Cryptography Research; Tal Rabin, IBM

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

monday05:15pm

Pulling Intelligent Signals Out of Cosmic Noise

Jill Tarter, Principal Investigator, SETI

A recipient of a Lifetime Achievement Award for her contribution to the field of exobiology, Dr. Jill Tarter is Director for Project Phoenix, the SETI Institute's privately funded continuation of HRMS.

"The probability of success is difficult to estimate, but if we never search, the chance of success is zero" (Cocconi and Morrison, 1959). After 40 years, we still have hardly begun to search. Fortunately, new technology for signal processing and antenna construction is about to change all that. Dr. Tarter gives us an update on the search – and the latest scientific thinking on the prospects for success.

tuesday02:00pm

Security for the New Millennium

Michael Fister, VP and GM, Intel

Mr. Fister leads the organization that develops, markets and supports building blocks for enterprise computing including the design of IA-32 and IA-64 processors, chipsets and platforms for workstations and servers.

In 2001, Intel-based servers combined with optimized RSA Security libraries offer the world access to trusted secure transactions, thus enabling transparent anytime, anywhere communications by LAN, WAN, wireless network, or Internet.

tuesday02:45pm

The Year of PKI

Panelists: Art Coviello, President & CEO, RSA Security; John Ryan, President & CEO, Entrust Technologies; Fran Rooney, CEO, Baltimore Technologies; Stratton Sclavos, President & CEO, VeriSign

Moderators: Victor Wheatman, Gartner Group; George Hulme, Information Week; Jim Kerstetter, BusinessWeek

What's changing to make 2001 the "Year of PKI"? What are the attributes of PKI-centric computing? What applications are requiring PKI implementation? What are today's customers doing differently that is driving the need for PKI in 2001? Who better to ask than our distinguished panel of CEOs from the leading PKI vendors, who will be in the hot seat to answer the tough questions about successful implementations of PKI, ROI and the future of PKI.

tuesday03:30pm

Enabling Collaboration

Alex van Someren, CEO, nCipher

Mr. van Someren oversees corporate, strategic and emerging business for nCipher. He has 20 years experience in the IT sector and is the author of several books on the applications of computers and microprocessors.

The future of e-Business is one in which people connect with people freely. Effective security sets people free to take control of the way that they do business. Collaboration and openness become the norm, costs fall and we get things that really add value. The technology must be an enabler, freeing organizations to work in new ways and opening up a world in which customers can connect whenever and however they need to.

tuesday04:30pm

Ensuring Security in the .NET Era

Special Guest, Microsoft

*Microsoft's recently-announced .NET initiative promises to harness the power of the Internet to provide unprecedented scalability, reliability, and manageability for business-to-business and business-to-consumer services. Security is an integral part of the .NET vision, and will be vital in ensuring its widespread adoption. Hear how Microsoft is **already** refining its approach to product development.*

tuesday05:15pm

e-Business Infrastructure: Secrets for Success

Sanjay Kumar, President and CEO, Computer Associates International, Inc.

Under Mr. Kumar's guidance, CA has emerged as the leading provider of highly scalable e-Business solutions by extending its leadership in distributed management.

There are six infrastructure secrets critical to successful e-Business implementations — integration, portal-based access, personalization, scalability, manageability, and a focused e-Security approach. Mr. Kumar will explore the e-Business challenges facing leading enterprises, and particularly, the increasingly important role of e-Security as an enabling technology.

wednesday02:00pm

Future Domains: IP ID and Trust on the Internet

Stratton Sclavos, President & CEO, VeriSign

Mr. Sclavos joined Verisign as President and CEO in July of 1995. Under his guidance the company has grown to become the market leader in trusted certification services for the Internet.

Mr. Sclavos looks at the Internet of the future and the role digital identity will play. He offers a visionary perspective on digital identity and the Internet's central role as an easily accessed, universal locator and repository of personal information.

wednesday02:45pm

Secure Infrastructures and the New Realities

Shane Robison, Sr VP & CTO, Compaq

Mr. Robison is responsible for enhancing the integrated technical community within Compaq and providing leadership in identifying joint initiatives and business development opportunities.

Wireless technologies will unleash a torrent of new kinds of blended applications. They will also provide an unprecedented opportunity to create a new personalized channel with customers. Volumes will be unprecedented. Join Compaq Computer Corporation's Chief Technical Officer Shane Robison for a glimpse of the new infrastructures that will support this innovative era in secure computing.

wednesday03:30pm

The Threat

Richard Power, Editorial Director, Computer Security Institute; Martha Stansell-Gamm, Chief of Computer Crime & Intellectual Property Section, U.S. Department of Justice; (other guest panelists to be announced.)

How vulnerable is the Internet to hackers, terrorists, and criminals, really? Are cryptographic protocols enough to fix these problems? What would it take to bring down the Internet today? This panel explores the vulnerabilities, threat models, and possible solutions facing emerging networks, with an emphasis on understanding what cryptographic techniques can and can't do to protect networks against various attacks.

wednesday04:30pm

Securing the Infrastructure

Roberto Medrano, GM Internet Security Solutions Division, Hewlett Packard

Recognized as an international expert in the field of Internet security, Mr. Medrano educates business, academia, government and law enforcement about safety and security of the Internet.

The road to e-Business will continue to twist and turn as the technology matures and customers become even more comfortable with online commerce. Success will depend on how well businesses secure their infrastructure and how safe the public perceives it to be. This session will focus on what you need to do to secure your infrastructure and ensure safe passage online for customers and consumers.

wednesday05:15pm

How the War Was Won

Steven Levy, Sr Editor & Chief Technology Writer, Newsweek

Mr. Levy's articles have appeared in The New Yorker, Rolling Stone and The NY Times Magazine. His most recent book is "Crypto: How the Code Rebels Beat the Government."

How did cryptography blossom from a government-protected enclave, walled off by laws, secrecy orders and barbed wired, to a thriving industry devoted to protecting personal information and privacy? As a journalist, Steven Levy, author of the just-published book, "Crypto," has covered this fascinating rise and has some surprising stories to tell – as well as some insights into the future of the business.

thursday02:00pm

Trust - The Key to Unlocking the Digital Economy

Shakil Kidwai, VP Global Information Assurance Services, EDS

Mr. Kidwai designs and markets the life cycle approach of EDS to safeguarding information assets of organizations.

Mr. Kidwai will address the importance of trust between transacting parties in the digital economy. He will identify barriers that limit the amount of economic activity and highlight how implementing the concepts of information security can minimize those barriers. He will share examples of how EDS is implementing the principles of trust as enabler for its clients to maximize their success in the digital economy.

thursday02:45pm

Closing Comments

Dana Carvey, Comedian

Emmy-award winner Dana Carvey appeared on Saturday Night Live from 1986-1992, performing as The Church Lady, George Bush and others. He brought one of his characters to the big screen, appearing as Garth in "Wayne's World."

Join Dana Carvey for a hilarious closing keynote for this year's RSA Conference. (Mr. Carvey's performance may contain language and/or subject matter offensive to some. Audience discretion is advised).

Most of the SETI programs in existence today, including those at UC Berkeley, use large computers that analyze data from telescopes in real time. None of these computers look very deeply at the data for weak signals, nor do they look for a large class of signal types, because they are limited by the amount of computer power available for data analysis. To address this shortcoming, projects like SETI@Home use idle time on hundreds of thousands of PCs across the Internet as a "virtual supercomputer".

analysts' track

Topics of interest to industry analysts, public interest groups, lawmakers and the media.

monday08:00am

New Methods of Time Stamping & Blind Authentication

Ruven Schwartz, CertifiedTime; William Kobel, Deloitte & Touche; Robert Temple, BT; David Liu, Cal State University Northridge; Craig Honick, Firstuse.com

Delivering accurate and provable time is more difficult than might at first be realized. The complexities of establishing that connection and the value to the enterprise of establishing it will be revealed.

monday09:00am

Below The Fold

Kevin Poulsen, Editorial Director, SecurityFocus.com

Why do some computer security stories break into the mainstream, while others sink to the bottom? This session will look at some tales of crime and heroism that did not make the headlines, and count down the top ten underreported stories of 2000.

monday10:00am

Fiducia – Modeling Risk in PKI Interoperation

Jimmy Tseng, Researcher, London School of Economics

The interpretation of X.509v3 certificate policy extensions cannot be easily automated due to the absence of established registration authorities for CPs to which other CAs may refer before defining their own CPs, and the lack of mechanisms for determining the equivalence between CPs. What are the implications for trust models?

monday11:00am

The Coming IT Security Consolidation Wave: Implications and Opportunities

Don More, VP, Updata Capital Inc.; Chuck Jones Jr., Analyst, Salomon Smith Barney

Security M&A will markedly increase over the coming year, presenting opportunities to industry participants. The presenters extrapolate from past transactions to paint a picture of the future security software and services landscape.

tuesday08:00am

Everyone's Problem: Attracting and Retaining Information Security Professionals

Lee Kushner, CEO, LJ Kushner & Associates

The current shortage of information security professionals is well documented. Recruitment strategies, compensation guidelines, and retention plans will all be discussed. From practical examples one will learn what information security professionals are really searching for and how to attract them to a company's team.

tuesday09:00am

Selling Security: A History and Analysis of Marketing Strategies in the e-Security Industry

Kurt Stammberger, Principal, Coda Creative

How did companies like RSA, BBN, Trusted Information Systems and other members of the security Avant-Garde survive the lean years before the ascendance of the Internet? What lessons can they offer for today's startups? This talk will examine advertising, press relations, product positioning and branding strategies.

tuesday10:00am

B2B e-Commerce: The Migration From EDI to the Internet for Secure e-Transactions

Ambarish Malpani, Chief Architect, ValiCert

This presentation will examine how five different leading companies in banking/financial services and healthcare have migrated from EDI to the Internet in transacting business online.

tuesday11:00am

The Move to Wireless: Privacy Concerns and Solutions for Wireless Technology

Shawn Abbott, CTO, Rainbow Technologies

The rapid technology behind WAP and the wireless Web today presents a great challenge. Security holes exist yet the public expresses great concern over privacy. This talk will address the current standards for wireless security as well as its future.

wednesday08:00am

When and How to Use Security Consultants

Eran Feigenbaum, PricewaterhouseCoopers

This presentation will examine security implementation engagements from both sides: the client and the service provider. Often the client and the service provider have different agendas and success matrixes. While these are not hidden agendas, they do need to be managed.

wednesday09:00am

Directions in Password Based PKI

Ravi Sandhu, Professor, George Mason University

How does one build PKI infrastructures for consumers who do not have smartcards, roam between PCs, and between PCs and wireless devices? This talk compares and contrasts the practicality of various approaches.

thursday09:00am

PKI: Inhouse Vs. Outsource

Neal Creighton, Equifax Secure; Dean Coclin, Baltimore Technologies Inc.; Chris Bailey, Equifax Secure; Jason Alley, Xcert International

Organizations today have many PKI vendor choices. Some vendors focus on products, while others focus on services. This presentation takes a closer look at both solution methodologies and provide tools to measure when each solution is appropriate.

wednesday10:00am

How Do You Trust a Certificate Authority?

Alfred Van Ranst, Jr, Partner, KPMG LLP

The AICPA's CA Trust service allows independent auditors to examine CAs by comparison to a set of minimum criteria and issue seals that convey trust to relying parties. This presentation will also address the differences between CA Trust and SAS 70.

thursday10:00am

Aspects of the German and European Security Market

Johannes Wiele, Editor, Computer Reseller News Germany

U.S. companies presenting their products in Germany and other European states have to deal with unique laws and feelings about the Internet, e-Commerce and privacy. This talk will explain some of these and will try to analyze their influence on the market.

wednesday11:00am

People as Part of the Equation for Information Security

Mark McGovern, Sr Consultant, EDS

The implementation and adoption of information protection capabilities does not necessarily imply a secure environment. This presentation discusses ways to help encourage users to understand and participate in these sometimes seemingly intrusion into their current way of doing their work.

thursday11:00am

Source Code and Security: Myths and Realities

Steve Lipner, Lead Security Program Mgr, Microsoft Corporation

There has been much recent debate about the role of source code availability and open source development in the development of secure software. This talk will review the debate and present some evidence intended to inform evaluation of the alternatives.

cryptographers' track

Presentation of the latest developments in the science of cryptography, for mathematicians, academics and researchers

NEW CRYPTOSYSTEMS
Session Chair: Dan Boneh

monday08:00am

Fast Generation of NICE Schnorr Type Signatures

Detlef Huehnlein, Secunet AG

There is proposed a Schnorr-type signature scheme based on non-maximal, imaginary quadratic orders, which signature generation is – for the same conjectured level of security – about twice as fast as in the original scheme. In this work, speakers will significantly improve upon this result, by speeding up the generation of NICE-Schnorr-type signatures by another factor of two.

monday08:20am

New Key Agreement Protocols in Braid Group Cryptography

Michael Anshel, Iris Anshel, Dorian Goldfield, Benji Fisher; Arithmetica Inc.

KA protocols are presented whose security is based on the difficulty of inverting one-way functions derived from hard problems for braid groups. Efficient/low cost algorithms for key transfer/extraction are presented. Attacks/security parameters are discussed.

GAMBLING AND LOTTERIES
Session Chair: Burt Kaliski

monday11:00am

Fair e-Lotteries and e-Casinos

Eyal Kushilevitz, Technion; Tal Rabin, IBM Research

Discussion provides protocols for fair lottery and casino games. These fair protocols enable to remove the trust from the casino/lottery without resorting to another trusted third party, by allowing the user to participate in the generation of the specific run of the game. Furthermore, the user can verify the correctness of the execution at the end of the run.

monday11:20am

Secure Mobile Gambling

Dr. Markus Jakobsson, Bell Labs; David Pointcheval, ENS; Adam Young, Lockheed

Panelists study fair gambling methods with security against various disconnection and payment refusal attacks. They focus on computationally lightweight methods, allowing the games to be implemented and played on cellular phones without concerns of excessive computation or power consumption.

FLAWS AND ATTACKS
Session Chair: Josh Benaloh

tuesday03:00am

Security Weaknesses in Bluetooth

Susanne Wetzel, Markus Jakobsson; Bell Labs

Speakers point to three types of weaknesses in Bluetooth, allowing an attacker to geographically locate victim devices; derive plaintexts from ciphertexts without knowing the keys; and eavesdrop on and impersonate victim devices. Presenters also discuss possible countermeasures to the attacks.

RSA
Session Chair: Scott Vanstone

monday09:00am

Improving SSL Handshake Performance Via Batching

Dan Boneh, Hovav Shacham; Stanford Univ.

Speakers present an algorithmic approach for speeding up SSL's performance on a Web server. The approach improves the performance of SSL's handshake protocol by up to a factor of 2.5 for 1024-bit RSA keys. It is designed for heavily-loaded Web servers handling many concurrent SSL sessions, improving the server's performance by batching the SSL handshake protocol.

monday09:20am

From Fixed Length to Arbitrary – Length Practical RSA Padding Schemes

Genevieve Arboit, McGill University; Jean-Marc Robert, Gemplus

Presenters show how to construct a practical secure signature padding scheme for arbitrarily long messages from a secure signature padding scheme for fixed-length messages. This new construction is based on a one-way compression function respecting the division intractability assumption.

monday09:40am

An Advantage of Low-Exponent RSA with Primes Sharing LS Bits

Ron Steinfeld, Yuliang Zheng; Monash Univ.

The Boneh-Durfee-Frankel Partial Key Exposure (PKE) attack on low public-exponent RSA is shown intractable for RSA moduli with primes sharing m LS Bits (large m). Security against conventional attackers is shown to imply security against PKE attackers.

SYMMETRIC CRYPTOGRAPHY
Session Chair: Yuliang Zheng

monday10:00am

On the Strength of Simply-Iterated Feistel Ciphers With Whitening Keys

Paul Onions, Silicon Infusion Ltd.

The class of Feistel ciphers with identically keyed rounds and independent whitening keys is shown to be breakable with work factor dependent only on block size and to have security that is at best only comparable to the Even-Mansour model.

monday10:40am

Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays

Kris Gaj, Pawel Chodowiec; George Mason University

The results of implementing all five final AES candidates using Xilinx Virtex FPGA devices are presented and compared with results of other groups. Speeds in excess of 10 Gbits/s are demonstrated for all AES candidates working in non-feedback cipher modes.

monday10:20am

Analysis of SHA-1 in Encryption Mode

Lars Knudsen, Univeristy of Bergen; Matt Robshaw, Royal Holloway; Helena Handschuh, Gemplus

A detailed analysis is given of the resistance of SHA-1 used in encryption mode against the most powerful known attacks today. It is concluded that none of these attacks can be applied successfully in practice to SHA-1. The original motivation for this analysis is to investigate a block cipher named SHACAL based on these principles.

REDUCTIONS, CONSTRUCTIONS AND SECURITY PROOFS
Session Chair: Markus Jakobsson

tuesday08:00am

Formal Security Proofs for a Signature Scheme with Message Recovery

Daniel R.L. Brown, Don Johnson; Certicom

This talk will prove the security of the very efficient Pintsov-Vanstone signature scheme with partial message recovery (PVSSR), basing its security on the separate security of its three cryptographic primitives: a symmetric cipher, hash function and an elliptic curve group.

tuesday08:20am

The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES

Michel Abdalla, UCSD; Mihir Bellare, UCSD; Phillip Rogaway, UC San Diego

This talk analyzes the public-key encryption scheme DHIES which is in draft standards ANSI X9.63, SECG, and IEEE P1363a. Discussed are natural assumptions under which DHIES can be proven to provide security against chosen-ciphertext attacks. No random-oracle assumption is required.

tuesday08:40am

REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform

David Pointcheval, ENS; Tatsuaki Okamoto, NTT Labs

This panel presents REACT, a very efficient conversion which transforms, with a negligible computational overload (only two more hashings), any weakly secure encryption scheme into a chosen-ciphertext secure cryptosystem. It furthermore allows symmetric integration for improved efficiency.

tuesday03:20am

Distinguishing Exponent Digits by Observing Modular Subtractions

Colin Walter, UMIST/Datacard Platform Seven; Susan Thompson, Datacard Platform Seven

Modular multiplication algorithms may contain a conditional subtraction to keep output within a word boundary. This subtraction occurs with different frequencies for multiplications and squares, enabling a timing attack on exponentiation. A few hundred observations suffice to reveal the secret exponent, regardless of key length.

tuesday03:40am

On the Power of Misbehaving Adversaries & Cryptanalysis of EPOC

Marc Joye, Gemplus; Jean-Jacques Quisquater, UCL Crypto Group; Moti Yung, CertCo

Key-recovery attack against specific PK systems known to be chosen-ciphertext secure is presented (e.g., the initial EPOC proposal to IEEE-P1363). The attacker probes with valid/invalid ciphertexts, whereas the known security proofs considered valid ciphertexts only due to "modeling vagueness." Also shown is how to repair the systems.

Jupiter, the Great Red Spot, and two of its moons. From the Voyager probe.

IMPLEMENTATION
Session Chair: Jean-Jacques Quisquater

tuesday10:00am

Modular Exponentiation on Fine-Grained FPGA

Alexander Tiountchik, National Academy of Sciences Belarus; Elena Trichina, PACT Informationstechnologie

Panel uses an example of modular exponentiation with Montgomery multiplication to demonstrate a role of layout optimization and partitioning in mapping linear systolic arrays onto two-dimensional arrays of FPGA cells.

tuesday10:20am

Scalable Algorithm for Montgomery Multiplication and Its Implementation on the Coarse-Grain Reconfigurable Chip

Elena Trichina, PACT Informationstechnologie; Alexander Tiountchik, National Academy of Sciences of Belarus

We describe a coarse-grain reconfigurable chip that can perform simultaneously 128 multiply-accumulate operations on 32-bit numbers in one clock cycle. The implementation is fully scalable, with time increasing almost linearly with length of the operands.

tuesday10:40am

Software Implementation of the NIST Elliptic Curves Over Prime Fields

Michael Brown, University of Waterloo; Darrel Hankerson, Auburn University; Julio Lopez Hernandez, University of Valle, Colombia; Alfred Menezes, Certicom Research

Speakers present results of a software implementation of the NIST-recommended elliptic curves over prime fields and binary fields.

NUMBER THEORETIC PROBLEMS
Session Chair: Amir Herzberg

wednesday08:00am

Analysis of the Weil Descent Attack of Gaudry, Hess and Smart

Minghua Qu, Alfred Menezes; Certicom

The talk will analyze the Weil descent attack of Gaudry, Hess and Smart on the elliptic curve discrete logarithm problem for elliptic curves defined over finite fields of characteristic two.

wednesday08:20am

Using Fewer Qubits in Quantum Factorization

Jean-Pierre Seifert, Infineon Technologies

A method to reduce the number of needed qubits in Shor's quantum factorization algorithm to factor a RSA-modulus *N*. While the continued fraction algorithm finds a Diophantine approximation to a single known fraction with a denominator greater than N^2, our method computes approximations to known fractions with a denominator of size $N^{(1+E)}$, E being an arbitrarily small positive constant.

PASSWORDS AND CREDENTIALS
Session Chair: Yacov Yacobi

wednesday09:00am

Relying Party Credentials Framework

Amir Herzberg, NewGenPay Inc.; Yosi Mass, IBM Haifa Research Lab

Panel will present a framework for credentials-relying parties, to allow them to make access control and customer segmentation decisions based on different types of credentials (public key certificates, user-id/password, etc.). The framework collects credentials and maps them to a common structure.

wednesday09:20am

Password Authentication Using Multiple Servers

David Jablon, Integrity Sciences

Improved password-based roaming protocols let users retrieve secret credentials from N servers, while preventing guessing attacks from N-1 compromised servers. Methods provide better tolerance of human errors and increased performance over comparable methods of Ford & Kaliski, with fewer security assumptions.

wednesday09:40am

More Efficient Password-Authenticated Key Exchange

Philip MacKenzie, Lucent Technologies

Presentation will describe various ways to improve the efficiency of the PAK password-authenticated key exchange protocol while maintaining provable security. A simple modification to PAK that cuts the client-side computation in half is discussed.

PROTOCOLS I
Session Chair: Phil MacKenzie

wednesday10:00am

Passive Fingerprinting

Yacov Yacobi, Microsoft Corporation

This presentation discusses how to improve on the Boneh-Shaw Fingerprinting scheme in two ways, chief of which is merging a Direct Sequence Spread Spectrum (DSSS) embedding layer with the first Boneh-Shaw layer, effectively increasing the protected object size by about four orders of magnitude. As a result there is more than one order of magnitude improvement on the size of collusions that can be overcome.

wednesday10:20am

Efficient Asymmetric Public-Key Traitor Tracing without Trusted Agent

Yuji Watanabe, Goichiro Hanaoka, Hideki Imai; University of Tokyo

A new scheme of practical asymmetric public-key traitor tracing without involvement of trusted third parties will be presented. Our protocol contains other desirable features: direct nonrepudiation, full frameproof, black-box traceability for asymmetric scheme.

wednesday10:40am

Targeted Advertising and Privacy Too

Ari Juels, RSA Security Inc.

This talk will explore the notion that targeted advertising and privacy protection need not necessarily be conflicting goals. Presenter describes some conceptually simple and also more technically advanced schemes that facilitate targeted advertising, yet simultaneously offer protection for sensitive consumer data.

MULTIVARIATE CRYPTOGRAPHY
Session Chair: Alfred Menezes

tuesday11:00am

The Security of Hidden Field Equations (HFE)

Nicolas Courtois, INRIA and Toulon Univ.

Speaker presents another attack on HFE (Eurocrypt'96) that Shamir-Kipnis (Crypto '99). HFE is related to a hard problem MinRank. Both attacks give similar sub-exponential complexities. Improved attacks give 2^62 for the HFE Challenge 1, but fail for modified versions of HFE such as Quartz.

tuesday11:20am

QUARTZ, 128-bit long digital signatures

Nicolas Courtois, Louis Goubin, Jacques Patarin; Bull Smart Cards & Terminals

QUARTZ is a multivariate public key signature scheme. Though complex looking, it results from many simple ideas in the same direction: producing very short signatures (only 128-bits) with maximal security (i.e., the secret is hidden as well as possible)

tuesday11:40am

FLASH, A Fast Multivariate Signature Algorithm

Nicolas Courtois, Louis Goubin, Jacques Patarin; Bull Smart Cards & Terminals

FLASH is a very fast multivariate signature algorithm that allows signatures to be easily computed and checked by a low-cost smartcard. Speakers also propose SFLASH: a version that has a smaller public key.

PROTOCOLS II
Session Chair: Ari Juels

wednesday11:00am

Uncheatable Distributed Computations

Philippe Golle, Ilya Mironov; Stanford Univ.

The growth of Internet distributed computing, with financial incentives for participants, is hampered by the threat of cheating. Dishonest participants may claim credit for work they have not done. Speakers propose security schemes to defend against this threat with little overhead.

wednesday11:20am

Forward-Secure Threshold Signature Schemes

Michel Abdalla, Sara Miner, Chanathip Namprempre; UCSD

Panel constructs forward-secure threshold signature schemes: even if more than the threshold number of players are compromised, it is impossible to forge signatures relating to the past. One scheme tolerates mobile eavesdropping adversaries, and the other tolerates mobile halting adversaries.

wednesday11:40am

A Cost-Effective Pay-Per-Multiplication Comparison Method for Millionaires

Marc Fischlin, Goethe University

A non-interactive crypto-computing protocol for the greater-than function to compare two parties' values such that only the relation of the values is revealed. In comparison to previous solutions our protocol reduces the number of modular multiplications significantly.

developers' track

Classes for developers building security-enabled solutions.

monday 08:00am

Securing Mobile Devices for Mobile e-Commerce (m-Commerce) and Enterprise Data

Tim Dierks, VP Product Deveopment, Certicom

As technologies for mobile computing and wireless data advance, m-Commerce will account for an increasing portion of e-Commerce. This presentation will describe the particular requirements of secure wireless environments and describe potential solutions, including a review of the secured Palm VII platform.

monday 09:00am

Continual Improvement: Security Process Improvements in Windows Whistler

Michael Howard, Security Program Mgr, Microsoft Corporation

This talk discusses software development process refinements in Windows Whistler, including automated buffer analysis, and the buffer overrun failfast capabilities of Visual C++ v7. Also discussed is how internal audits and threat modeling techniques were used in the project.

tuesday 08:00am

How to Verify Electronic Signatures

Dennis Pinkas, Sr Security Consultant, Bull

Verifying an electronic signature that may be considered as an equivalent to a manual signature is much more complicated than verifying the validity of a digital signature. The techniques to be used and the architecture of the verification tools will be detailed.

monday 10:00am

What to Consider in Your Internet Security Plan

Robert Shields, Director of Marketing and Product Management, Rainbow Technologies

As businesses launch or evaluate e-Commerce and e-Business initiatives, security must be considered to protect the operation from fraud, unauthorized users and data piracy. This talk explores the high level business and technical issues and caveats of Internet security.

tuesday 09:00am

Integrating Legacy Applications into Your PKI

Steven Spicer, Principal Engineer, RSA Security Inc.

In this session two ways to PKI-enable legacy applications will be discussed. The first is to directly modify the application server and client. The second, more interesting method is to use PKI-enabled proxies to add encryption, authentication and reduced sign-on features to security-challenged apps without touching the applications themselves.

P.12

monday 11:00am

Integrating Authentication and Digital Certificate Technologies to Secure Applications, Transactions

Carl Stucke, VP e-Commerce Research and Development, Equifax Secure

Advancements in technology bring unique solutions to sensitive online transactions. But limitations exist when those advancements do not effectively work together. Successful integration of digital certificates and authentication allows enterprises to address multiple security concerns.

tuesday 10:00am

Advances in Wireless Security Using Application Specific Integrated Circuits (ASICs)

Randall Nichols, VP Cryptography, TeleHubLink

End-to-end wireless security means protecting voice/data with minimal cost, delay, complexity and bandwidth overhead in real-time. This session presents advances gained using encryption and DSP embedded in Application Specific Integrated Circuits (ASICs).

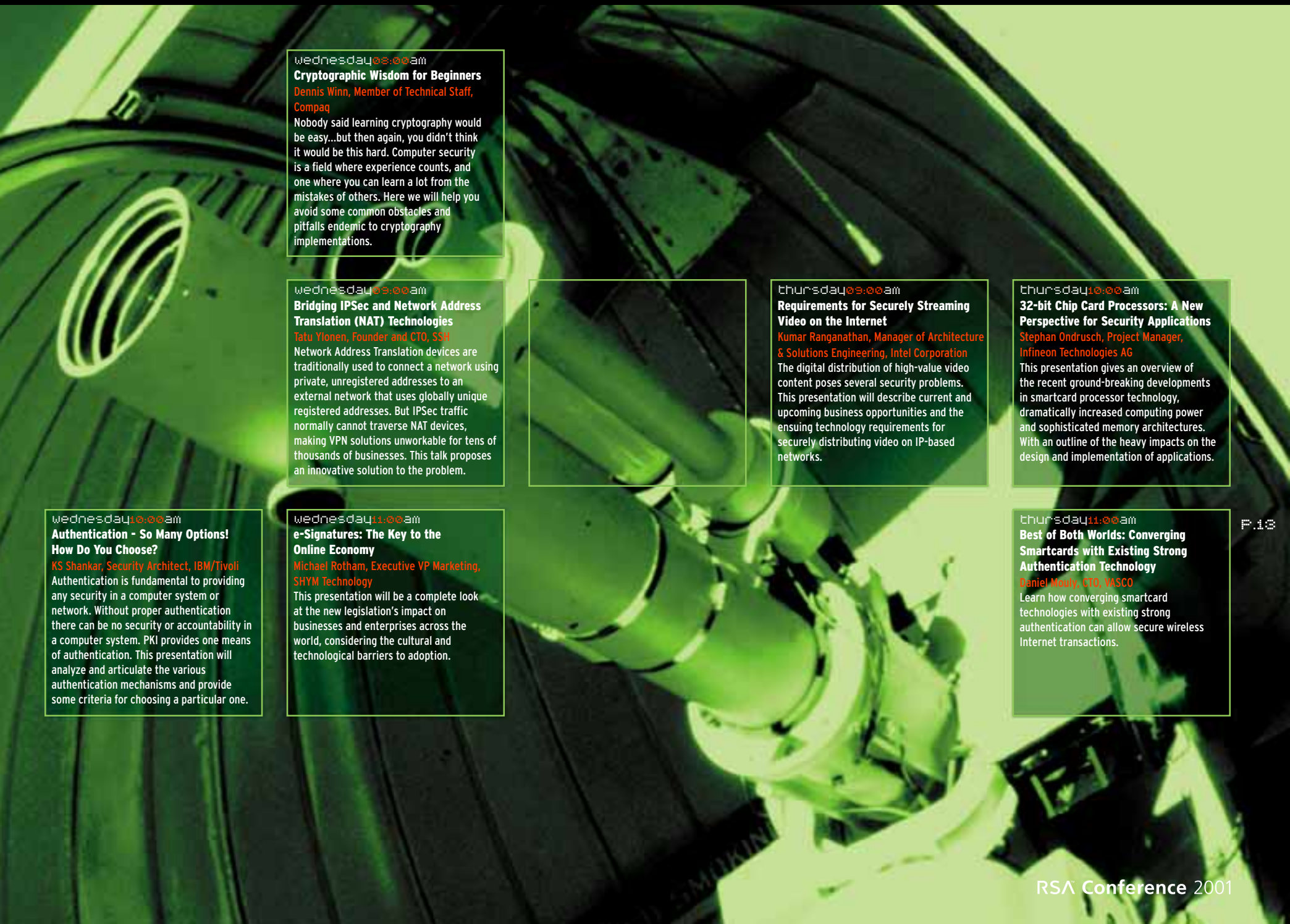
tuesday 11:00am

Performance Analysis of Security Workloads

David Grawrock, Security Architect, Intel

This talk shows how a security workload on a desktop platform affects the platform's available throughput. The security workload includes encrypted drives, IPSec, a trusted OS and TCPA compliance. Both startup time and operational load are examined.

The long cylinder of the NOAA patrol telescope system points from the open white spherical dome of an observation post in Boulder, Colorado.



wednesday08:00am
Cryptographic Wisdom for Beginners
Dennis Winn, Member of Technical Staff, Compaq
Nobody said learning cryptography would be easy...but then again, you didn't think it would be this hard. Computer security is a field where experience counts, and one where you can learn a lot from the mistakes of others. Here we will help you avoid some common obstacles and pitfalls endemic to cryptography implementations.

wednesday09:00am
Bridging IPSec and Network Address Translation (NAT) Technologies
Tatu Ylonen, Founder and CTO, SSH
Network Address Translation devices are traditionally used to connect a network using private, unregistered addresses to an external network that uses globally unique registered addresses. But IPSec traffic normally cannot traverse NAT devices, making VPN solutions unworkable for tens of thousands of businesses. This talk proposes an innovative solution to the problem.

thursday09:00am
Requirements for Securely Streaming Video on the Internet
Kumar Ranganathan, Manager of Architecture & Solutions Engineering, Intel Corporation
The digital distribution of high-value video content poses several security problems. This presentation will describe current and upcoming business opportunities and the ensuing technology requirements for securely distributing video on IP-based networks.

thursday10:00am
32-bit Chip Card Processors: A New Perspective for Security Applications
Stephan Ondrusch, Project Manager, Infineon Technologies AG
This presentation gives an overview of the recent ground-breaking developments in smartcard processor technology, dramatically increased computing power and sophisticated memory architectures. With an outline of the heavy impacts on the design and implementation of applications.

wednesday10:00am
Authentication - So Many Options! How Do You Choose?
KS Shankar, Security Architect, IBM/Tivoli
Authentication is fundamental to providing any security in a computer system or network. Without proper authentication there can be no security or accountability in a computer system. PKI provides one means of authentication. This presentation will analyze and articulate the various authentication mechanisms and provide some criteria for choosing a particular one.

wednesday11:00am
e-Signatures: The Key to the Online Economy
Michael Rotham, Executive VP Marketing, SHYM Technology
This presentation will be a complete look at the new legislation's impact on businesses and enterprises across the world, considering the cultural and technological barriers to adoption.

thursday11:00am
Best of Both Worlds: Converging Smartcards with Existing Strong Authentication Technology
Daniel Mouly, CTO, VASCO
Learn how converging smartcard technologies with existing strong authentication can allow secure wireless Internet transactions.

Law and policy track

Topics of interest to 'hacktivists,' privacy and civil rights activists, policy-makers, lawyers, lawmakers and public-interest groups.

monday 08:00am

Certification Polices and Practices

Stephen Wu, VeriSign; Robert Daniels, EDS; Sarbari Gupta, Conclusive Logic

Private and government organizations are adopting certificate policies as tools to help them control trust propagation. The presentation will cover certificate policies, their uses, and how they differ from practice statements. Finally, the speakers present lessons learned from developing leading private and government certificate policies.

monday 09:00am

E-SIGN: A Primer on the Law and Its Implications for the Future

Behnam Dayanim, Paul, Hastings, Janofsky & Walker; Amy Carlson, Preston Gates Ellis & Rouvelas Meeds; Bill Brice, AlphaTrust

Federal electronic signature legislation has fundamentally changed the legal landscape. This talk will provide a primer on the law's approach toward preemption of state law, technology neutrality, consumer protection and record-keeping, and will discuss lessons learned and future expectations.

tuesday 08:00am

PKI and Consumer Contracting

Hoyt Kesterson II, Consultant; Andreas Bertsch, SIZ; Samoera Jacobs, GlobalSign

A lot of attention has been paid over the last few years to the operation of a CA and the strength of the algorithm used to support a digital signature. A challenge to a signature is likely to focus on how the user signalled intent to sign and on the correct operation of the software. Views on the responsibility for ensuring proper operation vary between U.S. and Europe.

tuesday 09:00am

Consumer Rights on the Line

Andreas Mitrakas, Senior Legal Consultant, GlobalSign; Marguerite Gear, Independent Consultant

The mere fact that transactions are concluded digitally rather than on paper should not lead to the revision of established legal rules on consumer protection and commerce. Yet this seems to be exactly what is happening in the U.S. and the European Community. How will the level of legislators' understanding of technology affect the future of electronic business?

monday 10:00am

Liability Issues Within a PKI

Adrian McCullagh, Director of Electronic Commerce, Gadens Lawyers

Liability is an unresolved issue within the PKI environment. This presentation will discuss the latest advancements in understanding PKI liability and what role insurance will play in resolving the interaction between the subscriber, relying party, Certification Authority and Relying Parties.

tuesday 10:00am

Frontiers in Securing Copyright

Jean-Paul Cailloux, Professor of Law, EDHEC; Scott Moskowitz, Founder & CEO, Blue Spike

Intellectual property has, up until now, been very well protected in the U.S. and Europe via several powerful legal mechanisms. But new technologies are rendering those protections inadequate for copyrighted properties like music and movies. Speakers will discuss the latest advances in copyright protection technologies and deployments.

monday 11:00am

The Role of the Private Sector In Critical Infrastructure Protection

Bruce Heiman, Executive Director, Americans for Computer Privacy; Joseph Pato, CTO Internet Security Solutions, Hewlett-Packard

For e-Business to become business as usual, one must protect our critical infrastructure. But who must act? Are government technology mandates required? This talk will examine the creation of an IT Sector ISAC and its role in addressing information assurance.

tuesday 11:00am

A Survey of International Law and Policy Developments Affecting PKI

Douglas Sabo, VP Infosec Programs, ITAA; Joe Alhadeff, VP Global Public Policy, Oracle

When an issue like information security hits the headlines, governments are sure to follow. Around the world, governments and multilateral organizations are proposing new legislation and regulations for information security. This session will provide a snapshot and analysis of policy developments around the world.

A false-color radar image of the surface of the planet Venus.

freedom and privacy track

Sessions for privacy and civil rights activists, policy-makers and academics.

wednesday08:00am

Privacy Matters in Secure e-Commerce

Andreas Mitrakas, Sr Legal Consultant, GlobalSign; Steven Ross, Partner, Deloitte & Touche

Self-regulation has widely been seen as an appropriate way to resolve international regulatory conflicts in electronic commerce. Diverging views between EU and U.S. regarding the protection of privacy may affect users of security products and services in electronic commerce since the U.S. jurisdiction offers a lower level of protection.

wednesday09:00am

Privacy in the Firm

Brian Tretick, Principal, Ernst & Young; Ralph Poore, CTO, Privacy Infrastructure Inc.

Recent regulations have made the resale of personal information risky at best. This panel addresses the baseline technical and legal requirements for consumer privacy on website and Web-enabled services. This panel will also discuss alternatives and present solutions that enable data owners to generate revenue without releasing personal information.

wednesday10:00am

EU Privacy Laws: Relevance and Impact in the U.S.

Jean-Paul Cailloux, Professor of Law, EDHEC; Roger Merckling, Gemplus; Christopher Kuner, Morrison & Foerster

Privacy regulation in Europe is shifting its focus to building a privacy-friendly infrastructure through the design of hardware and software systems that minimize data processing. This talk will examine the legal and policy implications of such an infrastructure on Europe and the United States.

thursday09:00am

Digital Signatures: The New Rules

Behnam Dayanim, Paul, Hastings, Janofsky & Walker; Amy Carlson, Preston Gates Ellis & Rouvelas Meeds; Andreas Bertsch, SIZ

Just this summer, the Electronic Signatures in Global and National Commerce Act (E-SIGN) became law. What, exactly, will this legislation mean for the practice of digital signatures? What were the political dynamics behind the legislation? What will be the impact of the law on the government's ability to mandate standards?

wednesday11:00am

Privacy Rules, Regulations and Realities

Lawrence Dietz, Director of Strategic Marketing, AXENT Technologies; Jan Lovorn, Corporate Privacy Officer, Protegrity

Public concern for the protection of personal information is driving the development of regulations in financial, government and healthcare marketplaces internationally. We'll outline the new legislation and compare provisions of the U.S. Health Insurance Portability and Accountability Act of 1996 with the U.K. Data Protection Act of 1998.

thursday10:00am

International Commerce & Crypto Policy

Christian Erickson, CryptX; Marguerite Gear, Marguerite Gear Consulting; Richard Youell, nCipher

This panel explores the development and ramifications of modern governmental cryptography and surveillance policy. The discussion will also examine the ramifications of the decision in the landmark Berstein vs. U.S. DoJ case. Specific examples, comparisons and trends, from the perspective of a security vendor are included.

thursday11:00am

Client-Side Computing: Personalized Marketing With Privacy

Glenn Kramer, VP Engineering, Encirq

Who do you trust? Ultimately, it's yourself. Client-Side computing can put trust back in the hands of the individual, while new data engine architectures allow online vendors to market to individuals who opt-in, without revealing that individual's actual identity. The result will deliver individualized, consumer-centered marketing over the Internet in a way that preserves privacy.

government track

Topics of interest to the public sector and the industries that serve it; federal, state and local contractors and government employees.

monday08:00am
Information Assurance - What Is It? Why Should You Care?
Brian Snow, Technical Director Information Systems Security Organization, NSA
This talk will discuss Information Assurance (IA) and the potential impact of the government IA requirements on the business community. Also addressed is the establishment of government IA requirements as a standard and the implications of that standard to the larger commercial enterprise.

monday09:00am
NIST Cryptography Standards Update
Ed Roback, Acting Chief Computer Security Division, NIST
This session will review the status of the Advanced Encryption Algorithm and other components of the NIST cryptography toolkit (key management, hashing and signature algorithms).

tuesday08:00am
Information Assurance – Where Are We Going in the Future?
Daniel Knauf, William Maconachy, Brian Snow, R. Kris Britton, Chris Kubic, Chris Yazbeck; NSA
This panel will explore government IA policy to include: defense in depth, a strategy for robustness, and the use of evaluated products. The discussion entails how government, industry and academia are partnering to fill the critical shortage of IA professionals.

monday10:00am
FIPS 140-2 The Future
Ray Snouffer, Anabelle Lee; NIST; Randall Easter, Technical Engineer, NIST
The panel will provide information on the revised standard (FIPS 140-2), including a detailed description of the revisions and impact to Federal agencies, users, and vendors. Also, a summary analysis of cryptographic modules that have been validated to date and associated information on uses and applications will be provided.

tuesday09:00am
Implementation of e-Government I
Lynn McNulty, RSA Security Inc.; John Weigelt, Government of Canada; Dr. Alfred Tacke, State Secretary, German Federal Ministry of Economics and Technology
This panel will review the implementation of e-Government programs in Canada and Germany which make extensive use of PKI technology to deliver secure electronic services to trading partners and individual citizens.

tuesday10:00am
Implementation of e-Government II
Lynn McNulty, RSA Security Inc.; John Davenport, State of Pennsylvania; William Flanigan, Ballistic Missile Defense Organization; Kathryn Hollis, EDS
This panel examines representative electronic government initiatives that have been implemented at the federal and state level to provide the security needed for secure communications and strong user authentication. It will focus on the lessons learned from these implementations.

monday11:00am
The Common Criteria - Its Status and Impact on the Private Sector
William Miller, Maximum Control Technology; Ken Ayer, Visa; William Franklin, nCipher; Stuart Katzke, NSA
This panel will examine the current status of the Common Criteria, the National Information Assurance Partnership and the development of product specifications that give acquisition preference to certain products.

tuesday11:00am
Government Smartcard Programs
Jim Dray, NIST; Michael Brooks, GSA; Mary Dixon, DOD
This panel provides an overview of Government programs that are being implemented to provide for secure repositories for private keys associated with digital signature and encryption key pairs.

The Eagle nebula, a nearby star-forming region 7,000 light-years away in the constellation Serpens, from the Hubble Space Telescope. The columns — dubbed "elephant trunks" — protrude from the wall of a vast cloud of molecular hydrogen. Inside the light-years long gaseous towers, the interstellar gas collapses under its own weight to form new stars.

wednesday08:00am

Information Assurance - How Are We Going To Get There? Government Efforts to Advance Technology

Chris Kubic, Technical Director, NSA; Chris Yazbeck, Technical Director, NSA

This panel will discuss the migration to IP versus ATM as a target layer for network security moving from 2.4 gigabytes per second encryption to 10 gigabytes and beyond. The presentation will describe the DoD PKI initiative and where it is going.

wednesday09:00am

Enabling G2G and G2B e-Commerce with a Bridge Certification Authority/ Scalability Issues in PKIs

Tim Polk, Computer Scientist, NIST; Bill Burr, Mgr Security Technology Group, NIST

This session will discuss how bridge certificate authority (BCA) will provide the means for the interconnection of PKIs. This presentation describes the different PKI architectures, the difficulties in connecting disparate architectures, and how the BCA addresses these issues.

wednesday10:00am

The Marriage of IPSec and PKI: A Marriage Made in Heaven... or a Troubled Union?

Sheila Frankel, Computer Scientist, NIST; Kathy Lyons-Burke, Supervsr PKI & Apps, NIST

The Internet Key Exchange (IKE), the Key Management component of IPSec, uses PKI technology for the mutual authentication of peers. Presentation will discuss the use of PKI technology in IPSec and IKE, the PKI-related hurdles to interoperability, and NIST's contributions in this arena.

thursday09:00am

The Evolving Federal PKI and Related Activities and Programs

Judith Spencer, Chair-Federal PKI Steering Committee, GSA; Rich Guida, Chair-Federal PKI Steering Committee, Department of Treasury

The Federal Government is moving forward with several key initiatives to enabling public key technology for strong identity authentication. These initiatives, including ACES and the Federal Bridge CA will be discussed in this panel discussion.

thursday10:00am

System Integration and Security: Solution Transference from the Public to the Private Sector

Jonathan Chinitz, VP & GM, VASCO; William Flanigan, Chief IA Infrasturture Protection, Ballistic Missle Defense Organization

Security solutions for government system integration can be transferred to the private sector. Learn how the Department of Defense's health system allows sensitive information to be accessed worldwide while remaining secure.

wednesday11:00am

The New Regime of Government Regulation of Information Security

Peter Harter, Securify; Stewart Baker, Steptoe & Johnson; Chris Kuner, Morrison & Foerster; Masanobu Katoh, Fujitsu Limited

Unlike the crypto wars of the 1990s today's regime of information security government regulation encompasses the control of the data itself. Internationally recognized experts in the law and policy of the Internet, cryptography and trade will discuss this emerging issue.

thursday11:00am

Digital Certificates for Citizens

Stanley Choffrey, GSA; Martin Roe, UK Royal Mail; Keren Cummings, Digital Signature Trust; Donna Dodson, Social Security Administration

This panel will discuss the GSA Access Certificates for Electronic Services Program and the corresponding program of the UK Royal Mail to provide digital identities for citizens wishing to conduct business with government agencies.

hackers and threats track

Talks focusing on network forensics, hacks, attacks and countermeasures.

monday 08:00am

Computer Forensics: Unmasking the Network Intruder

Julie Lucas, Computer Security Practice Director, Global Network Technology Services

Computer forensics experts are making a paradigm shift to viewing the computer as a crime scene. Learn about network forensics, where evidence of an attack resides, and ways one can aid a response team in identifying the intruder.

monday 09:00am

Security Realities in the Age of e-Commerce

Bruce Schneier, CTO, Counterpane Internet Security, Inc.

The problem with bad security is that it looks just like good security. Presentation discusses failures of security testing and problems of securing modern complex systems. Strategies that leverage process are our only hope for a secure digital future.

monday 10:00am

You Are the Key: Biometric Access to Encryption Key Management

Jim Kawashima, Business Development Manager, SecuGen Corporation

Biometric technology uses a person's unique physical traits for secure access that is intuitive, convenient and conspicuously resistant to forgery. Speaker will present an overview of the theoretical and practical application of biometric enhancement of existing encryption key management systems.

monday 11:00am

Application-Level Forensics for MS Windows

Ryan Russell, Technical Editor, SecurityFocus.com

Learn how to examine a Windows computer to determine what the operator has been up to. Useful for both intrusion investigation, as well as simple policy violation.

tuesday 08:00am

Attacks Against the Netscape Browser

James Roskind, Chief Scientist, Netscape Communications Corporation

The Netscape browser is deployed on many millions of desktops. It has been the target of many attacks that attempt to gain access to system resources. There will be a review of the attacks, the product architecture and the ways to foil such efforts.

tuesday 09:00am

Making Reverse-Engineering Harder

Robert Baldwin, Partner, Plus Five Consulting Inc.

The security of many products rests on their ability to hide a secret key or prevent tampering. Follow along as we crack two programs, and explain several techniques to make reverse-engineering harder.

tuesday 10:00am

Security Issues for Voice Over IP

Gregory White, VP Professional Services, SecureLogix Corporation

With the movement towards a convergence of voice and data networks, it is important to understand the security implications. This talk will address Voice over IP and the security implications of this method to transmit voice.

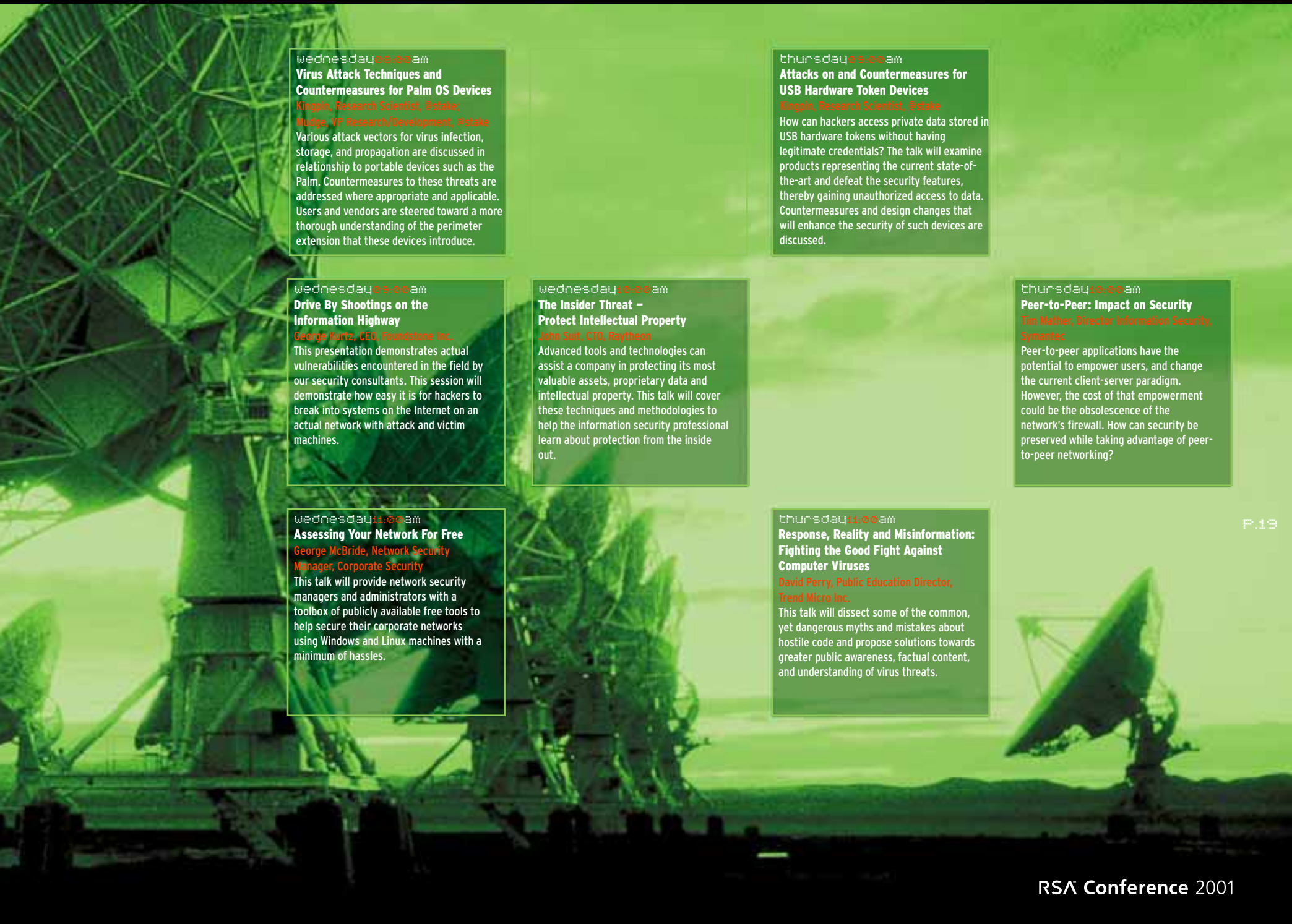
tuesday 11:00am

e-Marketplaces: Next in Line for Internet Fraud Crisis

Kristin Kupres, COO, Identrus

Internet fraud complaints rose 38 percent in 1999 with online auction sales making up 87 percent. B2B Internet auctions and marketplaces are next in line. Learn how auction fraud is perpetrated, where the big risks lie and how to apply solutions.

The dishes of the Very Large Array in New Mexico, one of the world's premier astronomical radio observatories. The VLA consists of 27 mobile antennas on tracks that can be arranged in a huge Y pattern up to 36km (22 miles) across — roughly one and a half times the size of Washington, DC.



wednesday 9:00am

Virus Attack Techniques and Countermeasures for Palm OS Devices

Kingpin, Research Scientist, @stake; Mudge, VP Research/Development, @stake

Various attack vectors for virus infection, storage, and propagation are discussed in relationship to portable devices such as the Palm. Countermeasures to these threats are addressed where appropriate and applicable. Users and vendors are steered toward a more thorough understanding of the perimeter extension that these devices introduce.

thursday 9:00am

Attacks on and Countermeasures for USB Hardware Token Devices

Kingpin, Research Scientist, @stake

How can hackers access private data stored in USB hardware tokens without having legitimate credentials? The talk will examine products representing the current state-of-the-art and defeat the security features, thereby gaining unauthorized access to data. Countermeasures and design changes that will enhance the security of such devices are discussed.

wednesday 9:00am

Drive By Shootings on the Information Highway

George Kurtz, CEO, Foundstone Inc.

This presentation demonstrates actual vulnerabilities encountered in the field by our security consultants. This session will demonstrate how easy it is for hackers to break into systems on the Internet on an actual network with attack and victim machines.

wednesday 10:00am

The Insider Threat – Protect Intellectual Property

John Suit, CTO, Raytheon

Advanced tools and technologies can assist a company in protecting its most valuable assets, proprietary data and intellectual property. This talk will cover these techniques and methodologies to help the information security professional learn about protection from the inside out.

thursday 10:00am

Peer-to-Peer: Impact on Security

Tim Mather, Director Information Security, Symantec

Peer-to-peer applications have the potential to empower users, and change the current client-server paradigm. However, the cost of that empowerment could be the obsolescence of the network's firewall. How can security be preserved while taking advantage of peer-to-peer networking?

wednesday 11:00am

Assessing Your Network For Free

George McBride, Network Security Manager, Corporate Security

This talk will provide network security managers and administrators with a toolbox of publicly available free tools to help secure their corporate networks using Windows and Linux machines with a minimum of hassles.

thursday 11:00am

Response, Reality and Misinformation: Fighting the Good Fight Against Computer Viruses

David Perry, Public Education Director, Trend Micro Inc.

This talk will dissect some of the common, yet dangerous myths and mistakes about hostile code and propose solutions towards greater public awareness, factual content, and understanding of virus threats.

implementers' track

Case studies and practical advice for the IS professional implementing security solutions in the enterprise.

monday08:00am
Enhancing Software Applications with Hardware Security Modules
Peter Woods, Director of Software Development, Compaq Corporation
The talk will include discussions of various hardware encryption technologies, both RSA and symmetric key, key storage and maintenance options, problems with software-only security solutions and integrating hardware into software systems. Methods of hardware tamper resistance will also be discussed.

tuesday08:00am
Enhancing Corporate Security with Smartcards
Scott Smith, Director e-Business Solutions, Gemplus
This session will cover the basics of smartcards, how they work with focusing on using smartcards for corporate and e-Commerce security. Attendees will get a basic idea on the implementation steps necessary to evaluate smartcards and their related technology.

monday09:00am
Deploying PKI Throughout the Enterprise
Bob Brandt, Security Technologist, Ford Motor Company
Ford is moving ahead with the deployment of a PKI. Learn how Ford is enabling the deployment of branded personal certificates to support secure email, file encryption, and strong authentication with smartcards. Branded Server certificates secure Ford's B2B environment.

tuesday09:00am
Real World VPN Deployment Issues – Easy, Right?
Dave Zwicker, VP Marketing, Indus River Networks
This presentation, will use real life examples while suggesting approaches and general product features that can help customers achieve real value when using VPNs. The focus will be on remote access VPNs.

monday10:00am
PKI Total Cost of Ownership – Determine the True Cost for Each of Your Sourcing Options
Bradley Hildreth, Research Director, Gartner Group
Determine the Total Cost of Ownership of implementing your PKI. Compare the costs of insourcing vs. outsourcing vs. a hybrid solution. This talk considers over 60 different cost factors such as root key ceremonies, lost keys, licenses, manpower, training and more.

monday11:00am
Gartner Group on PKI – Your PKI Options, Your PKI Questions
Victor Wheatman, Kristen Noakes-Fry, John Pescatore; Gartner Group
Speakers present current research perspectives on PKI, followed by a stump the analyst question session. Topic areas could include vendors, applications, insourcing vs. outsourcing, total costs, where to keep the private keys, cross certifications, policy agreements and more.

tuesday10:00am
Typical Stumbling Blocks of Implementing a PKI
Frank Heinzmann, Manager, PricewaterhouseCoopers
The presentation is based on real life experience. It reflects the errors and mistakes that can be made implementing projects and gives hints and advice how to avoid these pitfalls.

tuesday11:00am
Assessing e-Business for PKI
Celia Joseph, Principal Engineer, RSA Security Inc.
E-Business security is capturing headlines as big-name e-Merchants fall prey to hackers. This talk will discuss security issues in e-Business as drawn from RSA Security's design and assessment experience with e-Merchants.

The rotation of the Earth causes stars to leave trails in this time exposure of snowy Mount Taulliraju in Peru.

wednesday09:00am

PKI Forum on PKI Interoperability

Derek Brink, Director Product Marketing, RSA Security Inc.; Steve Lloyd, Senior Consultant, RSA Security Inc.

Multi-vendor interoperability is a catalyst for PKI market growth, but what does interoperability really mean? Two members of the PKI Forum's Executive Board present its definition of PKI interoperability and highlight key activities and work items since its kickoff at RSA Conference 2000.

wednesday09:00am

Ten Myths About PKI: A Rebuttal

Patrick Richard, Founder & CTO, Xcert

This talk rebukes "Ten Risks of PKI" by Carl Ellison and Bruce Schneier as implementation specific. This talk demystifies PKI with industry examples where the risks were mitigated by deployment and/or implementation decisions and reclassifies those risks as myths.

thursday09:00am

Deploying Integrated Directory and Security Systems

Daniel Blum, Senior VP, The Burton Group

Scaling and managing single sign on, PKI, and other security capabilities requires a strategy for integrated directory services. This talk identifies directory deployment roadmaps and best practices assembled by The Burton Group's senior consultants during over 100 directory consulting engagements.

wednesday10:00am

Intelligent Solutions to Email Security

Jahan Moreh, Chief Security Architect, Sigaba Corporation

This talk presents practical measures in implementing email solutions that exhibit end-to-end security. The presenter discusses six aspects of security (authentication, access control for senders and receivers, privacy protection, integrity protection, nonrepudiation and audit) in the context of email.

wednesday11:00am

Implementing PKI for a Decentralized Environment

Stanley Borawski, Deputy Division Administrator, State of Michigan Department of Treasury

The session will present the reasons PKI was chosen, the issues involved with obtaining support across the organization, the lessons learned from the deployment of PKI and the development of a PKI-enabled application as well as the overall benefits of choosing PKI.

thursday10:00am

How We Built a National Online Legal Community Using Trusted Digital Credentials and PKI

Ron Usher, CIO, Juricert

Juricert Services, Inc. recently launched a service that allows Canadians to send their most personal legal information over the Internet. This case study will describe how Juricert created a trusted online community for a nation's legal communications.

thursday11:00am

Secure Access Control for Trusted Execution

Nicko van Someren, Co-Founder and CTO, nCipher

This presentation will introduce a new model for trusted execution in which programs can be given different limited rights over different objects at a fine grain level. Programmers can be entrusted with only the limited rights they need while the model naturally supports multiple programs accessing the same objects with different rights.

industry track

Industry-specific case studies and solutions, focusing on Finance, Telecom/Wireless, Healthcare/Biotech and ASPs.

monday 08:00am
PKI in Global Finance – A Business-Enabling Technology
Gavin A. Grounds, Director Information Assurance Global Strategies, EDS
PKI has received both good and bad press. This presentation will demonstrate how PKI is already being used as both a defensive and business-enabling technology and outlines future opportunities for enhanced business processes and revenue.

tuesday 08:00am
Securing the Wireless Internet
Tatu Ylönen, Founder and CTO, SSH Communications Security
IP is the common denominator for the convergence of all wireless fixed data traffic - but how, exactly, will it be applied? Technologies such as Wireless Application Protocol, the 2G and 3G standards and Bluetooth attempt to address security concerns - but which technologies are appropriate for which applications?

monday 09:00am
Implementing B2B Banking to Scale Globally
Alan Lloyd, Strategic Security Development Mgr, Computer Associates
Bank of America has established a major new business-to-business eCommerce capability based on the Identrus infrastructure for worldwide Internet banking transactions. Hear how the Bank worked with CA's eTrust to deliver a highly scaleable OCSP solution layered atop X.500.

monday 10:00am
Trust in the Securities Industry
Eliot Solomon, Vice President, Sector
How do organizations like the New York Stock Exchange create the trust that enables global markets? This presentation discusses that trust and cryptosystems that could model it.

tuesday 09:00am
Wireless e-Business Value Chains
Heikki Heinaro, Director, Mobile e-Business Technology, Nokia
Wireless security is emerging as a strategic enabler for e-Business. But what, exactly, are the security issues relevant to wireless transactions? What part do trust roles and related business opportunities play in e-Business value chains?

tuesday 10:00am
New Trends in Mobile Phone Security
Yiqun Yin, Research Leader, NTT Multimedia Communications Labs
This talk will consider security requirements for mobile phone networks, then survey ongoing standards efforts and discuss how they might converge to provide a global secure network. The presentation we take a look at NTT DoCoMo's i-mode service for mobile phones.

monday 11:00am
Security and Usability in a B2C Financial Application
Alfred Castelberg, Director, Credit Suisse
Credit Suisse's new pan-European personal finance service for private clients. Learn about the infrastructure used to deliver the service and the security mechanisms Credit Suisse has put into place to protect customers, transactions and the bank.

tuesday 11:00am
Wireless Internet and VPNs
Bruce Perlmutter, Senior Product Manager, Nortel Networks
Wireless Internet technology will enhance traditional Internet access and transform the way we work, learn, and play on the Internet. This presentation reviews the role of VPNs within the emerging wireless technologies.

finance

wireless

wednesday08:00am
The Security Solution for Computerized Medical Records
Bill Jensen, Product Mktng Mgr, Check Point Software; Don Lyons, CIO, Valley Medical
New government regulations on electronic records have hospitals and health care facilities scrambling to learn about computer security. This case study will discuss the challenges of securing medical information and demonstrate how Seattle's Valley Medical and Check Point developed a comprehensive, flexible solution.

wednesday09:00am
The Healthcare PKI Value Proposition
Ann Geyer, Practice Partner, Tunitas Group
Industry barriers retarding the deployment of PKI and how they may be overcome. Framework for the construction and presentation of the successful healthcare PKI business case.

thursday08:00am
The ASP and The War College Mentality
Mudge, VP Research and Development, @stake
This session will address how to thwart future attacks before they have been invented. Discussion will cover digital security paradigm shift, how to strategically analyze threat models, and which industries can take advantage of this new security model.

wednesday10:00am
Achieving HIPAA Security Compliance
Soloman Appavu, Cook County Hospital; Bill Braithwaite, U.S. Dept of Health and Human Services; Shannah Koss, IBM
HIPAA 1996 mandates security standards and privacy regulations that will have a far-reaching impact on the healthcare industry. A panel of industry experts including healthcare providers, payers and the author of the legislation will review the impact of this sweeping legislation and the specific steps necessary to ensure compliance.

thursday10:00am
Practical Security for ASPs
Derek Brink, RSA Security Inc.; Ron Freedman; Eamus Halpin; Mark Milatovich; Jonathan Rodin; Tom Welch
This panel will discuss practical security solutions in use by ASPs today, and describe their views on how they will integrate additional security in the future.

wednesday11:00am
The Challenges of Complying with HIPAA
Alan Swope, VAR Sales Manager, Nokia
Managed health care providers must consider implementing high security standards to protect patient confidentiality and prepare for HIPAA legislation. This presentation addresses the issues, providers and solutions that will ensure network security, using Baylor Health Care Systems as an example.

thursday11:00am
Using PKI to Distribute ASP Services
Ed Murrer, VP Marketing, Xcert
How ASPs can use PKI to increase the level of access control and authentication for their offerings and what ASPs should look for in a PKI offering.

healthcare

ASPs

new products a

Demonstrations and product pitches featuring the latest crypto-enabled and e-security products.

monday08:00am

Big PKI

Garrett Hussey, Chief Technical Architect, Baltimore Technologies

Issuing and handing hundreds of millions of certificates presents new challenges to PKI systems. This presentation examines those challenges and how some may be addressed, especially those around running large scale CAs. Areas such as throughput, scaling, data management, sizing and management are explored.

monday09:00am

Neural Networks Role in Adaptive Authentication Management

Erik Johnston, Neural Network Engineer, Authentor Systems Inc.

The transition from static authentication to adaptive authentication requires the support of sophisticated neural networks, a version of artificial intelligence. The presentation will address the unique functionality garnered from deploying nested pairs of neural networks including fraud prevention and dynamic thresholding.

tuesday08:00am

Proactive Security Monitoring in the Security Chain Verification System

Geoffrey Cooper, Chief Scientist, Securify

The SVS system is a new class of proactive security monitoring system. It is capable of tracking violations missed by other monitoring systems such as: slow scans, violations of procedure, stolen credentials, rogue machines or routers.

tuesday09:00am

Content Assurance Management in the Digital Age

Dr. Prakash Ambegaonkar, Ray Langford, DeVaughn Barnum; E-Lock Technologies

Assurance Management is the providence of security and trust to e-Business transactions. In this Digital Age assurance management becomes a highly prized goal. E-Lock Technologies provides a complete assurance management solution for any organization's e-Business transactions through the use of PKI and Digital Signature Transactions.

monday10:00am

The Trusted Solution for Building Strong e-Business Relationships

Dana Hendrickson, Praesidium Product Solutions and Services Mgr, Hewlett-Packard

HP Praesidium DomainGuard 3.0: Introducing a truly scalable solution for secure business portal access management. DomainGuard 3.0 provides the integrated authentication, authorization, administration and auditing necessary for companies to rapidly deploy secure Web portal solutions for customers, partners and suppliers.

monday11:00am

Ensuring Access Control in Today's Mobile Wireless Environment

John Muir, President and CEO, Pointsec Mobile Technologies

Wireless devices require a new generation of tightly integrated security tools comprising of physical and electronic access controls, strong authentication and automatic encryption. This session will describe how Pointsec products using PKI, create a symbiotic relationship between physical access and access control.

tuesday10:00am

The First Cryptologically Secure Multi-Vendor E-commerce Service

Jim Rowan, President and CEO, EncrypTix

EncrypTix is launching, for several of its initial investor partners, its ultra-secure, stored-value service for wired and wireless Internet ticketing and other transactions, based on a single secure facility with cryptographic computers certified at NIST 140-1 Level 4.

tuesday11:00am

Building the Trust Behind PwC beTRUSTed

Richard Moulds, nCipher Inc.; Geoff Grabow, PricewaterhouseCoopers

PricewaterhouseCoopers went beyond pure security considerations to create a flexible, high capacity and highly trusted service. This case study, presented jointly by PwC and nCipher, explores the range of criteria that were met in delivering this world-class solution.

In 1985 astronomer Paul Horowitz of Harvard University began project META (Megachannel Extraterrestrial Assay). His equipment scanned the entire sky along eight million channels near a chosen central frequency, such as that of hydrogen [1.4 gigahertz]. or hydroxyl [1.7 gigahertz]. Horowitz found thirty-seven signals which "survived all our cuts" and still cannot be identified.

wednesday08:00am

New Developments in Chipcard Reader Architectures

Uwe Schnabel, Managing Partner, OMNIKEY AG

Smartcard applications will get closer binding to the cardholder via reader integrated biometrics. Contactless smartcard readers connected to the PC will bring a lot of advantages. Scalable security features for smartcard readers make one design available for different application requirements.

wednesday09:00am

Addressing the Need for Cryptographic Accelerators

John Dillon, Product Marketing Manager, AEP

The talk discusses the need for cryptographic accelerators in e-Commerce-enabled Web servers and how the development of the AEP1000™, with the fastest modular exponentiation chip in the world, has addressed the technology gap currently in the market.

thursday09:00am

Bridging the Gap Between e-Business and PKI

Sarbari Gupta, Senior VP, Conclusive Logic

Conclusive brings the vision of open PKI to reality, with a suite of products that allows the seamless integration of multiple PKI technologies into organizational business practices and workflow models while providing a facility for centralized trust and policy management.

wednesday10:00am

Encryption Interoperability Via SecureDelivery.com

David Cook, CEO, ZixIt Corporation

Overview of SecureDelivery.com the interoperable secure messaging portal. Topics include message origination and authentication techniques, delivery of secure messages to recipients not having decryption software, and interoperability between different secure formats, such as ZixMail, PGP, and S/MIME.

thursday10:00am

iPlanet Certificate Management System 4.3

Roland Jones, Product Manager, Sun Microsystems

The New iPlanet Certificate Management System is a scalable, flexible and high performance PKI solution designed with extensible, modular components that are easily customizable for easy integration with existing security infrastructures.

wednesday11:00am

Of Mice and Mainframes: Legacy Security Challenges in a Webified World

Steve Orrin, CTO, LockStar, Inc.

LockStar lets companies rapidly and safely integrate mainframes with Web applications, leveraging the real-time information, security and business intelligence housed in the legacy infrastructure. No client software or back-end re-engineering is required.

thursday11:00am

Technology Preview of SiteMinder 5.0

Sumner Blount, Senior Product Mgr, Netegrity

SiteMinder from Netegrity is the leading product for secure portal management. This session will examine the benefits of the SiteMinder 5.0 release including new features such as Secure XML support, enhanced Delegated Management Services, and support for wireless devices.

new products b

More demonstrations and product pitches featuring the latest crypto-enabled and e-security products.

monday 08:00am

The VeriSign Personal Trust Agent - Towards Ubiquitous PKI

Sameer Merchant, Senior Software Engineer, Verisign

The Personal Trust Agent is a thin client which interfaces with browsers and servers to provide client-authentication, digital signatures and other cryptographic features while making Digital ID's accessible from any location through VeriSign's unique roaming service.

tuesday 08:00am

Use of RSA Toolkits in the Development of a Voting Over the Internet (VOI)

Edward Rodriguez, Senior Associate, Booz, Allen & Hamilton

The Voting over the Internet (VOI) system incorporates various security mechanisms to provide the properties of confidentiality and data integrity for a ballot as well as user I&A. The VOI developers used the RSA BSAFE toolkit to implement a protocol that supports data integrity and digital certificate verification requirements.

monday 09:00am

Is Your Time... Trusted?

Mark Hastings, President, Datum eBusiness Solutions

Time manipulation within documents, financial transactions, and digital signatures seriously impairs an e-Transaction's time integrity. A solution exists with Trusted Time.

tuesday 09:00am

Secure Wireless Aggregation

Neil Daswani, Director Mobile Services, Yodlee

This talk describes a secure wireless aggregation service, a service that allows a user to view all of their personal information – bank balances, credit card balances, brokerage account balances, etc. – from any mobile device.

P.26

monday 10:00am

Microsoft Certificate Services and PKI Futures

David Cross, Security Program Manager, Microsoft Corporation

Discussion of the next generation of PKI and Certificate Services in Windows including discussion of the new x.509 standards, private key archival and recovery, CA cross-certification, qualified subordination, delta-CRLs and support for the federal Common Criteria guidelines.

monday 11:00am

Luna XPplus: The need for PKI Speed

Bruno Couillard, CTO, Chrysalis-ITS

Luna XPplus from Chrysalis-ITS addresses the need for trusted, high performance, PKI signing engines. Many systems involved with the processing of PKI management traffic depend heavily on verification and signature operations in huge quantities, pushing the demand for acceleration hardware.

tuesday 10:00am

RSA Cert-C in Use: DocuTouch Electronic Notary Service

Mir Hajmiragha, Founder & CEO, DocuTouch

The DocuTouch Electronic Notary Service is a secure, Web-enabled application. Notaries who register with DocuTouch receive a unique, notary certificate and tools that allow the notary to easily interrogate and validate the components that implement legally binding digital content.

tuesday 11:00am

Using Biometric Software to Protect Private Keys

Alec Main, VP Project Management, Cloakware Corporation

Portable devices are easily lost or stolen. Biometric authentication can prevent attackers from hacking simple passwords and gaining access to personal information, corporate networks and private signing keys. Combining tamper-resistant software and signature recognition provides a software only solution.

Four of the twenty-seven VLA radio telescopes in New Mexico at sunset.

wednesday08:00am

User-Centric Security - The Trusted Hardware Desktop

Christian Wettergren, President, MySpace AB

How does one make sure management of the private key is in their hands? Supported by the MySpace environment, the PC user is only a click away from performing all security-critical tasks in separate hardware connected to the keyboard and screen.

wednesday09:00am

An Efficient Wireless PKI

Alfred Arsenault, Chief Security Architect, Diversinet Corporation

This presentation describes an efficient encoding of certificates for use in wireless mobile-commerce environments. These certificates provide most of the essential functionality of X.509, without unnecessary encoding overhead.

wednesday10:00am

Security Processor Solutions

Robert Lutz, Marketing Director, Hi/fn

The 7851 allows network equipment manufacturers to come out of the starting block with very powerful security solutions. The 7851 raises the performance bar by providing 3DES encryption and LZS® compression at up to 500 and 700 megabits per second.

wednesday11:00am

Trust @ the Edge - Turning the Internet Inside Out

Gregory Kazmierczak, VP Technology Strategy, Wave Systems Corporation

Utilizing the EMBASSY platform and infrastructure, the execution of electronic transactions and value exchange can be moved from the server to the client while simultaneously improving the user's level of control and privacy.

thursday09:00am

Using the Telephone Network as the Solution to the First-Time Registration Problem

Thomas Swalla, Senior Product Manager, Authentify, Inc.

This presentation will introduce a highly-scalable, easy-to-deploy and cost efficient method for digital certificate registration that utilizes the Public Switched Telephone Network to provide real-time authentication. This automated process provides an enhanced audit trail for increased security.

thursday10:00am

ValiCert's Transaction Authority

Ram Krishnan, Senior Director of Product Marketing and Management, ValiCert

Companies conducting high-value business transactions must undergo real-time integration and automation of various processes spanning multiple applications and data sources. We'll look at ValiCert's Transaction Authority and see how it provides transaction coordination for all e-Commerce environments.

thursday11:00am

The iPlanet Internet Service Deployment Platform

David McNeely, Director of Product Marketing, Netscape Communications Corporation

The iPlanet Internet Service Deployment Platform is a comprehensive software infrastructure including application services, user management services, unified messaging services and portal services.

rsa products track

Immersion workshops for security professionals working with RSA Security products.

monday 08:00am
Deploying PKI Smartcards in Today's Enterprise
Roland Fournier, Product Manager, RSA Security Inc.
This session will discuss RSA Security smartcards and personalization systems. The topics covered will address how enterprises deploy single smart cards for PKI authentication, proximity building access and Employee ID to maximize ROI.

monday 09:00am
Wireless Security-Oxymoron or Reality?
Merrit Maxim, Product Manager, RSA Security Inc.
As wireless access increases, these systems must provide strong security features. This session will educate one on a variety of wireless security solutions ranging from authentication to public key infrastructure to developing secure wireless applications.

tuesday 08:00am
e-Security Solutions for VPNs
John Worral, Director Product Management, RSA Security Inc.
VPNs provide an encrypted tunnel that is private, but not necessarily secure and is usually protected merely by passwords. This session will educate one on a variety of VPN security solutions ranging from authentication to public key infrastructure to developing IPSec applications.

tuesday 09:00am
Bringing Security to the Internet Protocol
Matthew Henrickson, RSA Security Inc.
This presentation discusses RSA Security's implementation of the IPSec toolkit, both at a high level, and from the perspective of the integrator. It describes the IPSec toolkit in the context of its market space, and compares it with two RSA BSAFE offerings, SSL-C and WTLS-C.

tuesday 10:00am
Carrier Class Authentication
John Worral, Director Product Management, RSA Security Inc.
This session highlights RSA Security's ACE/Server v5.0, the carrier-class engine behind RSA SecurID® user authentication. Topics include new release features, including high availability and replication, centralized management tools such as Web administration and native LDAP interfaces.

monday 10:00am
Securing Mobile Applications with RSA BSAFE WTLS-C
Tim Hudson, Technical Director, RSA Security Inc; Ken Bolger, RSA Security Inc.
This presentation discusses WTLS, where it fits in the WAP architecture, and how application developers can build secure applications using the RSA BSAFE® WTLS-C toolkit. It will walk developers through the steps necessary to build secure mobile applications using sample code from the WTLS-C product.

monday 11:00am
RSA Keon® PKI Solutions for Secure Wireless Communications
Karla Rosen, Senior Product Manager, RSA Security Inc.
RSA Security will present solutions that enable PKI-based secured wireless communications. A PKI can provide a unified and scalable framework to deliver end-to-end security through strong encryption and authentication for a wide class of wired and wireless applications.

tuesday 11:00am
RSA Keon® PKI Solutions for Virtual Private Networks
Mark Diodati, Senior Product Manager, RSA Security Inc.
RSA Security's Keon provides scalable, secure VPN solutions with strong usability features that are interoperable across VPNs. RSA Keon VPN solutions that provide ease of use benefits for users and administrators while also providing additional security features will be presented.

wednesday08:00am

RSA Web Security Portfolio; Unlocking e-Business Applications on the Web

Gregg LaRoche, Marketing Program Manager, RSA Security Inc.

RSA Security will discuss a complete, flexible set of solutions and services tailored for securing Internet-based transactions.

thursday09:00am

New Features from RSA BSAFE Cert-C & Cert-J

Marina Milshtein, Sr Software Engineer, RSA Security Inc.

Learn how to use the RSA Security's BSAFE Cert tools to add PKI functionality to applications. The speaker will present the basic process of requesting a certificate from different CAs using different protocols and also show how to sign and verify XML documents, using the W3/IETF defined XML Signature protocol.

wednesday09:00am

Getting the Most from the New Features in RSA BSAFE Crypto Developer Tools

Steve Burnett, Crypto Engineer, RSA Security Inc.

RSA Security's BSAFE Crypto-C 5.1/5.2 and Crypto-J 3.1 introduced many new features. This talk covers how these features are used, and what to expect in terms of performance and functionality. Features covered include support for the Advanced Encryption Standard (AES), the MultiPrime™ RSA algorithm and devices with PKCS#11 interfaces.

wednesday10:00am

RSA SecurID Web Portfolio: Two-Factor Authentication for B2C, ASP and B2C Applications

Amy Speare, Sr Product Mgr, RSA Security Inc.

This session will discuss RSA Security's SecurID Web Portfolio, a solution package designed specifically for ASP, B2B, e-Marketplace, and B2C applications. This talk will cover RSA SecurID two-factor authentication – the solution's primary component – the remaining solution components and specific customer implementations.

thursday10:00am

The Next Evolution in SecurID Deployment: Web Based RSA SecurID Deployment

Carol Clark, Product Manager, RSA Security Inc.

This session will focus on RSA Security's SecurID Web Based Token Registration, the latest evolution in deployment tools for RSA SecurID tokens. This Web based workflow product allows organizations to deploy tokens faster, easier and reduce burden on their IT organizations.

thursday11:00am

RSA Keon PKI Solutions for Reduced Sign-on

Brian Breton, Product Marketing Manager, RSA Security Inc.

RSA Security's Keon provides a number of methods to enable an organization to PKI-enable applications to take advantage of reduced sign-on capabilities. This session focuses on methods for PKI-enabling applications by natively integrating PKI-functionality as well as unobtrusively securing applications.

wednesday11:00am

RSA Keon PKI Solutions for Secure Internet Transactions

Herb Mehlhorn, Senior Product Manager, RSA Security Inc.

RSA Keon PKI-based solutions allow enterprises to trust their Web-based transactions. This session will present the ease of use and deployment capabilities provided to enable a public key infrastructure within an enterprise as well as with business partners and customers.

standards track

Discussions covering domestic and international standards efforts in security and e-commerce.

monday 08:00 am

BioTrusT: A Multidimensional Approach to Biometric Identification

Henning Arendt, Consultant, @bc® - Arendt Business Consulting

BioTrusT, a project sponsored by TeleTrust, the German Government and the S-Finanzgruppe. A multidimensional approach with participation of consumer advocates, the state's data security agency and a German University to understand the requirements for biometric identification in e-Commerce applications.

monday 08:00 am

e-Business Security Challenges When English is Just Another Language

Bruce Franson, International Product Manager, RSA Security Inc.

As North American and English language dominance of the Internet and e-Business diminishes, this presentation explores the challenges of planning and deploying PKI and information security measures in an increasingly multinational and multilingual e-Business environment.

tuesday 08:00 am

Wireless PKI

Stephen Farrell, Chief Security Architect, Baltimore Technologies

The presentation contains an update on the status of various wireless PKI activities and shows how a standard PKIX-compliant PKI can be used in a wireless context. The special mechanisms that are required in wireless PKIs are also described.

tuesday 09:00 am

Biometric Information Management and Security

Jeff Stapleton, Manager Information Risk Management, KPMG LLP

Biometrics are the what you are of authentication mechanisms that are fastly being accepted by industries and their customers. The security, privacy, and the compliance to a standard is of utmost importance.

monday 10:00 am

Security Rules: Implications of Technical Standards

Carl Cargill, Director of Standards, Sun Microsystems

Standards impact the shape of security with regard to its deployment. They also impact the interoperability of different systems. Since the Internet was not designed for commercial activity nor the control of data, and since e-Commerce demands such control, technical standards have to work well together.

monday 11:00 am

Securely Available Credentials

Magnus Nystrom, Technical Director, RSA Security Inc.

The problem of non-portable PKI credentials due to application-specific stores and cumbersome export/import facilities is addressed by the IETF's sacred working group. This talk will describe the current status of its work, and its intended deliverables.

tuesday 10:00 am

A Survey of PKI Governance Models

Tim Moses, Director Advanced Security Technology, Entrust Technologies

The basic character of a PKI is determined by its governance model. This talk reviews the most popular governance models, identifying their most prominent characteristics and the circumstances in which they are most appropriately applied.

tuesday 11:00 am

X.509 Attribute Certificates in the Internet

Russell Housley, Chief Scientist, SPYRUS

The IETF PKIX working group has developed an attribute certificate profile with emphasis on support for Internet electronic mail, IPSec, and World Wide Web security.

The "wow!" radio emission, detected by the Big Ear radio telescope at Ohio State University at about 11:16 p.m. Eastern Daylight Savings Time on August 15, 1977. Engineer Jerry Ehman immediately recognized it as the pattern one would expect to see from a narrowband radio source of small angular diameter in the sky. In a red pen he circled six characters and wrote the notation "Wow!" in the left margin of the computer printout opposite them. The signal was only observed once — and after more than 20 years, it's still considered one of the strongest candidates to be a signal of actual extraterrestrial origin.

wednesday08:00am

Building Successful Standards

Paul Kocher, President, Cryptography Research

Some cryptography standards such as DES, SSL, and PKCS are used widely but most proposed standards fail for political or technical reasons. This talk will examine how security standards are actually developed and adopted, with several historical case studies.

wednesday09:00am

FIPS 140-2: International Cryptographic Conformance

John Morris, President, Corsec Security Inc.

FIPS 140-2 cryptographic module security requirements have replaced FIPS 140-1. The presentation will explain the new standard, international initiatives and future efforts. Hear candid advice on how to survive the FIPS 140-2 process, and the future of the program.

wednesday10:00am

Using Message List Agents for Secure Distribution Lists

Jim Schaad, CEO, Soaring Hawk Consulting; Sean Turner, Developer, IECA Inc.

The panel will discuss issues involved in the use of Mail List Agents. Included are a look at the reasons to use an MLA, the current state of standards and issues involved in using an MLA.

thursday08:00am

The Trouble with Standard Protocols

Robert Baldwin, Partner, Plus Five Consulting Inc.

Come learn why standard security protocols fail to meet the needs of several markets. These markets place unusual constraints on device and network capabilities as well as deep issues about the trade-off between trust, privacy, and control.

wednesday11:00am

What's New for X.509

Hoyt Kesterson II, Consultant, Private Consultant; Sharon Boeyen, Sr Consultant, Entrust Technologies

X.509 it is improved. Learn what is new in the new edition. Learn how it improves authentication and revolutionizes authorization. Take a peek behind the curtain and see what the elves are doing to build an even better X.509 for the future.

thursday10:00am

WAP Security: WTLS, WPKI and Beyond

Robert Zuccherato, Senior Cryptographer, Entrust Technologies

This talk will describe the security architecture used within the Wireless Application Protocol (WAP), show how the differences between the wireless and wired world affect the security choices to be made and look towards future directions for WAP security.

thursday11:00am

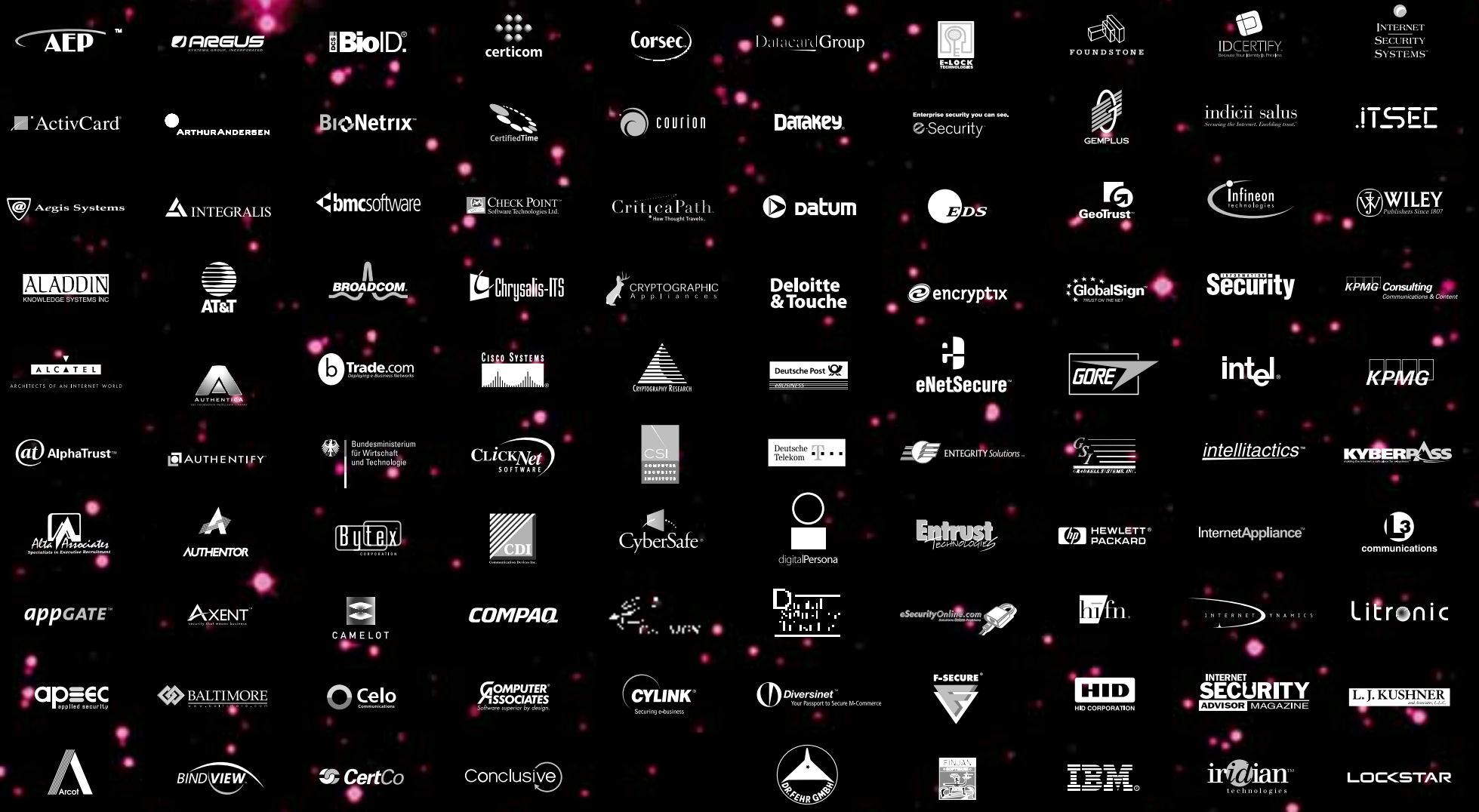
Emerging Credit and Debit Card Payment Protocols

Mark Peters, Product Architect, IBM

Learn about emerging payment guarantee protocols for credit and debit cards. Existing and emerging standards will be compared and evaluated.

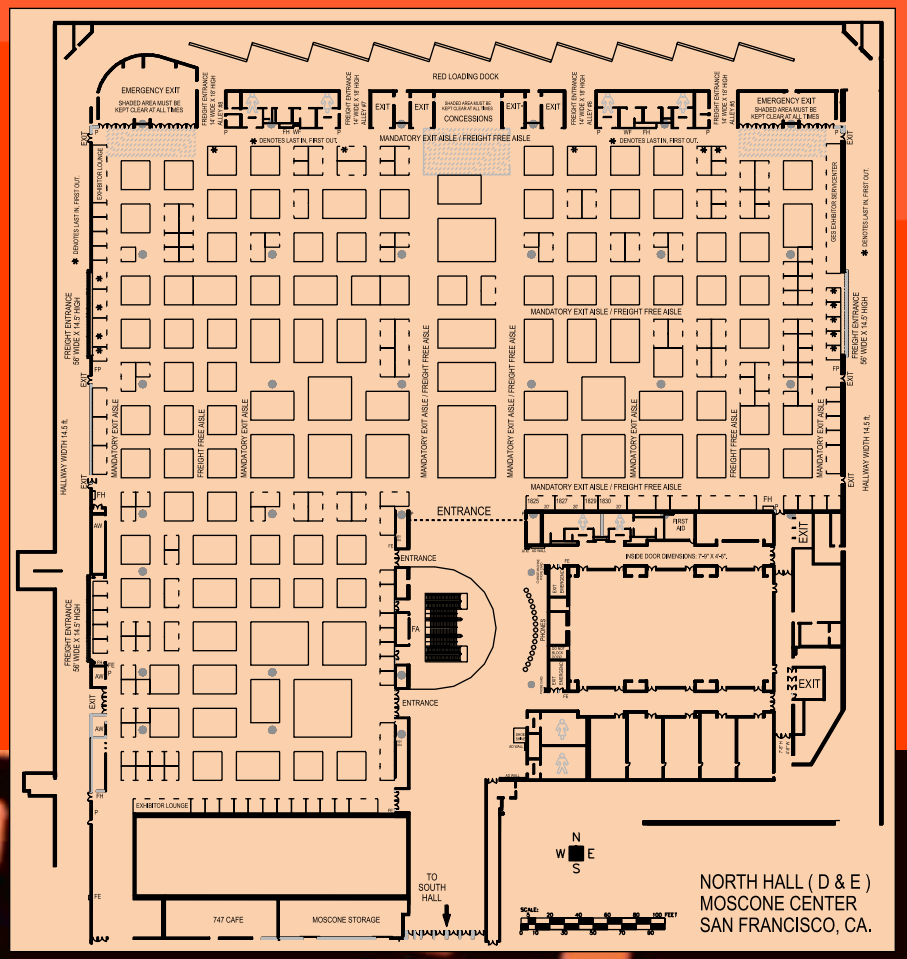
exhibits and demos

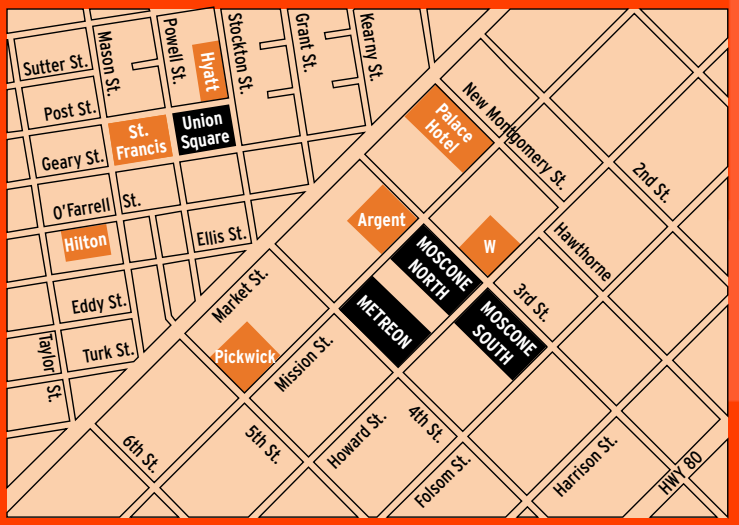
On April 9th, 10th and 11th, we are proud to invite you to join us at the largest computer security exposition ever staged. Over 181,000 square feet of exhibit space and more than 200 vendors will demonstrate products covering every aspect of the security market segment. From firewalls to crypto, from tokens to smart cards to digital certificates — if it has to do with enterprise data security, you will find it on the show floor at RSA Conference 2001. Here are just a few of the companies participating in this year's Expo:



RSA Conference 2001

conference venues





Condé Nast Traveler Magazine rates San Francisco the number one destination in the world. Natives just call it 'The City.' A thriving metropolis of technology, culture and global influence, San Francisco finds itself perfectly positioned at the dawn of the new millennium. In 2001, RSA Security is proud to return home to San Francisco for our annual U.S. gathering.

California Academy of Sciences

The California Academy of Sciences is the setting for Wednesday night's gala, hosted by nCipher. Sip champagne and nibble on hors d'oeuvres while browsing the spectacular exhibits.

Moscone Convention Center

The incomparable 1.2 million square foot Moscone Convention Center anchors the central blocks of the 87-acre Yerba Buena Gardens complex. This bustling and vibrant district includes the internationally renowned San Francisco Museum of Modern Art, the Yerba Buena Center for the Arts, the Rooftop at the Gardens and Metreon. Across the street, the resplendent Yerba Buena Gardens rests atop Moscone North, offering a beautiful six acres of urban-center park land.

Metreon – A Sony Entertainment Center®

Four floors and 350,000 square feet jam-packed with ways to entertain and escape into a whole new reality. Metreon combines the best of Sony with the original efforts of artists, technologists, writers, chefs, architects, animators and digital masterminds.

The Argent Hotel

The Argent Hotel is centrally located in San Francisco's new downtown, the buzzing South of Market area. Each of the Argent's 667 spacious guest rooms and 26 suites offer breathtaking floor-to-ceiling panoramic views of the City by the bay. Guests relax in luxury with artistic contemporary furnishings customized with modern elegance in mind.

The Pickwick

Built in 1926 as The Pickwick Stage Lines. Featured in the writings of renowned author Dashiell Hammett, in his classic mystery The Maltese Falcon. A landmark since its inception, The Pickwick Hotel is a fine example of Neo Gothic architecture. The Pickwick Hotel is located steps away from the San Francisco Shopping Center, cable cars and an array of international restaurants.

Grand Hyatt San Francisco

On Union Square in the heart of San Francisco, the Grand Hyatt San Francisco is near world-premier shopping, Chinatown, theatre district, Financial District, Moscone Convention Center and cable cars to Fisherman's Wharf and Ghirardelli Square.

W San Francisco

Set in the heart of downtown San Francisco's "South of Market", W San Francisco stands out with the offbeat, yet sophisticated spirit of the City. On the Third Street Podium of W San Francisco, towering 46 feet above street level, is a reclining figure made of irregularly sheared bronze strips woven together. Conceived by a local artist to complement to the neoclassical design of W San Francisco.

Hilton San Francisco

Located in the heart of the Theater District just two blocks from Union Square, the Hilton San Francisco and Towers is the largest hotel on the West Coast with close to 2,000 rooms, fixtures, paintings and valuable art objects.

The Westin St. Francis

Renowned for its legendary service, the historic Westin St. Francis boasts luxurious guest rooms, world-class dining and distinctive meeting facilities. Overlooking Union Square in downtown San Francisco, Westin's historic flagship hotel is just minutes from Chinatown, Fisherman's Wharf and San Francisco's financial district.

Palace Hotel

Since 1875, sophisticated travelers from around the world have called the Palace home. The Palace defines not only the spirit of San Francisco, but the city's cosmopolitan style as well. It's the combination of rich tradition and forward thinking that puts the Palace in a class by itself.

The Argent Hotel
Single $240 / Double $260

Grand Hyatt San Francisco
Single $210 / Double $230

Hilton San Francisco
Single or Double ROH $209
Single or Double Towers $244

Palace Hotel
Single $170, Double $190

The Pickwick
Single/Double $160

W San Francisco
Single/Double $250

The Westin St. Francis
Single $194, Double $214, Deluxe $234

These special discounted rates are available to conference attendees, but hurry, rooms will fill fast. Please make your reservations online at www.rsaconference.com/rsa2001 or fax the enclosed Hotel Form to 847-940-2386.

rsa founders' circle

Many attendees have been with us since the beginning – the first RSA Conference back in 1991, when the Conference was the meeting place for the truly crypto-aware and the Internet was something only college students and defense contractors used. When no one had email addresses on their business cards and "secure electronic commerce" meant sending cash via Western Union.

Other folks came on board a little later – when the first Mosaic browsers were released, S/MIME was introduced, and SSL was green. But they saw the potential, they got it – they came to the Conference, and kept coming.

We'd like to acknowledge the early vision of our loyal following by inviting them to join the RSA Founders' Circle.

The Founders' Circle is a "distinguished alumni" program for the RSA Conference. If you attended one of the first four RSA conferences – or attended RSA Conference 2000 and our three preceding conferences – you're automatically a member!

Membership benefits include:

- Red Carpet Registration
- VIP Badging
- Founders' Circle Lapel Pin
- VIP Luncheon with Jim Bidzos

So claim your membership. Join us at RSA Conference 2001 by registering today at www.rsaconference.com. Qualifying members will receive full details and benefits of the Founders' Circle in a special Conference sneak preview email in March.

how to register

register on the net

http://www.rsaconference.com

register by telephone

call LKE Productions at
800.340.3010 or +1.415.544.9300

register by fax

complete the attached form and fax to +1.415.544.9306

register by mail

complete the attached form and mail to:
RSA Conference 2001
c/o LKE Productions
1620 Montgomery Street, Suite 120
San Francisco, CA 94111

hurry!

register by February 2nd and save $800 off the standard registration fee of $1795
(early bird registration is $995).

Registrants who cancel prior to the conference or do not attend the conference forfeit their entire registration fee. Substitutions, including those made on site, are allowed with the written permission of the original registrant. A $75 process fee will be incurred for any and all substitutions.

kudos

"...the place to see and be seen - great networking."

"one of the best-organized, best-run conferences that i have ever attended."

"really good technical sessions."

"everyone who is anyone in the security field is likely to attend the rsa conference, making it a prime meeting place for debates about standards issues...or for more private matters."

"well worth the time, well run, and very enjoyable."

"overall, i got a lot out of this conference. thanks."

"the rsa conference is the best!"