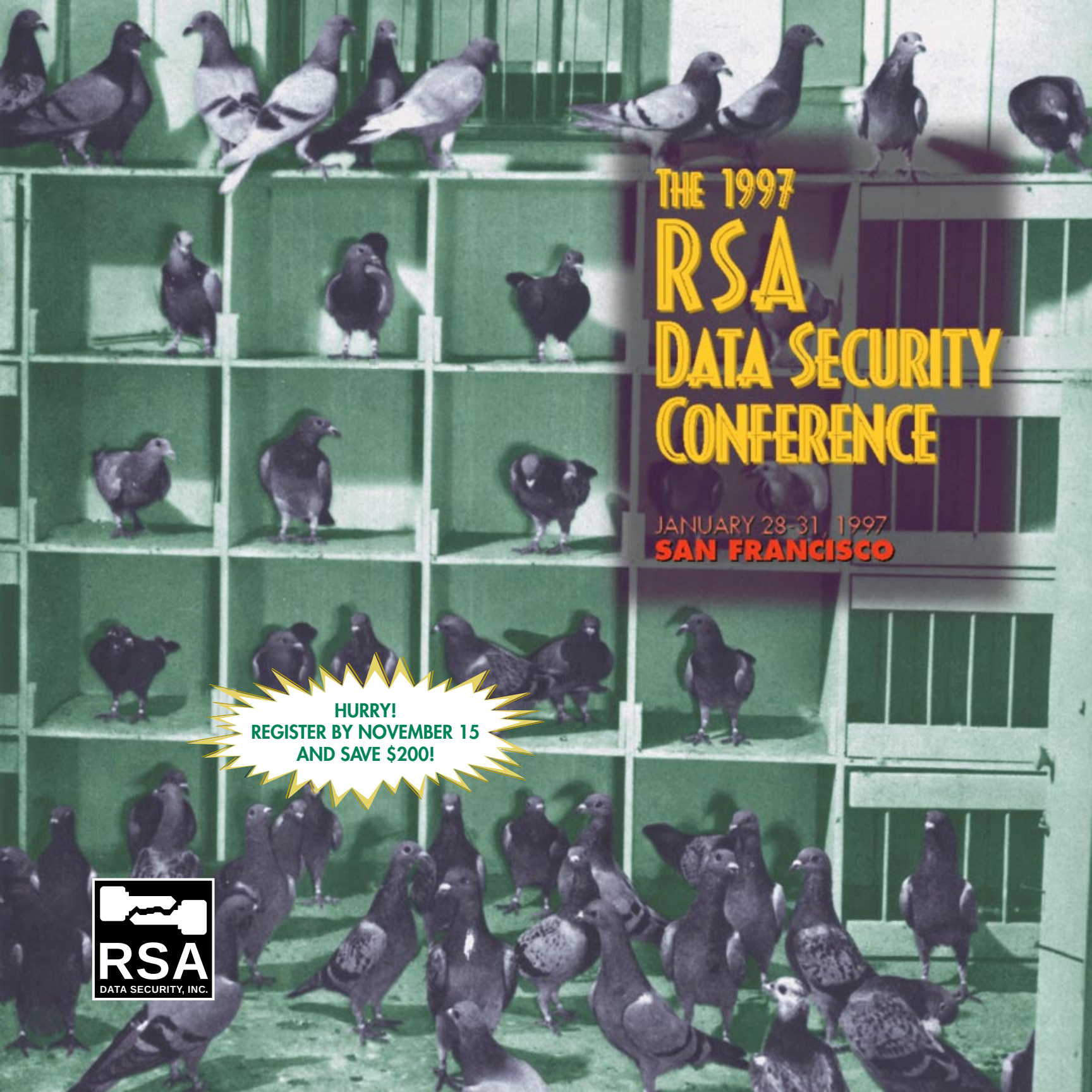

THE 1997
RSA
DATA SECURITY
CONFERENCE
JANUARY 28-31, 1997
SAN FRANCISCO
HURRY!
REGISTER BY NOVEMBER 15
AND SAVE $200!
RSA
DATA SECURITY, INC.

The sixth annual RSA Data Security Conference delivers four full days of cryptographic research, development, products and market analysis presented by some of the leading minds in the industry. An annual pilgrimage for the world's cryptography systems experts, policy-makers, business people and technology developers, the RSA Conference delivers breadth and depth far beyond any other computer security gathering.

During the first World War, carrier or "racing" pigeons were often the only means of secure communications between headquarters and the front lines. Secure electronic communications being unavailable in the early 1900's, both sides leveraged the technology at hand — using the speed, loyalty and unique homing instincts of carrier pigeons.

"Cher Ami" was one such extraordinary pigeon who, although mortally wounded, managed to complete his mission and deliver a message that saved the lives of 194 men caught behind enemy lines at Verdun.

While the technology — and the "carriers" — may have evolved dramatically over the past eighty years, the requirement for secure communications remains unchanged. The survival of companies in the competitive global marketplace depends upon their ability to keep their communications private and authenticated — while still making information accessible to those who need it most. Nearly two decades ago, RSA's founders invented the first practical public key cryptosystem, and ever since, our technologies have defined the perfect balance between openness and control.

As computer security professionals, whenever and wherever we gather, it is immediately apparent that we are somewhat of a breed apart. Well as such, we invite you "home to roost" with others who share a fascination with cryptography, at this, our sixth annual Conference.

"The sine-qua-non event of the crypto community..."

— Computerworld

WHO SHOULD ATTEND

• **ANALYSTS** – get a look at the future of cryptography and electronic commerce. See demonstrations of cutting-edge digital security technologies. Learn how policy and technology interact to determine future cryptography trends, and find out firsthand how companies are adapting advanced coding technologies to address their practical business requirements.

• **CRYPTOGRAPHERS** – meet some of the world's most famous mathematicians face-to-face. Attend seminars covering the very latest in cryptographic research. Find out which algorithms are in, out, up and down. Learn about the most exciting advances in factoring, cryptanalysis and large number theory.

• **DEVELOPERS** – spend a day or two at "Camp Crypto" and learn how to use the world's most advanced crypto tools from the engineers who designed them. Take advantage of this meeting of the minds to share your own insights and learn what other developers are working on. Receive the hottest technical information, evaluate the latest standards proposals, and find out what's really on the minds of today's end users.

• **BUSINESS PROFESSIONALS** – network with the world's most respected cryptographers and the business development professionals that are applying the technology to real-world solutions. Get the inside track on new security trends, products and services. Separate the wheat from the chaff and find out what's really going on in the electronic commerce arena.

Meet the minds behind the crypto products that you rely upon. Learn the underlying tenets of cryptography and what to look for in trusted applications and tools. Discover how cryptographic technologies currently under development may affect tomorrow's electronic commerce, copyright and international currency systems.

PARTICIPATING COMPANIES

The annual RSA Conference is unique in the disparate communities that it gathers together. Mathematicians, scientists, developers, and business people engaged in heated debate and serious discussion. You'll meet the best and brightest in fields like:

- Mathematics and Cryptography
- Internet Electronic Commerce, EDI and the Web
- Intellectual Property Protection, Copyright and Net Law
- Federal Cryptography Policy and Standards
- Privacy and Civil Rights

In addition, some of the hottest security vendors will be available to answer questions and demonstrate hundreds of secured products on our exhibit floor. Past participants include:

Microsoft, Digital Delivery, Lotus, IBM, Apple Computer, Premenos, TimeStep, CyberCash, Qualcomm Incorporated, Intuit, Nortel Northern Telecom, Security Dynamics, VeriSign, VeriFone, ftp Software, Netscape, Frontier Technologies Corporation, Attachmate

KEYNOTES & GENERAL SESSIONS

Welcome
Jim Bidzos, President, RSA Data Security
RSA president Jim Bidzos welcomes you to this, our sixth annual conference, recaps the year that was, and offers a preview of some of the more significant events coming up over the next four days. TUE. 9AM.

Keynote: To Be Announced
Don't miss this kickoff address: a surprise guest speaker offers a memorable launch for this year's conference. TUE. 9:30AM.

Cryptographers' Expert Panel
Peter Neumann, SRI — *Whit Diffie, Sun Microsystems*
Taher ElGamal, Netscape — *Burt Kaliski, RSA Labs*
Silvio Micali, MIT — *Hugo Krawczyk, IBM*
Ron Rivest, MIT — *Matthew Blaze, AT&T*
The single highest-rated session of the RSA conference, five years running! Join the most famous minds in mathematics in a traditional RSA free-for-all. Dr. Peter Neumann of SRI hosts, and no subject is off-limits. There will even be time for some audience Q&A. TUE. 11AM.

RSA Product Announcements
Scott Schnell & Victor Chang, RSA Data Security
What an incredible year! We'll briefly recap the year, and you'll be among the first to hear about our 1997 product plans, goals and major announcements. TUE. 2PM.

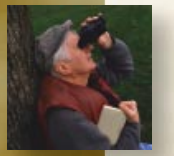
RSA, the Internet, and the Apple Renaissance
There has been a lot of press recently about Apple's problems. But to paraphrase Mark Twain, the rumors of their death have likely been greatly exaggerated. In our afternoon keynote, we're pleased to welcome a surprise speaker from Apple who will preview some of the tricks they've got up their sleeve for 1997... and some of those aces carry the "genuine RSA" logo. TUE. 2:30PM.

Authentication Practices & Market Adoption of Digital Certificates
Stratton Sclavos, VeriSign, Inc.
The financial services market is pioneering real-life Internet authentication applications by providing authenticated Internet services for their customers. Mr. Sclavos will present actual case studies of customers, banks and merchants who benefit from authentication solutions. Other industries like EDI, publishing, healthcare and transportation will also be discussed. TUE. 3PM.

Moderated Forum: Export Control, Encryption Policy & Washington Update
Ed Roback, NIST
Kenneth C. Bass III, Venable Baetjer & Howard LLP
Dorothy Denning, Georgetown University
Edward Appel, National Security Council
Nigel Hickson, Dept. of Trade and Industry
Bruce Heiman, Preston Gates Rouveles Meeds
Mark Rotenberg & David Sobel, EPIC
Find out the latest maneuverings on privacy, encryption, and national security issues inside the Beltway. TUE. 4PM.

Modern InfoSecurity Technology: the Bigger Picture
John Adams, Security Dynamics
In 1996, security technology is finally coming into the mainstream. But consumer and corporate understanding of the technology, and its ramifications is, in most cases, still quite inadequate. In this keynote, John Adams, VP of Engineering for

ANALYSTS TRACK



Developing Certification Practice Statements
Michael S. Baum, VeriSign, Inc.
This session will focus on certification practice statements, of which VeriSign has recently published the first in the industry. The role and implications of certification practice statements for secure commerce will also be discussed. THU. 8:30AM.

Enforceability of Internet Contracts in the Absence of a Pre-existing EDI "Trading Partner" Agreement
Richard Allan Horning, Esq.,
Tomlinson Zisko Morosoll & Maser LLP
There are no reported decisions upholding the enforceability of contracts negotiated over the Internet. This talk focuses on these issues in cases where both offer and acceptance are sent over the Internet, either computer-to-computer or via e-mail. THU. 9:30AM.

Consumer Payments Over the Internet
Daniel Orlow, Federal Reserve Bank of New York
This presentation will provide an integrated perspective on the cyberpayments system. Mr. Orlow will discuss digital signatures, the certification authority, and private-key management issues. THU. 11AM.

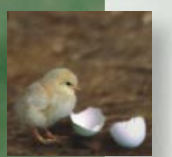
Information Security in the Enterprise
Walt Curtis, Entegrity Solutions Corporation
Distributed architectures for the enterprise must be high performance, highly secure, and operable within diverse security policy frameworks. This session will address enterprise absorption and deployment of these technologies over the next several years. THU. 1:30PM.

Influence of US Export Regulations on Russian Cryptography
Anatoly Lebedev, LAN Crypto, Ltd.
This presentation gives an overview of the US cryptography regulations and their influence on the development of Russian cryptography in the past two decades, a glimpse of the current state of the art and some possible future consequences. THU. 2:30PM.

Certification Authority Security Requirements & Technologies
Dr. Stephen Kent, BBN Corporation
Dr. Kent will discuss technical, procedural, and physical security requirements for CA operation. He will also present the pros and cons of three distinct approaches to implementing critical CA cryptographic module functions. THU. 4PM.

Secure Intranet/Internet Solutions: A Case Study
David Luther, SecureWare, Inc.
SecureWare provided the security solution for Security First Network Bank, the world's first full-service virtual Internet bank. This solution will be discussed as a real-world example of the type of layered security required for secure Internet and Intranet enterprises. THU. 5PM.

DEVELOPERS TRACK



Cryptography Basics for Developers
Steve Dussé, RSA Data Security
A general review of cryptography basics that developers need to know to begin building secured applications. THU 8:30AM.

The BSAFE Toolkit: An Introduction to the World's #1 Encryption Engine
Steve Burnett, RSA Data Security
BSAFE is the world's best-selling encryption engine, with over 75 million copies installed and in use worldwide. BSAFE provides the advanced security features inside of Netscape Navigator, Intuit's Quicken, and forms the kernel of Microsoft's CryptoAPI. This session includes an introduction to BSAFE architecture and use. THU. 9:30AM.

S/MIME and the TIPEM Toolkit: Developing Secure Messaging Applications
Bob Baldwin, RSA Data Security
S/MIME has risen to become the standard for sending secure e-mail over the Internet, with heavy-hitting sponsors including Netscape, America Online, Microsoft, and of course, RSA. Learn how to build applications that speak S/MIME using RSA's TIPEM toolkit. THU. 11AM.

The BCERT Toolkit: Developing X.509 Certificate Management Applications
Hoa Ly, RSA Data Security
Issuing and managing X.509 certificates for public key systems can be a harrowing task for the developer - but BCERT makes it easy. Find out more about the new release of RSA's BCERT toolkit. THU. 1:30PM.

Using BSAFE, BCERT and TIPEM
Steve Dussé, RSA Data Security
RSA's Chief Technology Officer will bring it all together for you, and show you how to leverage RSA's entire encryption toolkit suite to build best-of-breed secured applications. THU. 2:30PM.

The SET Toolkit: Developing Security for Internet Bankcard Transactions
Bob Baldwin, RSA Data Security
Few security standards have taken off as fast as SET, MasterCard's and VISA's RSA-based standard for securing bankcard transactions over the Internet. And some of the world's biggest developers and financial institutions rely on RSA's SET toolkit suite to build their SET-compliant applications. You can, too. THU. 4PM.

The S/WAN Toolkit
Stephanie Lacelle, TimeStep Corporation
S/WAN is an initiative from RSA to promote multi-vendor Virtual Private Networking. Ms. Lacelle will discuss TimeStep's portable S/WAN toolkit for developing software that enables IETF IPSEC recommendations on confidentiality, authenticity and key exchange. THU. 5PM.

RSA's new parent company, SDTI, will provide an overview of the plethora of security options that face the IS professional, and try to make sense of it all. WED. 9AM.

Panel: Deploying SET – Bankcards on the Internet
Kevin Rowney, Verifone
Steve Crocker, CyberCash
William Powar, VISA International
TBA Representative, Mastercard International
SET is undoubtedly the most exciting, fast-moving and most widely adopted RSA-based Internet security standard ever. With the cooperation of merchants, banks, and of course VISA and Mastercard, SET promises to be one of the most useful standards for secure electronic commerce. Today's panel of distinguished speakers will offer an update on the status of the standard, as well as share some real-life stories of development and deployment. WED. 10AM.

Panel: Audit, Mediation and Trust – The Role of Third Parties in the Security Infrastructure
Todd Mitty, Deloitte & Touche
Richard Williams, NetDox
TBA Representative, Lotus
TBA Representative, Morgan Stanley
Michael Baum, VeriSign
Businesses traditionally rely on third parties for transactions, and these third parties are notoriously difficult – if not impossible – to replace with technology. As businesses move onto the Net, the need for trusted third parties grow. Who should they be? What roles should they attempt to fill? And who's doing it now? Our panel is sure to have a few opinions on the matter. WED. 11AM.

Panel: International Trends in Cryptography
William Powar, VISA International
Chris Goeltner, Siemans/Gemplus
Yanpin Hu, Ministry of Foreign Trade & Economic Cooperation, People's Republic of China
Katsuhiko Aoki, NTT/NEL Japan
Representative TBA, MITI Japan
Learn about the major industry initiatives currently underway to enable all aspects of the IT industry to utilize the power of smart card technology in business and consumer applications. WED. 2PM.

Panel: Cryptography and Information Warfare
Gerald Kovacich, Northrop-Grumman Corp.
Robert Minehart, NSA/U.S. Army War College
Information warfare is defined as the actions taken to achieve information superiority in support of national military strategy, by affecting the enemy's information and information systems – while protecting our own. Science fiction? Not really. Analysts believe that IW will be the predominant form of warfare in the 21st century, and cryptographic technologies play an important role. WED. 3PM.

Panel: Case Studies in the Deployment of Public Key Infrastructures
Bradley Wood, Sandia National Laboratories
Peter McNeil, Australian Postal Corporation
Claude Perreault, Notarius (TSIN) Inc.
Paul Kendall, Air Liquide America
TBA Representative, Siemens
As Nathan Myhrvold said, virtually everybody agrees that RSA is the way to go... but that's only part of the story. Often, actually rolling out the RSA public key infrastructure is the hard part! Our panel offers several first-hand perspectives on implementing and using RSA-based systems on a large scale. wed. 4pm.

The Digital Signatures Guidelines of the American Bar Association
Charles R. Merrill, Esq., McCarter & English
Mr. Merrill was a co-reporter of the project which drafted Digital Signature Guidelines, published by the American Bar Association in August. He will bring to life the joint techno-legal rules of the Guidelines which are likely to jumpstart the entire online industry. FRI. 8:30AM.

Economic Modeling & Risk Management in Public-Key Infrastructures
David G. Masse, Chait Amyot, & Andrew D. Fernandes, CryptoNym Corp.
Current public-key infrastructure (PKI) models will be considered in a broad spectrum of economic settings, and suggestions of avenues for commercially reasonable risk management will be discussed. FRI. 9:30AM.

Panel: Security and the Media
Dan Gillmore, San Jose Mercury News
Sasha Cavender, Freelance Journalist
Few technologies have received the coverage – or the hype – that security threats and modern cryptography have in the past few years. But how much of this threat is real, and how much is perception created by the media machine? And how can the modern media accurately cover an esoteric field like cryptography, without passing on misinformation or misinterpretations of scientific facts? FRI. 11AM.

Secure Electronic Commerce Technology Showcase (SECTS)
Dr. James M. Galvin, CommerceNet
CommerceNet has created a showcase of its members' commercial off-the-shelf products integrated to provide a vertical solution to the vulnerabilities threatening the Internet today. FRI. 1:30PM.

Security & Privacy Requirements for Federal & State Public Records on the Internet
Alan A. Mick, Johns Hopkins University
Learn about the security and privacy requirements for federal and state public records administration and how they may be satisfied on the Internet utilizing data encryption techniques. FRI. 2:30PM.

The Outlook for Consumer Adoption of Electronic Commerce
Ted Haynes, Haynes & Company
Mr. Haynes will present information on consumer responses to existing forms of electronic commerce, and a forecast of how consumer acceptance will evolve. His talk will include recommendations on where the best opportunities lie and will suggest how businesses can best take advantage of them. FRI. 4PM.

Call Now to Register:
415-544-9300

Security Programming Interfaces
Eric Greenberg, Netscape Communications Corp.
Internet and Enterprise application developers increasingly require more flexibility and control over product security functionality. Mr. Greenberg will present a multiplatform network-centric secure programming architectural framework which addresses these needs. FRI. 8:30AM.

Electronic Commerce in Java
Shannon L. Byrne, Paradata Systems, Inc.
This session will discuss the requirements for making Java a language for first class electronic commerce systems, and will propose an open standard for the development of complete Java-based electronic commerce applications. FRI. 9:30AM.

Digital Image Integrity
Derek Davis, Intel Corporation
Mr. Davis will address the issue of integrity for still images and video clips, with an emphasis on new techniques of image capture "time-bracketing" based on the prior work of Stuart Haber and Scott Stornetta in the area of hash-based time-stamping. FRI. 11AM.

Hardware Implementation of RSA Technology in Japan
Katsuhiko Aoki, NTT Electronics Technology, Inc.
Hardware implementation of RSA technology offers higher performance than can be achieved by software, as well as ultimate tamper-proof key saving. This session will introduce NTT Electronics' new products based on the latest LSI technology, and their implementations to secure systems. FRI. 1:30PM.

How to Crack a Smart Card
Thomas Rowley, National Semiconductor Corporation
This presentation discusses the defenses used to protect smart cards and the techniques used to defeat them. Topics will include specific examples of attacks, the use and value of cryptographic techniques for defense and guidelines for the use of smart cards in high risk situations. FRI. 2:30PM.

Panel: Securing Broadcast Transmissions
Dror Lapidot, Algorithmic Research, Ltd.
Howard Pinder, Scientific-Atlanta, Inc.
A unique combination of requirements and features has made security systems for digital cable TV an active area for work in low cost, upgradeable and standard space solutions. FRI. 4PM.

Panel: Securing ATM
Joyce Capell, Lockheed Martin
Christof Paar, Worcester Polytechnic Institute
This panel describes recent developments in the area of data security and cryptography for ATM networks. Case studies and proposed solutions from the research literature will be discussed. FRI. 5PM.

NOTE: Speakers and sessions are subject to change without notice.

CRYPTOGRAPHERS TRACK

1996: The Cryptographic Year in Review
Dr. Yiqun Lisa Yin, RSA Laboratories
Abstract: 1996 has been an exciting year in the field of cryptography and computer/Internet security. Research and development in cryptography continue to grow rapidly. This year we have seen many new algorithms proposed, and some existing ones attacked and even broken. There has been significant activity in the standards area, and an increasing synergy between the theoretical and the practical. This talk highlights cryptography in 1996 and gives some ideas for what to expect in 1997. THU 8:30AM.

The Cryptography of Law Enforcement
Dr. Taher ElGamal, Netscape Communications Corp.
two or three
lines
of text. THU 9:30AM.

Handling Crypto Bottlenecks
Dr. Yacov Yacobi, Microsoft Corporation
Public key protocols for specialized asymmetric scenarios are described. These protocols are tailored to resolve computational bottlenecks. Various methods are compared. THU 10:00AM.

SDSI: A Simple Distributed Security Infrastructure
Dr. Ron Rivest, MIT
SDSI is a recent proposal by Lampson and Rivest for a new infrastructure for public-key cryptography. This presentation offers an overview of SDSI and describes some of the design decisions made during its development. THU 11AM.

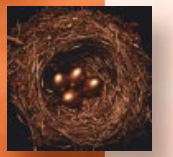
Symmetric Cipher Design & Implementation
Dr. Michael Wiener, Nortel Secure Networks
two or three
lines of text. THU 1:30PM.

Back to the Dark Ages
Dr. Richard Pinch, Cambridge University
Dr. Pinch states that the difficulty of factoring large numbers is the guarantee behind some public-key cryptosystems. The numbers employed must be carefully guarded against factoring methods old and new. THU 2PM.

Recent Developments in Hash Functions
Dr. Matthew Robshaw, RSA Laboratories
Mr. Robshaw will present a description of recent results in the analysis of hash functions and an assessment of their implications. THU 2:30PM.

Transferable and Online Secret Sharing
Dr. Richard Pinch, Cambridge University
Secret-sharing schemes allow participants to recover a secret only in legitimate combinations. Trusted third parties (key

STANDARDS TRACK



PKCS: The Next Generation, with a Progress Report on PKCS#11 (Cryptoki)
Dr. Ray Sidney, RSA Laboratories
The Public Key Cryptography Standards intervendor specifications are widely adopted in the industry and are the basis for a number of other security specifications – including SET, VISA/MasterCard's Secure Electronic Transactions. Dr. Sidney also gives us an update on the programming interface for portable cryptographic devices, such as smart cards and PC cards, developed by RSA Laboratories in conjunction with security vendors. THU. 8:30AM.

Domain Name System (DNS) Security
Donald E. Eastlake, III, CyberCash, Inc.
The Domain Name System is a critical operational part of the Internet infrastructure, yet it has had no strong security mechanisms for data integrity or authentication. Extensions to the DNS are described that provide these services through the use of cryptographic digital signatures. THU. 9:30AM.

Cryptography: Boardroom Buzzword
Sandra M. Lambert, Lambert & Associates
An update on business sector efforts to influence US and international OECD initiatives on cyber-security in commerce – issues of free choice in the use of crypto, government access, key management policies, liability and global availability and interoperability of crypto methods. THU. 11AM.

IETF IPSec & the S/WAN Initiative
Tony Rosati, TimeStep Corporation
This talk will discuss the IETF IPSEC Security Standards for extending corporate enterprises over public inter-networks for Secure Virtual Private Networking (SVPN). THU. 1:30PM.

The ISAKMP Application-Layer Protocol
Mark Schertler, Terisa Systems
A discussion of the Internet Security Association and Key Management Protocol (ISAKMP) as a security mechanism independent, application layer protocol. Mr. Schertler will address how ISAKMP establishes a coordinated security state for security protocols and enables session key generation. THU. 2:30PM.

X.509 v3 Revisited
Warwick Ford, Independent Consultant
Mr. Ford will provide an overview of the X.509 Version 3 certificate extensions which constituted a major updating of the world's dominant standard for public-key infrastructures. He will also discuss the new proposals in this area since the June 1996 completion of the revised standard. THU. 4PM.

Panel: Security for Interactive Broadband Cable Services
Robert Wilson, Concord Networks
Sid Gregory, TCI Technology Partners
Cable companies are looking to interactive broadband cable services and Internet access as their keys to maintaining profitability in the next few years. Find out how they're planning on securing these networks at data rates thousands of times faster than traditional modem access. THU. 5PM.

PRODUCT PRESENTATIONS

Security for Health Care Information Online
Peter O'Donnell, HealthDesk Corporation
HealthDesk's newest product, HealthDesk OnLine, links patients to the healthcare system, provides meaningful market and clinical data and still maintains patient confidentiality and a secure system. THU. 8:30AM.

Security Products for Mission Critical Environments
Stephen M. Weiss, AstraTek
THU. 8:30AM.

Secure Messenger S/MIME Products
Ron Craswell, Deming Software
See Deming's Secure Messenger S/MIME products, including plug-ins for Microsoft Exchange and Qualcomm's Eudora Pro. THU. 9:30AM.

The CipherNet™ System: Key Mgm't & Secure Messaging
Larry Frank, Motorola
The CipherNet™ System of software products protects sensitive electronic information through encryption, digital signatures and automated certificate management. THU. 11AM.

Incorporating Smart Card Technology Into Security Programs
Paul Pieske, Fischer International Systems Corporation
This session provides tips on incorporating smart cards within your organization, and presents case studies of smart cards in a variety of applications. THU. 11AM.

Securely Extending SNA to the World Wide Web
Stephen J. Clark, OpenConnect Systems, Inc.
Hear about security concerns facing corporations considering the integrating the Internet and World Wide Web with traditional SNA-based enterprise information systems. THU. 1:30PM.

GlobalKey-Worlds Apart in Secure Communications
Brenda Kallighan, GlobalKey, Inc.
A data and collaborative business communications system that ensures privacy and confidentiality between GlobalKey users anywhere in the world. THU. 1:30PM.

RADIUS: Centralized Security for Dial-In Users
Cimarron Boozer, Funk Software, Inc.
RADIUS is a centralized authentication service for managing multiple dial-in users on one or more Remote Access Servers using existing NetWare Directory Services or Bindery. THU. 2:30PM.

Internet Software Licensing and Distribution
Dr. Ganapathy Krishnan, Intelligent Software Solutions
An overview of a comprehensive solution for licensing and distributing software on the Internet. THU. 2:30PM.

Philips Third Generation of Crypto Controllers
Stefan Philips, Philips Semiconductors, Germany
These latest crypto controllers use cryptographic coprocessors as part of the smart card architecture to significantly reduce the execution time of cryptographic algorithms like DSS and RSA. THU. 4PM.

Security and Hardware Authentication
Russell Davidson, Net1, Inc.
The benefits of hardware-based authentication services, featuring a "real-time" demonstration of Net1's commercially available technology. THU. 4PM.

Performance Opportunities for Dedicated Cryptographic Processors in SSL
Shawn Abbott, Rainbow Technologies
Recent research into high performance secure server capacity and the use of hardware acceleration is the focus of this session. THU. 5PM.

Single Chip Security Solutions
David Auer, VLSI Technology, Inc.
Commercial data encryption processor architectures controlled by an on-chip microprocessor and cryptographic firmware. THU. 5PM.

escrow) systems across national boundaries may involve multiple sets of mutually distrustful participants. THU 4PM.

Proactive Security: Recovering from Penetrations
Amir Herzberg, IBM Research
two or three
lines
of text. FRI 8:30AM.

Subliminal Channels
Dr. Gustavus Simmons
Developments in the notion of subliminal channels will be discussed. With subliminal channels, redundant information introduced to ostensibly provide an overt function — such as digital signatures, error detection and/or correction, authentication, etc. — can be subverted to provide a covert communications channel. FRI 9:30AM.

Recent Trends in

Call Now to Register:
415-544-9300

Panel: Work with PKCS #11 (Cryptoki)
Stephen Matyas, IBM Corp.
Bruno Couillard, Chrysalis ITS, Inc.
Dave Balenson, Trusted Information Systems, Inc.
PKCS#11, or Cryptoki, is the dominant standard for integrating cryptographic technology with tokens. Our distinguished panel will discuss their companies' recent work with the standard.. FRI. 8:30AM.

Panel: The S/MIME Secure E-mail Standard
Bob Dickenson, Deming Corp.
Douglas Shoupp, Deloitte & Touche
S/MIME has emerged to become the dominant standard for secure e-mail. Find out more about it here. FRI. 9:30AM.

Architecture for Public Key Infrastructure (APKI)
Bob Blakely, IBM Corp.
A small, but influential working group including IBM, Novell, OpenMarket, HP and others have drafted a new proposed standard for public key architectures. Learn more about their work here. FRI. 11AM.

IEEE P1363: A Comprehensive Standard for Public-Key Cryptography
Dr. Burt Kaliski, RSA Laboratories
IEEE P1363 is a working group started in 1993 to develop comprehensive standards for public-key cryptography based on RSA, Diffie-Hellman and related algorithms. Dr. Kaliski will survey the developments of 1996, give an overview of the current draft, and summarize the issues remaining before completion of the standard. FRI. 1:30PM.

PFX: Personal Information Exchange, a.k.a., PKCS #12
Brian Beckman, Microsoft Corporation
Users of public-key technology have certain data units that should be considered "personal property." These include private keys, personal secrets such as account numbers, and certificates and revocation lists. Users must be able to transport this personal property securely-online or offline-from one browser to another and one platform to another. FRI. 2:30PM.

Reaching Consensus on Online Security Standards for Secure Financial Transactions
Allan Schiffman, Terisa Systems
The dialogue has broken down between IS personnel and executive management on issues of computer security. IS engineers do not adequately engage management to assess bottom-line security needs. A comprehensive security review process will be outlined to help the audience establish this critical dialogue. FRI 4PM.

Development of a Token-Enabled Secure Sockets Layer
Paul E. Onnen, Datakey, Inc.
This talk will give details regarding Datakey's implementation of a data security token-enabled Secure Sockets Layer (SSL) version 3, why they did it, and for what purposes it can and will be used. FRI. 5PM.

NetDox: Third Party Solution for Secure Internet Messaging
Dr. Todd Jay Mitty, Deloitte & Touche
NetDox is a standards-based, open architecture, third party service overlaid on secure messaging to support business communications via the Internet. FRI. 8:30AM.

The OpenSoft ExpressMail System
John T. Gildred, OpenSoft Corporation
The first comprehensive secure Internet e-mail system: OpenSoft's ExpressMail and Certificate Server provide a one-stop shop for secure Internet mail. FRI. 8:30AM.

IBM Cryptolopes, SuperDistribution & Digital Rights Mgm't
Dr. Marc A. Kaplan, IBM Corporation
IBM's Cryptolope architecture is a method for the controlled access to broadcasted information using several cryptographic techniques. FRI. 9:30AM.

Security Solutions for ATM Networks
Daniel S. Stevenson, Secant Network Technologies, Inc.
Hear the major challenges of security for Asynchronous Transfer Mode, and see Secant's CellCase product line of solutions. FRI. 9:30AM.

The Launching of the CyberCoin Micropayment Service
Stephen D. Crocker, CyberCash, Inc.
The "CyberCoin" micropayment system provides safe, efficient and prompt Internet transactions in the twenty-five cent to five dollar range. FRI. 11AM.

Norton "Your Eyes Only"
David Grawrock, Symantec Corporation
For Win95 users, this product provides a secure network administration of public and private keys and supports the RSA, RC4, RC5, DES, TripleDES and Blowfish algorithms. FRI. 11AM.

The Argent™ Digital Watermark System
Scott Moskowitz, The DICE Company
See a demonstration of this "master-independent," frame-based digital watermark system for audio and video content. FRI. 1:30PM.

Data Encryption & Security for Off-Line Transaction Processing
Huiping Wang, Tactica Corporation
Information on data encryption and security administration considerations for OFTP systems. FRI. 1:30PM.

The PECOS™ Electronic Commerce System
David Wolf, Elcom Systems, Inc.
PECOS is a client-server application and development environment which enables manufacturers, distributors and direct marketers to conduct RSA-secured transactions via LAN, WAN, Internet and Intranet communications. FRI. 2:30PM.

Security for Internet Commerce
Ken Mohr, Terisa Systems
Discover Terisa's SecureWeb Toolkit and Digitally Signed Documents products, including product demonstrations and a "security" Q&A session. FRI. 2:30PM.

Firewalls and Beyond-the Future of Network Security
James F. Chen, V-ONE
The future of firewalls, potential successor technologies and whether defensive measures will be able to keep up with the "bad guys." FRI. 4PM.

Single Point Security: The Unisys Vision for Enterprise Security
Bill Buffam, Unisys Corporation
Single Point Security provides highly customizable, seamless integration between business policies and IT resource management. FRI. 4PM.

Postal Electronic Commerce Services
Paul Raines, United States Postal Service
The US Postal Service plans a bold update to its services, allowing users to electronically postmark communications and encrypt, digitally sign & archive electronic files. FRI. 5PM.

TIS' RecoverKey Technology
David W. Carman, Trusted Information Systems
RecoverKey technology promotes global deployment of strong cryptography by satisfying US government export requirements. FRI. 5PM.

NOTE: Speakers and sessions are subject to change without notice.

Conference Details

Your attendance fee includes all of the following:

- Four full days of talks, seminars and workshops
- Comprehensive conference notes and materials on CD-ROM
- RSA Partner Fair and Partner Reception: see live demonstrations and exhibits featuring the latest RSA-enabled products
- Continental breakfasts and lunches
- A pre-conference Welcome Reception, Monday January 27
- A private cocktail party at San Francisco's stunning new Museum of Modern Art (MOMA)

Conference Fees

Register early. The RSA Conference always sells out.

- **"Early-bird" registration:** $795 per person (postmarked by November 15, 1996)
- **Standard registration:** $995 per person (postmarked by December 31st)
- **Late registration:** $1,295 per person, (after December 31st, on a space-available basis).

THERE WILL BE NO REGISTRATION AT THE DOOR.

Confirmed registrants who cancel prior to the conference or who do not attend the conference will forfeit their entire registration fee. All cancellations must be made in writing. Substitutions, including those made on-site, are allowed at any time with the written permission of the original registrant.

Call Now to Register:
415-544-9300

PLACE STAMP HERE
THE POST OFFICE WILL NOT DELIVER MAIL WITHOUT POSTAGE

RSA DATA SECURITY CONFERENCE
C/O LKE PRODUCTIONS
1620 MONTGOMERY ST SUITE 120
SAN FRANCISCO CA 94111

Conference Venues

San Francisco is one of the world's most popular travel destinations: a spectacular city noted for its climate, culture and contrasts. Right in its heart there lies a special neighborhood which embodies all the city's most beloved qualities: Nob Hill.

The 1997 RSA Data Security Conference will be held at four convenient Nob Hill venues: the Fairmont Hotel, the Mark Hopkins Inter-Continental, the Stanford Court Hotel and the Masonic Auditorium. These landmark hotels offer world-class accommodations in a quiet and stately location, yet are just a brief cable car ride away from Union Square, China-town, Ghirardelli Square and Fisherman's Wharf.

Special room rates have been negotiated for conference attendees. Call the hotels for reservations, and be sure to mention the RSA Data Security Conference to obtain the discounted rate.

Words of Praise From Past Attendees

"Outstanding as usual!"

"Excellent content, pace, humor, preparation, knowledge."

"[RSA's tutorials on] writing, compiling, and running a simple crypto application were excellent. Nice job!"

Excellent examples, good level of detail and relevance to my work..."

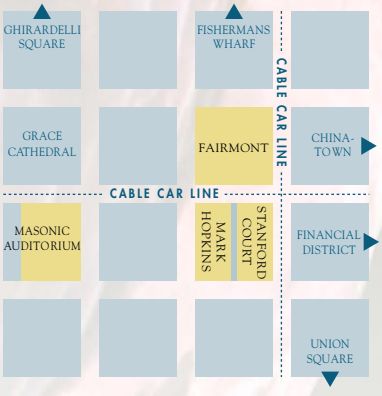
"Overall, a great informational conference..."

Call Now to Register: 415-544-9300

The Mark Hopkins Inter-Continental commands the address Number One Nob Hill. Since 1926, this 4-Star, 4-Diamond and Gold Key Award winner has been steeped in tradition, revered for the quality of its service, and has always set new standards in hotel luxury. Explore the Mark Hopkins and other fine San Francisco hotels at *www.travel2000.com*.

The stunning new San Francisco Museum of Modern Art (SFMOMA) is the setting for Wednesday night's cryptographers' gala. Sip champagne and nibble on hors d'oeuvres with us while browsing their spectacular collection. Find out more about the museum and even see a preview of their collections at *www.sfmoma.org*.

The Masonic Auditorium will host the general sessions and exhibit floor on the first two days of the conference. See the auditorium (and learn more about the Masons) at *www.freemason.org*.



The Fairmont Hotel:
415-772-5000

The Mark Hopkins Inter-Continental:
415-392-3434

The Stanford Court Hotel:
415-989-3500

The Fairmont Hotel, high atop Nob Hill, is RSA's headquarters during the conference. You can check out a live view of San Francisco snapped every few minutes from the top of the Fairmont at *www.kpix.com/live*.

How to Register

REGISTER ON THE NET

http://www.rsa.com

REGISTER BY E-MAIL

info@lke.com

REGISTER BY TELEPHONE

Call LKE Productions at:
(800) 340-0100 or
(415) 544-9300

REGISTER BY FAX

Photocopy and fax this completed form to:
(415) 544-9306

REGISTER BY MAIL

Complete the form, fold it and seal it with tape, and mail to:

RSA Conference, c/o LKE Productions
1620 Montgomery Street, Suite 120
San Francisco, CA 94111

☛ IMPORTANT: CLASS SIGN-UPS

Once you have registered for the conference, you will receive a confirmation number. **Don't lose this!** You will need it to sign up for classes. This year, in order to prevent overcrowding, you must **pre-register** for the classes you wish to attend. You can sign up with your confirmation number at *http://www.rsa.com* or simply call LKE Productions at (415) 544-9300.

FOLD HERE

1997 RSA CONFERENCE REGISTRATION FORM

Name: _____

Title: _____

Company: _____

Address 1: _____

Address 2: _____

City: _____

State: _____ Zip: _____

Country: _____

Phone: ( ) _____ Fax: ( ) _____

E-mail: _____

☐ Check here if you don't wish to be included on the published attendee list

Conference Fees

☐ "Early-bird" registration: **$795** (postmarked by November 15, 1996)

☐ Standard registration: **$995** (postmarked by December 31st)

☐ Late registration: **$1,295** (after December 31st, only if space is available)

Number of people attending: _____

Total amount enclosed: _____

Method of Payment

☐ Cashier's or Company Check enclosed (payable to RSA Data Security, Inc.)

☐ VISA ☐ Mastercard ☐ American Express

Credit Card Number: _____

Expiration Date: _____

Cardholder Name: _____

Signature: _____

Just So We Know:

Which conference track(s) are you most interested in following?
1. _____
2. _____

Will you be attending the Welcome Reception on Monday, January 27? ☐ Yes ☐ No

Will you be attending the cocktail party at the Museum of Modern Art? ☐ Yes ☐ No

Which hotel will you be staying at? _____

Are you an RSA customer? ☐ Yes ☐ No

Application in use: _____