cryptography basics tutorial

2:00 PM

Crypto 101: Intro to Cryptographic Concepts

Steve Burnett, Principal Engineer, RSA Security Inc.

The importance of cryptography as a foundation for e-commerce has transformed what was once an obscure discipline into an essential part of the working knowledge of every IT professional. This session explains the key concepts of modern cryptography, including high-level descriptions of public key, symmetric key, message digests, digital envelopes, digital signatures, and digital certificates. Brief summaries of current export policies, legal acceptance, and standards activities will be provided as well.

3:00 PM

Crypto 201: Advanced Cryptographic Concepts

Steve Burnett, Principal Engineer, RSA Security Inc.

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

4:00 PM

Crypto 202: Overview of Security Protocols

Dr. Jay McCauley, Dir. BSAFE Development, RSA Security Inc.

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

5:00 PM

Crypto 301: Practical Implementations of Cryptography

Dr. Jay McCauley, Dir. BSAFE Development, RSA Security Inc.

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

enterprise security basics tutorial

2:00 PM

Enterprise Security 101: Intro to Public Key Infrastructure

Andrew Nash, RSA Security Inc.

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

3:00 PM

Enterprise Security 201: Advanced PKI

Andrew Nash, RSA Security Inc.

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

4:00 PM

Enterprise Security 202: Authentication Options for PKI

Andy Kemshall, Pre-Sales Engineering Manager, RSA Security Inc. United Kingdom

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

5:00 PM

Enterprise Security 301: Making Applications PKI-Ready

Bronislav Kavsan, VP of Keon Development, RSA Security Inc.

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

pkcs basics tutorial

2:00 PM

PKCS 101: Introduction to the Public Key Cryptography Standards

Jakob Jonsson, Research Staff, RSA Laboratories Europe

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

3:00 PM

PKCS 102: An ASN.1 Primer

Magnus Nyström, Principal Research Engineer and Manager, RSA Laboratories

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

4:00 PM

PKCS 201: Cryptographic Techniques and Message Formats

Jakob Jonsson, Research Staff, RSA Laboratories Europe

Many of today's PKI standards and proposed standards are derived in some way from the four PKCS documents related to cryptographic techniques and message formats. PKCS #1, #5, #7 and #10. This session will give an overview of those four documents, as well as their relationship to the industry standards that include them.

5:00 PM

PKCS 202: Cryptographic Tokens and Data

Magnus Nyström, Principal Research Engineer and Manager, RSA Laboratories

Perhaps the most significant impact of the PKCS series has been in areas beyond the algorithms, relating to the storage and exchange of cryptographic data and implementation of cryptographic modules. This session will describe the three PKCS documents of this class: PKCS #11, PKCS #12 and PKCS #15.

Alexander the Great and Darius at the Battle of Issus, ca. 333 B.C.

featured speakers

Jim Bidzos
Vice Chairman, RSA Security Inc.

Jim Bidzos is vice chairman of RSA Security, and was previously president. Under his leadership, RSA has become the worldwide de facto standard for encryption, being included in such products as Netscape Navigator, Microsoft Internet Explorer, Lotus Notes, Novell Netware, Intuit's Quicken, and Microsoft Windows 95. Almost a half billion copies of RSA's software are in use today. No other company in the world comes close to matching this successful development of encryption technology. Recognized as a visionary and pioneer in the computer industry, Mr. Bidzos is credited with tirelessly promoting the need for encryption since the mid-1980's. He has received a number of industry awards in recognition of his vision, dedication, and accomplishments. In 1994, Mr. Bidzos was involved as an investor in the founding of Netscape and Cybercash, two leading Internet software companies.

Prof. Peter Cochrane
Chief Technologist, BT Laboratories

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

Jim Curtin
Vice President, Strategy, Business Development and Operations, Tivoli SecureWay, IBM

Mr. Curtin is Vice President, Strategy, Business Development, and Operations, for Tivoli SecureWay. Previously, Mr. Curtin has been President and CEO of Dascom, Inc., the industry leading provider of security authorization technology; Dascom was acquired by the IBM Corporation in September of 1999. A graduate of Harvard University, Mr. Curtin has also head significant leadership positions in the Open Systems Foundation, and has worked extensively outside the US.

Roger Farnsworth
Senior Manager, Security Solutions, Cisco Systems

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

Dr. Warwick Ford
Chief Technology Officer, VeriSign

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

Ingo Juraske
Director, Non-Stop E-Business Solutions, Compaq EMEA

Ingo Juraske is Director NonStop e-business Solutions, Industries & Marketing, Compaq Computer Europe, Middle East and Africa (EMEA). Ingo joined Compaq in 1991 and is responsible for driving business development, alliance management and marketing for Compaq EMEA's enterprise solutions business in e-commerce and a full range of vertical industry markets. He also was responsible for building the Compaq EMEA pre-sales competence centers network with a specific focus on Enterprise Applications. Before joining Compaq, Ingo worked at Nixdorf Computer in a variety of engineering management roles.

Ilkka Raiskinen
Vice President, Nokia Mobile Phones, Finland

Ilkka Raiskinen is working with Nokia where he is currently Vice President for Mobile Applications in Nokia Mobile Phones. He has been involved in Wireless Data related activities since the early days GSM technology. Currently his main interests are with the non-voice services and ubiquitous use of Mobile Terminals.

Richard Schlechter
European Commission – DG Information Society

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

Scott Schnell
Senior VP Marketing, RSA Security Inc.

Scott Schnell is senior vice president of marketing for RSA Security, where he directs the global marketing and communications efforts for the company. Mr. Schnell joined RSA as a vice president of marketing in 1996, where he was responsible for building the marketing organization and developing the company's long-term strategy. Previously, Mr. Schnell spent 15 years in product and strategic marketing positions at Apple, Photonics and McKinsey and Company.

general sessions

Special keynote addresses, expert panels and discussions of general interest

TUESDAY

9:00 AM

Welcome

Jim Bidzos, Vice Chairman, RSA Security Inc.

A special opening presentation and e-security year in review from RSA Vice Chairman Jim Bidzos.

9:15 AM

E-security Strategies for the New Millennium

Scott Schnell, Senior VP Marketing, RSA Security Inc.

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

10:30 AM

Cryptographers' Panel

Burt Kaliski, RSA Laboratories; Walter Fumy, Siemens AG; Claus P. Schnorr, J.W. Goethe University Frankfurt; Dr. David Naccache, Gemplus, France; Dr. Kaisa Nyberg, Research Fellow, Nokia Finland

Renowned cryptographers discuss current and future trends in e-security. Don't miss this favorite roundtable discussion on trends that will impact security in the new millennium.

11:30 AM

Now That Everyone Has a Certificate, How Do You Really Manage Your Enterprise's Security?

Jim Curtin, Vice President, Strategy, Business Development and Operations, Tivoli SecureWay, IBM

The infrastructure for secure operations is largely available: PKI certificates, firewalls, virtual private networking, and the like. But for many enterprises, this is no reason for comfort. Two substantial problems continue to plague information executives: the management of their security systems, and the expense of building security reliably into new applications. We provide a vision of the future of enterprise security that effectively addresses these issues.

WEDNESDAY

8:00 AM

VeriSign Keynote

Dr. Warwick Ford, Chief Technology Officer, VeriSign

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

9:00 AM

More Machines Than People

Professor Peter Cochrane, Chief Technologist, BT Laboratories

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

10:30 AM

Privacy and Security Challenges in an Era of Non-Stop, Continuously Available Computing

Ingo Juraske, Director, Non-Stop E-Business Solutions, Compaq EMEA

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

11:30 AM

Security in Electronic Communication – The EU Approach

Richard Schlechter, European Commission – DG Information Society

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

THURSDAY

11:15 AM

Securing Electronic Business

Roger Farnsworth, Senior Manager, Security Solutions, Cisco Systems

This session is designed to prepare managers to better understand the key information security issues facing them as they transition their infrastructures to successfully compete in the Internet economy. As internet technology revolutionizes business practices, the resulting enhancements to communication processes create increased challenges to information security.

12:15 AM

From Cellular Phone to Personal Trusted Device

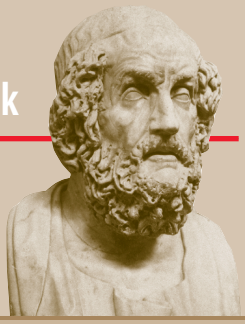
Ilkka Raiskinen, Vice President, Nokia Mobile Phones, Finland

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

Facing page: Apollo, Greek god of prophesy, music and healing

cryptographers' track

For mathematicians, academics and researchers



TUESDAY

2:00 PM

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

Burt Kaliski, Chief Scientist and Director, RSA Laboratories

The recent "unknown key-share" attack on the MQV key agreement protocol offers a classic example of the challenge of designing secure protocols. This talk will summarize the attack and its implications, highlighting several principles that are essential to the design of any protocol.

3:00 PM

FIPS 140-2 and Common Criteria Certification

John Hines, Engineering Manager, Netscape/Sun Alliance; John Morris, President, Corsec Security, Inc.; Ray Snouffer, FIPS 140-2 Program Manager, NIST; Dr. Sean Smith; IBM T.J. Watson Research Center

Worldwide acceptance of FIPS 140-2 and ANSI X9.66 is growing; however, Common Criteria (CC) evaluations are still the preferred international marque. Join a panel of FIPS 140-2 experts to discuss international cryptographic certification and evaluating FIPS 140-2 in a CC protection profile.

4:15 PM

WAP's WTLS Protocol – Lessons Learnt

Magnus Nyström, Manager, RSA Laboratories Europe, RSA Laboratories

Tentatively: The Wireless Transport Layer Security Protocol is the WAP forum's security layer protocol. In this talk, a selection of attacks against WAP's WTLS protocol is presented, together with suggestions for countermeasures and a discussion of protocol design lessons to be learnt.

5:15 PM

The Advanced Encryption Standard: Development and Status

Ray Snouffer, FIPS 140-2 Program Manager, NIST

The purpose of this presentation is to articulate the status of NIST's AES development effort. This presentation will include: a description of the overall AES development effort; discussion of the second round of analysis (Round 2), including significant Round 2 issues; and future plans for the AES and related standards.

WEDNESDAY

2:00 PM

Proofs of Knowledge of Discrete Logarithms and Applications

Marc Girault, Senior Expert, France Telecom/CNET

Proofs of knowledge of a discrete logarithm have become in recent years a central tool in the design of a great many cryptographic protocols. A unified presentation of these protocols will be given, stating their main properties (related to security and performances). Then specific variants and quite recent applications (very fast authentication, verifiable encryption of RSA keys, knowledge of RSA bits,...) will be shown.

3:00 PM

Fast Monte-Carlo Primality Evidence Shown in the Dark

Dr. Wenbo Mao, HP Laboratories, Bristol

Proof primality "in the dark" means to show that a number is a prime without disclosing the number. Its application includes that a user shows this to a key certification authority regarding a self-generated key, and that the key has been generated in uniformly random.

4:15 PM

Why Hyperelliptic Curves Might Be More Secure than Elliptic Curves

Detlef Huehnlein, Dipl. Inform., Secunet AG

It is shown that the group of points of E is isomorphic to the ring R=0/(Fr-1)0. We show that the latter DL-problem can be efficiently solved for practical parameter sizes of 160 bit p. Furthermore we investigate attempts to construct such a map and explain why a similar strategy should not apply to hyperelliptic curves. Thus hyperelliptic curves remain secure, even if a constructive version of above isomorphism is found.

5:15 PM

Privacy and Security of Public Databases

Dr. Susanne Wetzel, Lucent Technologies – Bell Laboratories

There are several settings in which the information stored in databases must be safeguarded against attacks. Confidentiality of records stored in such databases is typically ensured by restricting access to individuals who possess the correct credentials. We show how to protect the privacy of information stored in publicly available databases using biometric information.

THURSDAY

8:00 AM

Key Generation with Implicit Key Recovery

Nicko van Someren, nCipher

We present a new key generation technique which combines the archiving of a private key for recovery into the key generation and certificate generation processes. Keys generated using this technique can therefore be recovered post hoc without the participation of the keyholder. This allows for both a reduction in cost and an improvement in reliability in a Public Key Infrastructure which must support key recovery. A patent application for this technique has been filed.

10:00 AM

Class to be Announced

Guest Speaker

9:00 AM

How to Puzzle an Attacker

Ari Juels, Senior Research Scientist, RSA Laboratories

We present a series of recent research results from RSA Laboratories exploring the deployment of puzzles –that is, small cryptographically based problems– to achieve a range of different security goals. Applications of puzzles include defense against denial-of-service attacks and privacy protected distributed computing.

developers' track

Classes for developers working with security

TUESDAY

2:00 PM

Certificate Considerations in Wireless Environments

Dr. Warwick Ford, Chief Technology Officer, VeriSign

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

3:00 PM

Utilizing Secure Hardware

Joan Dyer, IBM

In this talk, we discuss how to use secure hardware to provide security for distributed e-commerce solutions. However, extended access increases exposure to attack... which cryptography can address... but cryptography only works if secrets remain uncompromised and algorithms remain unmodified. Incorporating elements of secure hardware can provide these properties. We will discuss design, engineering, and assessment issues for a spectrum of example problems and hardware.

4:15 PM

Digitally Signed XML: A New Internet Standard

Barbara Fox, Security Architect, Microsoft

The new XML Digital Signature Specification describes the standard mechanism for signing documents, transactions, and other resources on the Internet. This panel, comprised of members of the IETF working groups, will focus on the technical details of this emerging standard and its impact and users of web applications.

5:15 PM

Passwords: Beyond the Terminal Interaction Model

Niklas Frykholm, RSA Laboratories

Passwords originated as a means of identifying terminal users to mainframes. With the proliferation of keyboardless systems and password cracking programs the need for alternatives has increased. We present graphical password systems that offer more natural input on PDAs and, by better using human memory, a significant entropy increase.

WEDNESDAY

2:00 PM

Time Stamping Services – Motivation and Basic Techniques

Roland Mueller, TUVIT, Inc.

The talk motivates the need for secure time stamping, presents different approaches and discusses their requirements, and the services and entities involved. It presents various techniques how time parameters can be tied to electronic information and gives an overview on standardization activities in the area.

3:00 PM

Why Europe Hesitates to Buy American Electronic Stamps

Detlef Huehnlein, Dipl. Inform., Secunet AG

The U.S. postal service started the Information Based Indica Program (IBIP) to issue "electronic stamps" involving digital signatures. However it seems that European postal services hesitate to adopt the American program, because it seems to introduce an unreasonable overhead due to the verification of (asymmetric) digital signatures. We introduce an alternative approach based on symmetric algorithms which is more suitable for large scale deployments.

4:15 PM

Cryptography and Biometrics in Banking

Vashek Matyas, UBS AG, Ubilab

Our talk focuses on the cryptographic issues relevant to the deployment of various biometric authentication techniques. We look at various scenarios for deployment of biometrics within the banking environment and examine some of the critical issues of such applications where there is a potential to use cryptographic tools/techniques to resolve these issues.

5:15 PM

IPsec, A General Solution for Securing the Internet

Tatu Ylönen, Chairman and CTO, SSH Communications Security Ltd.

Cryptography is the only viable method in securing network traffic on the Internet without losing the flexibility. It offers confidentiality, integrity, authentication, and non-repudiation. Many applications using cryptography have emerged. IPsec (Internet Protocol Security) is a break-through in these technologies enabling the protection of all Internet traffic.

THURSDAY

8:00 AM

Replacing the Smartcard PIN: Fingerprint Matching on 8-bit Smartcards

Anthony Russo, Distinguished Staff Technologist, Veridicom, Inc.

Recent advances in biometric technology – specifically the author's development of the first high-performance fingerprint matching algorithm suitable for implementation on low-cost smartcards – can be employed together with those cards to boost all three of these aspects by allowing for replacement or augmentation of the PIN.

10:00 AM

Class to be Announced

Guest Speaker

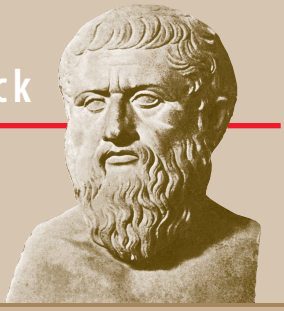
9:00 AM

Guest Speaker

Speaker to be announced

implementers' track

Case studies and practical advice for the IT professional deploying solutions for the enterprise



TUESDAY

2:00 PM

Wireless Payment Solutions

Marcus Berglund, Parallel Consulting Group AB

Within 2 years, more than 50 percent of all terminals connected to Internet will be cellular phones or mobile terminals. The key functionality for e-commerce is secure and user-friendly Internet payment methods. Examples of questions to be answered are: is it possible to use current payment standards? Is the functionality in todays wireless terminals, like SMS, SAT and WAP 1.1, enough for creating secure payments? Is there a need for a wireless PKI?

3:00 PM

Implementing a Wireless PKI to Secure Financial and Healthcare Applications

Michael Crerar, Cryptographer, Diversinet Corp.

This session discusses Diversinet's experience in designing and implementing a wireless PKI and the pilot with BellSouth to demonstrate the applications of wireless e-commerce in areas such as finance and health care. The challenges of working in a bandwidth and device constrained environment and working in WAP and other forums on achieving interoperability with existing infrastructure will also be discussed.

4:15 PM

Windows 2000 Authentication: Under the Hood

Jan De Clercq, Consultant, Compaq

This session focuses on one of the core operating system security services of Windows 2000: Authentication. Without a solid and trustworthy authentication mechanism network operating system security becomes completely unreliable and in a certain sense even worthless. Windows 2000 implements the IETF standard Kerberos as its new default authentication protocol. The primary focus of this talk is Kerberos.

5:15 PM

Requirements for a Card Management Infrastructrure

Laurent Den Hollander, Corporate Staff Scientist, Gemplus

The Card Management Infrastructure (CMI) proposes a framework to facilitate the integration and deployment of smart cards in enterprise information systems. The CMI takes into account both the integration of multiple legacy data sources and sinks (HR, PKI...) and card specifics (graphic and electric issuance, remote maintenance, multi application cards).

WEDNESDAY

2:00 PM

Nordic Standardization Moves to Interesting Implementations

May-Lis Farnes, President, SEIS

The SEIS work has contributed to building a necessary infrastructure of security, which makes e-commerce on Internet grow. SEIS started to work on technical standardization and the work continues on related policy and legislative questions and on implementing and establishing applications. The work is connected to the International standardization worldwide.

3:00 PM

Do-it-Yourself Certification Authorities: The Legal Toolkit

Samoera Jacobs, VP Practices and Procedures, GlobalSign

Digital signatures are widely seen as the staple of electronic commerce. Drawing from the experience of GlobalSign as a provider of PKI products and services this presentation shall show you how companies can build their own PKIs in-house and beyond. This presentation provides answers to questions related with the legal infrastructure of a CA and the requirements to underpin the legality of its operation.

4:15 PM

Deploying S/MIME in the Enterprise

Blake Ramsdell, Chief Technology Officer, Worldtalk Corporation

There are many factors to consider when deploying S/MIME in the enterprise. This presentation will explain what components are available, how they can be combined to effect a corporate S/MIME strategy, and how they can be incrementally deployed for minimal disruption. Native client applications, client plugins, server-based S/MIME, cryptographic hardware tokens, public certification authorities and enterprise PKI will be discussed.

5:15 PM

Certificate Based Access Control Mechanisms for the Web

Scott Shorter, Manager, PKI Consulting Services, CygnaCom Solutions

An examination of the current state of the art in certificate based access control for the world wide web, including the use of attribute certificates for authorization, role- and rule-based access control procedures, access control granularity, and the different delivery methods for getting the authorization information to the web server.

THURSDAY

8:00 AM

What to Look at in a Practical PKI

Dominic Storey, Technical Director, RSA Security

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

10:00 AM

Enterprise PKI Implementation Strategies

Guest Speaker

Four top security companies discuss strategies for implementing heterogeneous, multi-vendor public key infrastructures that work. You'll learn what's compatible and, more importantly, what isn't at this eminently practical expert panel.

9:00 AM

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

Paul Paget, Vice President, Marketing, CyberTrust

This case study presents how Italy used CA's to take the lead in supporting secure electronic transactions for its business and financial communities. We'll discuss technical issues of how the solution was integrated into SIA's timestamping services and how it supports multiple variations of certificate content, format and security in a single system.

new products track

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

TUESDAY

2:00 PM

IPlanet Certificate Management System 4.2

John Hines, Engineering Manager, Netscape/Sun Alliance

Netscape will present the architecture of its Certificate Management System 4.11 product. Technical details of the product will be presented along with possible deployment scenarios. Details about interoperability with a variety of client, server, and hardware vendors will also be presented.

4:15 PM

Super Scalable Server-Based S/MIME for the Enterprise

Blake Ramsdell, Chief Technology Officer, Worldtalk Corporation

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

3:00 PM

Network Security Beyond Firewalls and VPN´s

Tomas Olovsson, CTO, AppGate

Many companies and organizations base their security around a firewall. But a firewall offers only a perimeter protection. An external attacker would not attack the firewall unless it is known to be flawed, but instead concentrate on external weak points. This talk will give a view of which techniques should be used to protect your network.

5:15 PM

Building an Enterprise PKI

Bob Pratt, Group Product Manager, VeriSign

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

WEDNESDAY

2:00 PM

Lock up Your Keys! The nCipher Key Management Tool

Alex van Someren, Cryptographer, nCipher Corporation Ltd

The new nCipher key management tool – KMtool – works with nCipher's nFast/KM products to manage the digital certificate public and private keys used in e-commerce. Its easy-to-use interface maintains keys' life cycles in hardware for premium security and cryptographic performance while supporting advanced key management features such as key sharing and access control lists for application policy flexibility.

4:15 PM

Extraordinary Extranets: Effectively Teaming VPNs and PKI

Melanie Ciosek Francis, Product Marketing Manager, CyberTrust

Although many CA/PKI vendors have addressed using digital certificates to enable VPNs, to date no one has addressed the "bigger picture" to show how VPN technology can be used in conjunction with a PKI-based solution to provide secure communications in an extranet environment. This session provides the technical information to make the logical next-step in the evolution of VPNs and PKI.

3:00 PM

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

Peter Forret, VP, GlobalSign

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

5:15 PM

Class to be Announced

Sam Asseer, LCI

THURSDAY

8:00 AM

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

Elad Baron, CEO and Founder, Whale Communications

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

9:00 AM

MAILguardian Enterprise: The Ultimate Enterprise E-Mail Security Solution

Raviv Karnieli, CTO, Vanguard Security Technologies

E-Mail is the most used Internet applications by business users. Yet, it is not widely used for e-business because of lack of good security solutions. While several e-mail encryption solutions exist today, they are not used by enterprises. The reason is that all of the existing solutions either put the security responsibility on the end-users or provide only partial solutions via servers or gateways. Vanguard Security Technologies released the first E-Mail security solution that provides enterprises with a whole solution.

10:00 AM

Class to be Announced

Guest Speaker

rsa™ products track

Immersion workshops for developers, IT professionals, and customers working with RSA products

TUESDAY

2:00 PM

RSA™ BSAFE SSL-C in-Depth

Tim Hudson, Technical Director, RSA Security

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

3:00 PM

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

Steve Burnett, RSA Security Inc.

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

4:15 PM

PKI Case Study: Enabling Secure Inter-Company Collaboration

Lina Liberti, Director, RSA Security Inc.

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

5:15 PM

Enabling PKI with the RSA BSAFE Cert Tools

Marina Milshtein, Software Engineer, RSA Security Inc.

This presentation will show how developers can use RSA BSAFE Cert tools to add PKI to their applications. It will demonstrate the general Cert tools model and examples of how to use Cert-C and Cert-J products. It will walk through the basics of creating CertRequests and submitting them to Certificate Authorities (CA). It will show how to parse, create, sign, and use service providers to validate certificates.

WEDNESDAY

2:00 PM

RSA Keon™ Agent Software Developer Kit (SDK)

Peter Röstin, Technical Director, RSA Security

RSA Keon Agent software is used to provide security solutions for client-server based applications. The Keon Agents are "plug-in" solutions which can be installed in existing application environments, without modifications of the original application installations. The Keon Agent Software Developer Kit allows developers to develop their own agents for in-house or 3rd-party developed applications.

3:00 PM

RSA Keon™ Single Sign-On Software Developer Kit (SDK)

Peter Röstin, Technical Director, RSA Security

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

4:15 PM

RSA SecurID in a Wireless Environment

Göran Walles, Senior Systems Engineer, RSA Security Sweden

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

5:15 PM

RSA SecurID for Web Applications

Norbert Olbrich, Pre-Sales Engineering Manager, RSA Security Germany

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

THURSDAY

8:00 AM

RSA SecurID in a Managed Service Environment

Jonathan Smith, Pre-Sales Engineering, RSA Security

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

9:00 AM

RSA SecurID, A Critical Component of Your PKI

Ted Kamionek, Senior Product Manager, RSA Security Inc.

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

10:00 AM

Class to be Announced

Guest Speaker