



---

## SJSU-PDC and SecureNode Present

---

### Getting Practical with Privacy and Security

Saturday, May 8<sup>th</sup>, 2004

San Jose State University – Professional Development Center

#### Speakers

- Matt Pauker, Founder Voltage Security
- Ray Bayer, VP Product Marketing, Mail-Filters
- Steve Phelan, Director Product/Sales, Fortinet
- Dean Hipwell, CISSP, Sr. Security Consultant, SecureNode
- Ron Conover, CISSP, Security Consultant, SecureNode

#### Panelists

- Judy Kaiser, Director, San Jose State University – Professional Development Center
- Tasawar Jalali, Founder, SecureNode Inc.,

#### Moderator

- Brian Smithson

#### Topics

1. Introduction by SecureNode/SJSU
2. IBE (Identity based Encryption): An alternative to Public-key infrastructure (PKI)
3. Beating Spam - The Tricks Spammers Use and How to Defeat Them
4. Cyber-Security and Your Organization
5. Privacy and Cryptography – A CISSP Domain
6. Getting A Handle on: HIPAA, Sarbanes Oxley and GLBA

#### Registration: <http://www.sjsu.edu>

- \$49.00 Thru Monday May 3<sup>rd</sup>, 2004
- \$59.00 Thru Friday May 7<sup>th</sup>, 2004
- \$69.00 Day of the event Walk-ins at the door (\*space permitting).
- NO RESERVATIONS ACCEPTED AFTER May 7<sup>th</sup>, 2004

## Synopsis:

Information security is a business problem. With the focus on information security in the media, and in legislatures around the world, organizations are facing complex requirements to comply with security and privacy standards and regulations. Relying on yesterday's technology to secure your network is an open invitation to hackers and other malicious intruders.

This one-day seminar introduces you to the latest trends and technologies being adopted by network security experts today. In this seminar we gather various experts in the field of IT Security who are relentlessly developing new security solutions to protect the IT networks.

In discussing Information security, few basic things will be addressed during this seminar:

- An overview of security issues, techniques, and trends related to the confidentiality, integrity, and availability of information assets on an organization's computer systems.
- The different protective tools available these days may not be enough to avert the threats to your network. A weakness in one part undermines the security of them all. Security tools have evolved in response to the increasing complexity of the networks, including the number and type of users, OS'es, and programs supported. This complexity also includes the increasing number of system software components. Find out how these challenges are being addressed by the pioneers of Information security technology.
- As new hacking tools increase in sophistication, it has become very challenging for the Network Administrators to keep up with these tools. This requires attention and greater effort by security administrators to ensure that cutting edge security technology is used rigorously and consistently. Find out what you can do to defend your networks against such threats.

## **Detailed Topics:**

---

### **Mail-Filters:**

- Beating Spam - The Tricks Spammers Use and How to Defeat Them
  - Spam is causing a significant security risk
    - Malicious Code
    - The sheer volume is causing an effective Denial of Service Attack
    - Interesting Statistics / Antidotes
  - Spammers are becoming adept at evading filters
    - Economic incentive to get around the filters
    - Tools they use
    - Tricks:
      - Snowflaking, Embedded URLs, HTML, Baysean Poisoning, Hash Busting
  - How to Win
    - Support legislative efforts, but..
    - Focus on Technology
      - Heuristics
      - Baysean (Statistical)
      - Signatures
      - New Technologies
  - Measurements (How do we know when we've won)
    - The Catch-Rate Dilemma
    - False Positives and why they count 10x more than Spam Catch Rate
      - The 1% Fallacy

### **Voltage Security:**

- IBE (Identity based Encryption): An alternative to Public-key infrastructure (PKI)
  - PKI market background
  - PKI Technical Limitations and Advantages
  - Why PKI has underperformed to Market Expectations
  - How Ease of Use ensures Security
  - IBE as a technology

### **SecureNode:**

- Privacy
  - What's considered to be "personal" or "private" data anyway?
  - Identity theft, "phishing", "phatbots" and other threats to privacy.
  - Who can find you? Answer: Anyone. Example: [www.usatrace.com](http://www.usatrace.com)
  - Who "owns" your Tax ID? Answer: That's unclear, but compromises must be reported to them.
  - What is profiling?
    - Consumer Profiling
    - Airline Passenger Profiling
  - Whatever happened to facial recognition software?

- What's a RFID used for?
- What's the significance of Google's "Gmail" to privacy?
  
- Cryptography
  - What's cryptography good for?
    - Thwarts identity theft if your laptop or PDA is misplaced or stolen.
    - Prevents someone from eavesdropping your e-mail.
    - Thwarts intellectual property theft if your server is hacked.
    - CIPA reporting (fka SB1386) is not required.
  - What kinds of crypto are there?
    - Answer: PGP, SSL, VPN, RSA SecureIDs and other selected products.
    - Pitfalls: The "WAP gap" and other so-called secure services.
  
- Law
  - HIPAA - Health Insurance Portability and Accountability Act of 1996
    - The Privacy Rule
    - The Security Rule
    - Administrative, Technical, and Physical Safeguards
  - SOXA – Sarbanes-Oxley Act of 2002
    - Section 302 – Controlling Disclosures
    - Section 404 – Internal Controls
  - GLBA – Gramm-Leach-Bliley Act of 1999
    - Financial Data Privacy
    - Compliance
  - USAPA – USA Patriot Act of 2001
    - Financial Data Reporting
    - Terrorism Information Awareness
  - FISMA
    - Protecting the Nation's Critical Information Infrastructure (Source: <http://csrc.nist.gov/sec-cert/index.html>)
  - CIPA – California Information Protection Act (SB 1386)
    - Responding and reporting compromises of personal information.
  - CMIA – Confidential Medical Information Act
  
- Compliance
  - Twelve Steps For Compliance
    - Identify and Classify Information
    - Study Current Processes
    - Perform Gap Analysis and Risk Assessment
    - Appoint Information Owners and Define Ownership Hierarchy
    - Authorize Content Usage and Processing Policies
    - Design Access Monitoring and Control Paradigm
    - Create a Monitoring and Enforcement Plan
    - Construct Audit and Detection Program
    - Retention Policy
    - Plan Data Storage and Availability

- Implement and Deploy New Information Security Policies.
- Standards
  - ISO 17799
    - What does ISO 17799 say about SOXA
    - Critical Success Factors
      - security policy, objectives and activities that properly reflect business objectives
      - a sound understanding of security risk analysis, risk management and security requirements
      - an approach to security implementation which is consistent with the organization's own culture
      - clear management commitment and support
      - effective 'marketing' of security to employees (including managers)
      - proper distribution and guidance on security policy to all employees and contractors
      - provision of adequate education and training
      - a balanced and comprehensive measurement system to evaluate performance in IS management and feedback suggestions for improvement
  - NIST Standards and Guidelines
  - COBIT - Best Practices for auditors.



---

**Speaker Profiles:**

---

- **Matt Pauker, Founder Voltage Security**

Matt Pauker co-founded what is now Voltage Security while attending Stanford University in 2001. In 2002, Matt graduated from Stanford with a Bachelor of Science in Computer Science. Matt has completed coursework for a Masters in Management Science and Engineering from Stanford.

While at Stanford, Matt was involved in various computer science research projects, one of which, during the summer of 2001, led to the creation of Voltage Security. Matt and Rishi began collaborating as dorm mates when they both reached Stanford in 1999.

- **Ray Bayer, VP Product Marketing, Mail-Filters**

Mr. Ray Bayer, Vice President of Product Marketing and Business Development, Mail-Filters

Ray Bayer manages the product requirements and strategic direction of Mail-Filters messaging security products. Mr. Bayer is responsible for working closely with Mail-Filters' customers and OEM's and the development team to ensure that the company's anti-spam and other messaging security products meet their needs. With over 20 years of software security experience, Mr. Bayer is recognized as an expert on spam and how to prevent it.

Prior to joining Mail-Filters in November, 2001, Mr. Bayer was the Director of Product Marketing with Voice over IP technology developer, HearMe, Inc. He has managed product lines ranging from \$5 million to \$200 million with communication, anti-virus, and storage companies Central Point Software (Symantec), Cheyenne Software (Computer Associates), Global Village Communications, and Netopia. Mr. Bayer holds a BS in Marketing and a Master of Business Administration from East Carolina University.

- **Dean Hipwell, CISSP, Sr. Security Consultant, SecureNode Inc.,**

Dean is a computer systems engineer with 25 years experience in telecommunications and computer systems. He is currently an information systems security consultant, adjunct professor of computer science at CSU-Sacramento, and Director of Training & Education for ISSA-Sacramento Valley.

Dean holds a BSEE from Penn State and an MS in Computer Engineering from the U.S. Air Force Institute of Technology.

- **Ron Conover, CISSP, Security Consultant, SecureNode Inc.,**

Ron is a network engineer with 18+ years of progressive experience. He has extensive experience in the design; installation, securing and support of IP based networks. He is proficient with the complete life cycle of network infrastructure deployment, including needs analysis, solution generation, and operations management. Ron is an expert in health information security and related legislation, particularly the Health Insurance Portability and Accountability Act (HIPAA).



---

---

## **Company Profile:**

### **About SecureNode Inc.,**

Founded in 2000 by a team of Internet security experts, SecureNode is headquartered in the heart of Silicon Valley, California. SecureNode is the leading provider of Information Security Education, Information Security Services, and Outsourcing solutions. SecureNode's strong network of partners offers a comprehensive set of IT security solutions and services that help establish security infrastructures protect critical business assets and preserve the privacy of customers.

SecureNode is Voltage Security's primary partner for product training. SecureNode's extensive experience in delivering CISSP certified training as well as their world class facilities and staff led Voltage to select them for delivery of system administrator training.

### **About SJSU-PDC**

San José State University's location in the Silicon Valley makes it an exceptionally rewarding learning environment for students. Silicon Valley firms and agencies seek SJSU students for internships, summer work programs and for assistance with research and development projects. Silicon Valley firms employ more graduates from SJSU than from any other university in the nation.

Located on 154 acres in downtown San José, the university offers the excitement of studying at a large, metropolitan campus where many cultures meet. Yet students find personal attention from faculty members in the smaller setting of the university's eight colleges. For more details please visit <http://iesweb.sjsu.edu/profdev/index.html>

### **About Voltage, Inc**

Voltage Security, Inc. is a new information security company focused on providing secure multi-channel business communication solutions based on a revolutionary breakthrough called Identity-Based Encryption or IBE. Voltage is the first to use identity to bring confidence to business communication. Voltage solutions secure business communication by making anytime, anywhere communication easy to use and painless to deploy.

### **About Mail-Filters**

Mail-Filters.com is dedicated to protecting businesses from spam. The company develops, operates and licenses technology that seamlessly and effectively detects spam. Mail-Filters.com, Inc. has two solutions: SpamRepellent for organizations that want Mail-Filters to host the filtering and SpamCure for organizations that prefer to maintain their e-mail filtering on-site. Founded in 2001, Mail-Filters.com is located in San Mateo, California.



**For more information:**

Call us @ 408-519-1272, or by email at [jjacks@profdev.sjsu.edu](mailto:jjacks@profdev.sjsu.edu) / [cissp@securenode.com](mailto:cissp@securenode.com) or visit us at <http://www.profdev.sjsu.edu> / <http://www.securenod.com/>

\*\*Your registration fee includes the hors d'oeuvres reception

If you know someone else, an associate or friend, who might like to attend, please feel free to invite him or her. The SecureNode/SJSU-PDC seminar is open to everyone.