Securing and Auditing Virtual Office Networks
September 24 – 26, 2003

Description
The combination of dialup access, small office/home high-speed Internet service, virtual private networks, mobile computing, and wireless technology have empowered a rapidly growing population of highly mobile, decentralized workers. These technologies have also unfortunately spawned opportunities to create numerous backdoors on many enterprise networks for both inbound and outbound access. In this diversified network security workshop, you will explore and leverage understanding of the TCP/IP protocol as a basis for understanding various access methods and issues associated with extending the reach of the enterprise network apart from the firewalled connection to the Internet. You will evaluate different security safeguards including: authentication mechanisms, enterprise authentication systems, remote access server configuration, session-level encryption, virtual private networks, and wireless application security. You will also be exposed to methods for developing creative auditing techniques for locating the "screen doors on the back of the safe" including: modem hunting, packet sniffing, and "moonlight audits". Demonstrations will include the configuration and auditing of: remote access servers, virtual private network end-points, and authentication servers.

Focus
This three-day workshop is designed for Information Security Managers and Analysts, IT Planners, Security Architects, IT Managers, Network and Systems Administrators, Technical Consultants, and IT Auditors. **A basic working knowledge of networking and client/server technology is necessary.**

Topics

1. **Defining the network environment**
   - Scope of network security programs
   - LAN vs. WAN
   - WAN/Internet connection methods
   - Open Systems Interconnection (OSI) Model
   - Transmission Control Protocol/Internet Protocol (TCP/IP)
   - Network security strategies
2. **Understanding the TCP/IP protocol**
   - Requests for Comment (RFCs)
   - TCP/IP addressing
   - TCP/IP packet headers and applications
   - Common threats to TCP/IP networks
   - TCP/IP application risk analysis

3. **TCP/IP application security**

- Network address directory services: DNS, DHCP, LDAP, NIS
- Lookup and diagnostic services: finger, netstat, ping, traceroute, SNMP
- Remote access/terminal interface: telnet, X-Windows, r-commands
- File transport, sharing, and messaging: ftp, tftp, NFS, e-mail

4. **Developing a Remote Access Security Plan**
   - Remote access/dialup applications
   - Operational and security issues associated with different types of remote access services and methods: remote node, remote control, dedicated application
   - Sorting out the choices for remote user and small office Internet access: modem, ISDN, cable modem, Digital Subscriber Line (DSL), satellite
   - Wide area network encapsulation protocols for remote access: SLIP, PPP, PPPoE
   - Security issues associated with remote access/dialup
   - Criteria for selecting remote access servers
   - Configuring a remote access server: Microsoft example

5. **Security for Residential Broadband and other Remote User Internet Connections**
   - Security issues with residential broadband Internet connections
   - Distributed file sharing security issues and safeguards: Windows file shares, Instant Messaging (IM)
   - Security issues associated with personal web servers, file transfer protocol (FTP), telnet, and other potentially dangerous TCP/IP workstation application servers
   - Developing security baselines for individual user and small office Internet connections
   - Criteria for selecting and deploying personal firewall software and appliances
   - Using low-cost tools and services for self-testing the security of individual Internet connections and personal firewalls

6. **Sorting out the choices for enhanced user authentication protocols and mechanisms**
   - Authentication protocols for PPP applications: PAP, CHAP
   - One-time dynamic passwords: S/Key, OPIE, and other software-based one-time password schemes
   - Smart cards
   - Biometrics
   - Digital certificates
   - Extensible Authentication Protocol (EAP)
   - Risk-based methodology for selecting authentication mechanisms
   - Enterprise Authentication Systems: RADIUS, TACACS+, Diameter

7. **Virtual private networks (VPN), tunnels, and secure session tools**
   - Defining the major types of VPNs: trusted, secure, hybrid
   - Tunneling and VPN concepts
   - VPN applications
   - Security features for VPN applications

- Sorting out the major VPN protocols: PPTP, L2TP, IPSec, SSL
- Personal VPNs using Secure Shell (SSH)
- Securing remote control programs: pcAnywhere, Virtual Network Computer (VNC)
- Methods for detecting and filtering VPN protocols
- Tools and techniques for auditing and testing the security of VPN connections

8. Securing mobile applications

- Security issues associated with the use of hand-held and other portable computers: portable host security, potential for undermining existing network infrastructure security
- Evaluating built-in and add-on safeguards for portable computers and handheld devices: data protection, user authentication, anti-theft
- Using hand-held devices for network user authentication
- Defining effective policies for the safe use of portable and handheld computers

9. Securing wireless network applications

- Making sense out the myriad of wireless technologies: PANs, LANs, WANs
- Operating and securing wireless Personal Area Networks: Infrared, Bluetooth
- Keeping a lid on 802.11 wireless local area networks security:
- Designing and securing mobile wireless WAN applications: Wireless Application Protocol (WAP)

10. Locating unauthorized network backdoors and insecure network entry points

- Wargames dialers, moonlight audits, and other creative modem detection techniques
- Focused port scans and remote access client probes for locating unauthorized and/or insecure remote control/access services
- Using Simple Network Management Protocol (SNMP) scanners for locating potential backdoor entry points
- War driving, packet sniffing tools, and wired techniques for locating and testing the security of wireless networks

About the Author
Ken Cutler, CISSP, CISA
Vice President for MIS Training Institute

Ken Cutler is the Vice President of Curriculum Development and Professional Services at MIS Training Institute, and Vice President of Information Security Institute (ISI), the security division of MIS Training Institute. His responsibilities include directing MIS' public training programs, including audit and information security seminars and symposia. In addition, he sets strategy for MIS and ISI's seminar curriculum and certificate programs, and manages and serves as principal consultant of ISI's Professional Services. He is also the principal consultant for Ken Cutler & Associates (KCA), an independent information security consulting firm.

Previously, Mr. Cutler headed up companywide information security programs for American Express Travel Related Services and Martin Marietta Data Systems. His responsibilities at these major corporations included developing security policies and standards, creating awareness programs, conducting security risk assessments, providing consulting services, and guiding security technology selection on a worldwide basis.

Mr. Cutler has over 25 years of experience in information security, auditing, quality assurance, and information services. His industry experience includes insurance and financial services, natural resources, manufacturing, government contracting, consulting and training.

An internationally recognized expert in the information security and audit fields, Mr. Cutler is the primary author of the widely acclaimed Commercial International Security Requirements (CISR), which offers a commercial alternative to military security standards for system design. He has also published works on network security, security architecture, wireless networks, and single sign-on. Mr. Cutler has been an active participant in international government and industry security standards initiatives, including the President's Commission on Critical Infrastructure Protection, Generally Accepted System Security Principles (GSSP), Information Technology Security Evaluation Criteria (ITSEC), and the US Federal Criteria. He previously served on the Member Advisory Council for the International Information Integrity Institute (I-4) and is currently serving as an Advisory Member of the ISSA Board of Directors.

A much-in-demand speaker and consultant, Mr. Cutler frequently lectures and provides hands-on consulting services in the areas of information security management and architecture, network vulnerability testing, Unix and Windows-based systems, Internet/Web security, dial-up/remote access security, wireless security, and local area network security. He has lectured at many major industry and regional professional association events, including US and international COMDEX shows in 1997-2002.

Mr. Cutler is frequently quoted in popular trade publications such as *Computerworld*, *Information Security, CIO Bulletin, Healthcare Information Security Newsletter, InfoWorld, InformationWeek, HP Professional*, and *Bank Systems and Technology*. He also served as technical advisor on the Editorial Advisory Board of *SC Magazine*. Mr. Cutler was featured on *Crime Talk*, broadcast on the Talk America Radio Network.