CERT® Conference 2002

Computer Security and Information Assurance

August 6 - 9, 2002

Scott Conference Center
Omaha, Nebraska, USA

Presented by

NEbraskaCERT

Tuesday	8:00 - 8:45	8:45 - 10:00	10:15 - 11:30	11:30 - 12:30
Technical	REGISTRATION & CONTINENTAL BREAKFAST	TT-1: Security Realities	TT-2: Script Kiddees - Windows	LUNCH
Expert		TE-1: Samba Secured - I	TE-2: Samba Secured - II	
Management		TM-1: Risk Management	TM-2: Internet Anonymity	
Wireless		TW-1: Wireless Security Architecture - I	TW-2: Wireless Security Architecture - II	

Wednesday	8:00 - 8:45	8:45 - 10:00	10:15 - 11:30	11:30 - 12:30
Technical	REGISTRATION & CONTINENTAL BREAKFAST	WT-1: Protecting Apache	WT-2: ADSL Security for Business	LUNCH
Expert		WE-1: WWW Hacking - I	WE-2: WWW Hacking - II	
Management		WM-1: Incident Management	WM-2: Beyond the Firewall	
Wireless		WW-1: Wireless & IPSec	WW-2: Wireless Snooping	

Thursday	8:00 - 8:45	8:45 - 10:00	10:15 - 11:30	11:30 - 12:30
Technical	REGISTRATION & CONTINENTAL BREAKFAST	HT-1: Critical Infrastructure Protection	HT-2: Cyberspace Autopsy	LUNCH
Expert		HE-1: IDS Log Analysis - I	HE-2: IDS Log Analysis - II	
Management		HM-1: Writing Security Policies	HM-2: World Class Security	
Wireless		HW-1: Wireless Security Demo - I	HW-2: Wireless Security Demo - II	

Friday	8:00 - 8:45	8:30 - 12:00	12:00 - 1:30
Tutorial	REGISTRATION & CONTINENTAL BREAKFAST	FT-1A: Checkpoint NG Firewall Essentials - I	LUNCH
Tutorial		FT-2A: Secure Wireless Networks	
Tutorial		FT-3A: Disaster Preparedness	
Tutorial		FT-4A: Viewing Cyber Survivability from Expanded Perspectives	

12:30 - 1:30	1:45 - 3:00	3:15 - 4:30
Keynote Speaker: Rob Rosenberger	TT-3: Common Internet Attacks	TT-4: Internal Security
	TE-3: SNMPv3	TE-4: Cisco SNMPv3 & Security
	TM-3: HIPAA Overview	TM-4: Security Policies
	TW-3: Hands-On Wireless Lab - I	TW-4: Hands-On Wireless Lab - II

12:30 - 1:30	1:45 - 3:00	3:15 - 4:30
Keynote Speaker: Elias Levy	WT-3: ISO 17799 Description	WT-4: VoIP through VPN
	WE-3: Secure Programming - I	WE-4: Secure Programming - II
	WM-3: Vulnerability Disclosure	WM-4: Insider Security
	WW-3: Wireless Internet Threats	WW-4: Wireless Security

12:30 - 1:30	1:45 - 3:00	3:15 - 4:30
Keynote Speaker: Joel Scambray	HT-3: Directory Security	HT-4: General Unix Security
	HE-3: AI IDS Techniques	HE-4: IDS for ISPs
	HM-3: Passwords Weak Link	HM-4: Incident Response Teams
	HW-3: HIPAA, GLB & Wireless	HW-4: Security Risks

1:30 - 5:00
FT-1B: Checkpoint NG Firewall Essentials - II
FT-2B: IDS System Usage
FT-3B: Incident Response Teams
FT-4B: Wireless Lab and Demonstration

AT A GLANCE

About CERT Conference 2002

Who's Listening?

Wireless communications offer great flexibility in a market that demands instant communications. But who is listening in on your conversations?

The government, sure.
Competitors, probably.
Terrorists, unlikely but *very* possible.

Make sure to shore up your wireless implementation by attending our featured track at CERT Conference 2002. We'll explore wireless architecture, threats, legalities and much more.

Make sure no one is listening in on you!

CERT Conference is presented by NEbraskaCERT, which is comprised of volunteers dedicated to information security awareness and sharing, presents the 4th annual Computer Security and Information Assurance conference in Omaha, Nebraska.

This year we offer 3 days of general sessions and activities with four consecutive tracks -- Technical, Expert, Management, and a special track dedicated to Wireless -- that explore many issues facing individuals, businesses, industry, and government. We explore new regulations, ethics, and cutting-edge technology, as well as provide a solid foundation for those new to the information security world. New this year is an additional optional day of hands-on tutorials where presenters provide practical, hands-on information to attendees.

CISSP / SSCP Exams August 5, 2002

As an additional attraction, NEbraskaCERT is hosting the CISSP and SSCP certification exams one day prior to the conference. Anyone who sits and passes one of these exams and attends the conference will be eligible to claim CPE credits toward maintaining their certification.

CISSP

The CISSP certification identifies you as a security professional who has met a certain standard of knowledge and experience and who continues to keep his/her knowledge current and relevant to what is happening in the practice of Information Security. CISSPs must have a minimum of three years experience in one or more of the ten Common Body of Knowledge (CBK) domains. The CISSP program certifies IT professionals who are responsible for developing the information security policies, standards, and procedures and managing their implementation across an organization.

SSCP

The SSCP certification identifies you as a security practitioner who has met a certain standard of knowledge and experience and who continues to keep his/her knowledge current and relevant to what is happening in the practice of Information Security. SSCPs must have a minimum of one year experience in one or more of the seven CBK domains. The certification is targeted at network and systems security administrators, who provide day-to-day support of the network and security infrastructure.

Registration for these Exams

These exams are conducted by $(ISC)^2$.
To register, you must do so separately from any registration for CERT Conference 2002.
Registration information is available at www.isc2.org.

REASONS TO ATTEND

Networking Opportunities

Past attendees cite networking opportunities as the number one benefit and reason to attend this conference! Sure, there's plenty of quality speakers and sessions, but the real value comes from sharing experiences and learning from others interested and concerned with security. The schedule is set up to ensure you'll have plenty of time to meet others and make long-lasting and helpful contacts at breakfasts, lunches and breaks, giving you the opportunity to learn from other attendees, not just the speakers.

Pick Your Sessions

CERT Conference 2002 has arranged its sessions into four tracks; Technical, Expert, Management, and Wireless, to give you an idea what type of session to expect before you walk in the room. However, you're not locked into a track. Feel free to mix and match the sessions you think interest you the most, regardless what track they've been categorized into.

Security Information & Solutions You Can Use

Speakers with real-world experience will discuss solutions you can take back with you and implement. Our sessions have been selected to provide you with the opportunity to achieve just the right balance between technical and management issues.

Take advantage of available Discounts

CERT Conference has revised its discount process for this year's conference, creating additional discount opportunities. Anyone who has attended a previous CERT Conference sponsored by NEbraskaCERT, is a Full-time Student, works for the Government **or** holds their CISSP certification is eligible to take advantage of a $50 discount off a full conference registration. In addition, NEbraskaCERT members are eligible to take advantage of an additional $50 discount off full conference registrations. See page 17 for more information.

Wake up to Continental Breakfast

Continental Breakfast is provided each day you attend.

Lunch is on us!

Full course lunch buffet is included in the conference fee and provided for each day you attend.

CONTENTS:

KEYNOTE SPEAKERS

Elias Levy

Co-founder and Chief Technical Officer, SecurityFocus.com
Elias Levy is Chief Technical Officer and a co-founder of SecurityFocus, responsible for overall site operations. Mr. Levy is a well respected and sought after computer security spokesperson and visionary. He has been in countless publication, television and radio shows with the press. Elias has hands-on, insider and an analyst's expertise in the security business. He learned security working for several large US corporations as a security administrator and as a consultant. He also has insider experience from his working with the security community as the former moderator and keeper of the Bugtraq vulnerability database and mailing list. Elias' seven years of experience with Bugtraq, first as a contributor and then as the moderator, gave him a daily pulse on the strengths and weaknesses in Information Security.

Last year, Elias Levy was chosen as one of Network Computing's "10 Most Important People of the Decade." The much respected publication noted that "Levy has helped educate hundreds of thousands of system administrators, network engineers and developers across the planet, while miraculously remaining free from vendor and political bias."

Rob Rosenberger

Editor, Vmyths.com
Mr. Rob Rosenberger edits Vmyths.com as a full-time job and writes as a columnist. He is one of the "original" virus experts from the 1980s, and the first to focus on virus hysteria. Red Herring magazine describes him as "one of the most visible and cursed critics in computer security" today, and PC World magazine says he "is merciless with self-appointed virus experts and the credulous publication that quote them." Rosenberger was one of only a dozen industry experts invited to the White House's first-ever antivirus summit meetings.

Rosenberger's credentials include a critically acclaimed 1988 treatise on computer virus myths which appeared in over 230 books & publications around the world in four official translations. [Plus at least two unauthorized translations: Hebrew & Arabic versions surfaced during "Operation Desert Storm."] U.S. Defense Department point papers cite Rosenberger's treatise on virus myths as a bibliographic source.

Joel Scambray

Co-author of Hacking Exposed: Network Security Secrets and Solutions,
the international best-selling Internet security book that reached its Third Edition in October 2001. He is also lead author of Hacking Exposed Windows 2000, the definitive analysis of Microsoft's flagship product security.
Joel's past publications have included his co-founding role at InfoWorld's Security Watch column, InfoWorld Test Center Analyst, and inaugural author of Microsoft's TechNet "Ask Us About...Security" forum.

Joel's writing draws primarily on his years of experience as an IT security consultant for clients ranging from members of the Fortune 50 to newly minted startups, where he has gained extensive, field-tested knowledge of information system security. Joel's consulting background also encompasses an unparalleled record of successfully managed projects (including several multiyear, multinational engagements), development and leadership of a Product Security Review service line accounting for substantial annual revenues, and ongoing thought leadership in the design and analysis of security architectures. He has participated in many network and product security reviews contracted by Microsoft Corp., including audits of ISA Server and the .NET Framework. Joel also maintains his own test laboratory, where he continues to research the frontiers of information system security.

Joel speaks widely on Windows 2000 security for organizations including The Computer Security Institute and many large corporations, and he also maintains and teaches Foundstone's Ultimate Hacking: Windows hands-on training course.

Joel is currently Managing Principal with Foundstone Inc., and previously held positions as a Manager for Ernst & Young, Senior Test Center Analyst for InfoWorld, and Director of IT for a major commercial real estate firm. Joel's academic background includes advanced degrees from the University of California at Davis and Los Angeles (UCLA), and he is a Certified Information Systems Security Professional (CISSP).

TUTORIALS

FT-1A, FT-1B:
Check Point NG Firewall Essentials, Parts I & II
Barry Cooper, Training Director, FishNet Security
Learn the ins and outs of VPN-1/FireWall-1 NG in a fast-paced, one day session. Topics will include, installation, configuration, SIC architecture, system architecture, firewall management, policy, and more! Stateful Inspection, NAT, VPN, Authentication, and the new NG Policy Editor will be covered in-depth.

FT-2A:
Secure Wireless Networks
Matthew Marsh, Paktronix Systems and Steve Nugen, NuGenSoft
Wireless networks are little different from any other network structure in terms of the need for management. However they provide a greater challenge given the potential scope of protection. In this tutorial we will see how the standard methods of network management and security can be used within the challenges of the wireless network.

FT-2B:
IDS System Usage
IP Revolution
This session will identify methods of addressing security issues at a level required by ISPs and other major network infrastructures. Specific examples of implementations will be provided.

FT-3A:
Disaster Preparedness
Harry Bouris
The goal of the workshop is to provide the student with the requisite knowledge and tools to develop a viable disaster preparedness plan. The workshop will focus on the relationship between a business continuity plan and a disaster recovery plan and identify the components of a disaster recovery plan. A practical framework developing and implementing a viable disaster recovery plan will be provided through a short information briefing, workshop discussions, and practical exercise. Students will leave the workshop with a practical example of a disaster recovery plan and associated emergency action plan attachments.

FT-3B:
Incident Response Teams
Marty Gillespie
Incident Response provides an introduction to the various phases of planning, developing and implementing an Incident Response Team. The presentation will cover pre-incident planning to post-incident analysis. The presentation will do so by providing a methodology consisting of 6 phases: preparation, identification, containment, eradication, recovery and lessons learned.

FT-4A:
Viewing Cyber Survivability from Expanded Perspectives
CERT/CC
The Internet was originally developed as a means of survivable communication for a nuclear holocaust. Is this still the valid mechanism for communications delivery within today's networking environments. In this session CERT/CC will explore the way in which networks have evolved to meet the new consumer and business mandates.

FT-4B:
Wireless Lab and Demonstration
NUCIA
This session will provide real world examples of wireless security as researched by UNO's College of Information Science and Technology students.

TT-1:
Security Realities - Interface Between the Cyber and Physical Worlds

CERT/CC

This session will be presented by an individual from the CERT Coordination Center, Carnegie Mellon University. Providing information critical to understanding the link between the physical and cyber worlds of security.

TT-2:
Script Kiddees - Windows

Eric Hjelmstad, PoliVec, Inc.

Scriptkiddees are looking for a victim and you don't want to be on their list. Learn about common Windows NT and 2000 exploits and their fixes. An actual penetration on a live system will be demonstrated, providing you with the tools and understanding to perform your own penetration tests.

TT-3:
Common Internet Attacks

NEbraskaCERT

In this session, we will continue the coverage of scriptkiddees and talk about common Internet attack themes. We will look at how standard Firewall and DMZ scenarios lend themselves to certain types of attack and what you can do to mitigate the risk.

TT-4:
Internal Security

Dr. Guy Helmer, Palisade Systems

With over 85% of large companies and government agencies reporting computer breaches in the past year (most being internal breaches), the need for internal security solutions has been a growing focus of organizations. Perimeter security is no longer enough--a huge security hole remains with internal access at the network level. Without an extra layer of security beyond application-layer protections to shield important servers, people are virtually free within the network to explore or hack these assets. Today, multiple levels of security are necessary to improve effectiveness and provide contingency. Existing products such as firewalls, switching/routing components, and intrusion detection systems can be force fit in an attempt to address unrestricted network level access, but they suffer severe functional limitations that render them impractical for most implementations. This presentation will cover all aspects of protecting against inside attack.

WT-1:
Protecting Apache

Dave Burgess, UNO, MITRE Corporation, Nebraska On-Ramp

In this session you will see how to configure and use an Apache webserver for enhanced security. The trade-off between usability and high security will be illustrated and common external security measures will be discussed.

WT-2:
ADSL Security for Business

Dave Burgess, UNO, MITRE Corporation, Nebraska On-Ramp

What is ADSL and how can a business use it effectively and securely? The myths surrounding ADSL features and security will be unwrapped and the true feature set and secure usage of ADSL within the business environment will be explored. Practical examples of common uses will be illustrated including VPN and remote branch connections.

WT-3:
ISO 17799

Chet Uber, SecurityPosture

ISO 17799 is the most widely recognized security standard. It is based upon BS7799, which was last published in May 1999, an edition which itself included many enhancements and improvements on previous versions. The first version of ISO 17799 was published in December 2000. ISO 17799 is comprehensive in its coverage of security issues. It contains a substantial number of control requirements, some extremely complex. Compliance with ISO 17799, or indeed any detailed security standard, is therefore a far from trivial task, even for the most security conscious of organizations. Certification can be even more daunting. It is recommended therefore that ISO 17799 is approached step by step. The best starting point is often an assessment of the current position, followed by identification of what changes are needed for ISO 17799. From here, planning and implementation must be undertaken.

WT-4:
VoIP through VPN

Simeon Corey, Asita

This presentation will provide an introduction to VPNs, outlining what is a data VPN, reasons for implementation, scenarios & solutions, and commonality of data and voice VPNs. How VPNs can help VoIP deployment will be considered and key issues concerning implementation of a VPN will be outlined.

TECHNICAL TRACK

HT-1:
Critical Infrastructure Protection
CERT/CC

This presentation, provided by an individual from the CERT Coordination Center, Carnegie Mellon University, will focus on the protection of our nation's critical infrastructure. What is critical infrastructure? What has been done to protect it? What new legislation are we facing to enforce protection? How great is our weakness? The answers to these questions and more are expected in this presentation.

HT-2:
Cyberspace Autopsy
Douglas G. Conorich, IBM Global Services

In today's network-centric world, where technology and business are converging, any disruption to the flow of information can be devastating. If someone were to breach the security of your system today, would you be ready? Are you prepared to track these perpetrators to find out what they accomplished during this breach? What will you do now that you have the evidence? This session will discuss computer forensics showing step-by-step how a break-in can be discovered and how the hacker can be tracked through the system. We will discuss some tricks hackers use to prevent discovery and what you can do to thwart them, along with how a company can handle incident management including some of the legal considerations a company must consider when investigating an incident.

HT-3:
Directory Security
Alan Mark, Novell, Inc.

When directories were first implemented, their main role was maintaining basic identities. Access was required to many different systems, and a central directory could have been utilized to maintain users and their access lists. However, even a decade later, many systems and applications are not "directory enabled." And to make matters worse, most organizations (usually due to internal politics) created multiple directories, even though they didn't exchange data with one another. Using open standards such as XML, it's possible for these disparate directories and applications to communicate with one another. This presentation covers how a directory service provides an integrated solution for managing identities, policies, and security controls.

HT-4:
General Unix Security
T. Steven Barker, Raytheon Company

This presentation is designed to introduce the UNIX operating system features and describe mechanisms and features which help create a more secure computing environment. Upon conclusion of this presentation, attendees will have a basic understanding of UNIX operating system features that can be used to enhance security and those features of the UNIX operating system that pose potential system vulnerabilities.

TE-1, TE-2:
Samba Secured, Parts I & II

D. F. Roberts, University of Otago New Zealand

The purpose of this presentation is to illustrate the option of using Linux servers instead of Windows servers on LANs. This topic is approached from the network and security perspective. There are many well-known security issues with Windows NT 4 that can make it unacceptable as a domain controller for a local area network. Linux has fewer security issues which provides both a better perception and that assist in securing the server space. This work will look at combining the strengths of Linux servers with the commonplace Windows desktop. In this session we will address issues of setting up a Linux server to act as a domain controller for Windows desktops using Samba. We then will address the design of Linux file system security and how it can be adapted to make it more secure than NTFS. Finally, we will discuss currently available enhanced security techniques, such as SSL connectivity, that are available to Unix desktops connecting to the server.

TE-3:
SNMPv3

W. Hardaker

In this session we will show the full spectrum and strength of SNMPv3 using the code base of the most popular SNMP utility suite available. We will discuss the separation of Authentication and Privacy as performed within v3 and illustrate using multiple authPriv passphrase structures. We then cover how the v2 notion of Views and Scoping can be applied to further limit and segment the information. Finally we show how the various security enhancements do not allow an attacker with physical access to the managed machine to know or subvert the authentication and privacy schemas.

TE-4:
Cisco SNMPv3 & Security

S. Morris

In this session the application and use of SNMPv3 and other security measures such as SSH connectivity are applied to Cisco equipment. In this discussion we will look at the various types and uses of Cisco equipment within organizations and show the methods and uses of the security features provided. We will concentrate on the use of SNMPv3 and SSH in securing and monitoring equipment in high security situations.

WE-1, WE-2:
WWW Hacking, Parts I & II

Yaron Galant, Sanctum, Inc.

As the saying goes, if you don't learn from your past mistakes, you are doomed to repeat them again in the future. An important step in beginning to smartly address security is to take stock of what is going on and begin to understand where problems may exist. This is most accurately done through the use of network and application level forensics. While network hacks aim at the TCP/IP level, and usually require deep understanding of its behavior (e.g. buffer overflows, syn/fin floods, etc.) one simple request to the web server might grant the attacker the ability to run shell commands without any interference (e.g. Microsoft IIS Unicode vulnerability). Monitoring network traffic, installing tripwire and honeypots, and monitoring logs are all good network security practices. However, most IT professionals have little practice with actual traffic over the WWW. In this two part session we will cover what various attacks are prevalent on the WWW. Then we will delve down into the methods and techniques for reading and analyzing web data streams. This presentation uses detailed code examples to demonstrate techniques for manually identifying website attacks, including simple, complex and HTTP attacks.

WE-3, WE-4:
Secure Programming, Parts I & II

Brian Smith, Solutionary, Inc.

In this double session, the structure and tips for pursuing secure programming will be explored and illustrated. In the first session the basics will be covered. These include the nature of buffer overflows, the use of systems command escapes, and the formatting of I/O. In the second session we will explore deeper into the use of automated and manual tools for checking and assisting with the discovery of security problems before the code is released. Additionally the use of testing and QA methodologies to test code after it has been compiled will

be illustrated. You will leave these sessions understanding how to develop your own methodology for creating secure code and with a better understanding of how to look for security problems in both source and binary code bases.

HE-1, HE-2:
IDS Log Analysis, Parts I & II

Marcus J. Ranum

This session will cover designing generalized rules-based log coalescing software which provides reliable and rapid basic log processing. This software is useful as a standalone tool for analyzing a variety of logs, as well as a useful post-facto analysis and processing system for stored logs that you may have archived. In this session we will cover the design reasons and the construction of the formatting language for the transformation of various log formats into a single tagged output stream.

HE-3:
AI IDS Techniques

Stephen Nugen, NuGenSoft

This topic will discuss and explore means and possibilities for incorporating different AI (Artificial Intelligence) techniques into adaptive strategies and tools for:
-Learning to recognize intrusions through AI-based simulations and training exercises,
-Recognizing new intrusions, not yet described by existing rulesets,
-Adaptively reconfiguring defended systems to limit the scope of the intrusion,

No special knowledge of AI is assumed, but the discussion assumes general expertise in Information Security.

HE-4:
IDS for ISPs

IP Revolution

The need for Intrusion Detection for ISPs is a necessary, but difficult problem. With such a great amount of traffic and bandwidth, it is difficult to effectively address Intrusion Detection needs. This session will talk about ways of accomplishing Intrusion Detection at the ISP level and how it can help ensure a more secure Internet environment.

TM-1:
RSK-Risk Management
Andrew T. Robinson, NMI Information Security

RSK is a process for measuring information security risk, and is intended as a tool to supplement existing security testing methodologies. Security testing has become a standard of care for organizations connected to the Internet, and is even required by law for regulated industries such as banking and financial services. While a security test is an excellent tool for identifying vulnerabilities, it is difficult to compare the results of two security tests, whether they are taken of the same testing domain over time, or of two different testing domains. RSK is designed to enable these comparisons.

TM-2:
Internet Anonymity
Aaron Grothe

The purpose of this talk is to discuss the possibility of reducing the ability of people to track your movements on the Internet as well as reducing the amount of information you are providing. As part of the presentation a description of some of the current services and tools that may be used to achieve these goals. It will also provide a small tutorial describing how a user can reduce their footprint while using the Internet.

TM-3:
HIPAA Overview
Bridges

This session will provide an overview of the requirements that are expected to be mandated by HIPAA laws. This presentation will be especially useful to individuals in the Health Care industry or individuals interested to know if HIPAA applies to them.

TM-4:
Security Policies
Dr. Bruce V. Hartley, PoliVec, Inc.

The foundation of a successful information security program is a strong security policy. Without one, your company's systems are more vulnerable to attack, both internally and externally. Creating a policy that supports your company's goals is critical to the success of the document. The initial policy must also be continually reviewed, updated, and communicated to ensure it addresses your changing business needs and/or regulatory requirements, such as the Gramm-Leach-Bliley Act and HIPAA. An equally important part of an effective security policy is the development of implementation standards, which are designed to translate the policy into operating system-specific configuration guidelines. These guidelines ensure that IT professionals can easily implement the policy for each operating system on the network.

WM-1:
Incident Management
Douglas G. Conorich, IBM Global Services

In this presentation, Mr. Conorich will discuss how a company can handle incident management. The presentation will cover types of incidents, the value of written policies and procedures, the phases of an incident, legal considerations, and evidence collection. He will touch on some of the legal considerations (an outline of some of the major computer related issues) a company must consider when investigating an incident. Mr. Conorich will present some tips and hints of evidence collection that will aid you during incident management. This will include what to collect, chain of evidence, and custody issues.

WM-2:
Beyond the Firewall
Ulf Mattsson, Protegrity

In spite of the efforts of many corporations to implement information security, the incidents of successful network intrusions where data has been compromised are on the rise. Part of the problem lies in the fact that most companies solely implement perimeter-based security solutions, even though the greatest threats are from internal sources. Additionally, companies implement network-based security solutions that are designed to protect network resources, despite the fact that the information is more often the target of the attack. Yet nothing is being done to protect the information. Recent developments in information-based security solutions address a defense-in-depth strategy and is independent of the platform or the database that it protects.

WM-3:
Vulnerability Disclosure
Elias Levy

When new vulnerabilities are discovered, should they immediately be broadcasted to the world to allow IT professionals to adequately protect their information systems, or are we giving the bad guys all the information they need to further the exploitation of the vulnerability? In this session, one of this year's keynote speakers discusses the pros and cons of vulnerability disclosure and talks about the best way to handle new vulnerability discoveries.

WM-4:
Insider Security
Dr. Bruce V. Hartley, PoliVec, Inc.

Most companies recognize the need for network security and continually focus on maintaining adequate protection. Many have

taken the steps necessary to safeguard their systems from external attacks. Often, however, these same companies overlook internal security despite the fact that a significant percentage of computer abuse stems from internal problems. Because an insider already has physical and logical access to the system, an understanding of what data is sensitive, and possibly an understanding of the security controls, the potential for misuse is very high. This oversight can unnecessarily expose a company to not only internal threats, but also successful penetration when internal attacks occur. Additionally, many available security mechanisms, such as minimum password lengths, password histories, and security auditing, are not used. These vulnerabilities are easily preventable when strong internal security is maintained. This session will address the importance of protecting your organization from internal attacks, as well as provide information on how to improve your internal security.

HM-1:
Writing Security Policies
Douglas G. Conorich, IBM Global Services

In the past business managers have regarded computer security as something that doesn't have to concern them. However, recent events such as the continuous attack by viruses, network worm invasions and high school pranksters have increased their awareness and concern. A good security policy contains guidelines that address these protection issues.

HM-2:
World Class Security
Walter S. Kobus, Jr., Security Consulting Services

In this presentation, Mr. Kobus will discuss developing a World-Class Security Management Program. He will cover how to assess risk and determine needs, how to establish a centrally managed focal point, the necessity to implement appropriate policies and related controls, how to promote awareness, and how to monitor and evaluate policy and control effectiveness. Additionally, he will look at nine organizations you can use to benchmark your effectiveness.

HM-3:
Passwords Weak Link
Erik Hjelmstad, PoliVec, Inc.

Breaking computer security is essentially a search for the weakest link and poor password choices are often that link. One of the easiest ways for attackers to enter your network is by guessing a weak password. Weak passwords include default passwords, dictionary words, basic personal information (such as the name of your spouse, child, or pet), common local terms, and anything that is written down and left near your computer. Statistics show that in most computer networks, 35 to 80 percent of passwords can be easily guessed.

HM-4:
Incident Response Teams
Gillespie

This session will provide an introduction to the various phases of planning, developing and implementing an Incident Response Team. The presentation will cover pre-incident planning to post-incident analysis. The presentation will do so by providing a methodology consisting of 6 phases: preparation, identification, containment, eradication, recovery and lessons learned. This session is also being presented in an expanded 3 hour tutorial on Friday.

TW-1, TW-2:
Wireless Security Architecture, Parts I & II
Janus

Wireless technology can enable businesses to provide ubiquitous and flexible network access for critical applications that require increased levels of user mobility. This computing freedom may provide for increased operational efficiency and functionality, however wireless technology does introduce a magnitude of critical security risks, and many feel that achieving wireless security is an insurmountable task. As a result, businesses have been reluctant to implement wireless technology, and for most that have taken the leap into wireless have done so insecurely. You will walk away from this presentation armed with the knowledge that wireless security can be achieved, and will understand the fundamentals of wireless technology, wireless security threats, and wireless security methods. In addition, you will learn the critical processes for successfully performing wireless audits.

TW-3, TW-4:
Hands-On Wireless Lab, Parts I & II
OLUG

In this session participants will learn first hand how to setup and run a wireless network. We will take the Conference wireless network and show how it has been created and the various levels of security and dangers that are present. After this session participants will see how a wireless network operates and understand the common targets of attack on a wireless network.

WW-1:
Wireless & IPSec
Matthew Marsh, Paktronix Systems

Given the ease with which WEP is broken there is a need to authenticate and privatize the communication over a wireless network. In this session we will examine the opportune merger between the IP Security Protocol Suite (IPSec) and wireless IP networking. Most of the session will be focused on use within the IPv4 spectrum and as time permits we will discuss the use of IPv6 within wireless networks.

WW-2:
Wireless Snooping
Brian Roberson, President/Founder, Omaha Linux User Group

In this session you will see how to snoop on a wireless network. We will illustrate the use of WEPcrack and AIRSnort as tools for external analysis. We will also look into the use of standard mapping and penetration tools such as NESSUS in the mapping and scanning of wireless networks.

WW-3:
Wireless Internet Threats
TBD

This session will provide general information necessary when considering wireless networks in your home or office environment. Individuals interested in how wireless networks work, and how to secure them should attend.

WW-4:
Wireless Security
Ashok Fichadia, Union Pacific Railroad

As companies and users move to the 802.11 wireless networks, new security exposures and privacy issues have come to the fore. Existing wired networks require that intruders have physical access to the network to compromise security - wireless networks do away with this restriction. Consequently, intruders have been able to successfully engage in "drive-by hacking" and compromise network security by merely driving by wireless installations and capturing traffic via homemade "Pringles" cans antennas. This presentation will highlight various security exposures and controls required to securely implement wireless networks. The presentation will include a discussion of basic access control and encryption methods available in today's wireless systems, their flaws and applicability for businesses, and some proposed solutions to ensure secure and scalable implementation of wireless networks.

HW-1, HW-2:

Wireless Security Demo, Parts I & II

James Nelson

In this session we take the wireless network setup for the Conference on Tuesday and participants will learn first hand how to scan and crack a wireless network. We then illustrate the various methods for enhancing the authentication and privacy structure of the network. After this session participants will see how a wireless network operates and understand the common targets of attack and the best methods of defense on a wireless network.

HW-3

HIPAA, GLB & Wireless

Ross

Now that you know how to install, maintain, manage, and secure a wireless network - how does it fit into the regulatory landscape? In this session we explore the unique structures of a wireless network as they pertain to several USA legal arenas like HIPAA and GLB.

HW-4:

Security Risks

Jeff Guilfoyle, VP e-Security, Solutionary, Inc.

There are many issues and challenges facing the deployment of wireless networks today. We will explore the different types of configuring wireless networking, and the challenges of securing them. From the technical issues with the encryption algorithms used in the hardware to the insecurities of default installations, each major weakness will be addressed, and solutions to the problems will be presented.

PLATINUM SPONSORS

Carnegie Mellon Software Engineering Institute CERT® Coordination Center

NEbraskaCERT

Paktronix Systems
Network Security Solutions

CONTRIBUTING SPONSORS

FISHNET SECURITY.COM

BAE SYSTEMS

NuGenSoft

Sumaria

Solutionary
reliable, responsible e-security

First Technology Solutions

About Omaha, Nebraska

Omaha is a dynamic metropolitan area of 700,000 with over 18,000 businesses. Omaha has long been known as a destination where visitors can have fun and not have to worry about budget constraints. Some of the Midwest's finest visitor attractions are located here. This is a city with a rich past, vibrant present and exciting future. There is always something to see or do in Omaha. The community has a wide array of parks, museums, historical sites and entertainment areas that are open year-round. A number of activities are free or cost only a few dollars. Many of these attractions are unique to the Omaha area.

continued..

About Omaha ..continued

Omaha is the corporate headquarters and main residential campus of Boys Town, which continues to provide care to hundreds of children and is open to the public. The Henry Doorly Zoo has won numerous awards and is one of the region's most popular attractions. This world-class zoo sits on 130 acres and is home to over 600 species and more than 18,600 specimens. Among the numerous exhibits are the world's largest indoor rainforest, an aquarium complex that includes a walk-through tunnel, the second largest free-flight aviary, and the newly opened Desert Dome, where three diverse desert environments have been re-created under the world's largest glazed geodesic dome.

The Omaha metropolitan area is also an active and diverse arts and entertainment base for the region, attracting artists from around the world. There is a professional symphony and opera company, as well as dozens of theaters and performing arts venues. The arts community welcomes everyone to participate in cultural activities.

Omaha Area Attractions:

The Old Market / Downtown
Henry Doorly Zoo; Desert Dome, Aquarium, Indoor Rainforest & IMAX 3D
Joslyn Art Museum
Strategic Air Command Museum
General Crook House
Mallory Kountze Planetarium
Riverboat Casinos
Heartland of America Park and Fountain
Omaha's Rosenblatt Stadium, Home of the College World Series
Durham Western Heritage Museum
Boys Town USA
Gerald Ford Birthsite
Omaha Botanical Gardens
River City Star

Airline and Hotel Information

Airline Travel to Omaha

Save up to 10% on airline travel by booking your flight with Midwest Express, the official airline carrier for CERT Conference 2002.
For more information or to book your flight, visit: http://www.midwestexpress.com/conventions

Hotels

The following hotels are located in close proximity to the Scott Conference Center:

Doubletree Guest Suites (402) 397-5141
7270 Cedar Street
Omaha, NE 68124

Quality Inn (402) 397-7137
2808 S. 72nd Street
Omaha, NE 68124

Super 8 (402) 390-0700
7111 Spring Street
Omaha, NE 68106

Hampton Inn (402) 391-8129
3301 S. 72nd Street
Omaha, NE 68124

Homewood Suites (402) 397-7500
7010 Hascall Street
Omaha, NE 68106

Holiday Inn (402) 393-3950
3321 S. 72nd Street
Omaha, NE 68106

Clarion (402) 397-3700
3650 S. 72nd Street
Omaha, NE 68124

Travelodge (402) 391-5757
7101 Grover Street
Omaha, NE 68106

Red Lion (402) 397-7030
7007 Grover Street
Omaha, NE 68106

REGISTRATION INFORMATION

Registration Fees:

Early Bird **Full** Conference Registration (through July 18, 2001) = **$695**
Full Conference Registration (after July 20, 2001) = **$795**
Conference *Sessions* (August 6-8) Only = **$695**
Conference *Tutorial* (August 9) Only = **$150**

Discounts:

NEbraskaCERT Member Discount = **$50***
Alumni / Full-time Student / Government / CISSP Discount = **$50****

* *Discount available for full conference registrations only. See www.NEbraskaCERT.org for more information.*
** *Alumni discount available to registrants who attended past CERT Conferences presented by NEbraskaCERT. To qualify for Full-time Student, Government, or CISSP discount, attendee must show valid ID during Conference Check-in. These discounts are only available on full conference registrations AND each registrant may claim only 1 (one) of the discounts in this category for a maximum of $50.*

Conference Fees Include:

- Attendance to Sessions, Tutorials, and Panels for each day of registration
- Full Lunch
- Continental Breakfast and Afternoon Refreshments
- Printed Materials for sessions you attend*
- Access to electronic copy of presentation materials**

Conference Schedule subject to change due to availability of speakers and presentation materials.

* When available, presentation materials will be available to attendees at the beginning of each session. A limited quantity of copies will be available, therefore availability will be on a first come, first served basis.
** Updated presentation materials will be available on the conference website as soon as presenters provide make them available to conference staff. Not all presenters provide their presentations for publication.

*** ATTENDANCE IS LIMITED TO FIRST 200 PAID REGISTRATIONS - REGISTER TODAY! ***

Register by Mail:

CERT Conference
P.O. Box 825
Bellevue, NE 68005-0825

Register on the Web at:

http://www.certconf.org/register

Fax Registration form to:

(402) 397-5537

Cancellation Policy:

All cancellations must be made in writing and sent by mail using the address or fax # listed. All written cancellations must be received by July 18, 2002 and a $25 administrative fee will apply. All refunds will be processed within 30 days following the conference. If you cannot attend, you may transfer your registration to another employee within your company, provided notification of such change is made as early as possible.

REGISTRATION FORM

Name: _____

LAST *FIRST* *MI.*

Title: _____

Company: _____

Address: _____

STREET ADDRESS / P.O. BOX *MAIL STOP / FLOOR*

_____

CITY *STATE* *ZIP / POSTAL CODE*

Phone: _____ **Fax:** _____

E-mail: _____

I would like my name to be included on the CERT Conference mailing list, YES____ or NO____

Payment Information:

Early Bird Full Conference Registration *(through July 18, 2002)*:	$695	$_____
Full Conference Registration *(after July 18, 2001)*:	$795	$_____
Conference *Sessions* (August 6-8, 2002) Only:	$695	$_____
Conference *Tutorial* (August 9, 2002) Only:	$150	$_____
NEbraskaCERT Member Discount	-$50*	$_____
Alumni / Full-time Student / Government / CISSP Discount	-$50**	$_____
	TOTAL:	$_____

**See Registration Information Page for qualification requirements and restrictions*

CISSP Certification Number: _____, to be used to submit CPE credits to $(ISC)^2$

Payment Method:

_____Check, *enclosed payable to CERT Conference*

_____Purchase Order, *P.O. Number:* _____

_____Credit Card - Type: AMEX:____ VISA:____ Mastercard:____ Discover:____

Credit Card Number:_____Expiration Date: _____

Card Verification Value (last three digits of the number located on the signature strip):_____

Cardholder's Name:_____

Cardholder's Address:_____Zip Code: _____

Cardholder's Signature: _____

See Registration Information Page for Cancellation Policy