FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1321038-0

Total Deleted Page(s) = 8
Page 30 ~ b6; b7C; b7E;
Page 31 ~ b6; b7C; b7E;
Page 32 ~ b6; b7C; b7E;
Page 33 ~ b6; b7C; b7E;
Page 34 ~ b6; b7C; b7E;
Page 99 ~ b6; b7C; b7E;
Page 100 ~ b7E;
Page 101 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1257632-0

Total Deleted Page(s) = 8
Page 30 ~ b6; b7C; b7E;
Page 31 ~ b6; b7C; b7E;
Page 32 ~ b6; b7C; b7E;
Page 33 ~ b6; b7C; b7E;
Page 34 ~ b6; b7C; b7E;
Page 99 ~ b6; b7C; b7E;
Page 100 ~ b7E;
Page 101 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 07/27/2004

To: Las Vegas

From: Las Vegas
Squad 8/NRIC
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted] :rmm

Case ID #: 300A-LV-NEW (K) RMM

Title: DEFCON 12 LAS VEGAS 2004
ALEXIS PARK HOTEL
07/30/2004 - 08/01/2004

Synopsis: To open and assign captioned special event to SA [redacted] A subsequent communication will be sent to Counterterrorism and all field offices requesting positive threat information and intelligence be forwarded to Las Vegas. b6 b7C

Details: DEFCON 12 is an annual event that will be held at the Alexis Park Hotel in Las Vegas, Nevada. This event is billed as the largest underground hacking event in the world. The conference is expected to attract 6,000 attendees.

A partial list of topics to be covered during the conference will include the following:

*Introduction to hardware hacking
*Bluesnarfing - The risk from digital pickpockets
*Hack the vote - Election 2004
*RF-ID and Smart labels
*Weakness in satellite television protection schemes
*Smart Card security
*Meet the Fed
*Quantum Hacking
*Hacking the Spectrum
*Down with the RIAA - Musicians against the recording industry
*Hacking the media
*Credit card networks
*Counterintelligence/Counterespionage
*Electronic civil disobedience and the Republican National Convention
*Virus, worms, and trojans, where are we going?

OGA 7-28-04
SA D 7/27/04
b6 b7C

300A-LV-38111-1

52788

The DEFCON 12 conference is expected to bring together white, gray, and black hat hackers from many countries around the world. Several of the speakers include security consultants from private industry, professors, and known credible hackers, who are lecturing during the conference.

It is requested this case be opened and assigned to SA [redacted]

b6
b7C

♦♦

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 1

TAPE 1 OF 6 - CHANNEL 25 - 5:30 PM DEFCON 12 CONFERENCE;

Barcode: E02284884 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS

300A-LV-38111-1D1

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 2

TAPE 2 OF 6 - CHANNEL 25 - 3:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284885 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS

300A-LV-38111-1D2

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 3

TAPE 3 OF 6 - CHANNEL 25 - 11:10 AM DEFCON 12 CONFERENCE;

Barcode: E02284886 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS

300A-LV-38111-1D3

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 4

TAPE 4 OF 6 - CHANNEL 25 - 11:10 AM DEFCON 12 CONFERENCE;

Barcode: E02284887 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DQD/JW

300A-LV-38111-1D4

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 5

TAPE 5 OF 6 - CHANNEL 25 - 1:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284888 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DDD/no

300A-LV-38111-1D5

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 6

TAPE 6 OF 6 - CHANNEL 25 - 3:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284889 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DDP/ms

300A-LV-38111-1D6

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property: Date Entered

1D 7

TAPE 1 OF 6 - CHANNEL 32 - 5:20 PM DEFCON 12 CONFERENCE;

Barcode: E02284890 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DDD/MD

300A-LV-38111-1D7

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 8

TAPE 2 OF 6 - CHANNEL 32 - 11:05 AM DEFCON CONFERENCE;

Barcode: E02284891 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS

300A-LV-38111-1D8

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 9

TAPE 3 OF 6 - CHANNEL 32 - 3:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284892 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DDD/mb

300A-LV-38111-1D9

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired:
VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 10

TAPE 4 OF 6 - CHANNEL 32 - 12:00 PM DEFCON CONFERENCE;

Barcode: E02284893 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS JQ/19

300A-LV-38111-1D10

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 11

TAPE 5 OF 6 - CHANNEL 32 - 1:00 PM DEFCON CONFERENCE;

Barcode: E02284894 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DAD/MS

300A-LV-38111-1D11

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: Source from which Property Acquired:
VOLUNTEERED VIDEO
08/01/2004

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted] b6 b7C

Description of Property: Date Entered
1D 12

TAPE 6 OF 6 - CHANNEL 32 - 3:00 PM DEFCON CONFERENCE;

Barcode: E02284895 Location: ELSUR1 08/04/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DJD/10

300A-LV-38111-1D 12

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 13

TAPE 1 OF 10 - CHANNEL 28 - 4:15 PM DEFCON 12 CONFERENCE;

Barcode: E02284896 Location: ELSUR1 08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DDD/ad

300A-LV-38111-1D13

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 14

TAPE 2 OF 10 - CHANNEL 28 - 6:10 PM DEFCON 12 CONFERENCE;

Barcode: E02284897 Location: ELSUR1 08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS

300A-LV-38111-1D14

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property: Date Entered

1D 15

TAPE 3 OF 10 - CHANNEL 28 - 11:05 AM DEFCON 12 CONFERENCE;

Barcode: E02284898 Location: ELSUR1 08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DJP 1/20

300A-LV-38111-1D15

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 16

TAPE 4 OF 10 - CHANNEL 28 - 1:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284899 Location: ELSUR1

08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS

300A-LV-38111-1D16

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 17

TAPE 5 OF 10 - CHANNEL 28 - 3:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284900 Location: ELSUR1 08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DMP/20

300A-LV-38111-1D17

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 18

TAPE 6 OF 10 - CHANNEL 28 - 5:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284901 Location: ELSUR1

08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DGJ/mo

300A-LV-38111-1D18

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: Source from which Property Acquired:
VOLUNTEERED VIDEO

08/01/2004

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted]

b6
b7C

Description of Property: Date Entered

1D 19

TAPE 7 OF 10 - CHANNEL 28;

Barcode: E02284902 Location: ELSUR1 08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DOP/mb

300A-LV-38111-1D19

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: Source from which Property Acquired:
VOLUNTEERED VIDEO
08/01/2004

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted] b6 b7C

Description of Property: Date Entered
1D 20

TAPE 8 OF 10 - CHANNEL 28 - 11:10 AM;

Barcode: E02284903 Location: ELSUR1 08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DQP/mms

300A-LV-38111 - 1D20

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

1D 21

TAPE 9 OF 10 - CHANNEL 28 - 1:00 PM;

Barcode: E02284904 Location: ELSUR1

Date Entered 08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DSD/10

300A-LV-38111-1D21

Title and Character of Case:

DEFCON 12 LAS VEGAS 2004
-

Date Property Acquired: 08/01/2004

Source from which Property Acquired: VOLUNTEERED VIDEO

Anticipated Disposition:

Acquired By: [redacted]

Case Agent: [redacted]

b6
b7C

Description of Property:

Date Entered

1D 22

TAPE 10 OF 10 - CHANNEL 28 - 3:00 PM DEFCON 12 CONFERENCE;

Barcode: E02284905 Location: ELSUR1

08/05/2004

Case Number: 300A-LV-38111
Owning Office: LAS VEGAS

SUPV. INITIALS DJFD/hs

300A-LV-38111-1D22

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 07/28/2004

To: All Field Offices **Attn:** Special Event Supervisors
Field Intelligence Group SSA's
FBIHQ, Manuals Desk

Counterterrorism **Attn:** SEMU, SSA [redacted]

Cyber **Attn:** AD Jana D. Monroe

General Counsel **Attn:** UC [redacted]
SSA [redacted]

b6
b7C

From: Las Vegas
Squad 8/NRIC
Contact: SA [redacted]

Approved By: [redacted]

b6
b7C

Drafted By: [redacted] rmm

Case ID #: 300A-LV-38111 (Pending)
66F-HQ-C1384970

Title: DEFCON 12 LAS VEGAS 2004;
ALEXIS PARK HOTEL;
07/30/2004 - 08/01/2004

Synopsis: To advise Counterterrorism, Cyber Division, Office of General Counsel, and all receiving offices of upcoming SERL IV special event and request field offices canvas logical sources and provide positive threat and intelligence information regarding the event.

Reference: 66F-HQ-C1417607-F Serial 11
62F-HQ-C1413697 Serial 31

Details: DEFCON 12 is an annual event that will be held at the Alexis Park Hotel in Las Vegas, Nevada. This event is billed as the largest underground hacking event in the world. The conference is expected to attract 6,000 attendees. Information regarding the event can be found at www.defcon.org.

300A LV-38111-2

A partial list of topics to be covered during the conference will include the following:

*Introduction to hardware hacking
*Bluesnarfing - The risk from digital pickpockets
*Hack the vote - Election 2004
*RF-ID and Smart labels
*Weakness in satellite television protection schemes
*Smart Card security
*Meet the Fed
*Quantum Hacking
*Hacking the Spectrum
*Down with the RIAA - Musicians against the recording industry
*Hacking the media
*Credit card networks
*Counterintelligence/Counterespionage
*Electronic civil disobedience and the Republican National Convention
*Virus, worms, and trojans, where are we going?

The DEFCON 12 conference is expected to bring together white, gray, and black hat hackers from many countries around the world. Several of the speakers include security consultants from private industry, professors, and known credible hackers, who are lecturing during the conference.

This communication is to serve as notice to all field offices that any planned travel by Agents or sources to DEFCON 12, or any future Las Vegas special event, is to be approved by SAC Las Vegas and coordinated with special event coordinator SA [redacted] Las Vegas understands that offices that have received concurrence to travel to DEFCON 12 [redacted] As of the date of this communication, only Phoenix and Miami Divisions have received the requisite travel concurrence by SAC Las Vegas to attend DEFCON 12.

b6
b7C
b7E

[redacted]

b7E

To: All Field Offices From: Las Vegas
Re: 300A-LV-38111, 07/28/2004

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

[redacted] b6 b7C b7E

[redacted] Please provide information obtained to SA [redacted]

♦♦

speakers

v.12 • 2004 • July 30- August 1 • Alexis Park • Las Vegas, NV

DEFCON 12 Speakers & Abstracts

A-G

A
A
Tony Arcieri

B
Kevin Bankston
Jay Beale
Beetle
Adam Bresson
Jamie Butler

C
Jon Callas
Strom Carlson
Cazz
Tzi-cker Chiueh
Ian Clarke
Greg Conti
CrimethInc
Gene Cronk

D
Michael Davis
Dario D. Diaz
Dead Addict
Dipl.-Jur. Maximillian Dornseif
Roger Dingledine
Maximillian Dornseif
Robert "hackajar" Imhoff-Dousharm
Elonka Dunin
Jonathan "ripshy" Duncan

E
D. Egan
Charles Edge
Rakan El-Khalil

F
FX
Nicholas Farr
Mark Farver
Peter D. Feaver
Halvar Flake
Bob Fleck
Seth Fogie
Foofus

G-P

G
Kenneth Geers
Geoffrey
Andre Goldman
Sarah Gordon
Joe Grand
Rachel Greenstadt
Jennifer Granick
Grifter
Lukas Grunwald

H
Nathan Hamiel
Seth Hardy
Bev Harris
Deral Heiland
Martin Herfurt
h1kari
Cameron "nummish"
Hotchkies
Thorsten Holz

I
IcE tRe
Ichabod Ver7

J
Eric Johanson
Richard Johnson

K
Dan Kaminsky
Christian Klein
Jesse Krembs

L
Adam Laurie
Lucky225
Peter Leung
j0hnny Long

M
Kevin Mahaffey
Nick Mathewson
Jon McClintock
Rebecca Mercuri
Mike Messick
Doug Mohney

N-Z

N
Brett Neilson
Ne0nRa1n
Annalee Newitz
n0namehere
Nothingface

O
Sean O'Toole
Laurent Oudot

P
Dr. Larry Ponemon
Bruce Potter

R
Michael T. Raggo
Michael Rash
Russ Rogers

S
Len Sassaman
Seth Schoen
Jason Scott
Wendy Seltzer
Sensepost
The Shmoo Group
Peter Silberman
Snax
Holt Sorenson
spoonm

T
Joshua Teitelbaum
Rodney Thayer
Richard Thieme
Grifter

V
Ian Vitek

W
Kathy Wang
Wavyhill
Paul Wouters

Scott Fullam

Brett Moore
HD Moore
Todd Moore
Robert Morris
Mudge

presenter

TOP

A

Weaknesses in Satellite Television Protection Schemes, or "How I Learned to Love The Dish"

This is a beginning to intermediate level talk designed to give the participant a broad overview of satellite technology and where the holes are. I will not be teaching you how to steal service, but I will give you the background and information to understand how it could be done. Topics covered will include different programing you can receive, what kind of hardware you will need, and where to look for more info on the shadier side of things.

A has been involved in the local SLC "scene" for almost a decade, and is well read in many topics. He has many years of experience in most (legal) aspects of satellite and related technologies. A is always willing to help out those with a true interest in learning. He is currently working on a bachelor of science degree at Weber State University in Ogden, Utah.

presenter

TOP

Tony Arcieri
PDTP.org

PDTP – The Peer Distributed Transfer Protocol

Despite decades of evolution, Internet file transfer is still plagued with problems to which formalized solutions are either inadequate or nonexistent. Lack of server-side bandwidth often renders high demand content inaccessible (which we affectionately refer to as the Slashdot effect). When the ability of a single server to provide content is exceeded, manual mirror selection is often utilized, providing an unnecessary and often problematic experience for end users. No formalized cryptographic mechanism exists for preventing tampering of files located on a particular server, and consequently malicious individuals have managed to place trojans in the releases of many high profile open source applications.

The Peer Distributed Transfer Protocol (PDTP) aims to solve all these problems. PDTP can either function with a network of servers providing content directly to clients, or can provide BitTorrent-like "download swarming" by forcing clients to participate in file transfers. PDTP includes built-in mechanisms to prevent file tampering through the use of the Digital Signature Standard, and is able to automatically verify that a given file has been signed by a DSA key with a complete x.509 certificate check to ensure a given certificate can be trusted. PDTP also provides a UDP-based decentralized search mechanism which, unlike current systems such as FastTrack, Gnutella, or FreeNet, does not consume undue bandwidth or system resources, all while removing legal liability for content indexing from the central services being utilized as entry points to the search system.

Tony Arcieri is a system administrator and programmer for the Pielke Research Group and Colorado Climate Center at Colorado State University. He has also contributed to a number of open

source projects, including authoring the Ogg Vorbis plugin for XMMS, the cdcd and gdcd X11 CD player applications, and various contributions to other projects such as the Subversion version control system and the FreeBSD operating system.

presenter
Jay Beale

Locking Down Apache

Apache is the most popular webserver in use by most counts. While it doesn't have IIS's reputation as a worm target, it has still shown itself to be nowhere near invulnerable. Many Apache vulnerabilities can be countered proactively with hardening techniques—this talk will show you how to harden Apache to defeat exploits and worms that haven't yet been developed, or at least released.

Jay Beale is a security specialist focused on host lockdown and security audits. He is the Lead Developer of the Bastille project, which creates a hardening script for Linux, HP-UX, FreeBSD and Mac OS X, a member of the Honeynet Project, and the Linux technical lead in the Center for Internet Security, where he wrote the Unix host auditing tool in wide use today. Jay is a columnist with Information Security Magazine and has written for SecurityFocus, SecurityPortal and Incidents.org. Jay co-authored the Syngress international best-selling book on Snort, the new Stealing the Network: How to Own a Continent fictional book and serves as the series editor of the Syngress Open Source Security series, where he, HD Moore and Renaud Deraison have just finished edits on a new book on Nessus. Jay makes his living as a security consultant through the MD-based firm Intelguardians, LLC.

TOP

presenter
Adam Bresson
IT Manager

Identification Evasion: Knowledge & Countermeasures

Everyday you're right to privacy is being compromised! From security cameras, to illegal searches, to unauthorized monitoring you are being watched. You must protect yourself...and your rights. Using Identification Evasion, you can immediately strengthen your protections. I'll discuss knowledge & countermeasures in the Computer and Real Worlds while presenting many great methods to turn the tables on surveillance. In addition to other in-depth demonstrations and examples, you'll see Identification Evasion in action as I present the video 'Night As Jason Biggs' (for the first time, unedited) where I applied these techniques in Las Vegas. You'll learn some things, enjoy the talk and be entertained!

Adam Bresson (adambresson.com) works during the day as an I.T. Manager for a Santa Monica Investment Banking firm. He also hosts a weekly Los Angeles open mic night, independently codes commercial web sites and challenges corrupt authority as often as possible. At DEFCON 8, he spoke on Palm Security. At DEFCON 9, he spoke on PHP, Data Mining & Web Security. At DEFCON 10, he spoke on Consumer Media Protections (CMP) generating considerable industry interest and press. At DEFCON 11, he spoke on Manyonymity: PHP Distributed Encryption releasing a GPL'ed suite of web application tools. Can you recognize him?

TOP

presenter
Jamie Butler

VICE - Catch the Hookers!

Director of Engineering, HBGary, LLC

Rootkits are the backbone of software penetrations. They provide stealth and consistent access to a computer system. Rootkits employ technology for covert ex-filtration of data, IDS evasion, and anti-forensics. Rootkit technology is now incorporated into the most deadly of threats, network worms. Serious security professionals must understand rootkit technology in detail. Commercial anti-virus technology is woefully inadequate at dealing with the threat. There is no magic security tool that will protect your system. Rootkits now employ specific methods to evade many security utilities, including host-based intrusion prevention systems (HIPS).

This talk focuses on specific rootkit threats and more importantly, how intrusion-prevention software can be designed to detect these threats. Illustrated threats include direct kernel object manipulation (DKOM), hooking, and runtime code patching. We will release a new version of our freeware tool, called 'VICE', that can detect many of these rootkit threats.

Jamie Butler is the Director of Engineering at HBGary specializing in rootkits and other subversive technologies. He is the co-author and a teacher of "Aspects of Offensive Root-kit Technologies." Prior to accepting the position at HBGary, he was a senior developer on the Windows Host Sensor at Enterasys Networks, Inc. He holds a MS in Computer Science from the University of Maryland, Baltimore County. Over the past few years his focus has been on Windows servers concentrating in host based intrusion detection and prevention; buffer overflows; and reverse engineering. Jamie is also a contributor at rootkit.com.

TOP

presenter

Jon Callas
CTO, PGP

How Do We Get The World To Use Message Security

The time has come for people to start using email encryption extensively. There is enough threat from attackers as well as ignorant judges that email is not safe. SSL isn't good enough.

But how? How do we get people to do this? How do you get people whose VCRs blink 12:00 to use encryption? How do you get people to remember to encrypt?

This talk discusses both specific answers as well as open architectures to nudge people down the road of encrypting their email.

TOP

presenter

Tzi-cker Chiueh
Professor, Stony Brook University/Rether Networks Inc.

Program Semantics—Aware Intrusion Detection

One of the most dangerous cybersecurity threats is ``control hijacking'' attacks, which hijack the control of a victim application, and execute arbitrary system calls assuming the identity of the victim program's effective user. These types of attacks are viperous because they do not require any special set-up and because production-mode programs with such vulnerabilities appear to be wide spread. System call monitoring has been touted as an effective defense against control hijacking attacks because it could prevent remote attackers from inflicting damage upon a victim system even if they can successfully compromise certain applications running on the system. However, the Achilles' heel of the system call monitoring

approach is the construction of accurate system call behavior model that minimizes false positives and negatives. This presentation describes the design, implementation, and evaluation of a Program semantics-Aware Intrusion Detection system called PAID, which automatically derives an application-specific system call behavior model from the application's source code, and checks the application's run-time system call pattern against this model to thwart any control hijacking attacks. The per-application behavior model is in the form of the sites and ordering of system calls made in the application, as well as its partial control flow. Experiments on a fully working PAID prototype show that PAID can indeed stop attacks that exploit non-standard security holes, such as format string attacks that modify function pointers, and that the run-time latency and throughput penalty of PAID are under 11.66% and 10.44%, respectively, for a set of production-mode network server applications including Apache, Sendmail, Ftp daemon, etc.

Dr. Tzi-cker Chiueh is currently an Associate Professor in Computer Science Department of Stony Brook University, and the Chief Scientist of Rether Networks Inc. He received his B.S. in Electrical Engineering from National Taiwan University, M.S. in Computer Science from Stanford University, and Ph.D. in Computer Science from University of California at Berkeley in 1984, 1988, and 1992, respectively. He received an NSF CAREER award in 1995. Dr. Chiueh's research interest is on computer security, network/storage QoS, and wireless networking. Dr. Chiueh's group developed the world's fastest array bound checking compiler that incurs less than 10% run-time overhead than programs without checking under Gcc, and built the world's fastest disk-based logging system, which accomplishes a single-sector disk write operation within 450 micro-seconds.

TOP

presenter

Ian Clarke

Freenet: Taming the World's Largest Tamagotchi

Since March 2000 the Freenet project has been the very embodiment of the "release early, release often" mantra, gaining invaluable experience of the unpredictable challenges encountered when deploying a P2P architecture on a large scale. This talk will discuss recent developments in the project including our "next generation" routing algorithm, and a sophisticated but elegant new load balancing mechanism called "adaptive rate limiting". Expect the talk to employ lots of real-world data to illustrate how theory translates to practice when looking after the world's largest Tamagotchi.

Ian Clarke is the architect and coordinator of The Freenet Project, and the Chief Executive Officer of Cematics Ltd, a company he founded to realize commercial applications for the Freenet technology. Ian is the co-founder and formerly the Chief Technology Officer of Uprizer Inc., which was successful in raising $4 million in A-round venture capital from investors including Intel Capital. In October 2003, Ian was selected as one of the top 100 innovators under the age of 35 by the Massachusetts Institute of Technology's Technology Review magazine. Ian holds a degree in Artificial Intelligence and Computer Science from Edinburgh University, Scotland. He has also worked as a consultant for a number of companies including 3Com, and Logica UK's Space Division. He is originally from County Meath, Ireland.

TOP

presenter

Greg Conti
Assistant Professor of Computer Science, US Military Academy

Network Attack Visualization

On even a moderately sized network, activity can easily reach the order of millions, perhaps billions, of packets. Hidden in this sea of data is malicious activity. Current network analysis and monitoring tools primarily use text and simple charting to present information. These methods, while effective in some circumstances, can overwhelm the analyst with too much, or the wrong type of, information. This situation is worsened by today's algorithmic intrusion detection systems, which, although generally effective, can overwhelm the analyst with unacceptably high false positive and false negative rates.

This talk explores the possibilities of visually presenting network traffic in a way that complements existing text-based analysis tools and intrusion detection systems. By graphically presenting information in the right way, we can tap into the high-bandwidth capability and visual recognition power of the human mind. Using the proper visualizations, previously masked anomalous activity can become readily apparent.

This talk will be of interest to those who wish to learn about information visualization as it applies to network security. It requires a basic understanding of the OSI model and packet encapsulation. Attendees will leave with an increased understanding of information visualization that they can apply to their own development projects and management of their networks.

Greg Conti is an Assistant Professor of Computer Science at the United States Military Academy. He holds a Masters Degree in Computer Science from Johns Hopkins University and a Bachelor of Science in Computer Science from the United States Military Academy. His areas of expertise include network security, interface design and information warfare. Greg has worked at a variety of military intelligence assignments specializing in Signals Intelligence. Currently he is on a Department of Defense Fellowship and is working on his PhD in Computer Science at Georgia Tech. He is conducting research into Denial of Information Attacks.

TOP

presenter

CrimethInc
Revolutionary Hacker Anarchist, CrimethInc Black Hat Hacker's Bloc

Electronic Civil Disobedience and the Republican National Convention

An introduction to the theory of hacktivism and the usage of hacking skills as a means of fighting for social justice by pressuring corporations and government to adopt progressive changes. Explores the history of electronic civil disobedience, tips on how to wage your own ECD campaigns, and how to participate in the upcoming actions to coincide with the protests against the Republican National Convention in late August.

CrimetheInc is an Anarchist hacker revolutionary having led successful electronic civil disobedience campaigns against a variety of government and corporate targets. Experienced political activist, having helped organize dozens of large protests against the war in Iraq, global capitalism and neo-liberal free trade agreements. Is currently organizing a multi-pronged hacktivist campaign against the Republican National Convention

to coincide with the massive demonstrations to take place in New York City. Specific history about the speaker is not available due to the nature of this project.

TOP

presenter

Gene Cronk, CISSP, NSA-IAM
North American IPv6 Task Force

IPv6 Primer

The IPv6 Primer will encompass the basics of IPv6, including some of its roots, the transitioning mechanisms available, and some security concerns early adopters should be aware of in several different environments. This presentation is meant for anyone who has heard about IPv6, but would like to know the basics of the protocol and its implementation.

Gene Cronk, CISSP, NSA-IAM, resides in Jacksonville, FL and is currently providing system administration services to an advertising and marketing firm.

He has 10 years of experience in electronics, system administration, networking and system security. Gene is best known for his work on the North American IPv6 Task Force, and his work on
Fu King Linux (an IPv6 enabled distribution of Linux), which includes security tools that can be run in IPv4 or IPv6 environments. He has also spoken on IPv6 and other topics at several venues.

When not totally absorbed by system security related issues, Gene can be found wardriving, actively participating as Vice President of the JaxLUG, and building a successful and dynamic 2600
chapter, of which he is currently president.

TOP

presenter

Dead Addict

Hacking the Media, and Avoiding Being Hacked by the Media

Hackers have been demonized and romantisized in the media. Some hackers interactions with the media have caused their eventual incarseration, while others seem to pimp the media to promote their careers. Dead Addict will provide a framework for manipulating the media and avoid being the victim of the media. While this talk will be relavent to hackers, it is applicable to all that consume or are consumed by media. Dead Addict will also discuss methods to improve the quality of reporting and influence the media without appearing in it.

TOP

presenter

Michael Davis
DSCI

The Open-Source Security Myth—and How to Make It A Reality

Open Source software is frequently described as more "secure" than closed source software for two reasons: the number of people available to correct a problem is potentially larger; and anyone can review the source code for vulnerabilities or malicious code. Unfortunately, the current state of design documentation does not support a cost-effective security review. In addition to compromising the confidence in the software, the lack of documentation also sets an unnecessarily high "bar" for new members to join an Open Source projects. This unintended consequence directly reduces the number of people available to

correct vulnerabilities or otherwise improve the software. The presentation provides a rationale for creating development documentation and identifies available tools.

Michael Davis oversees the Security Engineering services provided by Dynamic Security Concepts, Incorporated (DSCI). During recent efforts to encourage his customers to use Open Source solutions; he oversaw the security review of a number of Open Source security tools. He possesses a broad security background and has been a featured speaker for select audiences on the subject of intrusion detection and evaluating security solutions in general.

TOP

presenter

Dario D. Diaz

DMCA, Then and Now

A look at the Digital Millenium Copyright Act (DMCA), what it was originally meant to do, what it's done, and how it's been used and abused. The highly misunderstood statute was hastily enacted and has been put to the test. While most in the hacker community might agree that the DMCA has been a failure, the actual legal results might actually provide some interesting insight. The lecture will involve an analysis of the statute, the legislative history, case law (both criminal and civil), and a perspective of the DMCA's future.

Dario D. Diaz was born in Tampa, Florida, on June 26, 1967. His father immigrated from Cuba as a political exile first seeking asylum in Venezuela. His mother was the child of Spanish immigrants and a lifelong resident of Tampa. Diaz graduated from Tampa,s Jefferson High School and enrolled at the University of Florida.

Shortly after joining the firm Diaz immersed himself in high profile litigation assisting partner Ralph Fernandez. In 1997 Fernandez and Diaz assumed the representation of three alleged Cuban skyjackers, Adel Regalado, Jose Bello Puente and Leonardo Reyes, on the night before testimony began in United States District Court. At the conclusion of trial the three defendants were acquitted of air piracy. Immediately the Immigration Service proceeded with detention and removal proceedings. In a highly publicized case in 1998 the Immigration Court ruled in favor of the three men granting them political asylum and withholding of removal. The government appealed to the Board of Immigration Appeal. A massive appellate process was undertaken. In October of 2002 the BIA affirmed the decision of the lower court. Fernandez and Diaz also assumed the representation of Jose Dionisio Suarez Esquival, implicated by the United States in the assassination of former Chilean Ambassador Orlando Letelier in Washington D.C. in 1976. During the process Suarez became entangled in the extradition proceedings of General Augusto Pinochet by the Kingdom of Spain and the ancillary investigation by the Republic of Chile. In August 15, 2001, Suarez was freed after nearly a decade of detention. Diaz walked Suarez Esquival out of jail. The photo grabbed headline news around the world. Diaz later directed the successful defense in State of Florida v. Noe Ramirez, at one time identified as the individual that tossed a boulder off the I-75 overpass in Bradenton, Florida, tragically killing a well known and respected University of Alabama professor.

In August of 2000, Diaz was asked to speak at DEFCON, the largest conference for computer security, cryptography and hacking held in the United States. His lecture dealt with the Digital Millennium Copyright Act (DMCA) and the legal aspects of the law. A Russian programmer and citizen, Dmitri Sklyarov, who was also a conference lecturer, was arrested by federal authorities for criminal charges stemming from the DMCA. In news stories the national media identified Diaz as the leading expert in the area. Diaz', trial practice involves civil, criminal, and family law cases. He has tried cases in criminal, personal injury, negligence, and select family law matters.

Diaz is married to his high school sweetheart, Lisa. They have three children.

TOP

presenter

Roger Dingledine
The Free Haven Project

Tor: An Anonymizing Overlay Network for TCP

Tor (second-generation Onion Routing) is a distributed overlay network that anonymizes TCP-based applications like web browsing, secure shell, and instant messaging. We have a deployed network of 30 nodes in the US and Europe, and the code is released unencumbered as free software. Tor's rendezvous point design enables location-hidden services—users can run a standard webserver or other service without revealing its IP.

I'll give an overview of the Tor architecture, and talk about why you'd want to use it, what security it provides, and how user applications interface to it. I'll show a working Tor network, and invite the audience to connect to it and use it.

Roger Dingledine is a security and privacy researcher. While at MIT he developed Free Haven, one of the early peer-to-peer systems that emphasized resource management while retaining anonymity for its users. Currently he consults for the US Navy to design and develop systems for anonymity and traffic analysis resistance. Recent work includes anonymous publishing and communication systems, traffic analysis resistance, censorship resistance, attack resistance for decentralized networks, and reputation.

presenter

Maximillian Dornseif

Far More Than You Ever Wanted To Tell - Hidden Data In Document Formats

Applications usually put all kinds of information besides the ones which you intend to into saved documents. This can lead to embarrassing revelations. We will take a look into different types of application data and what can be hidden in there. This allows us to "scrub" our own documents to avoid unwanted information in there but also to look for information in documents which the authors didn't want to hand out. Go grasp the scope of the problem we will present a large scale study of hidden information in Documents on the Internet.

Maximillian Dornseif has studied laws and computer science at the University of Bonn, Germany where he wrote his PhD Thesis about the "Phenomenology of Cybercrime". He has been doing security consulting since the mid nineties. His clients included the industry but also government. At the moment he works on a third

party founded research project about measurement of security and security breaches taking place at the Laboratory for Dependable Distributed Systems, RWTH Aachen University. He also oversees several other projects in the area of detection and documentation of security incidents. Dornseif has published in the legal and computer science fields on a wide range of topics.

TOP

presenter

Robert "hackajar" Imhoff-Dousharm
Credit Card Compliancy & Fraud Analyst

Jonathan "ripshy" Duncan
Systems Developer to demonstration

Credit Card Networks Revisted: Penitration in Real-Time

Credit card authorization is the core to all major businesses, both on and off the Internet. Yet an alarming number of businesses are not taking the right steps to insure that your credit cards are secure against fraud and theft. In bringing this to light (Credit Card Networks 101, July 31 2003 - DC 11), you were awed at the posibility, but were not provided with any real proof. This year we, that's you and I, will walk through the process of identifying credit card traffic on a network, decyfering packets and propagated rouge credit card data to a host comeputer. You will be provided access to a private Wi-Fi network. This networks will have credit card data streamming across it for you to sniff. With your help, we will discover information about credit cards packets, and how to design our own packet to be sent.

Want to partcipate?

1. Login to http://www.hackajar.com/credi
2. Read "What's in a credit card" section for background on credit cards and their supporting networks
3. Read "What you'll need" section, and have said items at conference
4. Sign-up for fake credit card account, you will use this to keep track of your progress and win prizes

NOTE: You will have opportunity to sign-up for account during demonstration

Robert "hackajar" Imhoff-Dousharm—In the last 2 years, Robert has worked for Shift4, a Credit Transaction Gateway. As an Analyst he insures best fraud practices, compliceny and security are meet at all clients sites He has worked with government agency's during fraud investigations. He also works with new and potential clients to implement best practice in software design of credit card intigration software Robert has spoken at DefCon 11 (Credit Card Networks 101) about the potential risks currenly impeading on credit card networs. He will demonstrate those risks this year with "Credit Card Networks Revisted: Penitration in Real-Time".

TOP

presenter

Elonka Dunin

Kryptos and the Cracking of the Cyrillic Projector Cipher

In a courtyard at CIA Headquarters stands an encrypted sculpture called Kryptos. Its thousands of characters contain encoded messages, three of which have been solved. The fourth part, 97 or 98 characters at the very bottom, have withstood cryptanalysis for over a decade. The artist who created Kryptos, James Sanborn, has also created other encrypted sculptures such as the decade-old Cyrillic Projector, which was cracked last September by an international team led by Elonka Dunin. This talk is intended for a general audience with beginning to

intermediate cryptographic experience. Elonka will go over how the code was cracked, and the current state of knowledge about the Kryptos sculpture, its own encrypted messages, and its mysterious CIA surroundings.

Elonka Dunin is a professional game developer, working at Simutronics (play.net), a provider of massively multiplayer online games. Also an amateur cryptographer, Elonka led the international team that cracked the decade-old KGB Cyrillic Projector Code in September 2003.

Elonka was born in Los Angeles, studied Astronomy at UCLA, and then joined the United States Air Force, where she worked on the SR-71 and U-2 reconnaissance aircraft. Elonka is a world-traveler who speaks multiple languages, and has visited scores of countries around the world, and every continent (yes, including Antarctica). She has won awards for cracking various codes, such as when she cracked the PhreakNIC v3.0 Code, an up-until-Elonka unsolved puzzle created by se2600. Since September 11th, Elonka has also been helping out with the war on terrorism by teaching government agents about cryptography and what types of codes that Al Qaeda may be using. She is co-founder of the Kryptos Group, an online group of cryptographers and interested hobbyists trying to crack the last part of the code on the famous Kryptos sculpture at CIA Headquarters.

TOP

presenter

Charles Edge aka krypted
Senior Systems Engineer, Three18

Hacking/Security Mac OSX Server aka Wussy Panther

Panther Server, the highly touted new OS by Apple has some glaring security flaws, although Apple typically gets away easy because not a lot of people hack it. See what's being done against OSX Server and what can be done to guard against it.

During the talk, I will show exploits I've been working on since Panther was released and give honorable mention to the tools I've been using to help me out along the way.

Remember when BackOffice came out and there were a bunch of exploits against it? Well, imagine another server with web-based email, a full web development platform, SQL, and File Sharing over a proprietary protocol.

No Apple knowledge is required of the listener, only a working knowledge in UNIX.

Charles Edge has been setting up and maintaining hybrid networks for the entertainment industry (including the Osbournes) in Los Angeles for 5 years. This talk will focus on hardening OSX Server by showing its vulnerabilities.

TOP

presenter

D. Egan
Senior Web Applications Developer, ICS MT

MySQL Passwords— Password Strength and Cracking

This talk will cover best practices for choosing MySQL passwords as well as the tools available to "crack" a MySQL password hash. It will NOT cover how to obtain a password hash, however. During the talk I will be introducing a new dictionary-based auditing tool, named "phpMyAudit". The tool is written in PHP and allows a user to run the application as a shell-based script, yet it

also includes a web-based front end. This talk is primarily aimed at persons interested in choosing secure MySQL passwords, and persons who would like to "audit" an existing MySQL password hash.

D. Egan is a recent college graduate who has been a professional web-application developer for over 5 years. He currently works and lives in beautiful Missoula, Montana. This will be his 5th year attending Defcon, and his first Defcon speech.

TOP

presenter

Rakan El-Khalil

Information Hiding in Executable Binaries

Information Hiding techniques are much researched in the context of watermarking or fingerprinting images and sound files, mainly as a means of copyright protection and piracy prevention/detection. Those mediums offer a significant amount of redundancy, thus lending themselves to the implementation of robust IH systems. Executables however do not offer such amounts of redundancy, and have thus far proven to be a difficult and rarely used medium for steganographic and other IH purposes. The aim of this talk is to be an introduction to IH, with a thorough coverage of state of the art techniques for embedding into binaries. Hydan, a tool for performing such embeddings in machine code, will be presented. In addition to typical IH uses [steganography, watermarking], the tool and techniques shown can be used in anti-reverse engineering, trusted application execution, frustrate some buffer overflow attacks, and as an engine for metamorphic viruses. An interesting effect of the tool is that the executable remains the same size before and after embedding, while of course remaining functionally equivalent.

Rakan El-Khalil is currently on sabbatical in France. He is a recent MS CS graduate from Columbia University. While he was there he worked on a variety of projects at the CS Research Lab, such as an IDS that uses machine-learned models to detect network threats, and a syscall based permission system on OpenBSD [predating systrace]. He was also responsible for the short-lived official KaZaA Linux client `kza'. Currently he is involved with The Bastard, a powerful linux disassembler, and has been researching steganography and information hiding in machine code.

TOP

presenter

FX
Phenoelit

Halvar Flake

"We Can Take It From Here"

Sick of watching other people working their magic and still wondering how to get 0day? Write your own! This session is about the state of mind for finding and exploiting bugs. From web applications to client-server systems and multi-tier platforms down to routers, switches and wrist watches - everything has bugs and everything can be exploited one way or another.

But of course, a state of mind alone doesn't get you 0day. Now you need to find a crack in the armor that you can pry open and drive your truck through.

The session will try to guide you through how to find a bug, how to combine several of them or how to circumvent things that would ruin your plan, starting from how to do educated guesses down to diff and patch review.

Don't be scared, have no phear. Found a bug but you have no idea what to do with it? A strange CPU, a never-seen-before platform or an unknown protocol should not prevent you from getting r00t anyway. This last part deals with guidelines on shell and non-shell codes, binary or not, and with handling complicated platforms.

The goal is that you walk out with your own 0day already developing in your mind.

FX of Phenoelit is the leader of the German Phenoelit group. His and the group's primary interests are in security implementations and implications of standards or less-known protocols, as shown on past DefCon conventions. FX has a fairly special relationship with shops like Cisco Systems and HP as well as SAP. Currently, he works as a Security Solution Consultant at n.runs GmbH.

Halvar Flake is Black Hat's resident reverse engineer. Originating in the fields of copy protection, he moved more and more towards network security after realizing the potential for reverse engineering as a tool for vulnerability analysis. He spends most of his screen time in a disassembler (or developing extensions for the disassembler), likes to read source code diff's with his breakfast and enjoys giving talks about his research interests. He drinks tea but does not smoke camels.

TOP

presenter

Peter D. Feaver
Professor, Duke University

Kenneth Geers
Analyst, NCIS

The First International Cyber War: Computer Networks as a Battleground in the Middle East and Beyond

This briefing addresses the world's first global Internet war: the cyber skirmishes associated with the Palestinian intifadah. What started out as a localized conflict spread to battles around the globe as forces sympathetic to either the Israelis or the Palestinians joined the fray. With the Middle East cyber war as a backdrop, this presentation will cover the ways in which people can try to affect the course of world history through coordinated action in cyberspace.

The authors first describe the globalized and asymmetric nature of modern warfare, the asymmetry of computer hacking, and the psychology of subcultures. They outline the legal issues surrounding cyber warfare, from the perspective of a lone hacker to a massive government intelligence service, and discuss the problems inherent in cyber retaliation and in the prosecution of hackers.

On the technical side, this briefing discusses the targeting of Internet sites for attack, and the strategies used by hackers to bring them down or merely leverage them in more subtle ways to support their cause. The primary focus is the means used by cyber commanders to accomplish political and/or social goals, in particular the creation of Web portals through which their foot soldiers are able to unite and rain network packets down upon their enemies.

Finally, this briefing examines the difference between the perception and the reality of cyber attacks. We address the strategies that national governments are employing to combat the threat, the potential impact of cyber attacks on military

operations, and the vexing problem of Denial of Service attacks, Web defacements, and free speech. The authors assess the threat and the limits of the more powerful weapons in the cyber arsenal, and consider who might be the biggest target of cyber attacks in the coming years.

Peter D. Feaver (Ph.D., Harvard, 1990) is Professor of Political Science and Public Policy at Duke University and Director of the Triangle Institute for Security Studies (TISS). Feaver is co-directing (with Bruce Jentleson) a major research project funded by the Carnegie Corporation, "Wielding American Power: Managing Interventions after September 11." Feaver is author most recently of Armed Servants: Agency, Oversight, and Civil-Military Relations (Harvard Press, 2003),and co-author, with Christopher Gelpi, of Choosing Your Battles: American Civil-Military Relations and the Use of Force (Princeton University Press, 2004). He is co-editor, with Richard H. Kohn, of Soldiers and Civilians: The Civil-Military Gap and American National Security (MIT Press, 2001); and author of Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States (Cornell University Press, 1992). He has published several other monographs and over thirty articles and book chapters on American foreign policy, nuclear proliferation, civil-military relations, information warfare, and U.S. national security. He won the Duke Alumni Distinguished Undergraduate Teaching Award in 2001 and the Trinity College Distinguished Teaching Award in 1994-95. In 1993-94, Feaver served as Director for Defense Policy and Arms Control on the National Security Council at the White House where his responsibilities included counterproliferation policy, regional nuclear arms control, the national security strategy review, and other defense policy issues. He is a Lieutenant Commander in the U.S. Naval Reserve (IRR). He is married to Karen Feaver, and they have three children, two sons and a daughter.

Kenneth Geers (M.A., University of Washington, 1997) is a Computer Investigations & Operations analyst with the Naval Criminal Investigative Service (NCIS). His career at the Department of Defense also includes work at the National Security Agency, the Defense Intelligence Agency, an SAIC nuclear arms control support team, the John F. Kennedy Assassination Review Board, and the U.S. embassy in Brussels, Belgium. He is an expert in French and Russian, who finished first in a class of seventy at the Defense Language Institute at the Presidio of Monterey. Mr. Geers is the author of training and testing software to prepare U.S. Army Major Commands for Russian strategic arms inspections, and he has designed multiple U.S. Army Space and Missile Defense Command websites devoted to arms control. These days, he spends his time analyzing computer and network logs of all types. In his free time, he plays chess and serves as a SANS mentor in the Washington D.C. area. Over the years, he has taken the opportunity to see the world, stopping long enough to wait tables in Luxembourg, harvest grapes in the Middle East, climb Mount Kilimanjaro, and set his alarm clock for 3 AM in a strict Trappist monastery. He loves his wife Jeanne, and daughters Isabelle and Sophie.

TOP

presenter

Seth Fogie
VP, Airscanner

Attacking Windows Mobile PDA's

Microsoft's Pocket PC (AKA Windows Mobile) has remained

relatively free of all the nasty attacks that have bombarded its PC based cousins. Does this mean this OS is any more secure or safe from attack? Ironically, this is as far from the truth as one can get.

Using reverse-engineering techniques, this presentation will demonstrate just how easy it is to gain full remote unauthorized access to a PPC device. In addition, we will also provide an example of a remote buffer overflow attack against the PDA and the tricks needed to place working code on the proverbial stack.

This talk will be technical. However, if you want to gain a better understanding of the ARM processor, hacking Pocket PC programs, or just want to see how buffer overflow attacks work on the PDA, you will not be disappointed.

Seth Fogie is the VP of Dallas-based Airscanner Corporation where he oversees the development of security software for the Window Mobile (Pocket PC) platform. He has co-authored four technical books on information security, including the top selling "Maximum Wireless Security" from SAMS, and the recently released "Security Warrior" from O'Reilly. Mr. Fogie frequently speaks at IT and security conferences, including Defcon (10 & 11), CSI, and Dallascon. In addition, Seth is acting Site Host for Security at Pearson Education's "InformIT.com" website where he writes articles and reviews/manages weekly information security related books and articles.

TOP

presenter

Foofus

Old Tricks

In September of 2003, a noted security consultant was terminated from his job over controversy surrounding a document that he co-authored. One key focus of the document was the risk associated with operating system monocultures. This idea was nothing new. In fact, in 1989, the following passages appeared in a book that spent over four months on the New York Times best seller list:

> "Just like genetic diversity, which prevents an epidemic from wiping out a whole species at once, diversity in software is a good thing."
>
> "A computer virus is specialized: a virus that works on an IBM PC cannot do anything to a Macintosh or a Unix computer. [snip] Diversity, then, works against viruses. If all the systems on the Arpanet ran Berkeley Unix, the virus would have disabled all fifty thousand of them. Instead, it infected only a couple thousand."
>
> -- Stoll, Cliff. THE CUCKOO'S EGG, New York: Simon & Schuster
> Pocket Books, 1989. Pages 51 and 347.

The point of this citation is not to cast any disrespect on the authors of "CyberInsecurity: The Cost of Monopoly" (on the contrary, in fact). Rather, we wish merely to note that the risk of monocultures was identified at least fourteen years ago, and was widely published. Why fuss if someone repeats it?

Foofus.net wants in on this kind of action. In that spirit, we've looked high and low for a bunch of other old ideas so that we can breathe new life into them, and (in the famous words of a respected security research team), make "the theoretical practical," in an effort to tax the patience of those who would rather we kept our heads in the sand about ideas that are right there in the open, but inconvenient to demonstrate. Until now.

Come to this presentation, and savor some exquisite fun. We will demonstrate our tools and techniques, and we think you will find that they are interesting and useful. But not new. We promise that we have not invented a damn thing here; the basic concepts are 100% recycled, but we hope they will encourage people to get serious about areas where they've been coasting for too long.

The focus of the talk is Windows: tools will be presented for identifying potential trust relationships between disparate hosts, tinkering with friendly wireless interfaces, easy access to network shares without bothering to crack password hashes, and (if our luck holds) maybe even alittle more. It'll be really fun, and stuff.

Foofus leads a team of security engineers at a midsize technology consulting firm in the midwest, where he has worked for the past seven years. He has spoken at a variety of events and conferences including Toorcon and LISA. His chief technical interest is software security, and in his spare time he enjoys playing guitar, cooking, and attending the symphony.

TOP

presenter

Scott Fullam

Introduction to Hardware Hacking

Interested in hardware hacking but were not sure where to start? This presentation is for you. I will show you how to get started with modifying equipment for fun and useful purposes. I will show you the best ways for opening the enclosures for electronic equipment without destroying it, how to identify electronic components, how to solder together circuits, where to get parts, and will do a walk through of several hacks i have completed. the talk is intended for beginners, but all experience levels will get a kick out of it.

Scott Fullam is the author of the O'Reilly book "Hardware Hacking Projects for Geeks" published in February 2004.

Scott Fullam has been hacking hardware since he was 10 years old with his first RadioShack 100-in-1 electronic kit. He built an intruder alarm to keep his sister out of his room. Scott attended MIT earning Bachelors and Masters degrees in Electrical Engineering and Computer Science. While and undergraduate he built a shower detection system so that he could see if the community shower was in use to allow him to sleep in a few extra minutes in the morning if it was occupied. After graduating from MIT Scott designed children's toys and built close to 50 prototypes in 2 years. He then went to work at Apple Computer in the Advanced Technology Group designing digital still cameras. In 1995, Fullam co-founded PocketScience, which develops revolutionary mobile e-mail communications products and services. As the Chief Technology Officer (CTO), Fullam personally developed all of the algorithms for the company's products. He also led the team that developed PocketScience's products and reference hardware. Scott now works as an

independent consultant assisting consumer electronic companies design high quality products and manufacture them in the Far East. Scott holds 15 US patents. Never satisfied with how the consumer electronics products he own work, he often takes them apart and enhances their capabilities.

TOP

presenter

Geoffrey

This Space Intentionally Left Blank

Mark Farver

"This Space Intentionally Left Blank" covers work done to safely allow the transfer of unclassified data onto a sensitive (read highly classified) network for comingling with other data collects and
subsequent analysis. We devised a system using COTS (Commercial Off The Shelf) hardware, Open Source applications and a couple of custom programs to accomplish these ends. The main requirement was to ensure a one way flow of data from the antenna farm into the analysis network with no data drift back. The presentation will discuss the technical details of how this was managed.

Geoffrey has been a facility and network security officer and ComSec Manager in the Intelligence Community for fourteen years. His duties include shoring up network security at both contractor and government facilities. He is also available for childrens' parties.

Mark Farver has served 5 years as trampled network engineer and code monkey. He has spent the past two years as network administrator and ComSec manager for sensitive networks. He knows little of value and sometimes gets cranky without a nap.

TOP

presenter

Sarah Gordon

What Do You Mean, Privacy?

Privacy doesnt mean the same thing to everyone... Since you're interacting in a global space, you need to understand what people outside your immediate frame of reference are thinking when they talk about privacy—because what they think will influence ttheir expectations and their actions. This talk will give you the opportunity to examine some other views of privacy, explore your own thinking, and compare it with others—both from the global information security community and the audience. Finally, we'll look at how well those thoughts match up with behaviors related to various aspects of what we call "privacy".

Sarah Gordon has spoken at DEFCON on topics from the security of PGP, women of #hack, and the impact of legislation on virus writing, and done lots of security related stuff for lots of different groups.

TOP

presenter

Joe Grand, aka Kingpin
Electrical Engineer, Grand Idea Studio

Advanced Hardware Hacking: Designs and Attacks of Secure Hardware

This presentation looks at advanced hardware hacking and reverse engineering techniques. We'll look at the steps taken by designers to incorporate security into their hardware products and then examine ways to attack them. Learning from history is important, so successful hardware hacks against security

products will be discussed and copious references to other existing material will be provided.

Joe Grand (also known as Kingpin) is an electrical engineer at Grand Idea Studio, Inc., a product development and intellectual property licensing firm. He is a former member of the legendary hacker collective L0pht Heavy Industries (yes, which turned into @stake, but don't ask him about that) and specializes in embedded system design, computer security research, and inventing new concepts and technologies.

Oh, Joe is also the author of the Syngress book "Hardware Hacking: Have Fun While Voiding Your Warranty" published in January 2004 and contributor to a bunch of other books.

TOP

presenter

Rachel Greenstadt
Harvard University

Tools for Censorship Resistance

What censorship resistance technique is right for me? (And should my Chinese dissident friends use the same one?)

Nearly everyone in the world is affected by censorship to some degree. Whether from annoying corporate firewalls, nervous ISPs, or oppressive governments, the result is often the same; individuals and organizations are unable to obtain information they want, say the things they'd like, or communicate with others. A number of technologies are helpful in circumventing these restrictions, including covert channels, steganography, and peer-to-peer systems.

This presentation will survey the field of censorship resistance and discuss the maturity and promise of various techniques, as well as their promise and limitations from a theoretical perspective. I will present a range of capabilities and threat models and discuss which approach is best suited to each situation.

Rachel Greenstadt is a researcher at Harvard University and a DHS fellow. She studies how information is leaked, collected, and controlled. She has done research on privacy, steganography, covert channels, and peer-to-peer security. Rachel is a contributor to the forthcoming book, *The Economics of Information Security.* She attends small, academic conferences compulsively, takes ballet classes, and reads science fiction in her spare time.

TOP

presenter

Grifter

Russ Rogers
CEO & CTO, Security Horizon

Tierra

Project Prometheus

The goal of Prometheus is to create an Open Source project that takes into account the inherent flaws in the Microsoft implementation of Alternate Data Streams (ADS) and uses those attributes to create a tool for increased security. The concept is similar to making lemonade from lemons. We're taking an insecure component of the NTFS file system and creating a tool that will provide increased security. Russ and Grifter will be explaining and demonstrating the use of Alternate Data Streams and then discussing an Open Source project which they have currently begun development on.

Grifter has been involved in the scene for over a decade and

currently runs 2600SLC, the Salt Lake City 2600 meeting, and DC801 the Utah Defcon meeting; where he often lectures on a range of security related topics. He has been published in numerous online and print publications and has previously been a speaker at several Defcons. He has also been the subject of interviews for various online, print, and television pieces regarding different areas of the hacker culture over the years. He is a Defcon Goon and primary organizer of the Defcon Scavenger Hunt and Defcon Movie Channel.

Russ Rogers is the CEO and CTO of Security Horizon, a Colorado Springs based information security professional services firm and is a technology veteran with over 12 years of technology and information security experience. He has served in multiple technical and management information security positions that include Manager of Professional Services, Manager Security Support, Senior Security Consultant and Unix Systems Administrator. Mr. Rogers is a United States Air Force Veteran and has supported the National Security Agency and the Defense Information Systems Agency in both a military and contractor role. Russ is also an Arabic Linguist. He is a certified instructor for the National Security Agency's INFOSEC Assessment Methodology (IAM).

Tierra, while still somewhat new to the scene, has been manipulating bits since the 7th grade, and is currently working on his Computer Science degree at the University of Utah. He has been attending 2600 meetings for more than 3 years now in Salt Lake City, and has been helping run the Defcon Scavenger Hunt since Defcon 10 (you'll find him at the Scavenger Hunt table again this year). While working with the DC801 crew on projects such as this, he spends his time mastering his PHP and SQL skills on various personal projects such as TIMAP found on SourceForge.

TOP

presenter

Lukas Grunwald
CTO, DN-Systems Enterprise Internet Solutions GmbH

RF-ID and Smart-Labes: Myth, Technology and Attacks

This talk provides an overview of the RF-ID Smart-Labes, small labels on products with an embedded microchip and an antenna. Smart-Labes store product and serial-number, expiration date etc. and can be read from a distance.

The Industry is planning to put these labels with an international product code on every product within the next decade, effectively replacing the old bar-code system. Some stores already use Smart-Labes, for example certain pharmacies in the US, and in Europe the Metro Group in their Future Store.

At the end of this talk there is a practical demonstration of RF-DUMP, my tool to read and write Smart-Labes, check their meta-data and manipulate it.

Mr. Lukas Grunwald is CTO of DN-Systems Enterprise Internet Solutions GmbH (Hildesheim/Germany)—a globally acting consulting office working mainly in the field of security and internet/eCommerce solutions for enterprises. Mr. Grunwald has been working in the field of IT security for nearly 15 years now. He is specializing in security of wireless and wired data and communication networks, Forensic Analysis, Audits and Active Networking. Mr. Grunwald regularly publishes articles, talks and

press releases for specialist publications. He also participates actively in conferences such as Hackers at Large, Hacking in Progress, Network World, Internet World, Linux World (USA/Europe), Linux Day Luxembourg, Linux Tag, CeBIT Conference.

TOP

presenter

Nathan Hamiel (Ichabod Ver7)

Down with the RIAA, Musicians against the Recording Industry

Down with the RIAA is a look at the current state of the music business and where it is headed. The presentation uses statistics and facts to map out where the industry currently is and details the problems with the current model. After the problems with the current model are shown then the groundwork for the future of the music business is laid out showing how the recording industry is no longer needed. Included in the presentation is information on how artists can produce their own music cutting out the recording business.

The recent increase in quality and decrease in price of recording equipment has made it very feasible for artists to make very high quality recordings on their own. This is the way of the future, and the processes are detailed by an independent music producer with experience in the field. Most people do not know it is possible to make quality recordings that rival commercial ones from your apartment, without even disturbing your neighbors. People are screaming for a change in the music industry. With all of the problems that the RIAA is creating for the music consumer, consumers will begin to be open to a new model where the hassles of the RIAA will no longer be an issue. The future of the music business will also afford more opportunity to artists leveling the playing field and decreasing competition between artists.

Nathan Hamiel (Ichabod Ver7) is an independent artist and producer living in Jacksonville, FL. As an artist he has shared the stage with acts such as The Union Underground, Fuel, Scrape, 8Stops7, Phoenix TX, The Crux Shadows, and many more. Using his skills gained as a recording engineer he has been able to create high quality recordings using very reasonably priced equipment many times surpassing the quality of commercial recordings. He has many albums and recordings to his credit and shares the knowledge with other artists and producers world wide. He has created some of his own techniques, including ones on layering drum samples that can now be heard on many different recordings. On the technology side, he is a CISSP, was a presenter at Interz0ne 3, and VP of the Jacksonville 2600.

TOP

presenter

Seth Hardy

Subliminal Channels In Digital Signatures -or- Why it's VERY Important To Verify Trustworthiness of Encryption Programs

A number of papers about a subliminal channel in the Digital Signature Algorithm were published more than ten years ago, allowing for communication through digital signatures in an undetectable manner. The subliminal channel is generally viewed as a method of legitimate but hidden communication, but it can also be used for leaking secret information (such as keys) in a

undetectable way to anyone who knows what to look for. I will present on how this subliminal channel works, and demonstrate using a patched version of the GNU Privacy Guard how to use it for both benign and malicious reasons, both of which have little to no prior implementation in encryption programs.

Seth Hardy is involved in both research and implementation in the field of cryptology, both as part of a university research group and independently. His primary interest is the mathematics side of crypto, so he's been involved in a number of projects which involve translating new and better concepts from math into a working implementation in code. Seth has presented his work at a number of conferences, usually with his good friend Jose.

presenter
Bev Harris **Black Box Voting**

TOP

presenter
Deral Heiland **The Insecure Workstation**

The insecure workstation. A creative look at the windows group policies as a security solution in today's workplace and how easily they are circumvented. This talk will discuss the Were, What and Why on policies and also demonstrate simple tricks to bypass policies and exploiting poor policy implementation.

Deral Heiland has been in the IT field since 1994 working in the following industries; Newspaper media, System Integrator, Manufacturing. Held the following position Network Administrator, Financial systems manager, Network field engineer and Network Security Analyst. He presently holds the following certifications SSCP, CCNA, CCWS, CNE5 and CWSE.

TOP

presenter
h1kari **Smart Card Security: From GSM to Parking Meters**

Smart Cards are used all over the place in every day life. The unfortunate (or fortunate) side of Smart Cards is that most widely deployed systems don't use any real security and rely mostly on obscurity. This presentation will discuss the different types of Smart Cards, exactly how to reverse engineer the protocols they use, and how to exploit their security weaknesses. For demonstration, we will look at GSM SIM Cards and San Diego Parking Meter Debit Cards and show how their security can be defeated.

h1kari has been in the security field for the past 5 years and currently specializes in 802.11b Wireless Security, Smart Card, and GSM development specifically to exploit its various inherent design weeknesses. He is the main developer of the bsd-airtools project, a complete 802.11b penetration testing and auditing toolset, that implements all of the current methods of detecting access points as well as breaking wep on them and doing basic protocol analysis and injection. David has spoken at numerous international conferences on Wireless Security, has published multiple whitepapers, and is regularly interviewed by the media on computer security subjects.

h1kari is also the founder of Nightfall Security Solutions, LLC and one of the founding members of Dachb0den Research Labs, a

[redacted]-profit southern california based secur[redacted]esearch think-tank. He's also currently the chairman of ToorCon Information Security Conference and has helped start many of the security and unix oriented meetings in San Diego, CA.

TOP

presenter

Cameron "nummish" Hotchkies
0x90.org

Blind SQL Injection Automation Techniques

Due to improper software design and implementation practices, the number of web-based applications vulnerable to SQL injection is still alarmingly high. Yet the actual steps used to exploit these applications remain very tedious and repetitive. This presentation will focus on methods available to automate the task of exploiting blind sql injection holes. It will also feature a new tool, "SQueaL" and explain some of the research, used in the creation of this tool as well as ideas for expansion on the tool or other uses of the core libraries developed.

Cameron Hotchkies, aka nummish, is a member of the 0x90.org digital think-tank and head developer of the new blind injection tool, SQueaL. In his non-free time, he works as a web-application developer and has witnessed (and had to repair) great atrocities in web application design. This has left him a bitter and frail shell of his former self. Some people have suggested he get out more. He is currently struggling to write code to teach him how to properly pronounce the word "about". This will be his first time speaking at DEFCON.

TOP

presenter

Thorsten Holz
Laboratory for Dependable Distributed Systems (RWTH Aachen University)

Dipl.-Jur. Maximillian Dornseif
Laboratory for Dependable Distributed Systems (RWTH Aachen University)

Christian Klein
University of Bonn

NoSEBrEaK—Defeating Honeynets

Honeynets are one of the more recent toys in the white-hat arsenal. They are usually assumed to be hard to detect and attempts to detect or disable them can be unconditionally monitored. Sometimes it is even suggested that deploying honenets is a way to incerase security. We scrutinize this assumption and demonstrate a method how a host in a honeynet can be completely controlled by an attacker without any substantial logging taking place. We show how to detect honeynets, circumvent logging on a honeynet and finally 0wn a honeynet hard disabling all of a honeypots security features and present the tools to do so.

While being fairly technical the a basic knowledge how shellcode and the like works should be enough to follow the talk.

Thorsten Holz is a research student at the laboratory for dependable distributed systems at RWTH Aachen University where he is trying to bring a solid scientific foundation to Honeynet research.

Maximillian Dornseif and Christian N. Klein have studied computer science at the University of Bonn, Germany; Dornseif also holds a degree in laws. Both are involved in computer security and the German computer underground, namely the Chaos Computer Club, for a long time and are doing security consulting together since the late nineties. Their clients include the industry like Deutsche Telekom and T-Mobile but also government.

TOP

presenter

IcE tRe

Virus, Worms and Trojans: Where are we going?

It seems that the major target of most online bugs is actually quite the same. Over and over again the uninspired, pop the box, seems to be what most writers are after.

In this talk I will explore a bit of virus history in relation to goals, starting with older viral intentions, moving to what appears to be the intentions today and what possibly could be the intentions tomorrow.

This talk will be fairly abstract and I will setup the examples that I use so no previous knowledge will be needed other than a basic idea of how viruses work and what damage they can cause. This information, most people already have from the coverage gleaned from your average newscast, if not other places.

This talk in particular, should appeal to the broadest audience.

IcE tRe, Like many of the people attending DefCon has been involved with networking/internet/'new media' since the early 90's. Working with 2 major unnamed ISP over the years has helped these companies weather the storm of the past 10 years of viruses, ddos attacks and various other security problems.

TOP

presenter

Dan Kaminsky
Senior Security Consultant, Avaya Enterprise Security Practice

Black Ops of TCP/IP 2004

Continuing the research done in previous years on advanced protocol manipulation and the high speed evaluation of large network characteristics, this year's Black Ops of TCP/IP goes into new territory with a deep analysis of the Domain Name System. A core element of the TCP/IP application suite, it is everywhere—and there is unexpected power contained within.

- Interesting Facets of the Global DNS Architecture: A high speed scanner for DNS servers, modeled after my TCP scanner "scanrand", recently executed several Internet-scale sweeps of the net. Surprising results, with direct implications for computer forensics operations, will be discussed and analyzed.
- Distributed, High Speed, Large File Dissemination via DNS, A.K.A. "Reinventing the Square Wheel." Although there have been previous attempts to serve files over the DNS architecture, none have been even remotely usable. I will discuss a new approach that, through its significant performance improvement, is indeed remotely usable.
- One-To-Many Streaming Data Dissemination over DNS: The previous system maximizes speed at the expense of making streaming impossible. We will discuss an interesting alternate approach that almost usefully distributes streaming audio data to endpoints via their DNS queries.
- SSH over DNS: I will demonstrate a cross-platform, userspace mechanism for moving SSH data over DNS queries. This has implications for captive wireless portals, which often allow bidirectional DNS traffic.
- To complete this work, some enormously complex data needed to be understood, and tools were worked with and written towards that end. Experimental 3D information visualization mechanisms and tools are thus available to be demonstrated, extending from using a 3D renderer usually

used for MRI medical data as a generic static 3D canvas to using a custom OpenGL particle plotter to dynamically plot multidimensional factors of incoming data streams. A number of other topics will be raised as well, including:

- Uses and abuses of remotely visible incrementers and decrementers (such as the IPID field in many TCP/IP stacks, and initial TTL values on arbitrary DNS queries)
- Uses of generic packet race conditions, whereby useful information can be gleaned from which packet of a relatively large set effects the state change
- Protocol transliteration between TCP and UDP, allowing unreliable communication over what appears to be a TCP session, and allowing reliable data to be transmitted, with zero data expansion, over a UDP link
- Potential solutions to the SSH bastion host security problem, whereby the invocation of remote ssh binaries at a firewall or "bastion host" opens up a single point of major failure for a server infrastructure.

Dan Kaminsky, also known as Effugas, is a Senior Security Consultant for Avaya's Enterprise Security Practice, where he works on large-scale security infrastructure. Dan's experience includes two years at Cisco Systems designing security infrastructure for large-scale network monitoring systems, and he is best known for his work on the ultra-fast port scanner scanrand, part of the "Paketto Keiretsu", a collection of tools that use new and unusual strategies for manipulating TCP/IP networks. He authored the Spoofing and Tunneling chapters for "Hack Proofing Your Network: Second Edition", and has delivered presentations at several major industry conferences, including Linuxworld, DefCon, and past Black Hat Briefings. Dan was responsible for the Dynamic Forwarding patch to OpenSSH, integrating the majority of VPN-style functionality into the widely deployed cryptographic toolkit. Finally, he founded the cross-disciplinary DoxPara Research in 1997, seeking to integrate psychological and technological theory to create more effective systems for non-ideal but very real environments in the field. Dan is based in Silicon Valley.

TOP

presenter

Jesee Krembs (aka Agent X)
Acting Operation Manager, The Hacker Foundation

Nicholas Farr
Acting Secretary, The Hacker Foundation

The Hacker Foundation: An Introduction

The Hacker Foundation (THF) is a non-profit organization dedicated to establishing and maintaining a research and service organization to promote and explore the creative use of technological resources. Simply put, we want to help people do useful things with technology. This announcement is a formal launch of the foundation. There will be a brief statement about the foundation's goals, operations and how the foundation can work for you.

Jesse Krembs is a Defcon Speaker Goon. He's a cofounder of The Hacker Foundation.

Nicholas Farr: After an academic career focusing on memetic sociology and HCI, most of Nicholas Farr's professional career has been in non-profit management. Administrative work in academia, public radio and computer recycling strengthened his ability to navigate difficult bureaucratic situations. He works on The Hacker Foundations administrativa between MBA classes, press assignments and accounting work for a defense contractor

in Michigan.

TOP

presenter

Adam Laurie
CSO and Director of AL Digital Ltd

Martin Herfurt
Researcher, Salzburg Research Forschungsgesellschaft m.b.H and Lecturer. Salzburg University of Applied Sciences and Technologies

Bluesnarfing—The Risk From Digital Pickpockets

In November 2003, Adam discovered serious flaws in the authentication and data transfer mechanisms on some bluetooth enabled devices, and, in particular, mobile phones including commonly used Nokia, Sonv Ericsson and Motorola models. Shortly thereafter, Martin Herfurt of Salzburg Research Forschungsgesellschaft mbH expanded on these problems, and teamed up with Adam to investigate further.

This talk will cover the issues arising out of these flaws, including loss of personal data, identity theft, phone tapping, tracking, fraud and theft of service. The threat to individuals and corporates will be examined, and statistics and examples from the real world presented, as well as live demonstrations of each of the problems. Details of how the industry reacted, what they did, didn't and should have done will also be discussed.

This will be a fun talk and a real eye-opener for those with bluetooth enabled devices.

For further background information on the issue, see:
http://www.thebunker.net/release-bluestumbler.htm

Adam Laurie is Chief Security Officer and Director of AL Digital Ltd. and The Bunker. He started in the computer industry in the late Seventies, working as a computer programmer on PDP-8 and other mini computers, and then on various Unix, Dos and CP/M based micro computers as they emerged in the Eighties. He quickly became interested in the underlying network and data protocols, and moved his attention to those areas and away from programming, starting a data conversion company which rapidly grew to become Europe's largest specialist in that field (A.L. downloading Services). During this period, he successfully disproved the industry lie that music CDs could not be read by computers, and, with help from his brother Ben, wrote the world's first CD ripper, 'CDGRAB'. At this point, he and Ben became interested in the newly emerging concept of 'The Internet', and were involved in various early open source projects, the most well known of which is probably their own—'Apache-SSL'—which went on to become the de-facto standard secure web server. Since the late Nineties they have focused their attention on security, and have been the authors of various papers exposing flaws in Internet services and/or software, as well as pioneering the concept of re-using military data centres (housed in underground nuclear bunkers) as secure hosting facilities. Adam has been a senior member of staff at DEFCON since 1997, and also acted as a member of staff during the early years of the Black Hat Briefings.

Martin Herfurt is a researcher at the Salzburg Research Forschungsgesellschaft m.b.H and lecturer in Telecommunications Engineering Degree Program at the Salzburg University of Applied Sciences and Technologies.

He completed his Telecommunications Engineering Degree at the Salzburg University of Applied Sciences and Technologies in 2001. Alongside his study Martin was involved in numerous

industry projects, providing him with commercial programming practise.

In 2000 Martin followed up his formal study with a four-month internship at the telecommunications institute of TELCOT institute in San Ramon, California, USA.

Since the second half of 2000 Martin has been working as a full time researcher at Salzburg Research Forschungsgesellschaft m.b.H. His project responsibilities range from the co-ordination of a European IST project with a total budget of over 5 million Euro to software agents development.

Together with a Salzburg Research colleague, Martin began in the summer of 2003 a class on mobile data services at the Salzburg University of Applied Sciences and Technologies.

Martin is also currently working on a PhD in computer science at the University of Salzburg.

As part of his fascination with the rapid development in computer programming Martin has become a regular participant in the Chaos Communication Congress which is a yearly meeting of the German hacker association CCC.

TOP

presenter

j0hnny long
ihackstuff.com

Google Hacking][- The Return of the Googledorks

Google hacking is not new, but it's back and deadlier than ever. This talk is the follow-up to last years very successful talk "Watching the Watchers". Attendees will learn the tricks and tactics that any self-respecting Google hacker should know. Expanded extensively since last year, the techniques and always killer examples from the "googledorks" database are always a crowd-pleaser. Witness how sites from all over the net fall victim to seemingly impossible searches from hackers armed with only the world's hottest search engine. A special "security" section this year covers how to find everything from usernames and passwords to live IDS data, live vulnerability scanner output and SQL injection points. This talk intends to spread the word and help protect the security community from this dangerous and eye-opening form of information leakage.

Johnny Long "sold out" many years ago by accepting an I.T. position within a major international company. By promptly securing each and every site he breaks into, Johnny has managed to maintain his friendships with hackers on both sides of the security fence. Regardless of the color of his hat, Johnny is still passionate about hacking, and it shows through his work, his website and especially through his presentations which consistantly secure rave reviews.

TOP

presenter

Lucky 225
Default Radio

Strom Carlson

Phreaking in the Age of Voice Over IP

Phreaking in the age of Voice Over IP? What the hell is Voice Over IP? If you're asking this question and you're interested in phones and thought phreaking was dead back in the early '80s when blueboxing died, or 2002 when AT&T killed redboxing on long distance calls then this is the speech for you. Or if you know what VoIP is but want to know how the hell it has any impact on

phreaking you should also attend. This talk intends to educate it's audience on the new age phreakers. Most of the discussion will involve a detailed explanation of Calling Party Number(CPN), ANI, and Caller ID, and the differences between all three, we will also be covering the basics of phreaking with Voice Over IP technology, Asterisk, and VXML.

Not all of this presentation will be dealing with VoIP, this is a basic new age phreaking presentation that will show the latest techniques that phreaks are using today—it's not just about free calls either, hell you get that with VoIP anyways! You will learn not only why VoIP is important, but such things as Spoofing Caller ID(and no we don't mean orangeboxing, Social Engineering Telus, our methods are simple to use and will cost as little as $15/month)

As technology is rapidly changing, so is our phone system. We will be discussing a basic over view of Voice Over IP and some of the services provided by many of these so-called "Broadband phone companies." We will also be discussing Calling Cards that use VOIP technology to provide cheaper rates to their customers. We intend to explain how VoIP is changing the phone system and making it very easy for the every day consumer to spoof Caller ID by spoofing Calling Party Number(CPN), and how this can be exploited to circumvent security in such things as Voicemail, Credit Card Activations, and even Telephone company numbers that when you call from your "own phone" will give you complete control over your dial-tone telephone line. We also plan on showing how easy it is to get around services like "Call Intercept" without even spoofing Caller ID. We will also be discussing why *67 and Complete Caller ID block features offered from the phone company are not adequate privacy protection as anyone can still get your phone number when you call them with your number blocked, we'll of course describe how this can be possible. As time permits there may very well be much more, you wont want to miss this presentation.

Lucky225 is the co-host of an internet streaming radio show 'Default Radio' that streams on Rant Radio a free non-profit shoutcast server that has been running for 6 years). He has been a writer for 2600 magazine since 1999 and has spoken at both H2K2 and Defcon 11. He has been an avid phone phreak since his early teens in High School and has much experience with the telephone system and a wide variety of knowledge ranging from regular telephones, payphones, cell phones, and voicemail systems to ANI, Caller ID, PBX's, switches, VoIP and much more.

Strom Carlson is one of the last true phone phreaks; he has an intense interest in the structure and history of the telephone network and an intense distaste for fraud, theft, and vandalism. He collects all things related to telephony (including recordings), and although he is rapidly running out of space in which to store his many cubic meters of telephone equipment, he will eagerly and compulsively snap up anything made or published by Western Electric if given the chance. He encourages all phone phreaks and interested parties to learn what they're really talking about; he also encourages you to listen to everything on http://www.phonetrips.com/ and to poke around http://www.stromcarlson.com/

presenter

TOP

Kevin Mahaffey
Flexilis

[redacted]mile, You're on Candid Camera: The [redacted]nging Notions of Surveillance in Postmodern America

Recently, surveillance has become somewhat of a pop-culture fascination. From the Reality TV shows permeating every network's line up to the webcam phenomenon of the late 1990s, surveillance has become more a source of entertainment than ever before. Benjamin Franklin's quote, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety," has long served to exemplify the American, "Big Brother," notion of surveillance: that the government is the main aggressor and seeks to take away privacy and thereby, liberty. My talk will contrast traditional perceptions of surveillance in American culture with new notions brought forth in the emerging digital economy. The privacy of individuals is being bought from individuals through tangible or intangible rewards and resold as demographic data to the highest bidder. Instead of resisting the reduction of privacy, people are embracing surveillance as a benign improvement of everyday life. If we continue such a trend, will society be better for it, or will ubiquitous surveillance serve to implement Orwell's nightmare in 1984?

Kevin Mahaffey is an Electrical Engineering student at the University of Southern California. He has conducted extensive research regarding the sociological effects of the growth of commercial surveillance in American culture. When not confusing sociology with technology he is the Director of Software Development for Flexilis and is currently developing a few Bluetooth security tools hopefully to be released this year at Defcon. He also writes the occasional article for DailyWireless.com and has 6 years of experience working in commercial internet technology.

TOP

presenter

Nick Mathewson
Lead Developer, Mixminion and Core Developer, Tor Anonymyzing Proxy

Snake Oil Anonymity: How To Spot It, And How Not To Write It

Much software that promises "anonymity" fails to deliver, as witnessed by a succession of compromised file-trading networks, back-doored communications systems, overhyped vapornets, and insecure "improvements" on existing remailer networks. I'll discuss a bunch of allegedly anonymous systems, and explain how a clever attacker can defeat each of them. Audience members will learn to recognize the warning signs of broken anonymity in anonymous communications and P2P; and will learn a few principles to help them design the anonymity properties of their own systems.

Nick Mathewson is one of the main designers on Type III (a.k.a. Mixminion), the protocol that will replace the one currently used by the Mixmaster anonymous remail He is also the lead developer of the Mixminion software, and a core developer on the Tor anonymizing proxy. He lives in Cambridge, MA.

TOP

presenter

Rebecca Mercuri, Ph.D.

Hack the Vote: Election 2004

In the rush to solve problems that emerged from Florida's Presidential election dispute in 2000, computerized voting systems have been deployed in unprecedented numbers. Estimates indicate that 30% of the USA will be voting on fully

electronic equipment offering no capability for independent recounts, and another 50% of the country will be casting ballots tabulated by computer-based scanners. Vendors and promoters of these systems have made promises of reliability, accuracy and accessibility. Yet evidence from the 2004 primary season and earlier uses in 2002 and 2003 elections have demonstrated malfunctions resulting in irretrievable loss of vote data, usability issues including county-wide denial of service incidents, and fraud allegations due to software substitutions. This talk will explore the vulnerabilities of electronic voting systems to insider and outsider attacks, along with the possibilities and ramifications of large-scale vote fraud in the 2004 election and beyond.

Dr. Rebecca Mercuri became an overnight celebrity during the media frenzy that ensued when the U.S. Presidential election ended in a dead heat in November 2000. A few weeks earlier, she had successfully defended her Doctoral Dissertation "Electronic Vote Tabulation: Checks and Balances" at the University of Pennsylvania, and then found herself writing testimony in the now-legendary Bush v. Gore case that was working its way through the legal system. Her testimony was presented to the U.S. 11th Circuit Court of Appeals and referenced in the briefs to the U.S. Supreme Court. Since then, she has provided formal testimony on voting systems to the House Science Committee, Federal Election Commission, U.S. Commission of Civil Rights, and the U.K. Cabinet, has been quoted in the U.S. Congressional Record, and has played a direct role in municipal, state, federal, and international legislative initiatives. Rebecca's comments on election technology are frequently cited by the media, and she authors the quarterly "Security Watch" column in the Communications of the Association for Computing Machinery (archived at www.notablesoftware.com). Having recently completed a research fellowship at the John F. Kennedy School of Government in their Belfer Center for Science and International Affairs, Dr. Mercuri will be moving to Harvard University's Radcliffe Institute in the Fall.

Bev Harris, author of "Black Box Voting: Ballot-Tampering in the 21st Century," began writing on the subject of electronic voting machines in October 2002. Her investigative journalism has since been cited in The New York Times (three times), and on CBS, Fox News, and CNN. In writing Black Box Voting, Harris spent over two thousand hours researching voting machines, and interviewed hundreds of witnesses including many election officials and even voting machine programmers who work directly for the firms that build these machines. During the course of writing Black Box Voting, Harris discovered that one of the largest voting machine companies, Diebold Election Systems, had committed a massive security breach, leaving thousands of sensitive voting system program files on an unprotected Web site. These files have now triggered a national investigation and activism movement to restore clean, trustworthy voting systems.

TOP

presenter

Doug Mohney
Editor, VON Magazine and contributor to Mobile Radio Technology Magazine

DIGEX—At the Dawn of the Commercial Internet

Hearken back to the days of yesterday, circa 1993, when men were men, the Internet "backbone" was T3 and run by ANS, and a few brave start-up companies around Washington D.C. were fighting the phone company and each other to build the "commercial" Internet. One of them, DIGEX, literally started out in the founder's basement in '92 and rapidly grew to be a major

force in what ultimately became known as web hosting. DIGEX "invented" web hosting, was first to light-up mtv.com, collected a whole bunch of dot.gov sites including one for a Langley, VA-based agency, and grew into a 600+ person company with a 1996 IPO. Doug Mohney was employee #10 at DIGEX and witnessed a whole bunch of stuff from late '93 through 1997.

Doug Mohney was employee #10 at DIGEX. He is often confused with employee #1 (Doug Humphrey; Mohney does not have Humphrey's beard, wife, or bank balance). Currently, he is online editor for VON Magazine and a contributor to Mobile Radio Technology magazine. His first BOARDWATCH article, a history of DIGEX, was published in 1997 to critical acclaim by most and heartburn by a few.

TOP

presenter

Brett Moore
CTO, security-assessment.com

Shoot the Messenger—Using Window Messages to Exploit Local win32 Applications

The windows GDI interface uses messages to pass input and events to windows. As there is currently no way of determining who the sender of the message is, it is possible for a low privileged application to send messages to and interact with a process of higher privilege.

This presentation will cover in details some of the flaws exposed through these messages, and demonstrate how they can be exploited to conduct privilege escalation and other attacks. Attendees should be familiar with the shatter attack concept and may want to review the following documents before attending:

- Shatter Attacks—How to break Windows, Chris Paget
- Win32 Message Vulnerabilities Redux, Oliver Lavery
- Shattering by Example, Brett Moore

Brett Moore leads the security research and network intrusion teams at security-assessment.com. He has been credited with the discovery of multiple security vulnerabilities in both private and public software vendors' products including Microsoft web products.

TOP

presenter

Todd Moore
NetWitness Product Manager
Forensics Explorers, ManTech International Corp.

Cracking Net2Phone

Do you think using Internet Telephony is more secure than a regular phone? Think again! Internet Telephony is becoming more common and those that think it is safer from wiretaps than regular phone communications are wrong. This presentation will demonstrate how to decrypt Net2Phone's dialed phone numbers, and playback fully reconstructed audio conversations from network packet captures. Included will be a demonstration of NetWitness 5.0's VOIP playback capability.

Todd Moore is the product manager of NetWitness®, a commercially available cyber-forensics tool. Moore's extensive knowledge of Internet technologies, network security, and software development helped make NetWitness® well-known for providing powerful insight into network traffic.

Moore has over ten years of professional experience in the field

[redacted] network security and has extensive exp[redacted]ce developing commercial software applications. He has a bachelor in Computer Science from Old Dominion University and is a Microsoft Certified Solution Developer (MCSD). Moore started with CTX Corporation in 1996 securing global intranets and designing network security software to help audit and analyze network traffic. He joined Forensics Explorers, a Division of ManTech IS&T, as Director of Software Development in 1999 and later became the NetWitness® Product Manager.

Moore teaches classes on designing quality software and has made numerous television appearances presenting the latest in technology trends. He has two patent pending inventions in the field of cyber-forensics. Moore resides in the greater Washington, D.C. area.

TOP

presenter

Robert Morris
former chief scientist for the NSA

The History of the Future

Mr. Robert Morris received a B.A. in Mathematics from Harvard University in 1957 and a M.A. in Mathematics from Harvard in 1958. He was a member of the technical staff in the research department of Bell Laboratories from 1960 until 1986. On his retirement from Bell Laboratories in 1986 he began work at the National Security Agency. From 1986 to his (second) retirement in 1994, he was a senior adviser in the portion of NSA responsible for the protection of sensitive U.S. information.

TOP

presenter

Mudge

Counter Intelligence/Counter Espionage - How To Engage and Avoid In The Corporate Network (An Operatives View)

TOP

presenter

Brett Neilson

The Advantages of Being an Amateur

For close to 100 years amateurs have been working with radios and sending transmission all over the world. The dawn of the information age has inspired many new technologies and advancements in communication; and amateur radio is no exception. Today's modern amateur radio operators are building wireless networks and enjoying several advantages over their unlicensed counterparts. This presentation will review some of these advantages as well as talk about some of the newer areas of interest including HSMM and APRS.

Brett L. Neilson is a network security and systems engineer with a strong background in the wireless industry. Currently he is working for one of the world leaders in Intrusion Prevention supporting clients with network security related issues. He previously worked for one of the leading wireless communication companies as a Senior Systems Administrator and RF Field Technician. While there he worked to develop, deploy, and maintain their national infrastructure. Some of his work is currently published in two information security related books, Maximum Wireless Security & Maximum Security 4th Edition. Mr. Neilson is a former member of the North Texas FBI Emergency Response Team (InfraGard) and is an FCC-licensed amateur radio operator. In these roles he has worked with multiple government agencies providing emergency communication assistance and coordination. Mr. Neilson's broad knowledge and experience has allowed him to be involved with many organizations; providing network and security related solutions.

presenter

NeOnRa1n

Jon McClintock

Better than Life - Manipulation of The Human Brain With The Use of Machines

Just as the understanding of the human genome will soon allow us to control the essential physical processes that create our bodies, knowledge in the manipulation of the human brain with the use of machines will give us the ability to reconstruct ourselves mentally in a way that has only been imagined by the most outlandish of science fiction writers.

This speech will take you through the history of altered states, from ritual and religion, to drugs and chemicals right through to the future of the technology. You will be introduced to some of the mechanical tools that have existed for years that have only be talked about and affordable by a few. As well as showing you how to build your own home-brew mind machine, the presentation also will also be discussing other brain manipulating technologies.

NeOnRa1n has been involved in the computer underground for a decade and is also a world traveler and slacker extraordinaire. In her pursuit to understand how brain waves work, she has spent extensive time in a Buddhist hermitage where she was able to experience meditation first hand. Among her current projects is her quest to find a way to replace expensive chemical antidepressants with affordable Œdigital drugs.

Several years back, Jon McClintock received a Computer Science degree from a university of no consequence. Since then, he's bounced back and forth several times between enterprise and embedded software development. Equally comfortable debugging 8-bit microcontrollers using a logic analyser as he is developing highly available, multi-tier applications, Jon enjoys manipulating minds both large and small.

presenter

Annalee Newitz
Policy Analyst, Electronic Frontier Foundation

Wendy Seltzer
EFF Staff Attorney specializing in IP

Kevin Bankston
Equal Justice Rights Fellow at EFF specializing in privacy/surveillance

Seth Schoen
Staff Technologist, Electronic Frontier Foundation

Jennifer Stisa Granick
Executive Director of

Ask EFF: Discussion and Q/A on the State of Digital Liberties

The Electronic Frontier Foundation (EFF) is one of the premiere digital liberties organizations in the world. We fight for freedom of expression on the Internet, the right for researchers and consumers to reverse-engineer their devices, expansion of the public domain, and electronic privacy and anonymity. On this panel, three representatives of EFF will discuss the latest developments in digital liberties, including free speech on the Internet, copyright infringement lawsuits, and electronic surveillance laws under the USA-PATRIOT Act. Audience participation and discussion are part of the deal. Come with your legal and policy questions this is your chance to ask EFF!

Annalee Newitz (www.techsploitation.com) is EFF's Policy Analyst. She talks to the media, conducts research, and writes policy recommendations and white papers. Although she is a digital rights generalist, her special areas of interest are expanding the public domain, free speech, and network regulation. Previously, she was Culture Editor at the San Francisco Bay Guardian, and was the recipient of a Knight Science Journalism Fellowship in 2002. She writes a syndicated column called Techsploitation and

the Center for Internet and Society (CIS)

[redacted] published regularly in Wired, Security Fo[redacted]and Salon. In her off-hours, she edits an indie magazine called Other (www.othermag.org). She has a Ph.D. in English and American Studies from UC Berkeley.

Wendy Seltzer is a Staff Attorney with the Electronic Frontier Foundation, specializing in intellectual property and free speech issues. As a Fellow with Harvard's Berkman Center for Internet & Society, Wendy founded and leads the Chilling Effects Clearinghouse, helping Internet users to understand their rights in response to cease-and-desist threats. Prior to joining EFF, Wendy taught Internet Law as an Adjunct Professor at St. John's University School of Law and practiced intellectual property and technology litigation with Kramer Levin Naftalis & Frankel in New York. Wendy speaks frequently on copyright, trademark, open source, and the public interest online. She has an A.B. from Harvard College and J.D. from Harvard Law School, and occasionally takes a break from legal code to program in Perl.

Kevin Bankston, an attorney specializing in free speech and privacy law, is the Electronic Frontier Foundation's Equal Justice Works/Bruce J. Ennis Fellow for 2003-05. Before joining EFF, Kevin was the Justice William J. Brennan First Amendment Fellow for the American Civil Liberties Union in New York City. At the ACLU, Kevin litigated Internet-related free speech cases, including First Amendment challenges to both the Digital Millennium Copyright Act (Edelman v. N2H2, Inc.) and a federal statute regulating Internet speech in public libraries (American Library Association v. U.S.). Kevin received his J.D. in 2001 from the University of Southern California Law Center, and spent his undergraduate years at the University of Texas in Austin. Kevin's fellowship at the EFF is sponsored by Equal Justice Works Fellowships and the Bruce J. Ennis Foundation.

Seth Schoen created the position of EFF Staff Technologist, helping other technologists understand the civil liberties implications of their work, EFF staff better understand the underlying technology related to EFF's legal work, and the public understand what the technology products they use really do. Schoen comes to EFF from Linuxcare, where he worked for two years as a senior consultant. While at Linuxcare, Schoen helped create the Linuxcare Bootable Business Card CD-ROM. Prior to Linuxcare, Schoen worked at AtreNet, the National Energy Research Scientific Computing Center at Lawrence Berkeley National Laboratory, and Toronto Dominion Bank. Schoen attended the University of California at Berkeley with a Chancellor's Scholarship.

Jennifer Stisa Granick is Executive Director of the Center for Internet and Society (CIS). She teaches, speaks and writes on the full spectrum of Internet law issues including computer crime and security, national security, constitutional rights, and electronic surveillance, areas in which her expertise is recognized nationally. Previously, she founded the Law Offices of Jennifer S. Granick, where she focused on hacker defense and other computer law representations at the trial and appellate level in state and federal court. At Stanford, she currently teaches the Cyberlaw Clinic, one of the nation's few law and technology litigation clinics. Granick continues to consult on computer crime cases and serves on the Board of Directors of the Honeynet Project. She was selected by Information Security magazine in 2003 as one of 20 "Women of Vision" in the computer security

[redacted]field.

TOP

presenter

n0namehere

Real World Privacy, How to Leave Less of A Trail in Life

Like leaving breadcrumbs in the forest, individuals leave a data trail throughout their day. This talk will look at practical ways to leave a smaller data wake. Privacy isn't dead. Time, money and effort are needed to maintain and live outside the data collection mechanisms that are now
part of society.

Level of privacy achieved

How easy it is to lose one's privacy...

This is not a talk to look at the ways in which your data is shared, but a look at examples and methods by which one can minimize sharing the data in the first place. Topics to be covered include communications, money, medical, travel, shopping, rubbish and major life events. The key is to not leave any data, but, when one must leave data, leave it in a way which it won't trace back to you.

n0namehere started down the privacy route in the early 1990s after mistakenly hearing cell and cordless phone calls on his recently purchased scanner. Realizing the ease in which others could listen in on his life, this event led to a re-evaluation of his behavior which changed his life. He spreads the word among friends and family, encouraging many down the road to stronger privacy.

n0namehere is a big computer company survivor whose personal and professional work focuses on computer security and privacy issues ranging from running to designing to breaking systems, networks and applications. n0namehere has worked for Fortune 500 companies, consulted on hundreds of system and network designs and worked security/privacy issues during the Summer Olympic Games. n0namehere doesn't live in a cave but balances privacy and reality in his daily life.

TOP

presenter

Nothingface
Area 49

Automotive Networks

This presentation provides an introduction to the electronic networks present on late model automobiles. These networks will be described loosely following the OSI model of networking. Common uses of these networks will be presented, and the privacy implications of some uses will be questioned. The presentation will conclude with an introduction to OpenOtto, a free software and hardware project implementing the network protocols previously described.

Nothingface is formally educated in electrical and computer engineering and informally (i.e., not) educated in automotive maintenance and repair. He has been known to earn his keep doing software design, hardware design, and security consulting. Nothingface is currently employed designing hardware and software for two-way radio communication networks..

TOP

presenter

Sean O'Toole

Mutating the Mutators

Since the introduction of metamorphic stealth in the computer virus world, it has been suggested that the method can also be used to protect any, even legitimate, code. The only downfall of this technique is that how the engine manipulates the code remains constant. This allows the original code to be obtained by using an optimizer. The next step for this stealth method is to create an engine that will change how the code in manipulated. This speech will outline how to create an engine that integrates random code with alternate encoding of an instruction to create a semi-random set of instructions, which will fit into the metamorphic engine paradigm.

Sean O'Toole is fresh out of college for Computer Science and Mathematics. He has been playing around with viruses since high school and had also taken independent studies on computer viruses in college. As well as the above, he also helped institutions such as NCAR use Artificial Life Algorithms for modeling.

TOP

presenter

Laurent Oudot
Computer Security Engineer, Rstack

Digital Active Self Defense

In a cyberworld of never ending struggles, defenders might have a new weapon in the future in order to defeat attackers. This talk will focus on those possibilities called: digital active (self) defense.

For example, after a compromission, a victim might want to react and even hack back the aggressor. This potentialy natural idea might not be legal most of the time, and many drawbacks exist. Think about the case where an aggressor would use a connectionless attack ; the source of the intrusion could not be the real one (spoofing) so that a retaliation would not be a good idea!

This presentation aims at sharing ideas about digital active self defense to focus on the essential current questions: Why and when should we try to react like that? How could we play with incoming aggressors in order to limit the risks? What would be the limitations of such solutions (legal and technical issues)?

As a conclusion, we will evaluate the potential hidden by those technologies used for Information Assurance and imagine future kind of solutions, digital active self defense systems.

Laurent Oudot (http://rstack.org/oudot/) is a french security expert currently employed by the CEA (Commissariat Energie Atomique) which is the equivalent of the US Dept Of Energy. On his spare time, he is also a member of a security group called "Team Rstack" composed of security addicts and geeks. Laurent's research focus on defensive technologies highly closed to blackhats activities like honeypots, intrusion prevention, intrusion detection, firewalls, sandboxes, mandatory access control, etc.

Laurent is the (co-)author of several research papers recently published and released on Securityfocus, Institute of Internal Auditors UK, MISC magazine and Linux Magazine France. He has presented at national and international conferences and meetings

[redacted] as Cansecwest (Vancouver, 2004), Eu[redacted]sec (Paris, 2004), BlackHat Asia Briefings (Singapore, 2003), Honeynet Project Meeting (Chicago, 2003), Libre Software Meeting (Metz, 2003), FOSDEM (Bruxelles, 2003), etc.

He co-organized security events such as the Libre Software Meeting (co-chairman of the Security Topic with Bradley Spengler from Grsecurity, 2002), Symposium Securite des Technologies de l'Information et de la Communication (SSTIC 2003 and 2004), a Computer Security Summer School (2004), etc.

Laurent has taught network and system security in high schools for engineers and has managed numerous security projects on the last 7 years.

Recently with Nicolas Fischbach, he co-created the French Honeynet Project which is part of the international Alliance of honeynets. Now, Laurent is a member of the Steering Committee of the Honeynet Project leaded by Lance Spitzner.

TOP

presenter

Dr. Larry Ponemon
Chairman of Ponemon Institute

The DEFCON Surveys

Ponemon Institute recently conducted two independent surveys concerning individual privacy rights. The first study examines the public's perception concerning the safety and security of e-voting systems. The second study explores the public's reaction to the U.S. government's CAPPS II proposal that requires airlines to share personal data about passengers with the Department of Homeland Security. Dr. Larry will present an analysis that compares and contrasts the "DEFCON" community to members of the general public in terms of perceptions and beliefs about privacy issues.

Dr. Larry Ponemon is Chairman of Ponemon Institute, a "think tank" dedicated to privacy, data protection and information security policy research. He is also serves as an adjunct professor of privacy and ethics at Carnegie Mellon University's CIO Institute and CyLab.

TOP

presenter

Michael T. Raggo
Principal Security Consultant, VeriSign, Inc.

Steganography, Steganalysis & Cryptanalysis

This presentation will present Steganography and techniques for Steganalysis (identifying files with hidden messages). A review of Steganography will provide the basis for identifying and dissecting carrier files. There will also be a demonstration of carrier file analysis and disection. There will also be a demo of my new Steganography detection program, StegSpy. Cracking and reverse-engineering Steganography programs will also be covered. A cryptanalysis case study will review the steps necessary to reverse engineer and reveal a hidden message. Additionally, other steganalysis and password cracking tools will be highlighted.

Michael T. Raggo (CISSP, IAM, CCSA, CCSE, CCSI, MCP, SCSA) is a Principal Security Consultant for VeriSign, Inc. As a consultant, Mr. Raggo architects and deploys firewalls, intrusion detection systems, and PKI solutions. In addition, he also performs security assessments, penetration tests, and forensics investigations. He is also an instructor for VeriSign's suite of security classes

including Applied Hacking and Countermeasures and the author of StegSpy, a steganography detection program.

Mr. Raggo is a guest speaker at nationwide conferences including SANS, WebSec and InfoSec. Prior to joining VeriSign, Mr. Raggo was Supervisor of System Administration for www.nasdaq.com at the NASDAQ Stock Market. Mr. Raggo has 15 years experience in the information systems field including experience as a UNIX System Administrator, Network Administrator, and Firewall Administrator.

Mr. Raggo conducted graduate work in Information Systems at Johns Hopkins University. Prior to that, he earned his BSET in Electrical Engineering from Rochester Institute of Technology.

TOP

presenter

Michael Rash

Advanced Netfilter; Content Replacement (ala Snort_inline), and Port Knocking Based on Passive OS Fingerprinting

The boundaries between network access control devices and network monitoring devices are steadily becomming blured. Network intrusion detection systems are moving into the realm of not only monitoring network traffic, but also modifying it either through dynamic reconfiguration of firewall rulesets, spoofed session-busting traffic, or outright alteration of application layer data (ala Snort_inline). Firewalls themselves are also getting smarter about protocol validation and application layer data. This talk will discuss two main topics; 1) a patch to the iptables string match extension in the Linux kernel that allows iptables to perform the same data substitution as Snort_inline but three times faster, and 2) a new tool called "fwknop" that implements port knocking authentication based on passive operating system fingerprints as detected via iptables log messages. The latter makes it possible to allow only, say, Linux systems to connect to your SSH daemon.

Michael Rash holds a Master's Degree in applied mathematics with a concentration in computer security from the University of Maryland. Mr. Rash works as a security research engineer for Enterasys, Inc. where he develops signatures and writes code for the Dragon IDS. Previous to Enterasys, Michael developed a custom host-based intrusion detection system for USinternetworking, Inc. which was deployed on over one thousand systems from Linux to Cisco IOS. Michael frequently contributes to open source projects such as Netfilter and Bastille-Linux, and has written security related articles for the Linux Journal, Sys Admin Magazine, and Information Security Magazine. He is also a co-author of the book Snort-2.1 Intrusion Detection published by Syngress (to be published in late May, 2004). Michael is the developer of two open source tools "psad" and "fwsnort" that are designed to tear down the boundaries between iptables and the Snort IDS. More information about Michael and his open source projects can be found at: http://www.cipherdyne.org/

TOP

presenter

Len Sassaman

Mixmaster vs. Reliable: A Comparison of Two Anonymous Remailer Applications

The "Type II" remailer network has been operating since 1995, providing strong anonymity email services to the public. We

recently performed an analysis of the anonymity provided by the two independent implementations of the Type II protocol. This is joint work with Claudia Diaz and Evelyne Dewitte, to be presented at the ESORICS conference in September.

This talk will discuss the methods used to evaluate the anonymity provided by Mixmaster 3.0 and Reliable 1.0.5. It will explain the threat models considered for email anonymity and known attacks agaist them, highlight the differences in the mixing algorithms used, identify potential areas of
weakness in the applications, and explain the reasoning behind the different design decisions in the two applications.

Len Sassaman is a communication security consultant specializing in Internet privacy and anonymity technologies. Formerly the security architect for Anonymizer and a software engineer for PGP Security, Len is now focusing on research in the area of practical attack-resistant anonymity systems which can be widely deployed and used by large groups. Additionally, Len is an anonymous remailer operator, and maintainer of the oldest actively-used anonymity software, Mixmaster.

TOP

presenter

Jason Scott
Webmaster,
TEXTFILES.COM,
Director, BBS
Documentary

Digitizations And Documentary

Jason Scott of TEXTFILES.COM, a site dedicated to the history of Dial-Up Bulletin Board Systems, embarked on a quest to film an all-inclusive BBS documentary in 2001. What started out as a one-year project grew to three, and what started as a two-hour film will be a six-hour series. Thousands of miles of travel and 200 interviews later, the production is now nearing the end of editing and the release date. Jason tells you what he learned, why you shouldn't hesitate to make your own projects, and the occasional story that technically can't be mentioned in the film.

Jason Scott is the creator and webmaster of TEXTFILES.COM, a website dedicated to collecting the files and related materials from the era of the Dial-up BBS. This website, originally built from files he collected as a BBS user in his early teens, has expanded to many gigabytes of data and now recieves thousands of visitors a day.

Inspired to create "the ultimate BBS list" from the hundreds on his website, he suddenly started recieving dozens of stories from BBS users and operators who found their old BBSes listed among others. Recogizing a missing piece in the story of computers, Jason used his dormant filmmaking skills (Emerson College Film Degree, 1992) to create this documentary.

TOP

presenter

Sensepost

When the Tables Turn

Until now network security defences have largely been about building walls and fences around the network. This talk revolves around spiking those walls & electrifying those fences! During this talk we will highlight techniques (and tools) that can be used to turn the tables on prospective attackers with passive-Strike-Back. We will explore the possibilities across the assesment spectrum responding to the standard assesment phases of Intelligence gathering, Reconnaissance & Attack with Disinformation, Misdirection, Camouflage, Obfuscation & Proportional Response.

Roelof Temmingh is the technical director of SensePost where his primary function is that of external penetration specialist. Roelof is internationally recognized for his skills in the assessment of web servers. He has written various pieces of PERL code as proof of concept for known vulnerabilities, and coded the world-first anti-IDS web proxy "Pudding". He has spoken at many International Conferences and in the past year alone has been a keynote speaker at SummerCon (Holland) and a speaker at The Black Hat Briefings. Roelof drinks tea and smokes Camels.

Haroon Meer is currently SensePost's director of Development (and coffee drinking). He specializes in the research and development of new tools and techniques for network penetration and has released several tools, utilities and white-papers to the security community. He has been a guest speaker at many Security forums including the Black Hat Briefings. Haroon doesnt drink tea or smoke camels.

Charl van der Walt is a founder member of SensePost. He studied Computer Science at UNISA, Mathematics at the University of Heidelberg in Germany and has a Diploma in Information Security from the Rand Afrikaans University. He is an accredited BS7799 Lead Auditor with the British Institute of Standards in London. Charl has a number of years experience in Information Security and has been involved in a number of prestigious security projects in Africa, Asia and Europe. He is a regular speaker at seminars and conferences nationwide and is regularly published on internationally recognized forums like SecurityFocus. Charl has a dog called Fish.

TOP

presenter

Wendy Seltzer
Staff Attorney,
Electronic Frontier
Foundation

Seth Schoen
Staff Technologist,
Electronic Frontier
Foundation

Hacking the Spectrum: Open Source Software vs. the Broadcast Flag

The FCC, at Hollywood's request, has mandated a broadcast flag for high-definition digital television (HDTV). By July 2005, it will be unlawful to sell devices that don't respond to a "do not copy" flag or that provide unencumbered high-definition digital outputs. The flag's "robustness" requirement will make it impossible to build an open-source HDTV version of the TiVo. This talk will demonstrate how these rules thwart user innovation, showing an open-source HDTV PVR (MythTV on Linux) you soon won't be able to build. We'll discuss the law and challenges to receiver regulation, and encourage people to get HDTV cards while they still can.

Wendy Seltzer, Electronic Frontier Foundation Staff Attorney
Wendy Seltzer is a Staff Attorney with the Electronic Frontier Foundation, specializing in intellectual property and free speech issues. As a Fellow with Harvard's Berkman Center for Internet & Society, Wendy founded and leads the Chilling Effects Clearinghouse, helping Internet users to understand their rights in response to cease-and-desist threats. Prior to joining EFF, Wendy taught Internet Law as an Adjunct Professor at St. John's University School of Law and practiced intellectual property and technology litigation with Kramer Levin Naftalis & Frankel in New York. Wendy speaks frequently on copyright, trademark, open source, and the public interest online. She has an A.B. from Harvard College and J.D. from Harvard Law School, and occasionally takes a break from legal code to program (Perl).

Seth Schoen, Electronic Frontier Foundation Staff Technologist
Seth Schoen created the position of EFF Staff Technologist, helping other technologists understand the civil liberties implications of their work, EFF staff better understand the underlying technology related to EFF's legal work, and the public understand what the technology products they use really do. Schoen comes to EFF from Linuxcare, where he worked for two years as a senior consultant. While at Linuxcare, Schoen helped create the Linuxcare Bootable Business Card CD-ROM. Prior to Linuxcare, Schoen worked at AtreNet, the National Energy Research Scientific Computing Center at Lawrence Berkeley National Laboratory, and Toronto Dominion Bank. Schoen attended the University of California at Berkeley with a Chancellor's Scholarship.

TOP

presenter

The Shmoo Group

featuring:
Bruce Potter, Beetle, Cazz, Bob Fleck, Eric Johanson, Mike Messick, Myles, Holt Sorenson Len Sassaman, and Rodney Thayer

Wireless Weaponry

From the same crazy folks who brought you Airsnort, Airsnarf, Bluesniff, Fine Tooth Comb, HotspotDK, and yes, the HackerBot, comes the annual deluge of wireless wackiness. The Shmoo Group takes a break from beer, Root-Fu, and their constant media-whore campaign to just give Shmoo shtuff away, and it's all wireless-related for you RF rogues. Updated hardware. Updated software. Blah, blah, same old boring sh—WAIT! What's this?! NEW hardware? NEW software? OMFG. Bow before the Sniper Yagi! Bork all sorts of "secure" wireless networks with new tools from the Shmoon! It's time to update your kick-ass arsenal, folks! If you're a "Wireless Warrior", TSG has your "Wireless Weaponry"—and a saved-for-DefCon announcement sure to make the Shmoo in you rejoice!

The Shmoo Group is a non-profit think-tank comprised of security professionals from around the world who donate their free time and energy to information security research and development. They get a kick out of sharing their ideas, code, and stickers at DefCon. Whether it's Root-Fu, lock-picking, war-flying, or excessive drinking, TSG has become a friendly DefCon staple in recent years past. Visit www.shmoo.com for more info.

TOP

presenter

Peter Silberman
Security Engineer, iDEFENSE

Richard Johnson
Senior Security Engineer, iDEFENSE

A Comparison of Buffer Overflow Prevention Implementations and Weaknesses

Buffer overflows are historically the most commonly exploited software vulnerability in the security world. The last year has seen effective automated attacks such as the MS Blaster worm and SQL Slammer worms. Due to the rapid growth of worm technology and readily available automated worm generation tools, the need for buffer overflow protection software has dramatically increased.

This presentation will give the attendee an overview of the methods used by current stack protection technology.

We will discuss the varying types of stack overflow protection available for the Linux and Windows operating environments and the weaknesses that lie within each implementation. This will also be the first public discussion of available third-party buffer overflow prevention software for the Windows operating system. The test suite used to analyze the exploitability of common

software vulnerabilities has been modified with specialized shellcode to be used against buffer overflow protection methods. A demonstration will be provided and the tool is available to attendees for future testing of protection software.

The attendee should have basic knowledge of buffer overflow exploitation, but the presentation will build on itself, and in the end offer a tool that anyone can use to test their buffer overflow protection software.

Peter Silberman is a Security Engineer at iDEFENSE. Peter works in the iDEFENSE labs where he conducts vulnerability research in between going to high school. He is especially interested in advanced exploitation of the win32 platform, buffer overflow protection methods, and windows forensic analysis. Peter has been a professional vulnerability researcher for a year, and has spent two or three years as an independent researcher.

Richard Johnson is a Senior Security Engineer at iDEFENSE. He works in the iDEFENSE Labs where he is responsible for conducting vulnerability research, malicious code analysis, and developing reverse code engineering tools and methodologies. Areas of interest include run-time process modification, live kernel patching, embedded systems reverse engineering, and seeing how much beer a man can drink in an evening.

With three years professional vulnerability research experience, and many more as a hobbyist, he is considered a valuable resource with a wide breadth of knowledge at iDEFENSE Labs.

TOP

presenter

spoonm
Digital Disaster Inc.

HD Moore
Hack Master Supreme

Bubonic Buffer Overflow

The Metasploit Framework has progressed from a simple network game to a powerful tool for administrators and security analysts alike. Over the past several months, the Framework has been enhanced with improved exploit techniques and a truly advanced suite of payloads. This presentation provides a background on what exploit frameworks are, what they can provide you, and why you should be using one. A live demonstration will highlight many of the advanced features of the Framework, describe how they can be used to accomplish a variety of tasks, and show that the technology for "hacking like in the movies" is already available today. Attendees will be provided with an early-access copy of version 2.2 of the Metasploit Framework; which includes a number of techniques and exploit modules that are not publicly available anywhere else. Additionally, this release is the first version of the Framework to include a development kit for creating your own custom modules.

Spoonm is currently pursuing a Bachelors degree in Software Engineering. Much to the detriment of his early morning classes, he is an active researcher in many different security areas, most notably in the exploitation and post-explotation process. He has developed several post-exploitation tools, and between working as a security consultant, and asm wielding, he currently spends most of his
time working on the Metasploit Framework.

HD Moore is one of the founding members of Digital Defense, a

[redacted]curity firm that was created in 1999 to p[redacted]ide network risk assessment services. In the last four years, Digital Defense has become one of the leading security service providers for the financial industry, with over 200 clients across 43 states. Service offerings range from automated vulnerability assessments to customized security consulting and penetration testing. HD developed and maintains the assessment engine, performs application code reviews, develops exploits, and conducts vulnerability research.

TOP

presenter

Joshua Teitelbaum
Lead Developer, CryptoMail.org

Peter Leung
Webmaster & Project Manager, CryptoMail.org

CryptoMail Encrypted E-Mail for All (Including Grandma)

Four years ago, CryptoMail introduced the first secure open source web based email solution. System administrators and hostile parties no longer had the ability to read a users email. With functionality similar to Hushmail, the world was introduced to an open source solution that they themselves could host.

At Defcon 12, CryptoMail.org will be releasing to the public a major advance in its technology. Users will now be able to transparently and securely communicate with PGP users. Users will be able import their private PGP key set upon account creation as well as external PGP public keys.

Architect Joshua Teitelbaum and project manager Peter Leung will present the overall design of the architecture, the infrastructure and the logistics of the upcoming CryptoMail Email System release. We will demonstrate the technology integration inside the new release for the first time. At the conference, you will have the chance to preview the new release.

Joshua Teitelbaum developed the CryptoMail Email System and founded CryptoMail.org in 2000. Joshua is the primary developer and technical lead of the Email system. He communicates with other developers and members around the world to discuss future features and improvements to the CryptoMail Email System. Besides information security, Joshua holds an active interest in building scalable trading systems for broker/dealers and portfolio managers.

Peter Leung joined CryptoMail.org in 2000 as the webmaster and the project manager.His main task in the organization is to direct, manage, and organize the software release process. Peter collaborates with other members to document the Email system and informs everyone about the organization's activities. Peter holds a BS en mechanical engineering, BS in mathematics, and MBA from SFSU

TOP

presenter

Richard Thieme
Thiemeworks

Quantum Hacking: In Search of a Unified Theory

The search for a unified theory of everything in contemporary physics stems in part from the fundamental inability to reconcile quantum physics and relativity theory. This has pushed research toward complex mathematical models such as string theory in an effort to model a single way of looking at everything.

The same can be said of the distribution of power in networks and hierarchies. The individual person looks like one kind of thing

[redacted] viewed in the context of a network and another kind of thing when viewed in the context of a hierarchy. This is analogous to describing a photon as both a particle and a wave. The context of our inquiry determines the content that results and the primary object of that inquiry, the "individual person," is revealed to be a social construction, not an empirical fact.

The lack of a unified theory of humanity and computing is one reason we experience cognitive dissonance today. The notion of the "individual person" is central to current debates about privacy, intellectual property, and the legality or illegality of network aggression ("black hat hacking"), but from the point of view of the distributed network, there is no individual person, there are only nodes in the network.

In addition, we all inhabit nodes in multiple networks simultaneously. We can field any network-determined identity we choose but we do not determine an individual identityuntil we choose a network identity. That choice is made in the moment in which we act, so paradoxically, while context determines content, choice is always prior to context and creates it. Until we choose, it is impossible to predict with certainty which choice will be made and therefore what identity will be fielded. This is why security based on perimeter defense or authentication is by definition a failed model.

This analysis has profound implications for traditional notions of free will, loyalty, citizenship, and security. It explains why hackers who evolve from working in online meritocracies to working in corporate structures literally become different people. It explains why a disciplined hierarchical structure like the military can use network centric warriors and fight networks with networks while maintaining a basic identity—for the moment—as the machinery of a nation state. It explains why perspective is worth fifty points of IQ and why perception management creates perspective. It provides one more example in support of Alfred North Whitehead's assertion that "the major advances in civilizations are processes that all but wreck the societies in which they occur."

We are in search of a unified theory of an emergent multi-nodal cyborg personality and how it exercises power. This theory must address hierarchical and distributed structures and what they mean for human identity, law, and global organization and geopolitical strategy. What are the genuine sources of our power? What is the point of reference from which that power is exercised? Who do we believe ourselves to be in the moment in which we act and how do we thereby define ourselves not in theory but in practice, not in the chat room but on the field of action? And finally, why is knowing that we are doomed to fail the key to victory?

Richard Thieme shows how boundaries have morphed, power has been redefined, and The Matrix is more than a movie. Not since Blade Runner has a film described so well the territory that must be crossed. Owning our own souls is the ultimate intention of Third Generation Hacking, the only end that justifies the means.

Thieme holds nothing back as he addresses the deeper implications of what it means to be the network. The stakes are high and the battle is worthy of our best efforts. This talk is a call

[redacted]arms to accept responsibility for the life [redacted]death battle being waged for the hearts and minds of digital humanity.

presenter

Ian Vitek
Journalist, Patrik Karlsson

TOP

Exploring Terminal Services, The Last 12 Month of Research. Or, The Evil Admin And His Tools

Got shell? On a Citrix or Terminal Services server? The speech will demonstrate some common ways to explore Terminal Services. Uploading files with the keyboard and elevate luser rights to SYSTEM.

How secure is it for a client to connect to a Citrix or a Terminal Services server if an evil admin owns the box? Tools and exploits will be released.

Ian Vitek:
183 cm.
80 Kg.
Brown eyes.
Brown hair.
Eats meat.
Drinks almost every beer you buy him.
Interested in layer 2 network security (writer of macof).

If you approach Ian he probably wants to talk about privilege escalation or web application security.

presenter

Kathy Wang
Syn Ack Labs

TOP

Frustrating OS Fingerprinting with Morph

Sun Tzu once stated, "Know your enemy and know yourself, and in a hundred battles you will never be defeated." By denying outsiders information about our systems and software, we make it more difficult to mount successful attacks.

There are a wealth of options for OS-fingerprinting today, evolving from basic TCP-flag mangling tools such as Queso, through the ICMP quirk-detection of the original Xprobe, and the packet timing analysis of RING, to today's suite of multiple techniques employed by nmap. The ultimate advantage in the OS-detection game lies with the defender, however, as it is they who control what packets are sent in response.

Morph is a BSD-licensed remote OS detection spoofing tool. It is portable and configurable, and will frustrate current state-of-the-art OS fingerprinting. This presentation will discuss the current techniques used for OS fingerprinting, and how to frustrate them. A newer version of Morph will be released with the talk, as a concrete example of the discussed techniques.

Kathy Wang broke into programming with BASIC on the Apple IIgs. She has a bachelor's and master's degree in electrical engineering from the University of Michigan, where she specialized in VLSI chip design and semiconductor device physics and fabrication. She worked at Digital as part of the Next-Generation Alpha Chip Design Team, and got to spend an entire wonderful summer blowing up Alpha chips. She has published a paper on some of the work she did there at an IEEE conference. Kathy has instructed courses ranging from Semiconductor Device Physics to Vulnerability Assessment and Penetration Testing.

Since Digital got broken up by Compaq and Intel, Kathy has focused on the software side of things. She has worked at Counterpane Internet Security, and currently works as a Senior Infosec Engineer at The MITRE Corporation. Kathy is also a founder of Syn Ack Labs, a computer security research group focused on cryptography, steganography, and low-level packet hijinks.

TOP

presenter

Wavyhill

Toward a Private Digital Economy (Trusted Transactions In An Anonymous World)

Andre Goldman

Current financial privacy tools have drawbacks arising from centralized ownership and control, and the limitations of the service-for-profit model. A better approach is to construct a fully distributed environment for economic activity which mimics in freedom and variety of action the way cash is used in the physical world.The key to this variety is the element of locale.

We introduce the 'Farmer's Market' model of anonymous commerce and refine it to a software functional description. We explore some exotic kinds of business viable in this new environment and ways to connect them to the transparent banking world.

Number theory can be used to derive an 'algebra of trust', exploited in practical ways to reduce risk in anonymous transactions, and overcome barriers to adoption of this and other digital cash systems. We also discuss the boot-strapping problem and suggest some ways to address it. Afterward, everyone is invited to participate in a role-playing simulation experiment to test the viability of these ideas using a prototype graphical software environment

Wavyhill is a software engineer having a 25 year history with industrial research organizations and developers of operating system, video, and graphics products. An anarcho-capitalist without portfolio and advocate of privacy and anonymity, he has also done experimental engineering work on artificial islands. He has no academic credentials that he will admit to.

Andre Goldman writes on law and philosophy. He works in the area of non-jurisdictional law, and was the primary author of The Common Economic Protocols.

TOP

presenter

Paul Wouters

Windows Wavesec Deployment

Paul Wouters has been involved with Linux networking and security since he co-founded the Dutch ISP "Xtended Internet" back in 1996. His first article about network security was published in LinuxJournal in 1997 Since then, he has written mostly for the Dutch spin-off of the German "c't magazine", focussing on Linux, networking and the impact of the digital world on society. He has presented papers at SANS, OSA, CCC and HAL.

He is currently involved with the FreeS/WAN project, a Linux IPsec stack that aims to bring Opportunistic Encryption to everyone. For this feature, a secure DNS is needed, which

[redacted] [redacted] triggered his interest in assisting the widespread use of DNSSEC. Wouters received his Bachelors degree in Education in 1993

TOP

DEFCON

schedule

v.12 • 2004 • July 30- August 1 • Alexis Park • Las Vegas, NV

This Schedule & Speakers are Subject to Change.

Friday				
Day 1	**Track 1**	**Track 2**	**Track 3**	**Events**
bright & early	08:00 - 22:00 Registration - $80 USD CASH ONLY in Apollo Foyer 10:00 Vendor Area in Zeus until 20:00 Info Booth and Contests in Athena until 20:00 Check-in for Wardrive in Athena Coffee Wars in Athena Chill Out in Parthenon 2 The Dunk Tank opens at 11AM by Pool 2			
	Parthenon 3 & 4	**Tent**	**Apollo**	
11:00 - 11:50	Advanced Hardware Hacking Joe Grand	Freenet: Taming the World's Largest Tamagotchi Ian Clarke	The First International Cyber War Peter D. Feaver & Kenneth Geers	11:30 - Dunk Dan Huard (TechTV)
12:00 - 12:50	Windows WaveSEC Deployment Paul Wouters	How Do We Get The World To Use Message Security Jon Callas	Attacking Windows Mobile PDA's Seth Fogie	Book Signing: Joe Grand's "Hardware Hacking: Have Fun While Voiding Your Warranty" at Breakpoint Books 12:00 - Dunk TommEE Pickles (Hacker) 12:30 - Dunk Joe Grand
13:00 - 13:50		Real World Privacy, How to Leave Less of A Trail in	A Comparison of Buffer Overflow Prevention Implementations	Main WarDriving Contest Begins

		Life n0namehere	and Weaknesses Peter Silberman & Richard Johnson	(13:00-13:00 Sunday) 13:00 - Dunk Grifter (Goon) 13:30 - Dunk Russ Rogers (Goon)
14:00 - 14:50	Introduction to Hardware Hacking Scott Fullam	Tor: An Anonymizing Overlay Network For TCP Roger Dingledine	We Can Take It From Here FX & Halvar Flake	14:00 - Dunk Chris Hurley (Goon) 14:30 - Dunk Dead Addict (Goon)
15:00 - 15:50	Bluesnarfing—The Risk From Digital Pickpockets Adam Laurie & Martin Herfurt	Tools for Censorship Resistance Rachel Greenstadt		Book Signing: Scott Fullam's "Hardware Hacking Projects for Geeks" in Zeus
16:00 - 16:50	Hack the Vote: Election 2004 Rebecca Mercuri & Bev Harris	CryptoMail Encrypted E-Mail for All (Including Grandma) Joshua Teitelbaum & Peter Leung	Wireless Weaponry The Shmoo Group	
17:00 - 17:50		Mixmaster vs. Reliable Len Sassaman	Program Semantics-Aware Intrusion Detection Tzi-cker Chiueh	Booksigning: Bruce Potter's "802.11 Security" at Breakpoint Books
18:00 - 18:50	RF-ID and Smart-Labels Lukas Grunwald	Snake Oil Anonymity Nick Mathewson	VICE—Catch the Hookers! Jamie Butler	Book Signing: Bev Harris's "Black Box Voting" in Zeus Tag WarDriving Contest Mini-Game (18:00-21:00)
19:00 - 19:50	Weaknesses in Satellite Television Protection Schemes	Identification Evasion Adam Bresson	Bubonic Buffer Overflow spoonm & HD Moore	

	A			
20:00 - 20:50	Smart Card Security h1kari	NoSEBrEaK—Defeating Honeynets Thorsten Holz, Maximillian Dornseif, Christian Klein		DEFCON Forum Meet in Executive Boardroom in Building 23
21:00	Automotive Networks Nothingface	Leetest Link in Tent until 01:00	TCP/IP Drinking Game in Apollo until 22:00	
22:00	Registration closes			

Saturday					
Day 2	**Track 1**	**Track 2**	**Track 3**		**Events**
bright & early	08:00 - 22:00 Registration - $80 USD CASH ONLY in Apollo Foyer 08:00 DC Shoot 10:00 Vendor Area in Zeus until 20:00 Info Booth and Contests in Athena until 20:00 Chill Out in Parthenon 2 The Dunk Tank opens at 11AM by Pool 2				
	Parthenon 3 & 4	**Tent**	**Apollo**		
11:00 - 11:50	DIGEX—At the Dawn of the Commercial Internet Doug Mohney	When the Tables Turn Sensepost	Mutating the Mutators Sean O'Toole	11:00 - 11:20	Dunk - Wendy Seltzer (EFF)
			MySQL Passwords—Password Strength and Cracking D. Egan	11:30 - 11:50	
12:00 - 12:50	Digitizations And Documentary Jason Scott	Shoot the Messenger Brett Moore	The Hacker Foundation Jesse Krembs & Nicholas Farr	12:00 - 12:20	Booksigning: Roamer, Russ Rogers & Frank Fulton's "WarDriving: Drive, Detect, Defend, A Guide to

			Smile, You're on Candid Camera! Kevin Mahaffey	12:30 - 12:50	Wireless Security" in Zeus 12:00 - Dunk Patrick Norton (ex-TechTV)
13:00 - 13:50	Meet the Fed	Frustrating OS Fingerprinting with Morph Kathy Wang	What Do You Mean, Privacy? Sarah Gordon	13:00 - 13:20	Running Man WarDriving Contest (13:00-14:00) 13:00 - Dunk DJ Jackalope (Hacker DJ)
			Cracking Net2Phone Todd Moore	13:30 - 13:50	13:30 - Dunk Jason Scott (textfiles.org)
14:00 - 14:50	Quantum Hacking Richard Thieme	IPv6 Primer Gene Cronk	Electronic Civil Disobedience and the Republican National Convention CrimethInc	14:00 - 14:20	Booksigning: Jon Erickson's "Hacking: The Art of Exploitation" 14:00 - Dunk Jim Christy (Fed)
			The History of the Future Robert Morris	14:30 - 15:00	14:30 - Dunk the Dark Tangent
15:00 - 15:50	Ask EFF Annalee Newitz, Wendy Seltzer, Kevin Bankston, Seth Schoen & Jennifer Granick	Advanced Netfilter; Content Replacement (ala Snort_inline), and Port Knocking Based on Passive OS Fingerprinting Michael Rash	This Space Intentionally Left Blank Geoffrey & Mark Farver	15:00 - 15:50	Booksigning: Richard Thieme's "Islands in the Clickstream: Reflections on Life in a Virtual World" in Zeus
16:00 - 16:50		Virus, Worms and Trojans: Where are we going? IcE tRe	Project Prometheus Grifter, Russ Rogers & Tierra	16:00 - 16:50	PGP Keysigning Party with the Dark Tangent in the Athena

17:00 - 17:50	Down with the RIAA, Musicians Against the Recording Industry Nathan Hamiel	Black Ops of TCP/IP 2004 Dan Kaminsky	Kryptos and the Cracking of the Cyrillic Projector Cipher Elonka Dunin	17:00 - 17:50	
18:00 - 18:50	Hacking the Spectrum Wendy Seltzer & Seth Schoen	PDTP – The Peer Distributed Transfer Protocol Tony Arcieri	Far More Than You Ever Wanted To Tell— Hidden Data In Document Formats Maximillian Dornseif	18:00 - 18:50	Fox and Hound WarDriving Contest Mini-Game (18:00-21:00)
19:00 - 19:50	Hacking the Media, and avoiding being Hacked by the Media Dead Addict	Network Attack Visualization Greg Conti	Counter Intelligence/Counter Espionage Mudge	19:00 - 19:50	
20:00 - 20:50	Better than Life - Manipulation of The Human Brain With The Use of Machines NeOnRa1n	Toward a Private Digital Economy Wavyhill & Andre Goldman	Locking Down Apache Jay Beale	20:00 - 20:50	
21:00 - 21:50	Black & White Ball in Apollo until 04:00 Leetest Link in Tent Movies in Parthenon until 01:00				
22:00	Registration closes				

Sunday				
Day 3	Track 1	Track 2	Track 3	Events
bright & early	08:00 - 12:00 Registration - $80 USD CASH ONLY in Apollo Foyer 10:00 Vendor Area in Zeus until 18:00 Info Booth and Contests in Athena until 18:00 Chill Out in Parthenon 2 The Dunk Tank opens at 11AM by Pool 2			

	Parthenon 3 & 4	Tent	Apollo	
11:00 - 11:50	Steganography, Steganalysis, & Cryptanalysis Michael T. Raggo	DMCA, Then and Now Dario D. Diaz	Hacking/Security Mac OSX Server aka Wussy Panther Charles Edge	Booksigning: contributors of "Stealing the Network" in Zeus 11:00 - Dunk Kevin Rose (TechTV)
12:00 - 12:50	Subliminal Channels In Digital Signatures Seth Hardy	Google Hacking j0hnny long	The Advantages of Being an Amateur Brett Neilson	Booksigning: bunnie's "Hacking the Xbox" in Zeus Rant Radio in Parthenon 1 until 15:00 12:00 - Dunk Dan Kaminsky
13:00 - 13:50	Phreaking in the Age of Voice Over IP Lucky 225	The Insecure Workstation Deral Heiland	The Open Source Security Myth—And How to Make it A Reality Michael Davis	Main WarDriving Contest Ends
14:00 - 14:50	Information Hiding in Executable Binaries Rakan El-Khalil	Old Tricks Foofus	Exploring Terminal Services, The Last 12 Month of Research. Or, The Evil Admin And His Tools Ian Vitek	
15:00 - 15:50	Credit Card Networks Revisted: Penitration in Real-Time Robert "hackajar" Imhoff-Dousharm & Jonathan "ripshy" Duncan	Blind SQL Injection Automation Techniques Cameron "nummish" Hotchkies	Digital Active Self Defense Laurent Oudot	
15:20 - 15:50				The DEFCON Surveys Dr. Larry Ponemon Parthenon 1
16:00 -	**Award Ceremonies** hosted by Dark Tangent			

16:50

Comment on a presentation: Use the NoteEx

DEFCON

This page last updated on: Saturday, July 24, 2004

- Logisitics
- Resources
- Direct Action Handbook
- Media
- Flyers and Graphics
- About Us
- How to Help This Project
- No RNC Clearinghouse

- Home

RNC Events Calendar

Make a Donation

Subscribe to the noRNC **Announcement** List

Your e-mail here

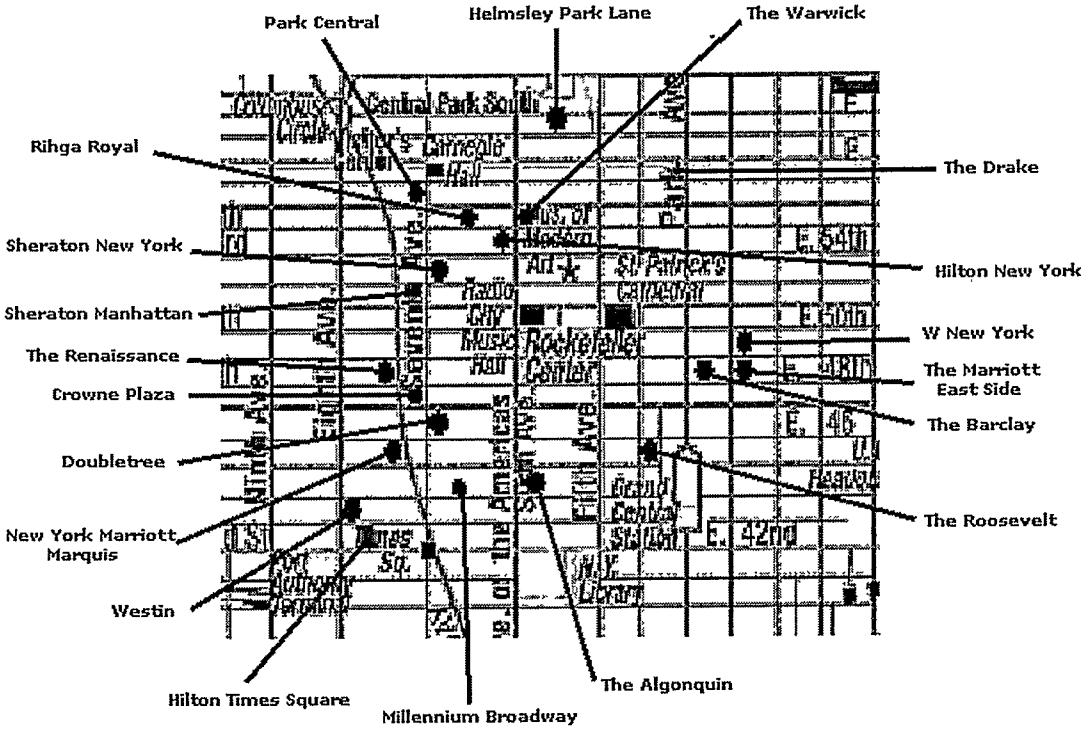
Subscribe to the noRNC **Discussion** List

Your e-mail here

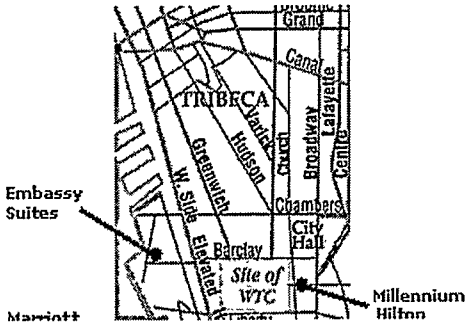
Where are the RNC Delegates Staying?

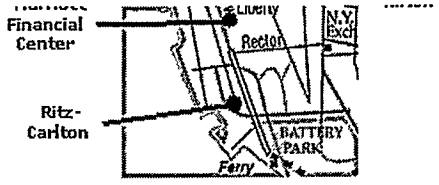
Can You Make a Better Map? Mail us at info@rncnotwelcome.org

Midtown Hotels



Downtown Hotels





The Algonquin - Washington D.C.
59 W. 44th St. betw. 5th and 6th

The Barclay - New Hampshire
111 E. 48th St.

Crowne Plaza - New Jersey
Broadway and 49th Street

Doubletree - Illinois
1568 Broadway at Times Square

The Drake - Massachusetts
440 Park Avenue at 56th St.

Embassy Suites - American Samoa, Indiana
102 North End Avenue

Helmsley Park Lane - Louisiana, South Carolina, Virginia
36 Central Park South

Hilton New York - Pennsylvania, Michigan, Florida, Texas
1335 Avenue of the Americas (6th Ave.) between 54th and 55th

Hilton Times Square - Mississippi, Vermont
234 West 42nd Street between 7th and 8th Ave.

The Marriott East Side - Colorado, Minnesota
525 Lexington Ave. at 49th St.

Mariott Financial Center - Guam, Hawaii, Nebraska, North Dakota
85 West St. between Alabany and Carlisle St.

Millennium Hilton - Rhode Island, Puerto Rico, Utah, Delaware
55 Church St.

Millennium Broadway - Washington, West Virginia, Wisconsin
145 West 44th St. between 6th Ave. and Broadway

New York Marriot Marquis - California, Ohio, Tennessee
1535 Broadway between 46th and 47th St.

Park Central - Idaho, Kansas, Maryland
870 7th Avenue at 56th St.

The Renaissance - Montana

714 Seventh Ave. at W. 48th St.

Rihga Royal - Nevada
151 W. 54th St between 6th and 7th Ave.

Ritz-Carlton - Georgia
First Pl., Little West Street, and Battery Place

The Roosevelt - Arizona, New Mexico, Oklahoma, Oregon
45 E. 45th St.

Sheraton Manhattan - Alaska, Iowa, South Dakota, Virgin Islands
790 7th Ave. between 51st and 52nd

Sheraton New York - Alabama, Connecticut, New York, Wyoming
811 7th Ave. between 52nd and 53rd

W New York - Arkansas, Maine
541 Lexington Ave. between 49th and 50th St.

The Warwick - North Carolina
65 West 54th St

Westin - Kentucky, Missouri
270 W. 43rd St. at 8th Ave.

Source: New York Times - February 2, 2004

Action ideas, links, comments, and offers of graphic design help can be sent to info@rncnotwelcome.org

Site launch-5/21/03. Voicemail: 212-696-6450 PGP Key Thanks to mutualaid.org for hosting this site.

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/03/2004

To: Counterterrorism **Attn:** Threat Task Force,
SC [redacted] Rm 4973

SEMU, SSA [redacted]
Rm 11795

Office of Intelligence **Attn:** SSA [redacted] Rm 5431

Cyber **Attn:** IA [redacted] Rm 5931

New York **Attn:** Assistant Director,
FIG Supervisor,
Special Events Supervisor

✓ Las Vegas ✓**Attn:** SSA [redacted]

From: Las Vegas
Squad 8/NRIC
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :rmm

Case ID #: 300A-LV-38111 (Pending)

Title: DEFCON 12 LAS VEGAS 2004;
ALEXIS PARK HOTEL;
07/30/2004 - 08/01/2004

Synopsis: [redacted] b7E

Enclosure(s): Enclosed for recipients is a [redacted] DEFCON 12 b7E conference information, to include a list of speakers and presentation schedules, [redacted]

300A-LV-38111-4

To: Counterterrorism From: Las Vegas
Re: 300A-LV-38111, 08/03/2004

Details:

b6
b7C
b7E

LEAD(s):

Set Lead 1: (Discretionary)

COUNTERTERRORISM

AT WASHINGTON D.C.

For appropriate action by the Threat Task Force.

Set Lead 2: (Info)

COUNTERTERRORISM

AT WASHINGTON D.C.

SEMU read and clear.

Set Lead 3: (Info)

OFFICE OF INTELLIGENCE

AT WASHINGTON, DC

Read and clear.

Set Lead 4: (Discretionary)

CYBER

AT WASHINGTON D. C.

For appropriate action by Cyber Division.

Set Lead 5: (Discretionary)

NEW YORK

AT NEW YORK

[redacted] b7E

Set Lead 6: (Info)

LAS VEGAS

AT LAS VEGAS, NEVADA

Read and clear.

♦♦

(Rev. 01-31-2003)

lsvegas wpd

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/02/2004

To: Las Vegas **ATTN:** SA [redacted]

From: Philadelphia
11/JTTF
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted] rrt

b6
b7C

Case ID #: 300A-LV-38111 (Pending) -5
66F-HQ-C1384970 -12419

Title: DEFCON 12 LAS VEGAS 2004;
ALEXIS PARK HOTEL;
07/30/2004 - 08/01/2004

Synopsis: Report negative investigation results in Philadelphia.

Details: Receiving offices were requested to query logical sources for threats to captioned event. Philadelphia has conducted logical investigation with negative results.

Philadelphia considers this lead covered.

300A-LV-38111-5
#8

LEAD(s):

Set Lead 1: (Info)

Las Vegas

AT Las Vegas, NV

Read and Clear.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/30/2004

To: Las Vegas

From: Las Vegas
Squad 4
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: 300A-LV-38111 (Pending)

Title: DEFCON 12 LAS VEGAS 2004
ALEXIS PARK HOTEL
07/30/2004 - 08/01/2004

Synopsis: [redacted] b7E

Details: [redacted] b7E

DEFCON 12 is an annual event that will be held at the Alexis Park Hotel in Las Vegas, Nevada. This event is billed as the largest underground hacking event in the world. The conference is expected to attract 6,000 attendees.

A partial list of topics to be covered during the conference will include the following:

*Introduction to hardware hacking
*Bluesnarfing - The risk from digital pickpockets
*Hack the vote - Election 2004
*RF-ID and Smart labels
*Weakness in satellite television protection schemes
*Meet the Fed
*Quantum Hacking
*Hacking the Spectrum
*Down with the RIAA - Musicians against therecording industry
*Hacking the media
*Credit card networks

58125.04

300A-LV-38111 - 7

*Counterintelligence/Counterespionage
*Electronic civil disobedience and the Republican National Convention
*Virus, worms, and trojans, where are we going?
*Smart Card security

The DEFCON 12 conference is expected to bring together white, gray, and black hat hackers from many countries around the world. Several of the speakers include security consultants from private industry, professors, and known credible hackers, who are lecturing during the conference.

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/10/2004

To: Counterterrorism **Attn:** SEMU, SSA [redacted]
Las Vegas

From: Las Vegas
Squad 8/NRIC
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted] :rmm Reviewed ⊗ Rmm

✓**Case ID #:** 300A-LV-38111 (Pending)

Title: DEFCON 12 LAS VEGAS 2004;
ALEXIS PARK HOTEL;
07/30/2004 - 08/01/2004

Synopsis: To provide results of captioned event and close case.

Details: DEFCON 12 was held at the Alexis Park Hotel, Las Vegas, Nevada, from 07/30/2004 - 08/01/2004.

[redacted] b6 b7C b7E

No other threats or incidents occurred and it is requested this case be closed at Las Vegas.

♦♦

C-4 8/12/04

8

5724

Office: LAS VEGAS

Case ID: 300A-LV-38111

Primary Investigator/ Set to Office	Squad	Serial	Lead Num	Set/ Assigned	Deadline/ Covered/ Discontinued	Location/Nature
(SN) A-2/CRT LOS ANGELES	3342	2	1	07/28/2004 08/16/2004	09/26/2004	AT: [redacted] Please provide information obta
(SN) [redacted] BALTIMORE	24	2	1	07/28/2004 08/17/2004	09/26/2004	AT: [redacted] Please provide information obta

[redacted]

Albany NY CTD

b6
b7C
b7E

Gen Counsel WFO Seattle Mobile LA Detroit

Office: LAS VEGAS

Case ID: 300A-LV-38111

Primary Investigator/ Set to Office	Squad	Serial	Lead Num	Set/ Assigned	Deadline/ Covered/ Discontinued	Location/Nature
(SN) [redacted] MOBILE	3	2	1	07/28/2004 08/02/2004	09/26/2004	AT: [redacted] [redacted] Please provide information obta [redacted]
(SN) [redacted] DETROIT	CT4	2	1	07/28/2004 07/30/2004	09/26/2004	AT: [redacted] [redacted] Please provide information obta [redacted]

b6
b7C
b7E

Office: LAS VEGAS

Case ID: 300A-LV-38111

Primary Investigator/ Set to Office	Squad	Serial	Lead Num	Set/ Assigned	Deadline/ Covered/ Discontinued	Location/Nature
(SN) [redacted] ALBANY	6	2	1	07/28/2004 07/30/2004	09/26/2004	AT: [redacted] Please provide information obta [redacted]
(SN) [redacted] GENERAL COUNSEL	GC	2	1	07/28/2004 07/29/2004	09/26/2004	AT: [redacted] Please provide information obta [redacted]

b6
b7C
b7E

Office: LAS VEGAS

Case ID: 300A-LV-38111

Primary Investigator/ Set to Office	Squad	Serial	Lead Num	Set/ Assigned	Deadline/ Covered/ Discontinued	Location/Nature
(SN) NEW YORK EW YORK	DT5	4	5	08/04/2004	10/03/2004	AT: NEW YORK [redacted]
(SN) [redacted] CYBER	CTCI	4	4	08/04/2004 08/09/2004	10/03/2004	AT: WASHINGTON D. C. For appropriate action by Cyber Division.
(SN) [redacted] NEW ORLEANS	7	2	1	07/28/2004 08/02/2004	09/26/2004	AT: [redacted] Please provide information obta [redacted]

b6
b7C
b7E

Office: LAS VEGAS

Case ID: 300A-LV-38111

Primary Investigator/ Set to Office	Squad	Serial	Lead Num	Set/ Assigned	Deadline/ Covered/ Discontinued	Location/Nature
(SN) [redacted] SEATTLE	8	2	1	07/28/2004 08/05/2004	09/26/2004	AT: [redacted] [redacted] Please provide information obta [redacted]
(SN) [redacted] SAN FRANCISCO	17C	2	1	07/28/2004 08/02/2004	09/26/2004	AT: [redacted] [redacted] Please provide information obta [redacted]

b6
b7C
b7E

Office: LAS VEGAS

Case ID: 300A-LV-38111

Primary Investigator/ Set to Office	Squad	Serial	Lead Num	Set/ Assigned	Deadline/ Covered/ Discontinued	Location/Nature
(SN) THREAT MONITORING UNIT COUNTERTERRORISM	TMU	4	1	08/04/2004 08/04/2004	10/03/2004	AT: WASHINGTON D.C. For appropriate action by the Threat Task Force.
(SN) WASHINGTON FIELD WASHINGTON FIELD	CT13	2	1	07/28/2004	09/26/2004	AT: [redacted] [redacted] Please provide information obta [redacted]

b6
b7C
b7E

300A-LV-38111 Total: 13

Office: LAS VEGAS

Case ID:

Primary Investigator/ Set to Office	Squad	Serial	Lead Num	Set/ Assigned	Deadline/ Covered/ Discontinued	Location/Nature

Report Total : 13