Workshops 1.1
Freitag

WS1

12 **How To Leave The Planet**

The Camp Crew

Welcome To The Camp.
Join The Crew.

Introduction To The Camp

14 **Politics of Creating Crypto Software**

Hugh Daniel

John Gilmore

How to create free strong crypto software without getting into trouble with the various regulatory agencies.

16 **Faktorisierung**

Lutz Donnerhacke

Nach Zuruf einer - sagen wir mal zwölfstelligen - Zahl versucht der Vortragende diese zu faktorisieren, ohne dabei auf spezialisierte Software zurückzugreifen. A Paper and Pencil Attack.

18

20 **"Secure and Fast Hard disk (and Pilot) Encryption with Smart Cards"**

Rüdiger Weis

Stefan Lucks

Smart cards are very user friendly and pretty tamper-proof - ok,ok not really if you hang on the CCC-Camp. But if you look at the performance, smart cards are like a compressed C64. So if you want to use a smart card supported files system, we have to use more sophisticated protocols. And we have developed some, free and even exportable to the US.
http://www.informatik.uni-mannheim.de/~rweis/usenix99/
http://www.informatik.uni-mannheim.de/~rweis/morehash/enix99/)

22 **Angel**

Antonomasia

A workshop about the development of the remailer-friendly cryptographic mail transfer agent "angel".

24 **Biometric Insecurity**

Biometrical Authentication is one of the most interesting fields for future hacking. Bypassing finger print scanners, hand shape scanners, and other biometric devices will be discussed in more or less detail as well as the basic theories behind it.

WS2

12

14 **"How to ask for help on the net" -- finding information**

Ron Fulda

Finding Information on the net is sometimes not as easy as it looks. The talk gives also some sort of introduction to the whole field of Search Engines, how to ask questions, Communities, generating information and beeing patient.

16 **Holographie Einführung**

Claus Cohnen

Claus gibt einen allgemeinen und einführenden Überblick über das weite Feld der Holographie.

18 **Security & Authentication Mechanisms NT vs. Linux vs. Novell**

Kurt Seifried

We will discuss and evaluate the Security and Authentication mechanisms in these three popular Operating Systems.

20 **Careerpunks**

Dave Del Torto

"A Career in Mischief: Cypherpunks in Corporate Security"
"How to Succeed in Business -- for Cypherpunks"
"It's Not Just a Job, It's a Hack" / "Cypherpunk Corporate Camoflage Camp"
"Take This Job and Ping It" / "Hacking the Corporate Ladder for Fun & Profit"

22 **Hacker Variety Pack**

Hugh Daniel,
John Gilmore
Lucky Green,
Sameer Parekh
Ian Goldberg
et. al.

The many ways one can be a hacker. Not all of which have anything to do with getting root on a machine. The panel will consist of Lucky Green, Ian Goldberg, John Gilmore, Hugh Daniel, and Sameer Parekh and some more people.
The idea is to teach the kids that there are other ways to do cool stuff than to just hack boxes. We need managers, social engineers, scientists, and more.

24 **Linux Security Summit**

Hugh Daniel

How to get strong encryption into main Linux distributions.

Workshops 1.1
Samstag

WS1

12 — **Secure Networks for the Future. DNSSEC, IPSEC, FreeSWAN**

Hugh Daniel

DNSSEC, IPSEC, FreeSWAN.

14 — **Sicherheit kommerzieller NT-basierter Firewalls**

Charly Kuehnast

Am praktischen Beispiel werden wir die Sicherheit von kommerziellen WindowsNT-basierten Firewalls erforschen und diskutieren. Ein Testsetup wird nach diesem Workshop im Camp-Netz stehen um weitere gezielte Forschungen durchzu führen.

16 — **Generic Bidirectional Mapper**

Lutz Donnerhacke

Vorgestellt wird ein Yacc-Nachfolger, der ausreichen komplex ist, um die praktischen externen Datenstrukturen in einem Ritt zu lesen und zu schreiben.

18 — **Multicast Protocolls (for Beginners)**

Andreas Bogk

Multicast is a more and more important field of the Internet development. This workshop will cover the basics as well as recent developments in this field.

20 — **Down with the DEA -State of Process for the next DES**

Ruediger Weis

"Advanced Encryption Standard: State of Process"
Down with the DEA! A new star will born soon.
A first closer look on the candidates for the Advanced Encryption Standard. Some of them are very secure, very fast and designed by very nice guys.
http://www.informatik.uni-mannheim.de/~rweis/research/
http://csrc.nist.gov/encryption/aes/aes_home.htm

22 — **Verschwörungstheorien**

Matthias Rehkop

Muster und Mechanismen von Verschörungstheorien. Wie verbreiten sie sich, welche Gemeinsamkeiten gibt es? Ein kulturwissenschaftlich-entspannter Betrachtungsversuch.

24 — **Poetry Slam**

gregor sedlag

Gedichte, Poetry, Lyrik, wasauchimmer

WS2

12 — **Telefonnetz-Hacking & servicewatch - Geschichten**

CCC-Team
ServiceWatch

Auch das Telefonnetz ist trotz oder gerade wegen des Internets interssant geblieben. Erörterungen zum Phreaking auch für Anfänger und servicewatch erzählt Geschichten.

14 — **Telephony voice encryption - project and therories**

Hacko

Projects on voice encryption show their state of development.

16 — **Intrusion Detection Systems - a Reality Check**

Felix von Leitner

This workshop will try to give an overview on the current state of Intrusion Detection Systems. Two or three commerial, semicommercial and free intrusion detection systems will be tested in a real hostile environment.

18 — **Advanced Image Manipulation with the GIMP**

Karin Kylander

Olof S Kylander

A tour of Gimp's image manipulation power. What is Gimp and why should you use it? Selections, masks, layers, modes and channels, or how do you do really advanced image manipulation. Map and distort, examples of how to make your own custom box in Gimp. Color and Image corrections with Gimp's powerful color manipulation plug-ins. A Quick tour of the GIMP plug-in Land.

20 — **Construction of WindowsNT shell code for Buffer Overflow**

Felix v. Leitner

Özgur Kesim

We will discuss and demonstrate how to construct, write and test insertion codes to exploit WindowsNT buffer overflow exploits.

22 — **CIPHR'00 planning meeting.**

Dave del Torto

This is the planing meeting for the Cypher Rights Conference in 2000

24 — **Nerdbank: Feasability of an open source banking**

Holger Blasum

Philipp Guehring
Felix von Leitner

After a brief introduction why banking may be good target for the open source paradigm, and various protocols considered possible the speakers would like to start a discussion on the overall doability of the open-source ecommerce as well as on the choice of protocols.

Workshops 1.1

Sonntag

		WS1			WS2
12	Jörg Jenetzky	**Eingeschränkt freie Berufswahl in der IT-Branche** Ein Erlebnisbericht zu den Risiken einer abweichenden Meinung für die Freiheit der Berufswahl.	12	Rüdiger Weis	**"Crypto-Hacking Export restrictions"** There are still many silly export restriction for cryptographic software. Therefore we have taken a closer look on nice mathematical tricks to improve key length, building encryption systems with signature cards and using "non decrypting" JAVA cards to do en- and decryption. For all these systems there exist nice mathematical security proofs, but perhaps we should do some funnier things too, like encrypting with Solitaire cards or PERL body painting. http://www.informatik.uni-mannheim.de/~rweis/research/ http://www.counterpane.com/solitaire.html http://www.dcs.exeter.ac.uk/~aba/rsa/tattoo.html
14	Pirx	**Das Chaos-CD Projekt** Das Projekt zur Erstellung des Inhalts der nächsten Chaos-CD stellt sein Konzept vor und verteilt Arbeits-Päckchen an Mitarbeitswillige Mitmenschen	14	Ian Goldberg	**Freedom - the pseudonymous IP Network - Introduction** In this workshop Ian Goldberg gives an overview of Freedom, a pseudonymous IP network that is soon to be released publicly.
16		**IP V6: Erfahrungen aus dem IP V6-Feldversuch auf dem Camp** Was ging, was ging nicht beim IP V6-Ackerversuch? Eine Bilanz.	16		
18	Lucky Green	**Chaos Communication Camp Reverse Engineering Award** A price for the best reverse engineering project at the Chaos Communication Camp will be handed out. IThe winner gets a very rare price: one of the only eight GSM diagnostic SIM's I know of with rewritable internal keys. A board of judges that consists of several well known and respected members of the hacker comunity will try to judge the winner independently.	18		
20			20		
22			22		
24			24		