

# 28th Chaos Communication Congress

Behind Enemy Lines · bcc, Berlin

Version 0.92µ

day 1 | 2011-12-27

Saal 1

11:30–12:30 society and politics

Marriage From Hell: On the Secret Love Affair Between Dictators and Western Technology Companies

12:45–13:45 society and politics · de

Sachsen dreht frei  
*On- und Offline-Überwachung:  
Weil sie es können*

14:00–15:00 hacking · en

Datamining for Hackers  
*Encrypted Traffic Mining*

16:00–18:15 hacking · de

Der Staatstrojaner  
*Vom braunen Briefumschlag  
bis zur Publikation*

18:30–19:30 hacking

802.11 Packets in Packets  
*A Standard-Compliant  
Exploit of Layer 1*

20:30–21:30 society and politics · en

The coming war on general computation  
*The copyright war was  
just the beginning*

21:45–22:45 hacking · en

Defending mobile phones

23:00–00:00 hacking · en

Black Ops of TCP/IP 2011

00:15–01:15 show

Pentanews Game Show 2k11/3  
*42 new questions, new jokers, same  
concept, more fun than last year!*

Saal 2

12:45–13:45 society and politics · en

What is WhiteIT and what does it aim for?  
*Why you probably want to be concerned  
about it and similiar alliances.*

14:00–15:00 hacking

roket++  
*The CCC-Badge*

16:00–17:00 hacking · en

SCADA and PLC Vulnerabilities in Correctional Facilities  
*Tiffany Rad, Teague  
Newman, John Strauchs*

17:15–18:15 society and politics · de

Almighty DNA?  
*Was die Tatort-Wahrheitsmaschine  
mit Überwachung zu tun hat*

18:30–19:30 society and politics · en

Does Hactivism Matter?  
*How the Btx hack changed computer  
law-making in Germany*

20:30–21:30 society and politics · en

What is in a name?  
*Identity-Regimes from 1500 to the 2000s*

21:45–22:45 society and politics · de

EU-Datenschutz und das Internet der Dinge

Saal 3

12:45–13:45 hacking · en

The Atari 2600 Video Computer System: The Ultimate Talk  
*The history, the hardware and  
how to write programs*

14:00–15:00 hacking

Can trains be hacked?  
*Die Technik der Eisen-  
bahnsicherungsanlagen*

16:00–17:00 society and politics · de

Demokratie auf Sächsisch

17:15–18:15 hacking · en

Automatic Algorithm Invention with a GPU  
*Hell Yeah, it's rocket science*

18:30–19:30 society and politics

The movements against state-controlled Internet in Turkey  
*A short account of its history  
and future challenges*

20:30–21:30 society and politics

BuggedPlanet  
*Surveillance Industry &  
Country's Actings*

21:45–22:45 hacking

Macro dragnets: Why you can do the whole ocean  
*What happens when data collection  
goes awry in the 21st century*

23:00–00:00 hacking

String Oriented Programming  
*Circumventing ASLR,  
DEP, and Other Guards*

# day 2 | 2011-12-28

Saal 1

**11:30–12:30** society and politics · de  
Politik hacken

*Kleine Anleitung zur Nutzung von Sicherheitslücken gesellschaftlicher und politischer Kommunikation*

**12:45–13:45** society and politics · de  
Echtes Netz

*Kampagne für Netzneutralität*

**14:00–15:00** hacking · en  
Effective Denial of Service attacks against web application platforms

*We are the 99% (CPU usage)*

**16:00–17:00** hacking · en  
The Science of Insecurity

**17:15–18:15** hacking · en  
Hacking MFPs

*Part2—PostScript: Um, you've been hacked*

**18:30–19:30** hacking  
How governments have tried to block Tor

**20:30–21:30** society and politics  
„Die Koalition setzt sich aber aktiv und ernsthaft dafür ein“

*Sprachlicher Nebel in der Politik*

**21:45–22:45** hacking · en  
Apple vs. Google Client Platforms

*How you end up being the Victim.*

**00:15–02:15** show  
Hacker Jeopardy

*Number guessing for geeks*

Saal 2

**11:30–12:30** culture · en  
Eating in the Anthropocene

*Transgenic Fish, Mutagenic Grapefruits and Space Potatoes*

**12:45–13:15** hacking  
Data Mining the Israeli Census

*Insights into a publicly available registry*

**13:15–13:45** hacking · en  
Don't scan, just ask

*A new approach of identifying vulnerable web applications*

**14:00–14:30** hacking · en  
Reverse Engineering USB Devices

**14:30–15:00** society and politics  
A Brief History of Plutocracy

**16:00–17:00** hacking  
Power gadgets with your own electricity

*escape the basement and make the sun work for you*

**17:15–18:15** hacking  
Bionic Ears

*Introduction into State-of-the-Art Hearing Aid Technology*

**18:30–19:30** hacking · en  
Time is on my Side

*Exploiting Timing Side Channel Vulnerabilities on the Web*

**20:30–21:30** hacking  
Rootkits in your Web application

*Achieving a permanent stealthy compromise of user accounts with XSS and JS injection attacks.*

**21:45–22:45** hacking · en  
Building a Distributed Satellite Ground Station Network—A Call To Arms

*Hackers need satellites. Hackers need internet over satellites. Satellites require ground stations. Let's build them!*

**23:00–00:00** hacking · en  
Quantified-Self and OpenBCI Neurofeedback Mind-Hacking

*Transhumanism, Self-Optimization and Neurofeedback for post-modern hackers*

**00:15–01:15** show  
NPC - Nerds' Pissing Contest

*Mein Ruby ist besser als dein urxvt!*

Saal 3

**12:45–15:00** community · en  
Lightning Talks Day 2

**16:00–17:00** society and politics · en  
Privacy Invasion or Innovative Science?

*Academia, social media data, and privacy*

**17:15–18:15** society and politics  
Counterlobbying EU institutions

*How to attempt to counter the influence of industry lobbyists and political forces aiming towards increasing control over the Internet*

**18:30–19:30** hacking  
Ein Mittelsmannangriff auf ein digitales Signiergerät

*Bachelorarbeit Informatik Uni Kiel SS 2011*

**20:30–21:30** hacking · en  
Reverse-engineering a Qualcomm baseband

**21:45–22:45** hacking  
Post Memory Corruption Memory Analysis

*Automating exploitation of invalid memory writes*

**23:00–00:00** science  
Crowdsourcing Genome Wide Association Studies

*Freeing Genetic Data from Corporate Vaults*

# day 3 | 2011-12-29

Saal 1

11:30–13:45 society and politics · de  
Jahresrückblick

14:00–15:00 hacking · en  
Bitcoin—An Analysis

16:00–17:00 community  
7 years, 400+ podcasts,  
and a whole lot of  
Frequent Flyer Miles  
*Lessons learned from producing  
a weekly independent podcast on  
international conflicts and concerns.*

17:15–18:15 hacking · en  
Cellular protocol  
stacks for Internet  
GPRS, EDGE, UMTS,  
HSPA demystified

18:30–19:30 hacking · en  
Implementation of  
MITM Attack on  
HDCP-Secured Links  
*A non-copyright circumventing  
application of the HDCP master key*

20:30–21:30 culture · en  
The Hack will not  
be televised?  
*Hacker in Movies*

21:45–22:45 hacking · en  
New Ways I'm Going to  
Hack Your Web App

23:00–00:00 community · de  
Fnord-Jahresrückblick  
*von Atomendlager bis Zensus*

Saal 2

11:30–12:30 making  
Not your Grandfathers  
moon landing  
*Hell yeah, it's Rocket Science  
3.1415926535897932384626!*

13:15–13:45 hacking · en  
Security Log Visualization  
with a Correlation Engine  
*What's inside your network?*

14:00–14:30 society and politics · de  
Frag den Staat  
*Praktische Informationsfreiheit*

14:30–15:00 hacking · de  
TRESOR: Festplatten  
sicher verschlüsseln

16:00–16:30 hacking · en  
Oops I hacked my PBX  
*Why auditing proprietary  
protocols matters*

16:30–17:00 hacking · en  
Open source music:  
Tracking 2.0

17:15–18:15 culture · en  
The best of The oXcars  
*the greatest free/Libre  
culture show of all times*

18:30–19:30 hacking  
Print Me If You Dare  
*Firmware Modification Attacks  
and the Rise of Printer Malware*

20:30–21:30 hacking  
The future of cryptology:  
which 3 letters algorithm(s)  
could be our Titanic?  
*RMS Olympic, RMS Titanic, HMHS  
Britannic vs Discrete Logarithm, Integer  
factorization, Conjectured hard problems*

21:45–22:45 society and politics · en  
Towards a Single Secure  
European Cyberspace?  
*What the European Union wants.  
What the hackerdom can do..*

Saal 3

11:30–12:30 hacking · en  
Taking control over  
the Tor network

12:45–15:00 community · en  
Lightning Talks Day 3  
*Pecha Kucha Round!*

16:00–17:00 hacking · en  
Deceiving Author-  
ship Detection  
*Tools to Maintain Anonymity  
Through Writing Style & Current  
Trends in Adversarial Stylometry*

17:15–18:15 hacking  
Electronic money: The road to  
Bitcoin and a glimpse forward  
*How the e-money systems  
can be made better*

18:30–19:30 hacking  
Datenvieh oder Daten-Fee  
*Welchen Wert haben Trackingdaten?*

20:30–21:30 hacking · en  
Introducing Osmo-GMR  
*Building a sniffer for  
the GMR satphones*

21:45–22:45 hacking · en  
Behind the scenes  
of a C64 demo

23:00–00:00 hacking · en  
Sovereign Keys  
*A proposal for fixing attacks  
on CAs and DNSSEC*

# day 4 | 2011-12-30

## Saal 1

**11:30-12:30** science · en  
KinectFusion  
*Real-time 3D Reconstruction and Interaction Using a Moving Depth Camera*

**12:45-13:45** society and politics  
From Press Freedom to the Freedom of information  
*Why every citizen should be concerned*

**14:00-15:00** hacking  
The engineering part of social engineering  
*Why just lying your way in won't get you anywhere*

**16:00-17:00** science · en  
Quantum of Science  
*How quantum information differs from classical*

**17:15-18:15** hacking  
Security Nightmares

**18:30-19:00** community · en  
Closing Event

## Saal 2

**11:30-12:30** society and politics  
Resilience Towards Leaking or Why Julian Assange Might Be Wrong After All

**12:45-13:15** hacking  
Antiforensik  
*Einführung in das Thema Antiforensik am Beispiel eines neuen Angriffsvektors*

**13:15-13:45** hacking · en  
bup: Git for backups

**14:00-14:30** hacking  
ChokePointProject - Quis custodiet ipsos custodes?  
*Aggregating and Visualizing (lack of) Transparency Data in near-realtime*

**14:30-15:00** hacking · en  
NOC Review  
*NOC Review about the Camp 2011 and the 28C3*

**16:00-17:00** hacking · en  
Smart Hacking For Privacy

**17:15-18:15** society and politics · en  
Changing techno-optimists by shaking up the bureaucrats

## Saal 3

**11:30-12:30** hacking · en  
Your Disaster/Crisis/Revolution just got Pwned  
*Telecomix and Geeks without Bounds on Security and Crisis Response*

**12:45-15:00** community · en  
Lightning Talks Day 4

**16:00-17:00** hacking  
DC+, The Protocol  
*Even slower than Tor and JAP together!*

**17:15-18:15** hacking · en  
Evolving custom communication protocols  
*Hell Yeah, it's rocket science*