



Site Map

Search

# COMPUTERWORLD

Contact Us

Subscri

News & Features

Resource Center

IT Careers

Computerworld

## News

- Latest news headlines
- News by category
- CW Minute (audio)
- Continued from print

## Features

- Managing
- Year 2000
- Field Report
- In Depth

## Viewpoint

- Maryfran Johnson
- More columnists

## Latest publications

- Most recent publications

*(Online News, 08/10/99 11:27 AM)*

### Reporter's notebook: Hackers on holiday

By Ann Harrison

ALTLANDSBERG, GERMANY -- CAMPnet, billed as the largest civilian open-air Internet network ever created, sprang to life last weekend when 1,800 European and American hackers gathered at the Chaos Communication Camp outside Berlin. In a tent city, connected by a switched Gigabit Ethernet, hackers on holiday swapped security tools, ate waffles, viewed fire-eating demonstrations, discussed encryption politics and went for dips in the local lake. A camper who attempted to attack the network was subjected to local justice and found himself cleaning toilets.

Constructed around a fable involving an alien spaceship which hailed a group of hackers and touched down for repairs to their damaged computers, the camp featured a sculpted spaceship and a "landing area" illuminated by ghostly neon pillars. Inside the 300-foot Hacktent, long tables held hundreds of PCs brought by participants to connect to CAMPnet, which supported 1,500 hosts and carried an aggregate Internet bandwidth of 20M bit/sec.

Lounging outside near one of the seventeen "data toilet" portapotties that housed the network routers, Andy Muller-Maguhn said the camp reflected a cultural movement concerned with data security, privacy and the free flow of information.

"It's one thing to be on a mailing list," said Muller-Maguhn, who serves as a spokesperson for the Berlin-based Chaos Computer Club (CCC) that created the event. "But sitting in a campground and having discussions all night gets people networked more closely together and helps develop solutions to problems we haven't even faced yet, while computer companies sell solutions to problems we wouldn't have without them."

The featured event Saturday night was the Linux Death Match, in which teams of network administrators tried to halt one another's network services. The match was won by a team from Munich that chose not to attack, but instead fortified its machine with FreeBSD tools.

Tobias, a programmer and software developer from Berlin who was watching the match, said he was impressed by the level of expertise. "It's pretty amazing to see the knowledge these people have, all these people sitting here in front of these machines will never have problem finding a job," Tobias said. "Everyone around here knows how useful it

is to find vulnerabilities, and most of these people don't destroy systems, don't crack systems, they just look at them."

David Del Torto, director of technology for security services at Deloitte & Touche, taught a workshop entitled "Take This Job and Ping It/Hacking the Corporate Ladder for Fun and Profit." He said hackers were working at all the Big Five accounting and auditing firms -- where their skills are in high demand. "As long as you are not hacking the company you work for and destroying your reputation, you are going to have no problem getting jobs," Del Torto said.

Security flaws in commercial software and hardware were popular topics at camp workshops, which included discussions on "Biometric Insecurity" and the construction of Windows NT Shell Code for Buffer Overflow Exploits. The camp's re-engineering awards went to a group that developed a technique to alter the ID numbers on Global System for Mobile Communications cell phones and to another team that found a way to defeat a biometric fingerprint scanning system.

Despite their demonization in the press, hackers have traditionally distributed critical information about insecure products and used this information to search for better solutions, attendees said. Hugh Daniels, a California resident who presented a workshop on the Linux FreeS/WAN encryption project, pointed to the high rate of online credit card fraud. He said users should demand the creation of networks that cannot be stolen from and strong encryption to protect personal data. "I'm trying to build a civil society that holds up through mathematics, not guns," Daniels told the crowd.

Muller-Maguhn noted that unlike the U.S., which imposes export restrictions on strong encryption, Germany has politicians who listened to advice from the hacker community and chose not to impose similar controls. "People here are always thinking critically about fascism, so people want to drive the technology, not be driven by it," he said.

Dave Boyce, who works for an Internet service provider in Amsterdam, declared that the ultimate purpose of the camp was to create networks of activists to defend such policies. "It's important that crypto is free from government control so that we can exchange information freely because ultimately your freedom starts with the exchange of information," said Boyce. "What we are doing here is creating frameworks for the freedom of information."

[View latest headlines](#)

---

[NEWS & FEATURES](#) | [RESOURCE CENTER](#) | [IT CAREERS](#) |  
[COMPUTERWORLD, INC.](#)  
[Contact Us](#) | [Search](#) | [Site Map](#) | [Subscribe](#)

**COMPUTERWORLD**

Copyright © 1999 Computerworld, Inc. All rights reserved. [Legal notices and trademark attributions](#)

## COMPUTERWORLD

[trademark attributions](#)

  
Back to top

