The 23rd Chaos Communication Congress in Berlin, Germany

RADIO CHIPS AND HACKER TOOLS

The 23rd annual Chaos Computer Club Congress offered a fresh perspective on topics such as RFID technology and cyber-crime laws.

BY JAN RÄHM

Figure 1: Atul Chitnis (left) talked about his work for free software in India; Melanie Rieback (right) demonstrated how to fool RFID scanners.

The offbeat and engaging Chaos Computer Club held their 23rd annual congress – dubbed 23C3 – in Berlin on December 27-30. Approximately 4,200 people attended the "four-day conference on technology, society, and utopia."

Under the motto "Who can you trust?" the 23rd Chaos Communication Congress (23C3) provided 130 talks and 20 workshops on network technology, hacking, and monitoring.

The talk topics ranged from purely technical subjects, like the development of an object-oriented, secure TCP/IP stack, to hacker advisories, like "What to do if the cops search your apartment."

Lawyer Peter Voigt talked about changes in German law with respect to hacking tools. Voigt says the new laws will present system administrators with the impossible task of reconciling the legal requirements with real-world technology.

Even home Linux users may be in danger of crossing the line by using normal Linux distributions, with their enormous range of programs and libraries, including some that might infringe on the new laws.

Free Software in India

Atul Chitnis, an IT consultant and software activist from Bangalore, talked about the popularity of free software in India. Chitnis explained how small initiatives can turn into movements that change the face of politics.

Chitnis said that success in India is not based on emphasizing the advantages and the (financial) freedom of open source software, but on helping people use programs.

Can You Trust RFID?

One popular topic was the problem of Radio Frequency Identifiers (RFIDs). The CCC Sputnik project, in fact, turned the congress into a huge RFID experiment. To participate, volunteers could buy an RFID tag for a small contribution and be monitored for four days. The movements of up to 600 tag wearers are being evaluated and the results will be published online [1].

Harald Welte and Milosch Meriac introduced the freely programmable OpenPICC [2] RFID tag, the counterpart to the OpenPCD [3] RFID reader. Both PCBs are equipped with an ARM micro-controller by Atmel and can be linked up to a computer via USB.

The hardware design was published under a Creative Commons license. The firmware and the supporting Linux library, Librfid [4], are both available under the GPL.

OpenPICC can emulate arbitrary RFID transponders and smartcards that use 13.56 MHz technology. It simulates a transponder built to ISO standards 14443 and 15693, as used in passports with RFID chips. The "RFID Hacking" lecture demonstrated how to hack the chip.

The "A Hacker's Guide to RFID Spoofing and Jamming" lecture by Melanie Rieback discussed how to protect yourself against evaluation of RFID transponders and have some electronic privacy. Rieback developed a kind of protective shield against RFID readers based on OpenPCD.

Conclusion

The CCC calls their annual congress "the European hacker party." This year's event covered a broad range of topics related to technology and culture.

In the end, the 23rd Chaos Communication Congress delivered a fresh perspective on computer technologies that you won't find at other mainstream corporate conference destinations. ■

INFO

[1] Sputnik: *http://www.openbeacon.org/ccc-sputnik.0.html*

[2] OpenPICC: *http://www.openpcd.org/openpicc.0.html*

[3] OpenPCD: *http://www.openpcd.org*

[4] Librfid: *http://openmrtd.org/projects/librfid/*

[5] Information on 23C3: *http://events.ccc.de/congress/2006/Home*