25th Chaos Communication Congress

NOTHING TO HIDE

Chaos Communication Congress visitors were probably more interested in their digital civil rights, as reflected in the congress motto "Nothing to hide," but first they had to cope with closed ticket counters and overflowing rooms. **BY ANIKA KEHRER, NILS MAGNUS**

According to a hand-written sign, visitors arriving too late or briefly vacating their seats had to wait outside the door (Figure 1). With more than 4000 visitors at the 25th Chaos Communication, the record attendance forced organizers to cancel sales of multiple-day tickets on day two.

Between the Scenes

Some 260 helpers – Chaos Angels – supported the organizers, as did various teams of volunteers, including the Network Operation Center (NOC), the Chaos CERT network police, the POC switchboard, and the video crew. A delegation of 11 helpers arrived from the Forschungsgemeinschaft elektronischer Medien (Research Community Electronic Media – FeM), a society connected with the Technical University of Ilmenau and also responsible for streaming the 100 or so talks on the network and recording about 130 hours of video [1]. Considering the care that volunteers put into this event each year, it stands to reason that the atmosphere on all three floors of the building on Berlin's Alexander Square is friendly (Figure 2).

Typically, anybody who has anything to show just sets up a stall in the hack center at Chaos Communication Congress and explains their work. Mitch Altman, who held a workshop in a separate room to demonstrate his TV-B-Gone TV sabotage device, invited attendees to join in a tinkering session between the lecture theaters, giving guests a decidedly non-rocket science explanation of what all the diodes and wire cutters were for.

Networking Hacker Biotopes

As part of a worldwide movement to help create more local and permanent meeting places for technology enthusiasts and creative souls, panel speakers appealed for more hacker spaces (see Figure 3). The online platform at Hackerspaces.org welcomes contributions. Berlin's C-Base, a mixture of a hacker meeting point and an underground club [2], and Vienna's Metalab are regarded as archetypal hacker spaces.

A couple of years ago, these spaces inspired Nick Farr to export the idea to other continents. Two CCC talks followed, and it became apparent that the U.S. did not have open meeting points for creative computing fans at the time. Finally, Farr founded Hac DC in Washington. Jacob Applebaum, also a member of the panel, reported on similar activities in San Francisco, in the form of the Noisebridge Initiative.

Monitoring Network Traffic

Other tinkerers again found grateful takers at the congress. Xavier Carcelle, a telecommunications engineer and CTO with French start-up OpenPattern [3], talked about Powerline Communications (PLC), which is a network technology that uses sockets and power lines for OSI layers 1 and 2. Although PLC hardware already exists (Figure 4), French hackers wanted a free platform. OpenPattern, which is a hybrid somewhere between a project and a corporation, is working on its own design based on an FPGA chip.

Figure 1: Rooms were packed and attendees had to wait outside.

Figure 2: A mind thing: Visitors had nothing to hide.

Figure 3: An international panel appealed for a more cooperation between hackers and the general public. Hackerspaces activists Paul Boehm, Jacob Applebaum, Philippe Langlois, Esther Schneeweisz, Nick Farr, Bre Pettis and CCC host Jens Ohlig (figure left, from left to right).

Carcelle and his colleagues Florian Fanelli showed their Faifa software [4] at the congress. The software gives users the ability to debug and monitor modulated control frames, for example, on PLC connections. The French developers have released the tool, along with their hardware design and control software under the GPLv2. They hope to establish a developer community that will create a software stack for the MAC layer. "The feedback has been positive since we published the code at the congress," says Xavier Carcelle.

Opening Black Boxes

One trend you couldn't fail to notice was the inroads that hackers have made into hardware black boxes. Collien Mulliner, from Fraunhofer SIT, demonstrated telephone vulnerabilities, investigating buffer overflows in Symbian OS in the process.

Harald Welte took this a step further in his guide to dismantling smartphones. More and more high-end mobile devices have two controllers: an Application Processor (AP) that handles application control, and a Baseband Processor (BP) that handles wireless activity and phone calls.

Dismantling Phones

Despite increasing numbers of SDKs for the AP – or for higher-level layers, such as Google Android – manufacturers are still reticent when it comes to hardware, which is all the more reason for Welte & Co. to investigate the hardware more closely. Many telephones have debugging soldering points for the JTAG interface on their PCBs. With more than a little dexterity and a trusty soldering iron, hackers can attach and fire up a serial console (Figure 5).

INFO

[1] 25c3 website with lecture notes: *http://events.ccc.de/congress/2008/*

[2] C-Base: *http://www.c-base.org*

[3] OpenPattern: *http://openpattern.org*

[4] Faifa: *https://dev.open-plc.org*

Genuine Vulnerabilities

Whereas the first days of the congress were colorful and entertaining, but lacking in novelties, the organizers pulled a security ace out of their sleeves on the final day. After all, data tourists used to visit Berlin to marvel over the latest vulnerabilities. An international team of researchers and hackers disclosed how they had exploited a known, but widely ignored, MD5 vulnerability, with a couple of hundred dollars, and 200 PlayStations to create a CA keypair that was indistinguishable from the real thing.

There was no answer to the question of whether investigation authorities have purchased CA certificates yet to comply with the BKA (Germany's Federal Criminal Police Office) rules introduced at the beginning of 2009. At the end of the event, our verdict was mixed – overfilled rooms, a variety of topics, and an audience that was wide awake but still slightly puzzled as to whether it was currently witnessing the sell-out of freedom on the network. ■

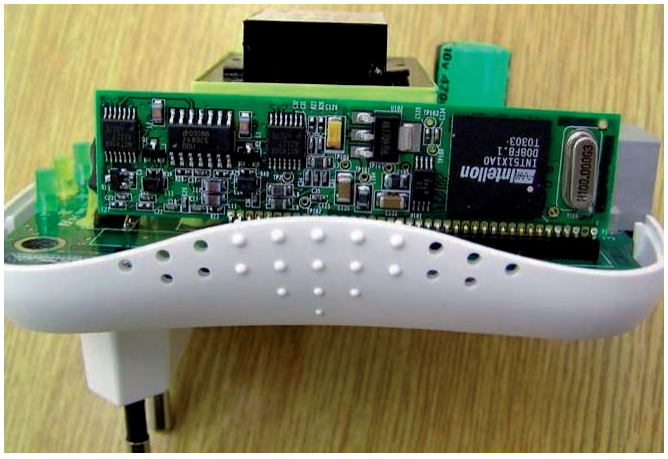

Figure 4: PLC devices use Ethernet to connect PCs with the mains network in the building. The Faifa tool, which is based on Open PLC architecture debugs networks of this kind.

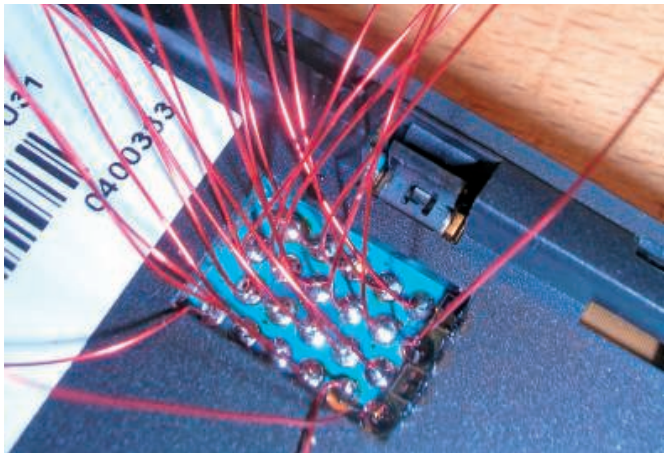

Figure 5: Wire and more than a little dexterity are needed to solder a serial console onto a Glofiish smartphone. JTAG connectors provide access.