

26th Chaos Communication Congress in Berlin

ENTER THE DRAGON



John Aslund, Creative Commons

Under a banner of “Here be dragons,” an inscription found on old navigational charts, the Chaos Computer Club held its annual conference for the 26th time. **BY ANIKA KEHRER AND NILS MAGNUS**

Guarded by a watchful dragon, the Chaos Computer Club (CCC) welcomed some 4,000 visitors to Berlin’s Congress Center at Alexanderplatz. Despite having to wait in line, visitors were able to experience around 80 talks.

The annual CCC event is known for its infectious blend of technology and politics. Spokesperson Frank Rieger echoed the navigation theme with his discussion of the similarities between seafarers of yore and the hacker community “seeking the unknown for treasure.” People are increasingly interested in discovering the truth behind systems and processes,” Frank said. He added that governments should place a high priority on free communication and transparency. “Business secrets can’t be a reason for hiding processes,” he said, referring to voting machine vendors that refused to reveal their protocols and code.

In line with this credo, most of the 83 contributions dealt with social and political topics ranging from the Access Impediment Act through network neutrality [1]. About one third of the talks under the “Hacking” umbrella focused on tangible, technical issues and mainly concerned network and system security – this seems to be a slight drop compared with previous years. In contrast, soldering courses and hardware tinkering conquered more floor space.

Tweakers and Castles

The main developer behind the Milkymist project [2], Sébastien Bourdeauducq, demonstrated a prototype of his Visual Synthesizer – an embedded helper for DJs that generates video from music. He implemented the first prototype of his System on Chip (SoC) on a US\$ 500 Xilinx ML401 board. The board runs a Linux 2.6.23 kernel and simula-

tors such as Verilog with GPL Cver. He has been working on his own board for around two months: It will be smaller and capable of processing both audio and video input, with Ethernet as well as USB ports. The system will run the embedded µClinux system.

Germany’s recently stalled Access Impediment Act, which was designed to display stop signs when users attempt to access child pornography sites, was the subject of several talks. One talk discussed the contradictions in the public discussion and proposed a replacement for DNS to decentralize control instances. Christian Bahls, the Initiator of the NGO Missbrauchsoffer gegen Internetsperren (MOGIS, which translates to *Victims of Abuse Against Internet Blocking*), took a pugnacious stand. MOGIS represents victims of sexual abuse who are opposed to Internet access impediments.

Bahls mentioned that the German newspaper *Die Welt* reported on a survey initiated by a German child aid association that stated that around 90 percent of all Germans are in favor of Internet blocks. To demonstrate that the ques-

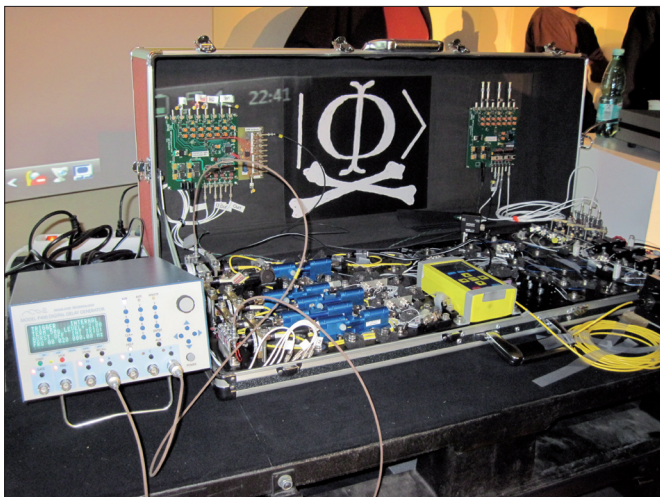


Figure 1: Setup of the MitM attack on quantum encryption - the box on the left is the impulse generator an attacker could use to manipulate the recipient's detectors.

tions were stated in a suggestive way, Bahls did a survey of his own and posted the results online just a day later. According to Bahls' survey, it would appear that 90 percent of all Germans are *against* the access impediments - depending on how you ask the questions.

A Final Quantum of Security

Not even quantum cryptography is secure any more, even though it doesn't really exist outside of university campuses. In 2009, a single large test network between Cern, Quantique, and a few universities went online [3]. Two years ago, enthusiastic young scientists demonstrated their command of quantum physics by using entangled photons to transmit confidential data. This year, however, Qin Liu from Norway's University of Science and Technology in Trondheim and Sebastien Sauge from the Royal Institute of Technology in Stockholm exposed the vulnerability of quantum cryptography by performing a public man-in-the-middle (MitM) attack.

After a 45-minute binge of physics slides by Sauge, Liu unveiled a device the size of a travel trunk (Figure 1). He demonstrated the vulnerabilities of commercial detectors that "go blind" - that is, fail to detect photons - at a certain brightness of the light reaching them. The reason for this problem is a simple restriction relating to the specific tolerances within which they must be constructed. Attackers can just grab quanta at will because the recipient would sim-

ply think nothing was coming down the line. On top of this, an attacker could use their own impulse generator to inject fake messages.

Conquering Iceland

The whistleblower Wikileaks platform (Figure 2), which is protected by a cascade of Tor servers, published a number of explosive documents in recent months, including previously secret Toll Collect contracts [4], a military police report concerning the controversial Kunduz bombing of a tanker in Afghanistan, and a comprehensive collection of pager messages before and after September 11, 2001. The project publicizes occurrences that might otherwise be unreported because the informer could face legal or political action. Wikileaks offers both technical and legal aid [5].

Because Julian Assange and Daniel Schmitt, representing the project at 26c3, felt that many published documents were too long or too complicated, the whistleblower project will be looking for a way to offer journalists exclusive rights for a short time to provide an incentive for further study.

The plan to set up "a data technology utopia; a kind of Switzerland of bits," as Schmitt called it in Iceland, takes things a step farther: "Following the demise of several Icelandic banks, we were able to present documents that listed insiders who had been able to rescue their valuables before the crunch hit home.

"All of a sudden, many Icelanders started listening to us." Now, the



Figure 2: Visitors learned about the work of Wikileaks and the Whistleblower project to protect the confidentiality of news sources. Pictured are Julian Assange and Daniel Schmitt (left to right).

Wikileaks team has put forward draft legislation at Iceland's parliament, hoping to see it passed before Iceland joins the European Union. The activists seek to compile "the best of all data protection acts and freedom guarantees from other constitutions."

Tongues of Angels

This annual meeting of the Chaos club does ask quite a bit of its visitors. Many visitors from outside Berlin stood in lines hundreds of yards long to purchase tickets for the congress, and on all days, tickets were sold out by noon.

Seats, or even access to the lecture theaters, were hard to come by. This prompted Hackerspaces activist Nick Farr to control rigorously (but without losing his humor) the placement of empty seats.

Video streams offered at several locations in and around Berlin were poor consolation. Rumors on the congress wiki hint that the congress will be changing location next year. ■

INFO

- [1] Overview of talks 26c3: <http://events.ccc.de/congress/2009/Fahrplan/>
- [2] Milkymist: <http://www.milkymist.org>
- [3] Test network for quantum cryptography: <http://www.swissquantum.com>
- [4] Toll Collect contracts: <http://netdefences.com/tag/toll-collect/>
- [5] Wikileaks: <http://wikileaks.org>