

## Researchers and practitioners head to San Jose

# USENIX SECURITY 2008

The 17th Security Symposium met in San Jose, California, USA, during the week of July 28, with a refereed paper track and Invited Talks. **BY RIK FARROW**

**U**SENIX Security might lack the buzz surrounding DefCon, but the content more than makes up for this. The competition for getting a paper accepted is fierce, with only 27 of 174 papers getting the nod from the Program Committee this year. And you will find the research behind some of the hot topics in security in these papers.

Niels Provos delivered a paper and an invited talk, both about the work he has been doing at Google to uncover infected websites. Google, like other search engine companies, creates constantly updated caches of web pages. Provos and his associates have built software that scans tens of millions of web pages each day, selecting a million URLs to load into instrumented virtual machines running Windows and IE.

Provos said that one in a thousand URLs will direct IE to a malware download site that can result in Windows being automatically exploited – a drive-by download. The distribution of malware-infected web servers by type is

roughly equivalent, so visiting a financial or social networking site is almost as dangerous as hitting sites with adult content.

Researchers like to collect new malware variants, and a team from Johns Hopkins (that included Provos) built the world's most flexible server to do just this. Sam Small explained how they used a natural language learning approach to design a server that can elicit responses from a wide range of protocols, allowing the researchers to collect malware for analysis – imagine a server that responds “correctly” as if it were running more than 500 web services.

Although MIT students were prevented from presenting their talk about getting free Mass Transit rides at DefCon, two students from the University of Virginia and two members of Chaos Computer Club Berlin wrote a paper detailing how to recover the encryption keys used in the same RFID chips (Mifare) that the MIT students wanted to describe. Their technique required both physical meth-

ods (acetone to separate the chip, then polishing to remove layers) and software techniques to identify the encryption key encoded in the revealed gates.

More recent research getting attention involved reading the DRAM of systems after they had been turned off. William Clarkson presented “Cold Boot Attacks on Encryption Keys,” which was awarded best student paper, and showed how data can be extracted from memory more than half an hour after a system has been shut down – if the RAM is kept cool. Clarkson proved that he and his co-authors could recover the encryption keys used by OS X's File Vault, Vista's Bit Locker, and several schemes used in Linux to encrypt hard drives.

The best paper award went to Jian Zhang, Phillip Porras, and Johannes Ullrich, who wrote about their system for creating highly predictive blacklisting. By grouping sites both regionally and according to their attack surface, they improved on the effectiveness of both the Global Worst Offender List (GWOL) and Local Worst Offender List (LWOL).

I found comments by Dawson Engler, one of the founders of Coverity, a static code-checking tool, really incredible. During his invited talk, Engler said that many of Coverity's customers object to improvements in their tools because it finds more potential bugs – and thus makes the customers' code look worse. It seems that many organizations would prefer not to know where their bugs are.

The papers are available at <http://www.usenix.org/events/sec08/tech/>, and you can find video streams of invited talks courtesy of *Linux Pro Magazine* [1] (Figure 1). ■



Figure 1: Linux Pro Magazine provided a live stream from the conference.

## INFO

- [1] *Linux Pro Magazine* video archives: [http://www.linuxpromagazine.com/usenix\\_sec08](http://www.linuxpromagazine.com/usenix_sec08)