The Hacker in Your Hardware

As if software viruses weren't bad enough, the microchips that power every aspect of our digital world are vulnerable to tampering in the factory. The consequences could be dire

BY JOHN VILLASENOR

KEY CONCEPTS

- Integrated circuits are increasingly complex and capable—but also increasingly vulnerable to attack.
- The circuits typically include designs from many sources. A "Trojan" attack hidden in one of these designs could surface long after the circuit has left the factory.
- A few relatively simple measures could go a long way toward protecting hardware from malicious hackers.

—The Editors

YOUR ONCE RELIABLE MOBILE phone suddenly freezes. The keypad no longer functions, and it cannot make or receive calls or text messages. You try to power off, but nothing happens. You remove the battery and reinsert it; the phone simply returns to its frozen state. Clearly, this is no ordinary glitch. Hours later you learn that yours is not an isolated problem: millions of other people also saw their phones suddenly, inexplicably, freeze.

This is one possible way that we might experience a large-scale hardware attack—one that is rooted in the increasingly sophisticated integrated circuits that serve as the brains of many of the devices we rely on every day. These circuits have become so complex that no single set of engineers can understand every piece of their design; instead teams of engineers on far-flung continents design parts of the chip, and it all comes together for the first time when the chip is printed onto silicon. The circuitry is so complex that exhaustive testing is impossible. Any bug placed in the chip's code will go unnoticed until it is activated by some sort of trigger, such as a specific date and time—like the Trojan horse, it initiates its attack after it is safely inside the guts of the hardware.

The physical nature of hardware attacks makes them potentially more problematic than worms, viruses and other malicious software. A virus can jump from machine to machine, but it can also in principle be wiped clean from any system it infects. In contrast, there is no fix for a hardware attack short of replacing the infected units. At least, not yet.

The difficulty of fixing a systemic, malicious hardware problem keeps cybersecurity experts up at night. Anything that uses a microprocessor—which is to say, just about everything electronic—is vulnerable. Integrated circuits lie at the heart of our communications systems and the world's electricity supply. They position the

KENN BROWN *Mondolithic Studios*

Security

Hacker Spoofs Cell Phone Tower to Intercept Calls

By Kim Zetter ✉ July 31, 2010 | 7:57 pm | Categories: Cybersecurity, DefCon, Surveillance

A directional antenna is set up for a demonstration by security researcher Chris Paget, center. (Photo: Dave Bullock)

LAS VEGAS — A security researcher created a cell phone base station that tricks cell phones into routing their outbound calls through his device, allowing someone to intercept even encrypted calls in the clear.

The device tricks the phones into disabling encryption and records call details and content before they're routed on their proper way through voice-over-IP.

The low-cost, home-brewed device, developed by researcher Chris Paget, mimics more expensive devices already used by intelligence and law enforcement agencies – called IMSI catchers – that can capture phone ID data and content. The devices essentially spoof a legitimate GSM tower and entice cell phones to send them data by emitting a signal that's stronger than legitimate towers in the area.

"If you have the ability to deliver a reasonably strong signal, then those around are owned," Paget said.

Paget's system costs only about $1,500, as opposed to several hundreds of thousands for professional products. Most of the price is for the laptop he used to operate the system.

Doing this kind of interception "used to be a million dollars, now you can do it with a thousand times less cost," Paget said during a press conference after his attack. "If it's $1,500, it's just beyond the range that people can start buying them for themselves and listening in on their neighbors."