SPECTRUM ONLINE
ABOUT IEEE SPECTRUM
READER SERVICES
CONTACT US
ADVERTISING MEDIA CENTER

IEEE
Search Spectrum go
Font Size: A A A

Jul 2006 Issue

SELECT AN ISSUE
July 2006
IN THIS ISSUE:
FEATURE ARTICLES
NEWS ANALYSIS
OPINIONS
RESOURCES
INDUSTRY FOCUS
UNIVERSITY FOCUS
SPECTRUM EXTRAS

July 26th, 2006

PICKING YOUR SECURITY APART

Today, Senior Associate Editor Stephen Cass reports on the Hackers on Planet Earth conference that took place over the weekend in New York City. Watch his accompanying video blog here. And click on the Read All link below to read a special item on protecting the physical security of your IT infrastructure.

Stephen Cass

Last weekend hackers from all around the world descended on New York City. They were in town for the sixth biannual HOPE conference. HOPE, which stands for Hackers on Planet Earth, is sponsored by *2600: The Hacker Quarterly*. The conference is very much a grassroots affair, with talks running from morning to midnight. Security and privacy concerns combined with a strong anti-authoritarian streak shaped most of the talks. The talks ranged from setting up community-based low power FM radio stations, exposing security weaknesses in wireless networks, and social engineering. Social engineering is the art and craft of getting people to tell you all sorts of information they really shouldn't on the strength of a believable line of patter, often over the phone. The best IT security in the world is useless if you haven't trained your intern not to give out passwords to anyone who calls claiming to be a harried technician at headquarters. (In the interests of full disclosure, I also gave a talk at the conference, giving out tips on dealing with the mainstream media.)

One of the most important talks however concerned not digital security but physical security. Barry Wells, of the Dutch lock-picking hobbyist group TOOOL (The Open Organization of Lockpickers) and Marc Tobias, a well-known security consultant, demonstrated a worrying new method to defeat many of the locks in use today. The technique, known as bumping, requires little training and can open susceptible locks in a few seconds.

Bumping works on most pin-tumbler locks, which make up the vast majority of locks. If you have a key that is basically flat and looks like a jagged line in profile, then you're putting it into a tumbler lock (dimple locks, which use keys that feature little circular pits in a flat key, are also at risk.) Many of these locks are used to protect vital public and private infrastructure, and this should be worrying to IT managers. While IT professionals often put long hours in to make sure their systems are secure from electronic attack, they often don't pay as much attention to securing server rooms and so on. Often they assume that the locks that came with their building can keep the bad guys out. However, in the U.S., the new Sarbanes-Oxley rules set out minimum standards for physical security. According to Tobias, the advent of bumping may keep many installations from meeting those standards.

About Tech Talk

RECENT POSTS
Tracking the Next Killer Storm
A Valley Blossoms Again
Shocking a Cancer Cell
Tricking the Eye
Katrina: FCC Seeks Comments

ARCHIVE
August 2006
July 2006
June 2006
May 2006
April 2006
March 2006
February 2006
January 2006
December 2005
November 2005
October 2005
September 2005

For a full discussion of how bumping works and an analysis of the risks, visit Tobias's website. In a nutshell, it works like this: First, the would-be intruder has to get the type of key that fits your lock. This is often not hard—hardware stores sell dozens of different locks and matching keys and many more can be obtained online. Next, the intruder files it down to make what is known as a "999" key, which has a low sawtooth shape. This filing can be done by hand—perfect accuracy is not required. The end and handle of the key are also filed down fractionally. Then the intruder simply inserts the key and hits it sharply with a hammer.

The shock travels inside, to a row of so-called key pins of varying heights. On top of each key pin sits a spring-loaded driver pin. Normally, when the correct key is inserted, the key pins raise the driver pins just enough to clear the barrel of the lock, allowing the cylinder containing the key to turn. The wrong key won't raise the key pins to their correct heights.

But the hammer-shock makes the driver pins leap upward, out of the cylinder, leaving the key pins in place. For a moment, there are no driver or key pins preventing the cylinder from turning, and so a well-timed twist can open the lock, usually with no sign of forced entry. Because bumping only takes a few seconds, a visitor to your facility could gain unauthorized access in the length of time it takes someone to find the restroom.

What's especially worrying is that the strategy defeats the natural response to a break-in, which is to replace the lock with another lock of the same, pin-tumbler kind. If that happens, a missing key, once filed down, could continue to give access almost as easily as before.

There are locks on the market which are not vulnerable to bumping, but these are not yet common. So, if you're responsible for protecting your company's digital assets, and you haven't given a thought to the door, desk, and cabinet locks protecting your hardware, it's time to think again.

Comments
YAAAAAAAAAAAAAAAAAAAAAAA
Posted by: rawr | 28 July 2006 2:19 PM

Post a Comment

Site Map | Copyright | Privacy | Terms of Use | RSS