Hal Berghel

DEFCON 16 REVISITED A HACKERS PARADICE

For those of you who don't already know about Defcon (defcon.org), it's the most well known, and so far as I know the largest, "hacker" conference in the world. It's held every August in Las Vegas the week after its smaller cousin, the Blackhat conference (blackhat.com). The Defcon and Blackhat Conferences have produced many of the vulnerability announcements that have shaken the IT world over the past few decades. You may recall the media frenzy over Michael Lynn's revelation in 2005 that Cisco's IOS contained a shellcode and remote execution vulnerability that prompted Cisco to sue Lynn and Blackhat (cf. www.infowarrior.org/users/rforno/lynn-cisco.pdf). Many of the presenters are shared by both conferences. Defcon is the more popular conference and appeals to a broader audience. For that reason I've chosen to cover it in this column.

Defcon is the public face of a relatively private community of geeks (in a positive sense of the term). Organizers include people with monikers like Dark Tangent, Kingpin, and Pyr0, while contributors include N.N.P, jur1st, and Major Malfunction. The pseudonyms are pretty harmless nowadays, as most of the insiders seem to know each other personally. In the old days, however, pseudonyms played a much more important role in the hacker community in maintaining hacker anonymity. But that was before the commercial Internet became a business necessity and federal legislation made computer and Internet hacks a felony. Of course 9/11 made hacking an even larger blip on 3-letter agency's radar. So, the latest Defcons are more restrained and politically responsible, but still quite interesting. I've selected a few presentations from this year's event that may be of interest to you.

Locksport Rules!

Lock picking has always fascinated me. My first acquaintance dates back to a presentation in an early Defcon in the past century. The speaker demonstrated his lock picking skills with homemade tools made from filed hacksaw blades as I recall. The art of lock picking seemed like good fun, and I had a considerable stash of dull hacksaw blades, so I was off to the races with a 99-cent Wal-Mart padlock. It took me a few weeks to open it the first time, but once I got the hang of it I found I could do it in a few seconds. In short order, I was up to cheap deadbolts from Home Depot.

In the intervening decade, locksport (what the enthusiasts call what they do) has reached unimagined heights. At Defcon 16, the big news was a vulnerability in 3rd generation Medeco locks - considered to be the best-of-breed in government and corporate security. What makes these locks so interesting, and difficult to pick, is that they use three levels of security. Like all tumbler/pin locks, the pins raise and lower to the shear line to allow the tumbler to turn. But with Medeco locks, each pin rotates individually and also slides into different positions in the pin set. For anyone with a mechanical bent, Medeco locks are a thing of beauty! Needless to say, two Defcon presenters demonstrated how one could pick this heretofore bastion-quality lock. One used a homemade tool crafted from guitar wire and a hollow tube filled with K-B Weld. The second presenter, Marc Tobias, discussed more sophisticated tools and achieved the same result. To give you an idea of how serious some folks take this work, Tobias has published a 1,400 page tome on the subject! I was impressed to say the least. For those interested in additional information, several websites serve the locksport community, such as www.locksport101.com and security.org in particular were touted by the speakers at Defcon. [FYI: presenters stated that they gave Medeco time to release a patch kit for their locks that overcome the vulnerability before making it public!]

Weaponizing Google

I heard a new term at Defcon, "Gmalware" - which stands for Google Malware. Google seems to be following Microsoft in terms of propriety and predatory disintermediation department, with equal disdain from the privacy and open source zealots.

I've had "issues" with Google's business practices since its infancy. For one thing, the harvesting of copyrighted material from networks without recognition of author's rights really irritated me. I threatened to sue one of my publishers several years ago if they didn't protect my copyright aggressively and stop Google from harvesting my work. Google seemed to be of the view that anything on the Internet can be appropriated without recognition of ownership or payment of royalty. The problem that many of us had with Google was that they generated advertising revenue from content that was appropriated from information providers who posted the content solely for individual and non-commercial use. Fortunately, an ever-growing community of copyright lawyers finally disabused Google from continuing that practice.

Today, Google engages in the more subtle, and what I consider more insidious, practice of retaining personal information about users (e.g., names, email addresses, billing information, IP address, URLs, date and time of request, browser type and language - basically anything they can get their hands on. (cf. google.com/privacy.html)). Let's be specific here: if you use any Google service, a record of that use and any personal information about you that Google can extract from that use is recorded in a Google database!

In order to make their job easier, Google uses "helplets" called Google Gadgets. That's where Gmalware comes in. These gadgets have been shown to have vulnerabilities that put users at considerable risk. This risk was discussed in a Defcon presentation entitled "Xploiting Google Gadgets: Gmalware and Beyond" by Robert Hansen and Tom Stracener. Hansen (aka 'Rsnake') apparently was the first to document this in a 2007 blog. According to Hansen, this vulnerability was reported to Google over a year ago but remains unpatched. Why? Hansen conjectured that the rather steep downside accrues to the user and not to Google, and the source of the malicious code is a 3rd party rather than Google, so it's not their problem. It would appear to me that Google's culpability akin to that of a property owner who's created a "convenient nuisance." In any case, Hansen's point seems convincing to me.

The Defcon and Blackhat Conferences have produced many of the vulnerability announcements that have shaken the IT world over the past few decades.

The risk has to do with Cross-site Scripting (aka XSS) which is a code injection attack that affects web sessions. XSS is now the leading web-based attack vector. Though there are many varieties of XSS, the one that affects Google gadgets is the arbitrary execution of javascript within the Gadget.

The general idea is this. First, Google gadgets support javascript by nature. One of the reasons for this is the online monitoring mentioned above. These javascripted gadgets allow Google to track user behavior. But the XSS vulnerability offers hidden "features" as well for the javascript executes whenever a browser activates the gadget: if a corrupted gadget (malware) can be substituted for the intended gadget (that's what XSS is all about) the gadget may become "weaponized" - read that as "hostile to the user."

Two points seem incontrovertible to me: first, javascript support is required by Google to support its own mischievous logging goals (cf. www.google.com/analytics) and will continue for the foreseeable future. Second, the XSS/javascript vulnerability is real and there doesn't seem to be much a Google gadgeteer can do to protect from it. As if that isn't enough, the next pair of speakers on the stage showed how XSS could be used to attack social networks! Maybe a future mantra will be "getting Facebook out of your face."

Newsworthy

Three days of Defcon produced much more interesting information that we can discuss here. The list below is just a smattering potpourri of topics covered.

- A website that allows you compromise Internet kiosks
- A tool that supports SQL injection of Oracle databases
- How Google harvesting can target celebrities and politicians
- LAN link-layer vulnerabilities that still exist in the enterprise
- A new rootkit for NetBSD
- Electronic billboard hacking
- Sniffing cable modem traffic

We would be remiss without reporting two that caught our eye as well as that of law enforcement. The scheduled presentation on War-Ballooning went off without a hitch. The same could not be said of planned launch of the test platform. War-ballooning is one of the later incarnations of war driving - a mobile platform for detection, analysis, and possible capture of Wi-Fi transmissions. Defcon has supported war driving competitions for quite a few years, but the use of balloons was thought to be a new twist on the old theme.

The presenter, Rick Hill, had apparently launched a prototype in Virginia this past June. The prototype consisted of both directional and omni-directional 801.11 antennas, a security camera, and a WAP, tethered by a fiber optic link to ground. The biggest obstacle was not the technology, but the approval process. Hill had sought permission to "fly" this war-balloon 150 feet above the Riviera Hotel (Defcon HQ) in Las Vegas during the conference. Needless to say, the FAA and local law enforcement were really not keen on the idea and Hill's hopes were quickly dashed prior to the event.

A second controversial presentation came from some MIT students who were pulled off the program by order of a US District Court. Their talk, "Anatomy of a Subway Hack," showed how to subvert the fare payment system on Boston subways. Ironically, by the time the Court issued a "prior restraint" order on Saturday, August 16, 2008, Defcon had already distributed the author's PowerPoint slides to all registrants. Within a few hours the information had penetrated more of cyberspace than economy and good taste would recommend.

Social Experience

Defcon is not a typical scientific or technical conference. If you attend Defcon in the future, don't expect a user-centric experience. No checks or credit cards taken - just cash. No receipts. For the $120 admission you get a goofy electronic badge and the opportunity to hear some interesting speakers if you can make locate and "interpret" the scarce signage. Expect a surplus of hubris and hyperbole with a shortage of humility.

Defcon is a social experience as much as a meeting. There is a "Leet" (geek speak for elite) skills competition, Hacker Jeopardy, a guitar hero competition, speed lockpicking competitions, "capture the flag" hacking contests, scavenger hunts, a wardriving competition, the Black and White ball, and so forth. If you don't mind maneuvering through somewhat ill-behaved crowds at times, Defcon remains a fun place to learn about a very different perspective on IT than one would find near the enterprises water coolers and boardrooms.

Hal Berghel is Associate Dean of the Howard R. Hughes College of Engineering at UNLV and Director of the new UNLV School of Informatics. He is also Director of the Identity Theft and Financial Fraud Research and Operations Center. His consultancy, Berghel.Net, provides security and management services to government and industry.