Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 55
05 Γενάρη 2007

Computer Warming a Privacy Risk
Wired News (12/29/06), Q. Norton

Cambridge University researcher S. Murdoch has found a method for bypassing online anonymity systems by analyzing a computer's temperature over the Internet. The technique utilizes the phenomenon called "clock skew," where precise clocks in computers drift away from the correct time at varying rates, depending on heat. Every crystal has a unique clock skew, Murdoch says. A UCLA PhD student displayed the ability to use clock skew to identify computers on the Internet through charting the timestamps of a machine's traffic, but this technique can get at best 64 fingerprints: a thousand computers connected in a network would contain 16 with identical clock skews. Murdoch became the first person to successfully carry out an anonymity attack online. He attacked Onion Router, or "Tor," a privacy system that allows users anonymous Internet access. He established a Tor network at Cambridge to try out his method. Murdoch says that in order to get the IP address of a hidden server on a Tor network, an attacker would request something complicated from the server, causing it to warm up, resulting in clock skew. The attacker then looks at computers he thinks may be the Tor server, searching for a change in skew over a few hours. He has found his match when he locates a computer with the specific change in its timestamps. Murdoch admits that it's not the ideal attack, but " it's a guide to what could be done in the future."

New Program by UMass Amherst Computer Scientist Prevents Crashes and Hacker Attacks,University of Massachusetts Amherst (12/26/06)

A new program, named DieHard, has been developed by University of Massachusetts Amherst computer scientist E. Berger and Microsoft researcher B. Zorn to remedy problems caused by programming that doesn't make proper use of the large amount of memory on today's computers. While running, programs request chunks of memory space to store items such as images, but often items will be assigned a space that is already occupied, or space that is not large enough, causing overflows into other spaces. The result of these mistakes can be a crash, or worse. "Ironically, crashing is the best thing that can happen," says Berger. "An overflow also can make your computer exploitable by hackers." Another danger is that the location that a password is given can be the same for every version of a given program, allowing a hacker who has overwritten a password to find this address on all existing versions. To prevent these dangers, DieHard distributes groups of memory, assigns random addresses to items during each session, launches several versions of a program being run in case one starts to crash, and detects the probability that a certain bug has affected a user. Berger blames the current problems on programmers who are too worried about speed and efficiency, at the expense of security. "Today we have way more memory and more computer power than we need," he says. "We want to use that to make systems more reliable and safer, without compromising speed." Free versions of DieHard are available for non-commercial use for both Linux and Windows.

Cybercrooks Deliver Trouble

Washington Post (12/27/06) P. D1; B. Krebs

A record-breaking rise in spam and more sophisticated cyberattacks were noted this year by computer security experts, who only expect worse things next year. "Criminals have gone from trying to hit as many machines as possible to focusing on techniques that allow them to remain undetected on infected machines longer," says Symantec's V. Weafer, while Postini estimates that over 90% of all email sent online in October was spam; computers controlled by cybercrooks, or "bots," are responsible for relaying a great volume of junk email. "We're getting an unprecedented amount of calls from people whose email systems are melting down under this onslaught," says Postini's D. Druker. Beyond Security's Gadi Evron reckons that at any given time there are 3-4 million compromised computers actively relaying spam, while millions more are used to launch distributed denial-of-service attacks. In addition, he believes organized criminals will net about $2 billion in 2006 via "phishing" scams. Experts are also signaling that online crime is becoming a full-time venue for many, as evidenced by a movement of online criminal activity from nights and weekends to weekdays. Furthermore, experts are seeing an increase in the sophistication of techniques cybercriminals are using to dodge anti-fraud initiatives. Attacks that exploited flaws in software applications that operate on top of operating systems were also a notable development this year, as were increasing numbers of zero-day software vulnerabilities.

Lessons for the Mentor
CIO Australia (12/11/06), B. Kunkel

B. Kunkel, CIO of a national law firm and member of the CIO Executive Council, understands the need to help young people interested in IT develop their potential, and has created a summer university internship program to provide much-needed resources to her department, while helping young women get a foothold in IT. She lists five lessons she has learned from her work with the interns: Assignments given to interns must be clearly connected to the overall work environment and objectives so interns are constantly reminded that their work makes a difference; teams are preferable to working alone for interns; interns will get more out of their work if they are challenged to think creatively; communication is a top priority, as young people respond to feedback; and a social environment in the work experience is extremely important. Kunkel used these concepts to sculpt a "work curriculum," similar to that of a college course. By linking assignments with objectives, she could see the interns' confidence and creativity flourishing, despite their being intimidated by the scope of the task set in front of them. Each week Kunkel met with interns to talk about expectations. Kunkel also demanded communication from the interns in the form of a weekly email, discussing their current assignment, as well as emails introducing themselves to the entire IT department. She claims her experience proves that effective mentoring is an undeniable way to nurture talent, calling it "one of the highlights of my career."

Q&A: E-Voting Issues Still There
IDG News Service (01/02/07), G. Gross

ACM US Policy Committee Chairman E. Spafford, executive director of the Purdue University Center for Education and Research in Information Assurance and Security, says much work remains to ensure the accuracy and reliability of e-voting systems. Spafford says that all e-voting equipment should have independent audit capabilities such as paper printouts by the next election. "The goal should be to design systems carefully with the fault levels in mind and an appropriate way of using paper, if that's the mechanism," he says. "If you look at it as a design issue, there are many ways of using paper appropriately that don't have the disadvantages." Spafford named optical scan machines as an appropriate use of paper ballots. While some ideas involving a cryptographic algorithm that outputs a cryptographic receipt have been put forth, he understands that most voters would not understand such technology and would have to take another person's word that their vote is both correct and confidential: "The method of having a paper record is a technology people can immediately grasp and understand. That's really important. We want not only to protect the vote, but we want people to feel comfortable that their vote matters." Spafford also says that many officials do not understand that reliability is just as big of a problem as security. He notes the recent Florida House of Representatives race, in which around 18,000 voters who voted in other races did not vote, seems to be the result of poor design or a machine failure, not a security issue.

Privacy, Patents on Agenda for New Congress
IDG News Service (01/01/07), G. Gross

The new Democratic Congress is eager to fulfill its campaign promises and address the tech issues that the outgoing Republican Congress failed to pass legislation on. Bush's surveillance program will come under scrutiny and further legislation to protect individuals' privacy is expected. However, the Supreme Court might have pre-empted any legislation concerning patent "trolls" in its ruling that eBay could use its "buy it now" function, after the feature had been ruled to be infringing on a copyright by a lower court. The Supreme Court also instructed lower courts not to issue automatic injunctions and to consider various factors before awarding a patent injunction. Nevertheless, Congress is expected to focus on creating a system for patent review. Although federal broadband reform may receive less focus from telecoms after a December FCC ruling that made franchising easier for broadband providers looking to provide IPTV, other elements of broadband reform bills could get passed, such as allowing local governments to provide wireless broadband and reforming the Universal Service Fund. Raising the limit on H-1B visas could come as part of a push for a wide-ranging "innovations agenda," aimed at boosting science and math education, as well as funding IT training programs and broadband access for all Americans.