Data defenders: Researchers try to ward off increasingly sophisticated cyber attacks

February 2 2010, by Anna Lynn Spitzer

Researchers Michael Goodrich (left) and Gene Tsudik, directors at UCI's Secure Computing & Networking Center, grapple with security and privacy issues in their quest to thwart "botnets" and other cyber attackers. Image: Paul R. Kennedy

(PhysOrg.com) -- Cyber attackers were busy last year. In July, a coordinated "denial of service" assault was launched on computers at the White House, Federal Trade Commission and departments of Treasury, Transportation and State, as well as the New York Stock Exchange and The Washington Post. The attack did little damage.

In August, social networking site Twitter suffered a similar assault that disabled it for hours, while Facebook and Google escaped without prolonged downtime.
In both cases, experts blamed “botnets,” huge armies of machines

infected with destructive software that can be remotely controlled to perpetrate network attacks.

UC Irvine researchers Michael Goodrich and Gene Tsudik, both directors at the campus's Secure Computing & Networking Center, work to stay one step ahead of botnets and a host of other nefarious schemes.

Goodrich, Chancellor's Professor of computer science, says that while electronic security has been a concern for more than two decades, the challenges are mounting.

"Computer viruses existed in the '80s. They were even distributed on floppy disks, and people were just physically handing them around," he says. "But the proliferation of networking has made security a bigger issue. There are all these problems popping up now that are a little more insidious."

Most are the result of malware, malicious computer code hidden in email or on Web sites. Users who open the email or visit the sites unwittingly install annoying or downright dangerous programs on their computers that can inflict disaster in a number of ways.

Malware can introduce unwanted spam and advertising pop-ups or track and duplicate personal information, leading to identity theft and financial loss. It can also hijack computers to produce the havoc-wreaking botnets.

Interestingly, while network security is a thoroughly modern pursuit, the methods employed by computer scientists are rooted in ancient Greece. Mathematician Euclid, born circa 325 B.C., developed the first algorithm - a step-by-step computational procedure for solving a problem - to determine the greatest common divisor of two numbers. It is still in use, forming the foundation of RSA, one of the best-known

public-key cryptography systems. Says Goodrich: “This algorithm is absolutely essential for Internet security today.”

Public- and private-key encryption, digital signatures, reverse Turing tests and boundary checks all implement algorithms in an effort to authenticate identity and prevent scams, which are becoming more and more sophisticated.

In August, a onetime government informant was indicted, along with two co-conspirators, on charges that he masterminded the largest identify theft operation ever prosecuted. Albert Gonzales of Miami is accused of infiltrating the computer systems of a payment-processing company and four large retailers, stealing more than 130 million credit and debit card numbers between late 2006 and early 2008.

The increasing use of radio-frequency identification also presents privacy and security issues. RFID tags - embedded in certain credit cards, badges, toll collection devices, hotel guest keys and passports - transmit information wirelessly to a reader, leaving personal data vulnerable to interception and misuse.

“When you swipe your ATM or credit card through a mechanical device, it’s almost impossible to eavesdrop,” says Tsudik, a computer science professor. “But when radio waves carry the same information, eavesdropping becomes very easy. Somebody could be sitting next door with a giant antenna picking up every bit of data being exchanged.”

Despite the risks, RFID systems are popular because they’re convenient and inexpensive. “But we’re paying a price,” Tsudik says, “and that’s privacy.” He and his colleagues, however, have devised a solution to this problem, and a patent is pending.

Privacy issues multiply with each new application, especially those used

in mobile networks. “The Internet of the future is going to consist of a lot more devices that move around, so location won’t be stable,” Goodrich says. “There will be information you wish to share with some parties and keep from others. That brings up a whole new set of questions we’re wrestling with. How do we maintain anonymity? What does privacy mean?”

Applications allowing users to connect with others in a specific area are already available, and Goodrich expects them to proliferate. “But as soon as you enable these,” he notes, “you’re reporting your location to a network of both trusted and untrusted people. We’re just now studying those safety concerns.”

Tsudik is also working on security protocols for tomorrow’s networks of autonomous drones or sensors. “For me, true research is trying to solve problems anticipated five to 10 years from now,” he says. “Only one out of 10 of those problems may actually pop up, but we’ll already have the answer when it does.”

Adds Goodrich: “What we do is focus on authentication, integrity and authorization - factors in any solution. We’re trying to learn how to protect against things we’ve never even thought of.”

Provided by UC Irvine

Citation: Data defenders: Researchers try to ward off increasingly sophisticated cyber attacks (2010, February 2) retrieved 19 April 2024 from https://phys.org/news/2010-02-defenders-ward-increasingly-sophisticated-cyber.html