SAND2006-5617P

News Release

FOR IMMEDIATE RELEASE
September xx, 2006

Sandia fingerprinting technique demonstrates wireless device driver vulnerabilities

LIVERMORE, Calif. – The next time you're sipping a latte and surfing the net at your favorite neighborhood wireless café, someone just a few seats away could be breaking into your laptop and causing irreparable damage to your computer's operating system by secretly tapping into your network card's unique device driver, a team of researchers at Sandia National Laboratories in Livermore, Calif., has concluded.

There is, however, more cheerful news. By role-playing the position of an adversary (also known as "red teaming"), Sandia researchers have demonstrated this unique "fingerprinting" technique that allows hackers with ill intent to identify a wireless driver without modification to or cooperation from a wireless device. Revealing this technique publicly, Sandia researchers hope, can aid in improving the security of wireless communications for devices that employ 802.11 networking.

Sandia is a National Nuclear Security Administration laboratory.

Wireless device drivers fraught with vulnerabilities

Device drivers, according to Sandia security researcher Jamie Van Randwyk, are becoming a primary source of security holes in modern operating systems. Through a laboratory-directed research grant, Van Randwyk and a team of college interns set out last year to design, implement, and evaluate a technique that has proved capable of passively identifying a wireless driver used by 802.11 wireless devices without specialized equipment and in realistic network conditions. Van Randwyk presented his team's findings last month at the USENIX Security Symposium in Vancouver, B.C.

Video and keyboard drivers are generally not exploited because of the difficulty in attaining physical access to those systems, leading some to believe that device drivers are immune to vulnerabilities. However, Van Randwyk points out, physical access is not necessary with some classes of drivers, including wireless cards, Ethernet cards, and modems.

"Wireless network drivers, in particular, are easy to interact with and potentially exploit if the attacker is within transmission range of the wireless device," said Van Randwyk. Because the IEEE 802.11 standard is the most common among today's wireless devices, he and his team chose to evaluate the ability of an attacker to launch a driver-specific exploit by first "fingerprinting" the device driver. "Fingerprinting" is a process by which a device or the software it is running is identified by its externally observable characteristics.

"Passive" approach and "probe request frames" are key

The passive approach used by Van Randwyk and his colleagues demonstrates that a fingerprinter (attacker) need only be in relatively close physical proximity of a target (victim) in order to monitor his or her wireless traffic. Anyone within transmission range of a wireless device, therefore, can conceivably "fingerprint" the device's wireless driver. Reconnaissance of this type is difficult to prevent since the attacker is not transmitting data, making the attack "invisible" and hard to detect.

Sandia's fingerprinting technique relies on the fact that computers with wireless configurations actively scan for access points to connect to by periodically sending out "probe request frames," of which there are no standard 802.11 specifications. Consequently, developers have created a multitude of wireless device drivers that each performs the "probe request" function differently than other wireless device drivers. Sandia's fingerprinting technique demonstrates the inherent vulnerabilities in this situation through statistical analysis of the inter-frame timing of transmitted probe requests.

"Fingerprinting" not a new concept

Fingerprinting an 802.11 network interface card (NIC) is not a new concept, says Van Randwyk, and many tools exist that can help identify card manufacturers and model numbers via a wireless device's Media Access Control (MAC) address. Sandia's approach, however, is more advantageous in that it fingerprints the device driver, where most exploits rest due to the driver's placement within the operating system. Additionally, the features used by the Sandia passive technique are not a configurable option in any of the drivers tested, unlike the MAC address in most operating systems.

Sandia's fingerprinting technique has proven to be highly reliable, achieving an accuracy rate ranging from 77 percent to 96 percent, depending on the network setting. Furthermore, the technique requires that only a few minutes worth of network data be collected, and tests confirm that it can withstand realistic network conditions.

The complete research paper prepared by Van Randwyk and his colleagues, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," discusses the technique in detail and can be found here (*note: a .PDF file link to the paper will go here*).

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin company, for the U.S. Department of Energy's National Nuclear Security Administration. With main facilities in Albuquerque, N.M., and Livermore, Calif., Sandia has major R&D responsibilities in national security, energy and environmental technologies, and economic competitiveness.

Sandia National Laboratories
Media contact: Mike Janes
Public and Media Relations Office
Livermore, California
(925) 294-2447, email mejanes@sandia.gov
www.ca.sandia.gov / www.sandia.gov