CompSci expert Wetzel spots weaknesses in Wi-Fi security

August 9 2004

Researcher and colleagues warn of battery-draining, node-killing strategies

A research team led by Dr. Susanne Wetzel, an Assistant Professor of Computer Science at Stevens Institute of Technology, has produced a study of the weaknesses of Wi-Fi networks. Specifically, Wetzel's team has discovered "stealth attack" methods of disrupting and draining power from individual nodes within an "ad hoc" wireless network – i.e., a network that one "connects to" as a visitor as one moves physically with one's mobile computer from location to location, without a dedicated access point.

While still rare, ad hoc modes are the underpinning for many of the advanced data networking schemes now being proposed.

"Most of today's communication infrastructure is based on trustworthy collaboration among information routers," says Wetzel. "However, given the increased economic reliance on a working communication infrastructure, this has become a potential target for terrorists and other criminals."

Working with researchers from Rensselaer Polytechnic Institute and RSA Labs of Bedford, Mass., as well as Stevens' own Wireless Network Security Center (WiNSeC), Wetzel experimented with two major types of stealth attack.

“In the first type of attack,” says Wetzel, “the adversary wishes to disconnect the network, whether by a general partition or the isolation of particular nodes. In our study, the adversary does not need to control nodes but simply manipulates the routing of honest information to cause disruption. This confuses nodes within the network, causing them to expend extra battery power and draining them to the point that they ‘disappear,’ disrupting the flow of information.”

Given the low exposure of the attacker during this act, says Dr. Paul J. Kolodzy, who directs Stevens’ WiNSeC, this scenario is a stealth version of the common Denial of Service (DoS) attack. “It’s like a child constantly yelling questions at an adult – and draining the adult’s ability to listen,” he says. “The adversarial computer just keeps asking and asking to connect, and no matter how often the victim network or node agrees, the adversary just keeps hurling requests to connect, draining the system. It’s cyber terror on the cheap, and the perpetrator is very hard to trace.”

The second type of attack that Wetzel studied involves an adversary who modifies the routing of information in order to hi-jack traffic from and to selected victim nodes. This technique can be used to perform traffic analysis, and it may be combined with selected filtering of data packets, which in turn can be used to make selected routers “disappear,” as in the first type of stealth attack.

“The hi-jacking attack is perpetrated remotely,” says Wetzel, “by abuse of routing protocols and detouring of messages. This type of eavesdropping is active in that the attacker is outside the transmission range of the victim, from which range he performs the eavesdropping by detouring the traffic through corrupted nodes within the transmission range of the victim.”

In both of the above described attacks, the adversary’s goal is not only to

perform the attack successfully, but also to do so with minimal effort, and in a way that hides his existence and whereabouts to the largest possible extent.

Given the seeming advantage that cyber criminals have in this realm, what are the practical solutions?
“A routing protocol that is immune to stealth attacks is better than one that is not,” says Wetzel. “We propose design techniques that can strengthen protocols against such attacks. Our proposed technique is for each router to keep (and possibly exchange) reputation-based information. Routers can then use this to resolve conflicting updating information, and to determine what control messages to handle and act on.”

According to Wetzel, the idea of reputation-based control is “simple and draws from the real world. Each person shapes an opinion of all entities, whether they are co-workers, merchants, media, or stock brokers. Similarly, routers may keep ‘reputation tables’ or ‘reputation caches’ that list nodes they trust.”
Not surprisingly, the US Army, through the Picatinny Arsenal in New Jersey, is taking a great interest in Wetzel’s solutions as they develop, and has provided further funding as she continues her work with Kolodzy at WiNSeC.

Dr. Susanne Wetzel
Wetzel joined the faculty in 2003 at the Computer Science Department of the Stevens as Assistant Professor. She received her Diploma in Computer Science from the University in Karlsruhe (Germany) and a doctoral degree in Computer Science from Saarland University (Germany) in 1998. Subsequently, she worked at DaimlerChrysler Research (Stuttgart, Germany), Lucent Technologies-Bell Laboratories (Murray Hill, USA) and RSA Laboratories (Stockholm, Sweden).
Her research interests are in cryptography and algorithmic number

theory. In the field of cryptography, her research is focused on wireless security, secret sharing, privacy, and biometrics, and her contributions range from analysis to protocol design. In algorithmic number theory, her research is centered on lattice theory, in particular on developing new algorithms and heuristics for lattice basis reduction.

About WiNSeC
The Wireless Network Security Center (www.stevens.edu/winsec) at Stevens Institute of Technology is focused on solving technical and organizational problems associated with secure communications platforms. Wireless technologies developed and tested by the center are certified to perform in even the most demanding situations. WiNSeC's cutting-edge wireless technology testbed is located in the heart of the New York-New Jersey metropolitan area.

Source: Stevens Institute of Technology