Simple security for wireless: no password required

August 22 2011, by Larry Hardesty

In early August, at the Def Con conference — a major annual gathering of computer hackers — someone apparently hacked into many of the attendees' cell phones, in what may have been the first successful breach of a 4G cellular network. If early reports are correct, the incident was a man-in-the-middle (MITM) attack, so called because the attacker interposes himself between two other wireless devices.

Coincidentally, a week later, at the 20th Usenix Security Symposium, MIT researchers presented the first security scheme that can automatically create connections between wireless devices and still defend against MITM attacks. Previously, thwarting the attacks required password protection or some additional communication mechanism, such as an infrared transmitter.

Showcasing novel ways to breach security is something of a tradition at Def Con. In previous years, MITM attacks had been launched against attendees' Wi-Fi devices; indeed, the MIT researchers demonstrated the effectiveness of their new scheme on a Wi-Fi network. But in principle, MITM attacks can target any type of wireless connection, not only between devices (phones or laptops) and base stations (cell towers or Wi-Fi routers), but also between a phone and a wireless headset, a medical implant and a wrist-mounted monitor, or a computer and a wireless speaker system.

Key change

Ordinarily, when two wireless devices establish a secure connection, they swap cryptographic keys — the unique codes they use to encrypt their transmissions. In an MITM attack, the attacker tries to broadcast his own key at the exact moment that the key swap takes place. If he's successful, one or both of the devices will mistake him for the other, and he will be able to intercept their transmissions.

Password protection can thwart MITM attacks, assuming the attacker doesn't know the password. But that's not always a safe assumption. At a hotel or airport that offers Wi-Fi, for instance, all authorized users are generally given the same password, which means that any one of them could launch an MITM attack against the others. Moreover, many casual computer users find it so complicated to set up home Wi-Fi networks that they don't bother to protect them; when they do, they often select passwords that are too simple to provide much security. That's led to the marketing of Wi-Fi transmitters with push-button configuration: To establish a secure link, you simply push a button on top of the transmitter and a corresponding button (or virtual button) on your wireless device. But such systems remain vulnerable to MITM attacks.

"None of these solutions are quite satisfactory," says Nickolai Zeldovich, the Douglas Ross (1954) Career Development Assistant Professor of Software Technology, who developed the new security scheme together with Dina Katabi, the Class of 1947 Career Development Associate Professor of Computer Science and Engineering, as well as postdoc Nabeel Ahmed and graduate student Shyam Gollakota, all of MIT's Department of Electrical Engineering and Computer Science. "The cool thing about this work is that it takes some insight from somewhat of a different field, from wireless communication — actually, fairly low-level details about what can happen in terms of wireless signals — and observes that, hey, if you assume some of these properties about wireless networks, you can actually get stronger guarantees."

Strength in silence

In an MITM attack, the attacker needs to drown out the signal from the legitimate sender. But the researchers' new system ensures that any attempt to do so will be detected. The trick is that, after transmitting its encryption key, the legitimate sender transmits a second string of numbers related to the key by a known mathematical operation. But whereas the key is converted into a wireless signal in the ordinary way — it's encoded as changes in the amplitude of a radio wave — the second string of numbers is encoded as alternating bursts of radiation and silences.

If an attacker tries to substitute his key for the legitimate sender's, he'll have to send the corresponding sequence of bursts and silences. But that sequence will differ from the legitimate one. Through the silences of one, the receiver will hear the bursts of the other. The overlapping sequences will look to the receiver like a wholly new sequence, which won't match up with the transmitted key, indicating an MITM attack.

Of course, the attacker could try to drown out the entirety of the legitimate transmission and then send his own key. But that would require broadcasting a signal of such long duration that it, too, would alert the receiver to an attack.

"Other people have been focusing on protecting against man-in-the-middle attacks and just assumed that an adversary would be able to tamper with messages," says Tadayoshi Kohno, an assistant professor of computer science and engineering at the University of Washington. "These guys look under the hood and say, 'Wait, if we actually know how wireless works, we can construct a system so that an adversary couldn't tamper with messages to begin with.' In a way, there was a fundamental assumption that all preceding work had, and this paper steps back and says that assumption is incorrect, and here's why it's

incorrect, and here's what we can do with it."

The reports of an MITM attack on 4G phones are still being verified, and 4G itself is a vague term that encompasses many different technical approaches. But if the reports prove true, then cell phones, too, could benefit from the MIT researchers' security scheme. "You could imagine that the same protocol could be used in cell phone networks as well," Zeldovich says. "At the design level, the idea sounds like it should be applicable."

More information: The new paper - people.csail.mit.edu/gshyam/Papers/TEP.pdf

Provided by Massachusetts Institute of Technology