Jamming Attacks

By Alexander Yared, ECE '16

An introduction to jamming attacks, sometimes referred to as availability attacks, and their role in the RollJam attack. The RollJam attack is used to break rolling code security, commonly found in garage doors and automobile doors, through a jam-intercept-replay attack.

Introduction

Wireless attacks fall into three general categories: confidentiality, integrity, and availability. The *confidentiality* of a network is the ability of a network to hide the data passing through it from unauthorized users. The *integrity* of a network is its ability to ensure that the data passing through it is valid, reliable and has not been modified by unwanted users. The *availability* of a network ensures that all authorized users can access the network or the information they need on the network when they need it. Should one of the fundamental pillars of network security fall to attack, the value of the entire network would collapse (Gibson, 2011). This note focuses on availability attacks to explore the various forms that they take and to understand the reason why jamming is the first step in the larger RollJam attack.

Types of Availability Attacks

Availability attacks, also called Denial of Service (DoS) attacks, are relatively simple to understand in that all they seek to do is render the network unusable. One common availability attack is network flooding, where the attacker transmits so many requests to the server that the server cannot process any packets sent by actual users. A more sophisticated form of the attack is the Distributed Denial of Service (DDoS), where the attacker sends requests from many computers which are not necessarily in the same place. DDoS has two distinct advantages over DoS for the attacker. The first is that multiple computers can send more packets than a single computer, reducing the time it takes to flood the server. Additionally, since the attack originates from many points, spread over the world if possible, it is easier for the attacker to cover his or her real location and avoid detection.

Another example of availability attacks is radio frequency (RF) jamming. The attacker broadcasts continuous, high power noise on a specific frequency or frequency band to prevent an antenna tuned to that frequency from intelligibly reading a message. This is distinct from RF interference, where a source inadvertently emits high power noise on some frequency band as a byproduct of its intended action, due to the malicious intent of jamming. There are two types of jamming, obvious and subtle, which depend on the nature of the signal used to jam. With obvious jamming, the attacker jams with a signal that is detectable at the receiver. A classic example of obvious jamming is the Firedrake, or FireDragon, jammer used by the Chinese government. The Firedrake jammer continuously transmits Chinese classical music at incredibly high power to drown out amateur and anti-government radio (Mellgrin, 2008). Subtle jamming uses specialized tools and techniques to prevent the receiver from seeing a jamming signal. From the receiver's point of view, there is simply nothing being transmitted over the channel. This form of jamming can be achieved by broadcasting a pure unmodulated carrier that is transmitting only the frequency of the channel without any message.

Availability attacks are not used only for malicious purposes. The U.S. military uses highly specialized RF jammers to prevent insurgents in Iraq and Afghanistan from detonating improvised explosive devices (IEDs) from remote locations using simple RF transmitters (Shachtman, 2011). After the U.S. invasion of

Afghanistan, Al-Qaeda bomb-makers created improvised IEDs by putting radio frequency receivers with signal decoders into the bases of fluorescent lamps. The lamps were then connected to firing circuits and Soviet-era munitions. Blocking this signal was non trivial; the IED's frequency band was unknown, and frequently changed from explosive to explosive depending on what kinds of radio receivers were available. So the jammer had to be able to sweep across multiple frequencies without interfering with the RF bands used by U.S. soldiers. As bomb-makers began making more sophisticated triggers, a race emerged to create better jammers to keep American and allied soldiers safe.

Availability Attacks and RollJam

The RollJam device was developed by Samy Kamkar, a white hat hacker, to demonstrate the vulnerability of modern security systems in cars and garage doors. The device uses a combination of all three types of wireless attacks to create its Jam Intercept Replay (JIR) attack. The goal of the JIR attack is to trick the user into thinking that he or she has successfully locked the door, while leaving the attacker with a code to access the system once the user leaves. Garage door openers use a system called a rolling code, where the transmitter generates a random number, adds it to its current number and transmits it to the door. The garage door has the same random number generator and current number, so it performs the same addition and checks to see if the transmitted number matches its own number. If the numbers match, the garage door will close if it is open, or open if it is closed. If the numbers do not match, the door will cycle through its list of numbers until it finds the transmitted number, and then wait to see if the next transmission matches its own next number (Greenberg, 2015). To break into this system, RollJam first performs an availability attack, by RF jamming at the frequency of the system to prevent the door from receiving the number from the transmitter.

However, the jamming is not done with random noise; instead it is done with a specific message. This enables the second phase, Intercept, to be performed. The interception is a confidentiality attack; when the user presses the button on his or her garage door opener there is too much noise on the channel for the door to receive it, but the attacker can use another antenna to read from the channel, subtract the message they jammed with, and then the attacker is left with transmitted message.

The jam and intercept process is performed twice. The natural response by the unsuspecting user when his or her first button press fails to close the garage door is to press the button again, sending a new number out for RollJam to intercept. Now armed with two numbers, the attacker can perform an integrity attack, in this case the replay attack. The attacker replays the first number captured, which the door was expecting, and the door closes. The user sees that the desired action has been accomplished and leaves. Now comfortably alone, the attacker can replay the second number, which they know the garage door is expecting next, and open the door for themselves. Nothing can be done about the jamming or intercepting of the JIR attack, the ability to jam or read off of an RF network is a fundamental property of wireless communication.

Conclusion

The goal of the Orange Team's project is to design a system that can prevent the RollJam device from

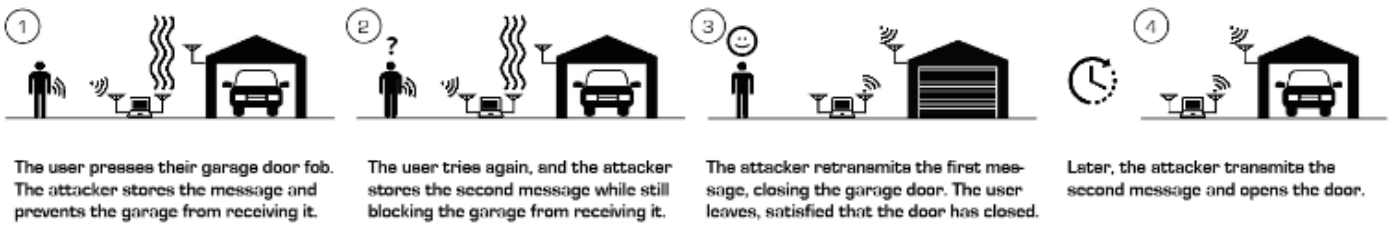

Figure 2. The Orange Team researched jamming technologies in order to develop a layer of protection against availability attacks.

reusing a code originally transmitted by the user. There are ways to circumvent some jamming attacks, such as specialized antennas and localization techniques for RF jamming, but others, like DDoS, cannot be truly stopped. As a result, there is significant research, both commercial and academic, being done to help detect jamming attacks before they overwhelm the system and to help systems deal with all the extra traffic.

References

Gibson, D. (2011, May 27). Understanding The Security Triad (Confidentiality, Integrity, and Availability). Retrieved from http://www.pearsonitcertification.com/articles/article.aspx?p=1708668

Greenberg, A. (2015, August 6). This Hacker's Tiny Device Unlocks Cars And Opens Garages. Retrieved from http://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

Mellgrin, D. (2008, April 2). Tibet Exile Radio says China Jamming it. Retrieved from http://usatoday30.usatoday.com/news/world/2008-04-02-934490960_x.htm

Shachtman, N. (2011, June 11). The Secret History of Iraq's Invisible War. Retrieved from http://www.wired.com/2011/06/iraqs-invisible-war/