Intercept - Replay Attack Vulnerabilities and Mitigation Strategies

By Alex Goldschmidt, ECE '16

As methods of encryption become more secure, methods of attacking encrypted networks are becoming more complex. Some attacks, called replay attacks, are even able to transcend the encryption and to break systems simply by playing back an encrypted message. Many of these attacks can occur on networks connected to the internet, but there is also an entire world of attacks on devices that are completely offline. One such attack is done by a device called RollJam, and is able to compromise car and garage door lock systems. The Orange Team developed a device which is able to protect against such an attack, but there still exist other attacks that don't yet have solutions..

Introduction

In the world of security, innumerable methods of compromising a network exist. Whether the attacker's goal is to shut down communication between parties, or to steal information from an unsuspecting victim, the security system in place must be able to defend against it. The best method of protecting information, which prevents a lot of these attacks from being feasible, is to encrypt all data that is transmitted from one place to another. However, what happens when the attacker doesn't need to know what the message actually says? This is the principle behind the replay attack.

Replay Attacks

Replay attack is a general term used to describe a plethora of attack methods. Because of the number of ways an attack can be executed, trying to find a unilateral solution is futile. Breaking them down into different classes of attack, though, make it much easier to identify how an attack method is being implemented, and defenses specific to that class of attack can be applied. Syverson (1994) outlines a thorough classification structure for replay attacks. The basic breakdown is to categorize the origin of the attack, which could be internal to the network or external, and then the destination of the attack after it is intercepted, which could be the intended recipient, the original sender, or another 3rd party.

Online Replay Attacks

The most obvious attack vector for any replay attack is the Internet. It is massive, crowded, and intrinsically insecure. IEEE 802.11 is the protocol invented in 1997 to standardize network traffic over the internet. It operates at the physical and transport layer in the OSI model (Cisco, 2002). This means that any messages being sent from Alice to Bob goes through this last. It is at the bottom of the stack, so any vulnerability in it means the whole stack is compromised. So, obviously, it is riddled with vulnerabilities. The catalyst behind a lot of existing security protocols is the fact that no security is offered at the Physical layer of the OSI model.

One low level defense is IP Protocol 51, the IP Authentication Header (IP AH). This header is attached to messages on the Transport Layer, and contains many of the techniques employed by SSL 3.0. The IP AH specifies the intended recipient to prevent deflection, sequence number to prevent delay, and length of message to prevent tampering. The IP AH also includes one extra measure, known as a nonce (AH, 2012). A cryptographic nonce is a one-time token used to verify the authenticity and uniqueness of a message. This prevents any sort of duplication attack, even if the sequence number is tampered with. The only truly secure encryption is the one time key, and a

nonce is the closest thing to a one time key in production today.

Offline Replay Attacks

While the taxonomy outlined previously was intended for analyzing replay attacks over the internet, offline systems, such as car and garage door locks, are just as, if not more, vulnerable. The internet is constantly changing and being improved, and changes are very easy to implement since it is all connected. Offline systems are harder to update, because they have no connection, mostly, to a main system. The only way to prevent replay attacks offline is to recognize the threat and prevent it before deploying the product, because once it leaves the factory it's too late to stop an attack.

One dire example of an offline replay attack involves the "secure" microchip technology found in most credit cards today. The purpose of these chips is to prevent counterfeiting and add an extra layer of encryption to users' information; however, several banks have lost over $100,000 due to transactions being intercepted and replayed back. Security measures, such as unique serial numbering of transactions, are in place to prevent such attacks from happening, but these require humans monitoring them and approving transactions, and scarily, a lot of banks choose not to even implement these measures. Another example is Samy Kamkar's RollJam device, which can intercept wireless car and garage door key fob signals, and replay them back later, granting the attacker access. Today, Ultimate KeeLoq ® which uses a time based nonce to prevent such an attack, is the most modern security protocol for wireless key fobs, but only a limited number of the newest cars on the market come equipped with it, leaving most of the cars in the world, and all of the garage doors, still vulnerable.

Conclusion

When it comes to securing devices, it is a fool's errand. No matter what defenses are put in place, it is very difficult to cover every corner case. As the taxonomy, beautifully organized by Syverson (2014) clearly shows, there is no single way to categorize replay attacks. Therefore, there is also no single way to prevent them. Kamkar, and others like him, are critical to preventing more and more advanced attacks, such as the Tor attack described above. In order to understand how a system needs to be protected, in most cases it first has to be broken. When the breaking is done by "white hat hackers" like Kamkar, the result is a heightened awareness of a serious issue or even a fix to the problem. In most cases, these attacks are carried out maliciously, leaving innocent victims behind not knowing what they did wrong.

Wireless security can be thought of as the man trying to fix the holes in the dam. Every time a new hole appears, the man must go and fill it up to stop the water from coming through. Every time he fills it in the dam becomes stronger, but the water will always find another way through. Still, it is better that the holes get filled in than that they are just left open, even if it is futile to try to stop the water from coming through forever. The only thing one can hope for is that more people join in to help the man filling the holes, because the water in the dam will never go away.

Future Work

The Orange Team is trying to play the role of the repairman. When cars and garage doors were first conceived of, the Internet of Things was nothing more than a distant concept, even a fantasy to some. But, in the ever changing world of technology, wireless networks are growing rapidly. If security doesn't keep up with the network, there are going to be a lot of holes that need to be filled up, many of which won't even be recognized until someone uses it maliciously, letting the water pour right through. The Orange Team's solution fills the hole that was *discovered* by Samy Kamkar but was initially *created* by the manufacturers who lacked the foresight to anticipate their technologies being targeted for a wireless attack.

References

"AH, Authentication Header." (2012) [Protocol]. Retrieved from http://www.networksorcery.com/enp/protocol/ah.htm

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/

Krebs. (2014, October 27). 'Replay' Attacks Spoof Chip Card Charges. *Krebs on Security.* Retrieved from http://krebsonsecurity.com/2014/10/replay-attacks-spoof-chip-card-charges/

Microsoft. (2015, December 2). *Replay Attacks.* Retrieved from https://msdn.microsoft.com/en-us/library/aa738652(v=vs.110).aspx

Microsoft. (2015, December 2). *What Is Windows Communication Foundation.* Retrieved from https://msdn.microsoft.com/en-us/library/ms731082(v=vs.110).aspx

Mitre. (2015, December 8). *Common Weakness Enumeration.* Retrieved from https://cwe.mitre.org/data/definitions/294.html

Pries, R., Yu, W., Fu, X., & Zhao, W. (2008, May). A new replay attack against anonymous communication networks. In *Communications, 2008. ICC'08. IEEE International Conference on* (pp. 1578-1582). doi: 10.1109/ICC.2008.305

Syverson, P. (1994, June). A taxonomy of replay attacks [cryptographic protocols]. In *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings* (pp. 187-191). doi: 10.1109/CSFW.1994.315935

Wagner, D., & Schneier, B. (1996, November). Analysis of the SSL 3.0 protocol. In *The Second USENIX Workshop on Electronic Commerce Proceedings* (pp. 29-40). Retrieved from https://www.usenix.org/legacy/publications/library/proceedings/ec96/wagner.html