Tufts University

School of Engineering

COMP 111 - Security

Why “Mobile” Security is the Hardest Security

By Kevin Dorosh

Abstract

Tech-savvy people understand that Android is less safe than iPhone, but most don't understand how glaring cell phone security is across the board. Android's particularly lackluster performance is exemplified in the MAC address randomization techniques employed to prevent others from being able to stalk your location through your mobile device. MAC address randomization was introduced by Apple in June of 2014 and by Google in 2015, although (glaringly) only 6% of Android devices today currently have this tech [3]. Sadly, in devices with the tech enabled, the Karma attack can still be exploited. Even worse, both iOS and Android are susceptible to RTS (request to send frame) attacks. Other power users have even seen success setting up desktop GSM towers as intermediaries between mobile devices and real cell phone towers to gather similar information [5].

This paper attempts to explain simple techniques to glean information from other mobile phones that can be used for nefarious purposes from stalking to identity fraud, but also by government agencies to monitor evildoers without their knowledge. As this paper should make clear, mobile security is far more difficult than "stationary security", for lack of a better term. Even worse, some of these flaws are problems exist with the Wi-Fi protocol itself, but we will still offer solutions to mitigate risks and fix the protocols. As we do more on our phones every day, it becomes imperative that we understand and address these risks.

Intro

Mobile security has never been more important than it has become today. Smartphones, which are effectively mini-computers in our palms that are the keys to our lives, have become ubiquitous. Finally, in 2017 we have seen mobile security in the forefront of the press. Apple refused to build the backdoor for the FBI; this was a landmark case that yielded interesting technological and societal debate. Yet, even given the new press and Apple's staunch protection of user security, there has not been enough focus on these and similar mobile vulnerabilities.

To The Community

Do you really understand how your phone works? Like REALLY understand it? How about cellular data, Wi-Fi, or similar protocols? Smartphones combine complicated technologies, all waiting to be attacked. Comprised of 10 million lines of code [6], it is naïve to believe that Android and iOS are air-tight. A common programming maxim exemplifies this unlikelihood: "code is liability." Security is already

an impossible problem. Once you take machines and make them portable, it only becomes that much harder to solve. That is why I chose this topic.

Fortunately, there are many steps we can take to protect ourselves. While MAC Address Randomization, the Wi-Fi protocol, and cell towers are not perfect, these vulnerabilities typically rely upon mistakes made by the end user. Most crackers attack the weakest link, obscuring their identity through trust relationships. Most script kiddies will just attack the technology, and these aren't the people we should be worried about. By understanding the technologies and becoming informed users, we can defend ourselves from the *truly dangerous* hackers.

Case Studies and Defenses

1. **MAC Address Randomization**

Most smartphone users aren't even aware of what a MAC Address is; never mind what MAC Address Randomization is, and how it can be exploited to stalk everyday smartphone users. Fortunately, the concept is quick to understand.

A MAC Address (Media Access Control) is a hardware address that every computer/smartphone has. It's tied to your NIC (Network Interface Card). It is an unwavering, globally unique identifier used by ARP (Address Resolution Protocol) to translate your hardware address to an IP, your software address. In short, it is used like mail forwarding, taking your mail from a P.O. Box (IP) and associating it with your real address (MAC), which nobody should have. This is a good system because your IP can change regularly and your true address is hidden.

The problem is that when phones are not connected to Wi-Fi, the 802.11 management frame probes for open networks to connect to, revealing your MAC Address [1]. This is typically not an issue on desktop machines because they are always connected or disconnected from the internet. For someone who leaves Wi-Fi on all the time to save on data (most users), whenever they leave home/work they become susceptible to attack. Access Points (APs) can log MAC Addresses revealed and track your location. Malicious users can figure out what your daily schedule looks like (e.g., your commute) and use this information to perform reconnaissance for more insidious acts.

MAC Address Randomization was invented to fix this problem. Apple's idea in 2014 was to create fake MAC Addresses for the 802.11 management frame probe, and only reveal your true MAC Address once you are connected to the network. Adopted by Google as well in 2015, this approach seems to fix the problem. Unfortunately, only 6% of Android devices out today employ this protection; even then, phone calls and screen use has shown to reveal the true MAC Address. Apple does better,

but researchers were able to attack the randomization and fingerprint both platforms to reveal 96% of true MAC Addresses anyways [3]. The best security is to turn off Wi-Fi when do not expect to find familiar Wi-Fi, or purchase a security minded smartphone such as Blackphone.

2. Karma Attack

Another common attack employed in the wild is the Karma attack. Similar to the MAC Address Randomization, the Karma attack takes advantage of devices looking to connect to familiar Wi-Fi; this danger is far more pronounced on mobile devices and laptops than stationary machines.

The attack differs this time around since the attacker sets up an AP (Access Point) with an SSID (Wi-Fi identifier/name) that matches something that a phone already trusts or has connected to. Often, this SSID looks something like logan-wifi, starbucks, or attwifi (AT&T phones ship with this one in memory!) [3]. This AP passively listens to 802.11 Access Point Probe Request Frames, and then the attacker changes the SSID to match, without a password. Effectively, it listens for devices yelling things like “Hi, I’m Kevin’s smartphone. I’m looking to connect to Mc-Donald’s Wi-Fi!” and then pretends to be McDonald’s Wi-Fi. This happens unbeknownst to the user, and is a mind bogglingly easy way to set up a Man in the Middle (MITM) attack to steal confidential information such as credit cards or social security numbers.

Fortunately, this attack is more involved since the attacker needs to set up a router to carry out the attack, and do so in a public place without arising suspicion. Nevertheless, connecting to the “evil twin” is a quite dangerous hack, and the best defense is to “forget all networks” on your cellular devices. Do not connect without your explicit permission!

3. RTS Frame Attack

The RTS frame attack is another devious method hackers have used to glean MAC Address information from users. Unfortunately, this method defeats MAC Address Randomization and is not specific to mobile devices, but fortunately the attacker must identify themselves by revealing their MAC Address. This is a hard problem to fix because it is an inherent flaw in the 802.11 Wi-Fi protocols. [3]

The RTS Frame was invented to solve the hidden node problem. The idea, simply, is to prevent computers A and C from connecting to B and overloading it with information, corrupting or losing packets along the way. This is called the hidden node problem because it assumes networks A and C cannot see each other, and detect the problem before it becomes an issue for computer B [7]. The solution is actually quite similar to handshaking communication requests among computers in a network

(SYN → SYN/ACK → ACK). For Wi-Fi, a requesting machine sends RTS (Request to Send Frame), an AP responds with CTS (Clear to Send) and an amount of time they are allowed to send, and then the AP responds with ACK (acknowledging that they received data and time is up!). [1]

The problem here is that an attacker can send an RTS frame to their target, forcing them to respond with a CTS Frame and their MAC Address. Similarly, people have attempted DDoS attacks by flooding the network with RTS frames, eating up all available bandwidth on the network. Unfortunately, no foolproof solutions have been proposed. Instead, it is possible to put ACKs in the data packets or change the frequency channel of the Wi-Fi, but neither solution is perfect. Fortunately, due to our ability to identify the attacker through their MAC Address as well as the limited danger in acquiring user MAC Addresses/DDoS'ing a small network should discourage most from trying this kind of attack.

4. Cell Site Emulators/Jamming

A final, more terrifying mobile security breach exploited by friends and foe alike are the use of cell tower emulators/jammers. The basic idea is that cell phones connect to the closest cell tower for data and SMS. This gives you the strongest signal and preserves battery life, so it is generally a good idea. The problem, however, is if a hacker set up a fake cell tower then local phones will connect to this tower instead. This tower just sits in the middle, intercepting and inspecting traffic before sending it on toward a real cell tower. To further exploit this loophole, cell phone jammers typically jam 3G and LTE connections, forcing phones to connect with the slower (and insecure) 2G network protocols. [2] The FBI itself has admitted to using these fake towers, called "Stingrays", to monitor the public. Fortunately, this tech is only sold (publicly) to the government. [5]

Fortunately, the hardware required to emulate a tower approaches $1500. [8] Even so, you could be attacked without your knowledge, and background processes on your phone can leak super sensitive information. The best protection is to disable 2G connections, if at all possible, from your phone. You would rather have no service than malicious service.

Conclusion/Summary

In conclusion, we clearly need to be much safer with our personal phones and data. Just take a tour nearby the Black Hat conference in Vegas last year, and you will see Stingrays and Karma attacks stealing your data live, put on the big screen to prove how easy it is and susceptible we are. [4] We must take steps to protect ourselves by disabling usability features in favor of increased security. This includes forgetting all networks, only turning on Wi-Fi in places where you expect to connect (this will save

battery too!), disabling 2G connection, and buying a phone that has MAC Address Randomization. This sounds like a lot of work – and it is. While you can never completely protect yourself, there are other options such as the Blackphone, a security-minded smartphone offering that can make protecting yourself easier. Even then, however, the best and **only** perfect security is to just power down.

Works Cited

[1] "802.11 Association Process Explained." *Cisco Meraki*, 21 Sept. 2017, documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_process_explained.

[2] "Cell-Site Simulators/IMSI Catchers." *Electronic Frontier Foundation*, 14 Nov. 2017, www.eff.org/sls/tech/cell-site-simulators/faq.

[3] Dan Goodin - Mar 23, 2017 5:17 pm UTC. "Shielding MAC Addresses from Stalkers Is Hard and Android Fails Miserably at It." *Ars Technica*, 23 Mar. 2017, arstechnica.com/information-technology/2017/03/shielding-mac-addresses-from-stalkers-is-hard-android-is-failing-miserably/.

[4] Eddy, Max. "First Look at a Wi-Fi Attack Happening at Black Hat Right Now." *PCMAG*, 4 Aug. 2016, www.pcmag.com/news/346757/first-look-at-a-wi-fi-attack-happening-at-black-hat-right-no.

[5] Koebler, Jason. "The FBI Admits It Uses Fake Cell Phone Towers to Track You." *Motherboard*, 16 Feb. 2015, motherboard.vice.com/en_us/article/jp5azg/fbi-admits-it-uses-fake-cell-phone-towers-to-track-you.

[6] McCandless, David. "Million Lines of Code — Information Is Beautiful." *Information Is Beautiful*, www.informationisbeautiful.net/visualizations/million-lines-of-code/.

[7] Sawwashere, Supriya & Nimbhorkar, S.U.. (2014). RTS/CTS Frame Synchronization to Minimize the Hidden Node Problem in Wireless Network. International Journal of Software Engineering and Knowledge EngineeringInternational Journal of Advanced Research in Computer Science and Software Engineering. 4. .

[8] Tanner, Adam. "Here's How Others Can Easily Snoop On Your Cell Phone." *Forbes*, Forbes Magazine, 23 Feb. 2014, www.forbes.com/sites/adamtanner/2014/02/18/heres-how-others-can-easily-snoop-on-your-cell-phone/#4f3c0959dbc0.