Testimony of Dr. Charles Clancy

Professor of Electrical and Computer Engineering, Virginia Tech

before the House Committee on Science, Space, and Technology, Subcommittee on Oversight, Hearing on "Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats"

June 27, 2018

Chairman Abraham, Ranking Member Beyer, and Subcommittee Members:

My name is Charles Clancy and I am a professor of electrical and computer engineering at Virginia Tech, where I direct the Hume Center for National Security and Technology. In these roles, I lead major university programs in security, resilience, and autonomy. I am an internationally-recognized expert in wireless security and have held leadership roles within international standards and technology organizations including the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE). My current research sits at the intersection of 5G wireless, the Internet of Things, cybersecurity, and artificial intelligence.

I am co-author to over 200 peer-reviewed academic publications, to include five books on digital communications; am co-inventor to over 20 patents; and am co-founder of four venture-back startup companies all focused in the wireless and security sectors.

Prior to joining Virginia Tech in 2010, I led a portfolio of wireless research and development programs at the National Security Agency.

It is my distinct pleasure to address this committee on topics of critical national importance.

Background

Wireless technologies are an intrinsic component of society. Today's social-mobile Internet provides ubiquitous connectivity and access to information. As the social-mobile Internet evolves into the Internet of Things over the next decade, wireless technologies will become even further ingrained into everything we do.

Security of wireless infrastructure is critical. This includes devices, wireless base stations and access points, and core network infrastructure. Historically cellular infrastructure equipment has been expensive, making it cost prohibitive for most hackers to tinker with wireless systems. As a result sophisticated attacks against wireless networks were the domain of nation-state actors. However

technologies like smallcells and software-defined radio have lowered the price point considerably and led to a significant expansion of public research into cellular network hacking.

While each generation of cellular technology improves security and privacy, the backward-compatibility challenge means that even if we deploy highly-secure 5G networks, most phones can still connect to insecure 2G networks even though many of the national carriers in the US have already decommissioned their 2G infrastructure. This mixture of old and new technologies in devices and carrier networks means that insecurity will always be part of the cellular ecosystem. Combating threats to wireless infrastructure requires a risk management approach that constantly evaluates potential vulnerabilities, observed threats, engineers countermeasures, and communicates best practices.

IMSI Catcher Technologies

The terms *IMSI Catcher* and *Stingray* have come to symbolize a range of cellular surveillance technologies and differentiating them is important.

Rogue base stations, also known as *cell site simulators*, are devices that act like cell towers from a particular carrier network, but are not part of that network. 2G technology is particularly susceptible to this threat because the authentication in 2G is weak – the network verifies the identity of the phone, but not vice versa – and all the standard encryption modes have been cracked. A 2G rogue base station is able to lure a phone into connecting; elicit its identity, known as its IMSI; prevent it from disconnecting; query the phone's precise GPS location; and intercept voice, data, and SMS content. 3G and 4G rogue base stations are less capable because the underlying standards employ stronger encryption and authentication. A 3G/4G rogue base station is able to elicit a phone's identity, but little else. Earlier this year, 5G adopted a proposal known as "IMSI encryption" that prevents a 5G rogue base station from successfully eliciting a phone's identity. While security has been improving within the standards, backward compatibility in phones means that 2G rogue base stations are still quite effective.

Rogue base stations can be used for a variety of applications, but are most commonly associated with "IMSI catching". They interact with phones for a few milliseconds to learn the phone's identity, and then pass the phone back to the real network. Law enforcement can use the technology to track down criminals. Intelligence and counter-intelligence services can gather data to track the movements of targets. While criminal organizations could theoretically take advantage of the technology as well, to date they have focused primarily on using jammers to disrupt GPS and cell phone networks[1].

---

1. Mike Brunker, "GPS Under Attack as Crooks, Rogue Workers Wage Electronic War", *NBC News*, 8 Aug 2016.

Another class of device is **cellular interception systems**. These devices passively scan the airwaves, identify active cell bands, and then decode the signals observed in those bands. Note that these systems are not always good at catching IMSIs because the IMSI is only sent over the air when a phone first connects to a network, so an interception system would have to get lucky in order to see an IMSI. Given the encryption in 2G has been cracked, these systems are able to decode all the voice, SMS, and data traffic between phones and 2G networks. For 3G and 4G, voice, SMS, and data are protected by strong encryption and therefore not readable by interception systems.

These technologies can also be used together, and in conjunction with a jammer. For example, if 3G and 4G bands are intermittently jammed, then a victim phone may attach to a rogue 2G base station which would then capture the phone and prevent it from returning to the 3G/4G network once the jamming is deactivated. These downgrade attacks undermine the improved security features in later cellular standards.

Closing the 2G Gap

Given its weak encryption and authentication, 2G represents a major security issue with modern cell phones. Similar to how security around WiFi was improved over the past decade with phones providing warnings before connecting to insecure WiFi networks, steps could be taken to treat 2G networks as less trusted.

Carriers who have already decommissioned their 2G networks could push policies to phones that prevent phones from connecting to 2G unless roaming to other networks. Current iPhones lack the ability for users to do this, and Android users need to type a secret code into the phone to open a hidden diagnostic menu in order to disable 2G. Making this the default and giving users more awareness and control through the user interface would address the majority of the operational security and privacy issues associated with 2G.

An important consideration however is rural areas that only have 2G service and legacy devices such as vehicle telematics and home security systems that only support 2G networks. These users and networks cannot be disenfranchised.

Catching IMSI Catchers

There have been several studies on how to detect rogue base stations and the proposed approaches generally fall into two categories: phone-based and carrier-based.

The first approach relies on phones to assess whether a base station looks suspicious[2]. Every cell tower broadcasts information about itself, including power levels needed to connect, types of encryption supported, and the identities of its adjacent towers. A rogue base station is likely to indicate that phones should connect at any power level, no encryption is supported, and there are no other towers in the area. These anomalies can be detected by the phone. There are a number of software apps available that purport to perform this task, but they are limited by the amount of cell network metadata provided by Android and Apple to apps[3]. Any reliable solution would need to be baked into device firmware.

Another approach is to leverage data within the network. Phones constantly track the power level of towers within range to determine if they should initiate a tower handover. Phones periodically send this data to the network in what's known as a *measurement report*. The new 5G security standards recommend that these reports can be used by carriers to identify when an unrecognized base station is visible to a phone[4].

Both of these approaches suffer from the "spy-versus-spy" phenomenon whereby improvements in detection technologies result in improvements in spoofing technologies. Any detection strategy would need to constantly evolve as adversary capabilities improve.

Regardless, when considering options for detecting and reporting rogue base stations, one must consider to what end the detection is being performed. If a phone detects a possible rogue base station, should it notify the user? Should the user then notify someone? If a carrier detects a rogue base station should it report it to the FBI? File an interference complaint with the FCC? Given the presumption is that some of these rogue base stations are being used by foreign intelligence and some by domestic law enforcement, how can you tackle the former without negatively impacting the latter? These issues need to be addressed first before the appropriate technical solution can be formulated.

---

2. A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers", *ACM Annual Computer Security Applications Conference (APSAC)*, December 2014.

3. R. Borgaonkar, A. Martin, S. Park, A. Shaif, J-P Seifert, "White-Stingray: Evaluating IMSI Catchers Detection Applications", *USENIX Workshop on Offensive Technologies (WOOT)*, August 2017.

4. P-K Nakarmi, K. Norrman, "Detecting false base stations in mobile networks", Ericsson Research Blog, 15 June 2018.

Recommendations

Looking forward, I encourage this subcommittee to consider the following.

First, carriers that have decommissioned their 2G infrastructure should update phone policies to only connect to 3G/4G networks when not roaming. This will address the majority of the security concerns around cell phone surveillance.

Next, individuals who are likely targets of foreign intelligence should use phones with the needed countermeasures to protect them from cell phone surveillance technologies, such as those recommended by NIST Special Publication 800-187[5] and DOD's Security Technical Implementation Guides for smartphones[6].

Finally, if tracking down IMSI catchers is a desired objective, first address issues with how this information will be used, by whom, and to what end. If the bulk of the risk can be effectively managed by closing 2G gaps and hardening phones for at-risk individuals then the utility of illegal IMSI catchers may decline sufficiently to avoid the need for more systematic approaches to detecting and reporting their operation.

Thank you for the opportunity to address the subcommittee today and I look forward to questions.

5. J. Cichonski, J. Franklin, M. Bartoch, "Guide to LTE Security", NIST Special Publication 800-187, December 2017.

6. Defense Information Systems Agency, "Mobility – Smartphone/Tablet Security Technical Implementation Guides", https://iase.disa.mil/stigs/mobility/Pages/smartphone.aspx