**EMCS2020: Advanced Topics in Computer Security**

Assignment: Multi-Factor Authentication

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

*Given the attacks presented in the article by Lorrie Cranor, please summarize effective measures that mobile carriers could adopt to protect customers from account hijacking. Ideally, these measures should not only accurately identify the customer, but also be usable and respect the customer’s privacy. For example, they should take into account the fact that users often forget account passwords/PINs and may be unable to read email when their phone is lost or not working. Hint: remember the “MFA Mantra” from the slides, where “something you have” can be rephrased as “something only you have access to.” Note that an approach that may work reasonably well for identification but has usability issues and reveals too much private information to the carrier would be asking for the adjusted gross income from last year’s tax return.*

Considering the fact that most physical identities can be stolen and forged, I highly recommend in-person biometric identification. Yes, that means fingerprints. I can imagine consumers would be sensitive to allowing a carrier to store their fingerprints, but working with trusted third parties may soften the shock of having to provide your fingerprint. Fingerprints are already required at banks when cashing checks and to obtain a TSA pre-check. As we can see from Dr. Cranor’s story a cell phone is a major attack vector because many times it is used as identification itself. It’s very sad but we often have to provide our cell number more often than our actual ID ( driver’s license, passport, etc ). Allowing someone to obtain possession of a cell phone number without stronger identification that cannot be easily forged is irresponsible. If carriers collect a fingerprint scan that is stored by a trusted third party service and require another in-person scan to restore a phone that was lost it might be inconvenient, but it would be near impossible to forge or bypass.

*Rank the three adversarial models described in the paper “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems” with respect to (a) how much equipment/technical knowledge they assume the attacker has, and (b) how much damage can the attacker cause.*

The researchers present the readers with three adversarial models, namely Passive, Semi-Active and Active. It pretty clear that the Active model requires the most equipment as it relates to hardware and software since it involves spinning up a part of the network namely a rogue eNodeB. Furthermore, the Active model requires advanced knowledge of how the complex LTE model works. The damage that is possible in this most aggressive attack is pretty daunting since the rouge eNodeB can basically own all of the communication coming in and out of the UE. According to the researcher, the UE may not even be able to make an emergency call, not to mention the fact that the attacker can inject their own malicious packets while communicating with the UE. While this attack seems like the hardest to pull off because it requires the most hardware and knowledge, a skilled attacker can walk away with the brass ring it the attack is executed successfully. Semi-Active attacks don’t require as much equipment, but they do require more specialized knowledge about the apps that help facilitate the attacks. Knowing what triggers a paging event and more importantly, when it has been triggered is not just a matter of understanding the protocols, but it also means the attacker is required to execute the attacks in coordination with the user’s activity. If it wasn’t for all the sophisticated equipment required for the Active attack, one might say that the Semi-Active attack is equally as hard to execute. When it comes to the damage the attack can inflict the Semi-Active attack is an attack that facilitates the leaking of information not owning the channel. So even though the perceived damage is not as high, I can see a more sophisticated attacker using this for reconnaissance instead of relying on this method as a way to cause damage. Lastly, the Passive attack has the smallest learning curve but also poses the least threat. Using OpenLTE and some pretty unsophisticated equipment to scan a network, track subscriber messages and link them to movements of the subscribers over time is a low energy / long term attack. Knowing the history of people’s movements over time might seem like unactionable information, but depending final goal of the attacker it can equate to more than just an invasion of privacy. This type of information in the hands of a violent domestic abuser could prove to be lethal.

*Referring to the video and article on the True2F protocol, explain in your own words and in layperson's terms what are U2F and True2F. Make sure to address the additional security properties provided by True2F over U2F.*

U2F or Universal 2nd Factor is a 2 Factor protocol that uses hardware with an embedded cryptological algorithm that is synced with the target site to create a matching public / private key pair. Since Universal 2nd Factor uses hardware and randomness to create keys it is vulnerable to attacks that seek to introduce insufficient randomness or supply chain tampering that may involve an attacker compromising the privacy of the private key. True2F tries to solve these problems by introducing the browser ( Chrome of course, since this was made by Google ) to introduce additional randomness to the cryptological algorithms so that malicious hardware can’t bypass strong encryption. It also seeks to verify the actions of the hardware by requiring an initialization sequence that the hardware but also continually verifies with the Browser in an effort to ensure that the actions of the hardware do not seem malicious. I like this approach because it seems like Browsers should be taking a more active role in the defense of the users.

*Provide a simple high-level explanation of the main attack from the paper “The Password Reset MitM Attack.”*

In my opinion, a descriptive analogy for the PRMitM Attack is what we like to “ear-hustling” ( my wife is a master of this ). “Ear Hustling” is similar to simple eavesdropping with one simple difference, the eavesdropper is usually doing so covertly whereas the ear hustler participates as an active listener in a public conversation in plain sight. This often happens in a crowded restaurant where the expectation of privacy pretty low, but common courtesy dictates that people mind their own business. The ear hustler violates this rule and does so in plain sight by listening to conversations when the expectation is that everyone is paying attention to their own conversation. It’s surprising what one can overhear by simply being hyper-aware of conversations around you in a crowded train or airplane. I’ve overheard personal information, social security numbers, passwords, credit card numbers and much more. But, since I am not a criminal, I don’t make plans to do anything with the information I just heard. In the PRMiTM attack, the attacker sets up a normal conversation with an albeit fake service that a user would have in the course of setting up a new account. The fake service asks all the normal information: name, email, password, phone number, personal challenge questions, etc. In the background, the attacker is using all this information to perform a password reset on the target’s Gmail, bank account or another sensitive service.

*Among the proposed defenses from the paper “The Password Reset MitM Attack,” pick the one you consider the most effective and usable. Give a brief description of the mitigation approach and explain why it is especially effective and usable.*

In my opinion, all the defenses proposed by the researchers are extremely weak, so I can’t answer the question as it has been offered. Instead, here is a short critique of the researcher’s defenses.

1. Use security questions that are related to the website. The researchers don’t give any examples of what a question like this would look like, however, the claim is that if the questions are specifically related to the site they are using they will be harder to reuse for another site. However this lack practicality. With the assumption that the challenge questions would be created when the account is new, how would a user create challenge questions specific to a service they have never used before?
2. The second defense was to ensure that SMS reset codes are not sent in clear text but instead in a link with a clear description of what the message is for. While I agree the use of a link is better than a message in cleartext. I am not clear on how a link would protect a user if their number was cloned. Furthermore it pretty trivial to distract the user from their phone, temporarily disable text messages, make the target restart their phone, socially engineer the target to block messages from the automated service -- on and on. Advocating the use of a link versus clear text is a little ignorant of the root problem: SMS is not safe. A problem which other security professionals who read the same article recognize. Hence one comment from a respected security blogger: “Better is not to send a code in clear text over SMS (and even better in my mind is not to use SMS, due to its vulnerabilities, but leaving that aside…), but instead to send a link via SMS.”[[1]](#footnote-0) I am pretty sure most seasoned Pen Testers would not consider this a defense at all and I tend to agree.
3. Next, the researchers suggest a phone call, which has the same vulnerabilities as SMS if not more. If I call the target in advance and warning them that we are experiencing increased phishing attempts and ignore all calls, I can get them to ignore the call and pick it up myself on a cloned phone.
4. Next, the researchers suggest the use of notifications ( push notifications, emails, etc ). The hope here seems to be that telling their users “something just changed in your account” would prompt the user to leap into action. But this too is easily foiled. In the notification happens in the middle of the night for example ( since there is no requirement that the attacker uses the stolen PR answers right away ) by the time they wake up the attacker could already have access to the user account and delete the notification emails. As for the push notifications and SMS notifications, a social savvy attacker could send a competing message telling the user to “ignore those as they were sent in error.”

I am way over the 100 words here but I think the main problem with these defenses is they are trying to force outdated and weak channels of communication to defend against sophisticated attacks. I wouldn’t consider myself a professional pentester and I could think of 10 different ways to get around each of these. The truth, in my opinion, is we probably need to start thinking more seriously about “Cryptography Without Using Secret Keys”, or Physical Unclonable Keys using quantum and fiber, making IPv6 a reality or simply improve the old school solid-state cryptography that is less at risk to SMS, voice and social engineering attacks.

1. Colyer, A. (2017, June 18). The password reset MitM attack. Retrieved October 27, 2019, from https://blog.acolyer.org/2017/06/21/the-password-reset-mitm-attack/. [↑](#footnote-ref-0)