CS 6480: Paper reading summary
HA 17.a

José Monterroso

School of Computing, University of Utah

October 30, 2020

1 Breaking LTE on Layer Two

Paper discussed in this summary is "Breaking LTE on Layer Two" [3].

1.1 First pass information

1. *Category:* This paper is an analysis of an existing system. The existing system being analyzed is Long Term Evolution (LTE). Specifically, the authors of this paper are analyzing the data link layer for potential security threats.

2. *Context:* The technical area of this paper relates to network security in mobile networks; specifically 4G LTE, and because 5G will use similar technology, 5G should be aware of these potential threats. Our paper on 5G [1] relates to this paper as it covers aspects of 4G LTE.

3. *Assumptions:* From what I have read in the first pass the authors assume that their experiments show that the three attacks they propose are feasible within a real-world commercial network. They show these results through the use of a software defined radio and an open source LTE stack implementation. I think their assumptions are valid because most open source technology are similar in nature to the real deal. So if their attacks work on the open source it could potentially work in a commercialized network. Furthermore, they list that they were able to build a proof of concept for the aLTEr attacks against a commercial network.

4. *Contributions:* The papers main contributions are listed as follows. First, they perform an extensive LTE layer two analysis. They specifically examine the control plane for possible information leaks that allow an attacker to gain access to sensitive data. Next based upon the performed analysis they present three attack: two passive attack, and one active attack. Lastly, they demonstrate that these attacks are real in nature.

5. *Clarity:* From what I have read this paper appears to be well written, and follows a nice format that is typical of high-end networking research conference papers.

1.2 Second pass information

- *Summary:* In this paper we learn of three new attack vectors on layer two of LTE. According to the authors this is the first, security analysis of data link layers protocols. The authors introduce two passive attacks, and one active attack. The two passive attacks are identity mapping, and website fingerprinting. With identity mapping an adversary could map a user to its transmission stream. This attack is a stepping stone for more in-depth attacks. The website fingerprinting attack is used to un-anonymize a connection; with this attack we can find the webpage that belongs to the encrypted connection. Lastly, the active attack is called aLTEr. aLTEr can actively manipulate the encrypted payload and control specific parts of the message. Each of these attacks are proven to be realistic threats. Specifically, these attacks are conducted between the victim user and a benign base station. The authors use the unique information of the RNTI to perform the identity mapping attack. The DCI information leaks sensitive information that enabled the authors to perform a website fingerprinting attack. Furthermore, the authors exploit the lack of user data integrity protection in the PDCP for their aLTEr attack. As the paper progresses the authors credit a number of small insight into the setup of LTE that leads to these attack vectors. In the background section, we establish all the necessary information that is needed to understand the attack vectors. In the later sections we get into the specifics of the passive and active attack vectors.

1.3 Third pass information

- *Strengths:* I really liked the abstract and introduction, they do a good job of establishing the setting, discussing the problem and explain what this paper is all about. I like how they had a discussion section for each attack. It brings validity to their work in showing that this is a serious threat. Although I didn't really seem to follow their math when they discussed the website fingerprinting, I believe that the way they showed their work to achieve the attack vector is a strength of this paper. Mentioning that their results for the website fingerprinting section are biased was a strength because they are telling people the truth, however, this seems to take credibility away from their results. I really did enjoy their figures and how they described them. Finally, I think it was great idea to not only find the problem using aLTEr but also propose potential counter measures.

- *Weaknesses:* I noticed that in later sections there was a lot of repetition of similar phrases and sentences that were used in the introduction. In fact the attack vectors are redefined multiple times using the same definition. I thought the background section had a lot of information which they did a decent job of managing content into sub-headings, but I think overall it would have been better to just make a new section. Their approach for their attack vectors were placed within an ideal bubble scenario. If this was a real world threat they wouldn't have such ideal conditions.

- *Questions:* I'm curious if hackers before this paper came out, figured out the same attack vectors. I'm also interested to see if the LTE implementors covered the security holes. I really don't know anything about time series so when the authors mentioned warp path I simply had no idea.

- *Interesting citations:* When it comes to mobile networks I truly don't understand much about them besides the basics. When we discussed the 5G [1] paper this helped alleviate some of the confusing because the 5G topics were defined through the use of 4G technologies. So, I was able to become better acquainted with 4G topics. Now, security is a hot topic in practically any field of computer science. So reading about LTE and its possible attack vectors makes me want to look up more information. So, I would like to read the paper on IMSI [2] detection which discuss the other side of security; policing.

- *Possible improvements:* They could divided some of their long sections into smaller more specific and detail oriented sections. There attack vectors were placed in ideal scenarios that made the attack easier to occur. Maybe they could limit the help they get from the ideal setting and try to make it more realistic.

- *Future work:* They mention how these types of attack vectors could also be possible in 5G because 5G follows similar technologies as in 4G, however, 5G offers added security that 4G doesn't have. So I look forward to seeing if you could still use these types of attacks. However, I think security in general is a continuous topic so we will mostly likely see more holes being opened when fixing other holes

References

[1] group companies, N. Making 5g a reality. *NEC White Paper* (Feb. 2018).

[2] Ney, P., Smith, G., and Kohno, T. Seaglass: Enabling city-wide imsi-catcher detection.

[3] Rupperecht, D., Kohls, K., Holz, T., and Popper, C. Breaking lte on layer two. *2019 IEEE Symposium on Security and Privacy (SP)* (May 2019).