Exposing Vulnerabilities in Mobile Networks: A Mobile Data Consumption Attack

Dean Wasil
Computer Science
Mount Vernon Nazarene University
wasildm@mail.mvnu.edu

Omar Nakhila
Computer Science
University of Central Florida
omar_hachum@knights.ucf.edu

Dr. Cliff Zou, Dr. Damla Turgut
Computer Science
University of Central Florida
czou@cs.ucf.edu, turgut@cs.ucf.edu

ABSTRACT

Mobile networks used by smartphones are responsible for keeping an accurate record of customer data usage for customer billing. In this work, I attempt to expose a vulnerability in the billing systems used by mobile networks. The vulnerability allows an attacker to target a victim's smartphone and cause the smartphone to consume data unbeknown to the victim. The attack used is a combination of software and social engineering. Thus, the attack relies on the victim and the victim's location and will not work under certain conditions. Initial tests demonstrate that the attack is feasible and that mobile networks do not record customer data usage accurately.

OBJECTIVE

- Expose a vulnerability in mobile networks' data usage billing systems.
- Develop an attack to demonstrate the existence of the vulnerability.

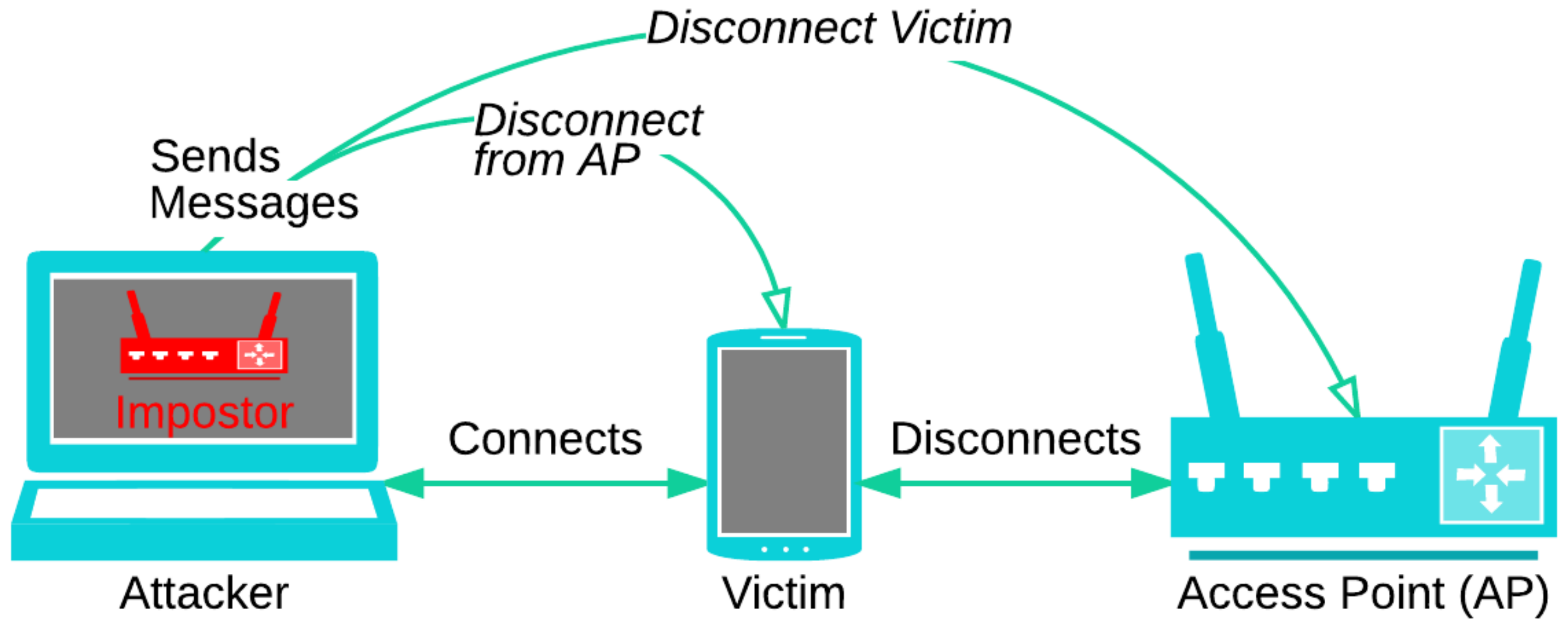
RESULTS

- The attack was tested using two Android 6 enabled smartphones both using chrome browsers.
- The rate of mobile data consumption from the attack depends on the speed at which the victim can download and the speed at which the uploader can push data out. However, the tests demonstrated that the mobile data consumption rate was often high enough to cause a severe amount of data consumption within an hour.
- The tests demonstrated that the attack is feasible, but that reliance on the victim and the victim's location are needed. Thus, the attack will not work under certain conditions, such as, the victim realizing they may be getting attacked or the victim being on a network that does not have a captive portal.
- There is potential for the victim to notice indicators of the attack, with the main indicator being that the victim's Wi-Fi will switch off. However, the attack attempts to cover up attack indicators through social engineering.
- The tests demonstrated that the attack can be performed with the attacker simply using a laptop with free-to-download software installed. A thorough understanding of computer networking and web development is also needed by the attacker.

ATTACK

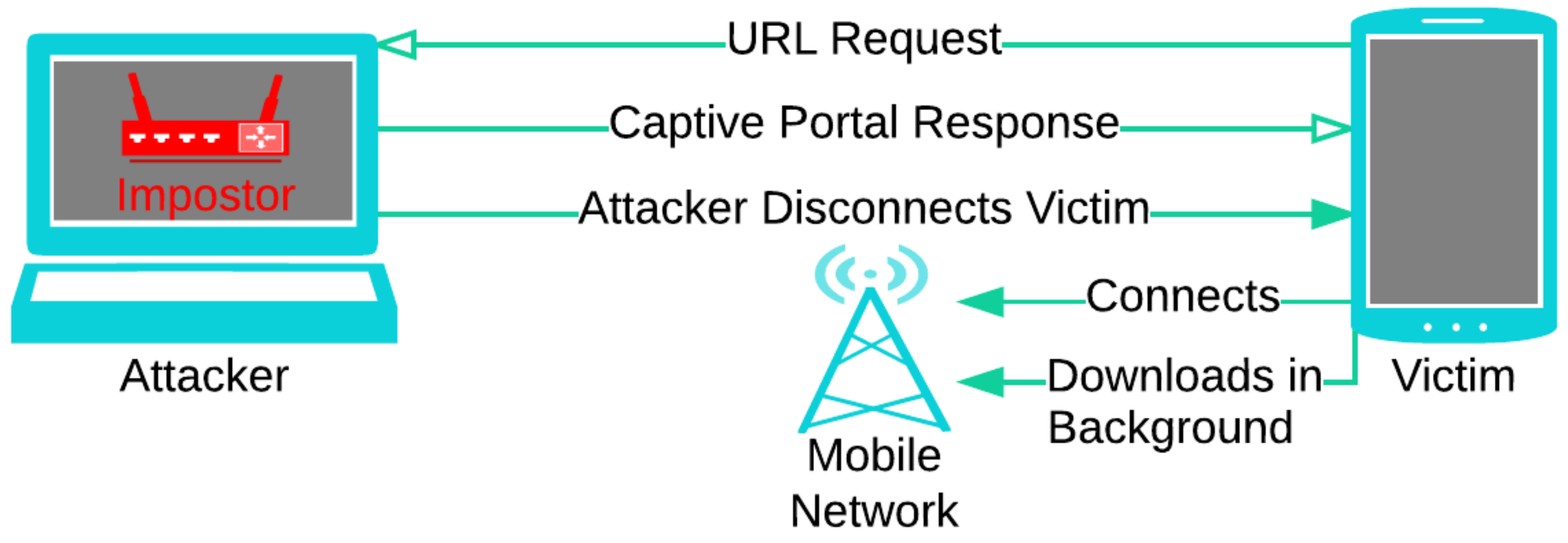
The attack begins by the attacker assuming which public access point (AP) the desired victim is connected to. This can normally be assumed based on the victim's location. The attacker then captures the AP's captive portal, a webpage that network users are redirected to in order to accept network usage conditions. Next, the attacker injects malicious code into the captive portal. The attacker then hosts the malicious captive portal on a fake copy of the AP. Next, the attacker sends a message to the public AP telling it to disconnect the victim along with a message to the victim telling it to disconnect from the public AP. The victim will respond by attempting to connect to an AP. As long as the attacker's AP has a stronger signal than the public AP, the victim will connect to the attacker.

Establishing Connection



Once connected to the attacker, the victim will send a URL request. The attacker will respond by sending the malicious captive portal to the victim. After the response, the attacker disconnects from the victim, forcing the victim to have no nearby Wi-Fi connection. With no nearby Wi-Fi connection, the victim automatically connects to the mobile network. Once connected to the mobile network, the captive portal downloads data in the background, consuming the victim's mobile data. Social engineering is used to keep the victim unaware of the data consumption. The social engineering includes a series of messages on the captive portal and a realistic captive portal feel.

Consuming Data



RELATED WORKS

- Peng (2012) describes a similar "stealth spam attack" which uses old connections made by a victim and sends data over them. Peng (2014) describes two similar attacks. The first is the "cloak-and-dagger spamming attack" where the victim's data is consumed by either spoofing the victim's IP address and using data as the victim, or by sending an MMS message which opens up a connection to spam the victim. The second attack in Peng (2014) is the "hit-but-no-touch attack" where data packets are sent to the victim with a shortened time-to-live value so that the packets pass though a mobile network's billing system, but never make it to the victim, thus invisibly using the victim's data.
- These three related attacks focus on consuming a victim's data just as the attack in this work does. The attacks, including the attack in this work, all exploit the inaccuracy of mobile network billing systems, but all focus on different vulnerabilities.

FUTURE WORK

- Redirect the victim to the captive portal by using software that supports captive portal redirects rather than a DNS redirect.
- Automatically switch the victim to mobile data upon captive portal response via captive-portal-to-attacker communication.
- Further test the attack on different smartphone operating systems and browsers.

REFERENCES

[1] C. Peng, C. Li, G. Tu, S. Lu, and L. Zhang. Mobile Data Charging: New Attacks and Countermeasures. In ACM CCS, 2012.

[2] C. Peng, C. Li, H. Wang, G. Tu, and S. Lu. Real Threats to Your Data Bills: Security Loopholes and Defenses in Mobile Data Charging. In ACM CCS, 2014.

ACKNOWLEDGEMENTS

The support for this work was provided by the National Science Foundation REU program under Award No. 1560302.
Any opinions, findings, and conclusions and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.