Assignment #1

Design of Secure Computer Systems

Anton Claes

0300042110

CEG4399

University of Ottawa

September 25th, 2017

Assignment # 1

One of the most impressive attacks performed recently is the attack against the Dyn company. Dyn's main business is Domain Name Servers managment. The company hosts canonical website names in it's DNS servers and provides the corresponding IP addresses to the users performing DNS lookups on these sites. The attack against the Dyn company occured on October 21st, 2016 and targetted Dyn's DNS servers. Hilton (2016)

The attack is a Distributed Denial of Service (DDos) Attack, which basiquely consists in flooding a system with request or bandwith until it can't handle it. DNS servers are designed to handle

Two attacks occurred, the first one in the morning and the second one in the afternoon. These attacks were effective as big websites like Airbnb, Github, were affected.

The attack was a Distributed Denial of Service (DDoS) attack. Hundred f thousands of devices connected at the same time to the servers and issued multiple requests, thus generating huge traffic that the servers couldn't deal with. At some point all requests (including the legitimate ones from the users) were no longer dealt with, thus denying service.

To do such attacks, the attackers can't use their personal devices as they wouldn't be able to generate sufficient traffic to flood the servers, which are designed to deals with great amount of data. So attackers first compromise other devices with some piece of software, and then trigger them to send as much requests as they can at the same time. What's original in this attack is that the compromised devices weren't laptops and computers like it usually is the case but they were connected objects like CCTVs and

other linux-running connected devices. The breach occurred because when these devices are sold by the manufacturer, they have default passwords set, which people don't bother changing. This way, it's easy for a piece of software (in this case a malicious software called Mirai) to store the default passwords, and spread from device. These devices usually aren't very powerful in terms of processing power or memory, but they can still perform DNS lookups, and their large number allows for huge traffic generation.

This case is very interesting because the vulnerability is not on the victim's side but on third-party devices' side. Furthermore, the breach is not directly due to a design or engineering failure, but it's due to people's not bothering about changing passwords. As it is not mandatory to change password for user, it's assumable that people will not change it.

As the breach used for this attack is not located on the victim's side, the victim of the attack is not to blame for lacking security. As it is not mandatory to change passwords, the users can not be blamed neither, although their not changing default password is quite unwise. The ones to blame here are the manufacturers, which should have initialized their devices with random default passwords, or force people to change password on first startup of the device.

show that "blablabla"Antonakakis et al. (2017)

References

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... Zhou, Y. (2017). Understanding the mirai botnet. In *Proceedings of the 26th usenix security symposium.* Retrieved from https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentatio

Hilton, S. (2016). *Dyn analysis summary of friday october 21 attack.* Retrieved 2016-10-26, from https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/