Trent Giever

Case Project 3-3

7/5/18

Lightweight cryptography

From fridges to light bulbs more and more devices are making up the internet of things. The internet of things is the target of botnets for being easy to gain access with little security protections. Cryptography is a possible solution to add an extra layer of security. The need for extra security in the unprotected devices from being used is needed.

Lightweight cryptography would seem to the non-informed user as common sense from day 1 that the data sent from the phone to the lamp smart plug is secured and not prone to hacks. But to the tech informed that is not the case, and there is a reason that I don’t have any smart speakers or Wi-Fi cameras that can be used against you. Devices are considered lightweight when it has limited processing power, slight delay, or low power restrictions (like battery powered devices). The idea to have security for these lightweight devices must have crossed the original creators of the smart device movement of how to protect the internet of things devices. The idea that protections was needed after DVR’S and Webcams got hacked and used by a botnet to cripple the East coast on October 21, 2016 with a denial of service attack (Newcomb, 2016). The goal seems like common sense that every device on the internet should have protections to avoid being taken over.

Since Russians and North Korans are unavoidable some sort of protect is needed. The NIST has in April issued “the first call for lightweight cryptography” to create a standard way to protect the easy target devices (Chad Boutin, 2018). The way that lightweight cryptography is proposed by NIST is symmetric cryptography with a key that both the sending server and the device can use to send and receive messages. Another way it can also work is to have asymmetric cryptography with a light key on the device and a stronger key on the server to reduce the processing needed (Chad Boutin, 2018) (OKAMURA Toshihiko, 2017). Most smart device markers are getting into the security side also and want to be the first to have less-hackable devices. The NIST wants to make a standard and major corporations also want to have an above standard security for marketing. In 2013 NSA created SIMON/SPECK with the need for little processing power (OKAMURA Toshihiko, 2017). Another possible solution is from NEC called OCB and in 2015 broke the theoretical limits with the ability to only use block cipher encryption (OKAMURA Toshihiko, 2017). One of the Battelle workers created a smart device add-on that only accepts certain IP addresses to reduce the risk of a hacked device. There is no question if it is going to be a standard, it is more when will the international community create the standard and will be in the next few years. Another solution that might be easier is to cut some fiber optic lines near Russia, North Korea and China and most of the hacking troubles will go away.

The need for security will not disappear and will become more obvious as more devices are connected to the world grid. Lightweight Cryptography can in theory solve the security problem the IoT devices have. With the ease for anyone to watch webcams online from babies crying to the free entertainment has been going on for too long. The idea is simple, but the hardest part might be the smaller device makers not wanting to change. The major corporations will adjust fast and make their devices safe. Change is fast online with the Asian hackers needed to be stopped before the attack.

# References

Chad Boutin. (2018, April 18). *NIST Issues First Call for 'Lightweight Cryptography' to Protect Small Electronics.* Retrieved from NIST: https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics

Newcomb, A. (2016, October 21). *Second Hack Fearted, After Massive Cyberattack Knocks Major Website Offline.* Retrieved from NBC News: https://www.nbcnews.com/tech/tech-news/massive-cyberattack-knocks-out-major-east-coast-websites-n670671

OKAMURA Toshihiko. (2017). *Lighweight Cryptography Applicable to various IoT devices.* Retrieved from NEC: https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html