Botnets - Refrigerators, DVRs, televisions being attacked

Cheng Shi, Mehmed Mladenov, Michael Chen, Seo Pallichirayil, and Sarth Desai

***Abstract*—In this part of the assignment we will explore one of our proposed solutions of preventing IOT devices attacks in detail, explaining and discussing the mechanics and feasibility of a multi-factor authentication on protecting the Internet of Devices.**

I. Introduction

Botnet is a collection of internet-connected devices, which includes pcs, mobile devices, servers and IOT devices that are infected by malware. Modern electrical appliances like smart refrigerators, TVs, and webcams are embedded with chips, connected directly to home internet, and thus become a new type of Internet of Things. However, with potential manufacturer flaw or weak default passwords, attackers are able to exploit these appliances and use them as bot devices to create a bot connection called the Botnet to perform DDoS attacks. In order to prevent similar attacks from happening, we introduce multi-factor authentication [1] as a method of securing user logins, forcing and encouraging users to use more than one way of checking their true identity. Implementation of multi-factor authentication on IOT devices can be either through a SMS verification code the device requested on your cell phone, or your biometrics (usually a fingerprint, retina scan or facial recognition pattern), or even hardware tokens and/or separate devices in addition to a standard password.

II. Background

A botnet attack is a type of malicious attack that utilizes a series of connected computers to attack or take down a network, network device, website or an IT environment.It is perpetrated with the sole intent to disrupt normal working operations or degrade the overall service of the target system.

Passwords have been the bane of information security and the user experience since the time they were necessary for switching between users on time-sharing systems. Too often, they are weak enough to be overcome with dictionary attacks, too complex to remember–or both. In part I of our assignment, we have already introduced cases where weak or default passwords led to the botnet attacks which could have been easily avoided. Since IOT device users are the bottlenecks for password strength, why not try to bundle up the security by adding extra layers of authentication? That's the intention of Two-factor/Multi-factor Authentication.

Cheng Shi (e-mail: cs5615@nyu.edu)
Mehmed Mladenov (e-mail: mm7277@nyu.edu)
Michael Chen (e-mail: mzc223@nyu.edu)
Seo Pallichirayil (e-mail: sgp322@nyu.edu)
Sarth Desai (e-mail: sjd445@nyu.edu)

A. Two-factor/Multi-factor Authentication [4] adds a second level of authentication to an account log-in. When you have to enter only your username and one password, that's considered a single-factor authentication. MFA/2FA requires the user to have two out of three types of credentials before being able to access an account. The three types are:

- Something you know, such as a personal identification number (PIN), password or a pattern
- Something you have, such as an ATM card, phone, or fob
- Something you are, such as a biometric like a fingerprint or voice print

For potential infiltration possibilities attackers must acquire all the factors before they can get access into the device. For 2FA, attackers must gain access to both the original password and the second factor, say, a token generated by a physical key fob. The latter one is almost impossible to get access to unless you break into their house. For MFA with three factors and more, risk is reduced onto separate factors as they need to be combined for an single access.

III. Threat Model

Threat Modelling is a process by which potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized from a attacker's point of view. In the previous assignment, we used generic threat models and attack trees. The review paper we studied on Botnet and Botnet Detection Techniques presents a significant amount of details about the botnets and how they can attack the devices and ways to detect them.

Let us review the basic botnet architecture.

Botnets are usually used for :

- Sending massive amounts of unsolicited e-mail (SPAM), the most popular way of using botnet, allowing to send millions of messages in a very short period of time. It is estimated that 80% of spam is sent by zombie computers. The use of botnets allows to circumvent this problem by sending spam from email addresses belonging to the owners of infected zombie devices.
- Distributed Denial of Service (DDoS), which means blocking access to Internet services by generating false traffic. Consequently, the attacked server is overloaded and becomes unavailable. Cybercriminals usually demand money to stop the attack. Unfortunately, at a time when a lot of companies operate online, the company owners often pay such ransom, without any involvement of the law enforcement authorities.

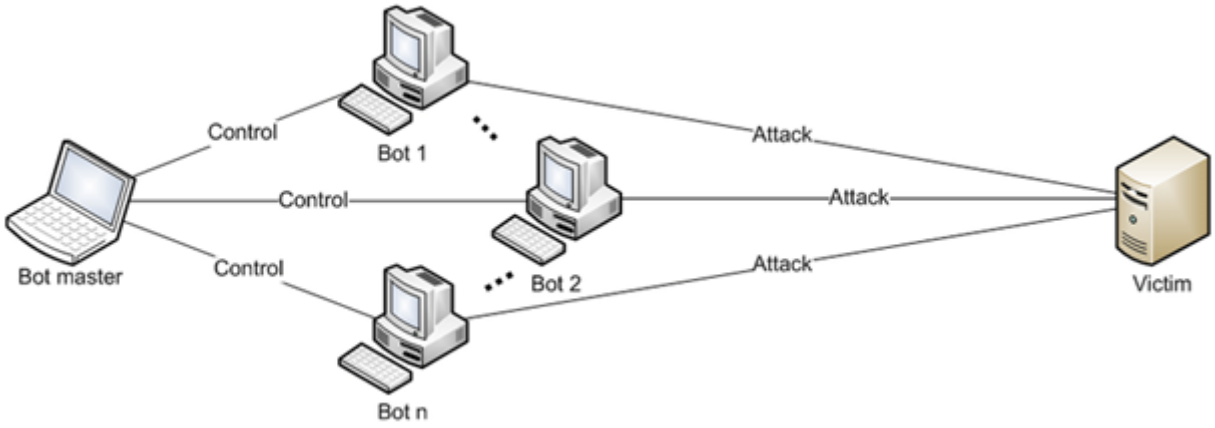

Fig. 1. CentralizedBotnet Architecture

TABLE I

Threat	Risk	Solutions
The resources attached with the device can be utilized by the attackers for performing any kind of attacks ranging from DDOS, sending massive amount of spam Emails, or Downloading or distributing other malware	The user may face reduced bandwidth and less resources available for useful purposes.	All communications between the host and the devices should be authenticated by using strong passwords or 2FA Authentication. The users may register their devices, whitelist them and any other connection will be blocked asking for authorization. This would allow users to keep track and restrict any potential malicious attacks.
Privacy of the user and sensitive information can be severely compromised by collecting information from the infected devices.	An attacker can easily commit Identity theft and internet fraud by collecting the user's personal information like SSN or credit card numbers.	Implement encrypted communications by default, so only the user will have the key and also restricted access using firewall to limit communication to trusted hosts.
Compromise the integrity of the system, the attacker can delete useful files or make changes making the system to work in unexpected ways.	The database or the content associated with the System cannot be trusted, and can mislead the user.	The devices should contain intrusion detection and file history, where modified data can be easily detected.

- Stealing confidential and private data, e.g. credit cards numbers, information allowing to get access to bank accounts, wide spectrum of logins and passwords. The collected data are then used for other illegal activities, for example, may be sold.
- Generating false clicks on pop-up ads, i.e. Pay-Per Click (PPC) by advertising agencies at various websites. The owners of such websites charge a commission per every click. By using zombie networks, it is also possible to generate thousands of such clicks within one day only, and each click comes from a different computer so as not to raise any suspicion. Therefore, the money spent on advertising campaigns go straight into the pockets of website owners.

There are several levels of a potential analysis of cyberspace phenomena :

- Host analysis - the analysis which is mainly based on raising awareness among users with respect to various cyber-threats, installation of anti-virus software and firewall software, and keeping used software up to date (latest updates always installed).
- Analysis of traffic - the analysis which is mainly based on the network traffic monitoring via Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
- Analysis of bot network and communication between the infected computers and C&C server - the analysis is aimed at monitoring the functioning of the Internet as a whole and may be performed by specialist institutions, such CERT, in particular with the assumption of their collaboration to ensure cyber security at a state level.

The threats resulting from the botnet network are really important in terms of cyberspace security. Additionally, great dynamics of changes in the manner of the botnet operations and methods of attacks resulting therefrom increase the need of their in-depth analysis. It is more and more necessary to have special skills for predicting attacks and launching protection methods right for the great dynamics of changes in the types of cyber attacks.

IV. Design

Since the danger of attacks on IoT devices is growing, MFA is a necessity. However, many IoT devices have limited storage and computational capabilities, so the security solution should be designed to be efficient.

The design for such security would be, whenever a user activates 2FA, a cryptographic strong key, which is shared in secret, is generated. Then, this key is used to generate a one-time code, which is used to authenticate the identity of the user. It works similarly to the existing login procedure. To generate these codes, we also need a counter, which in most cases is the current timestamp rounded down to an interval, known as TOTP, but in some cases a random number is generated. To

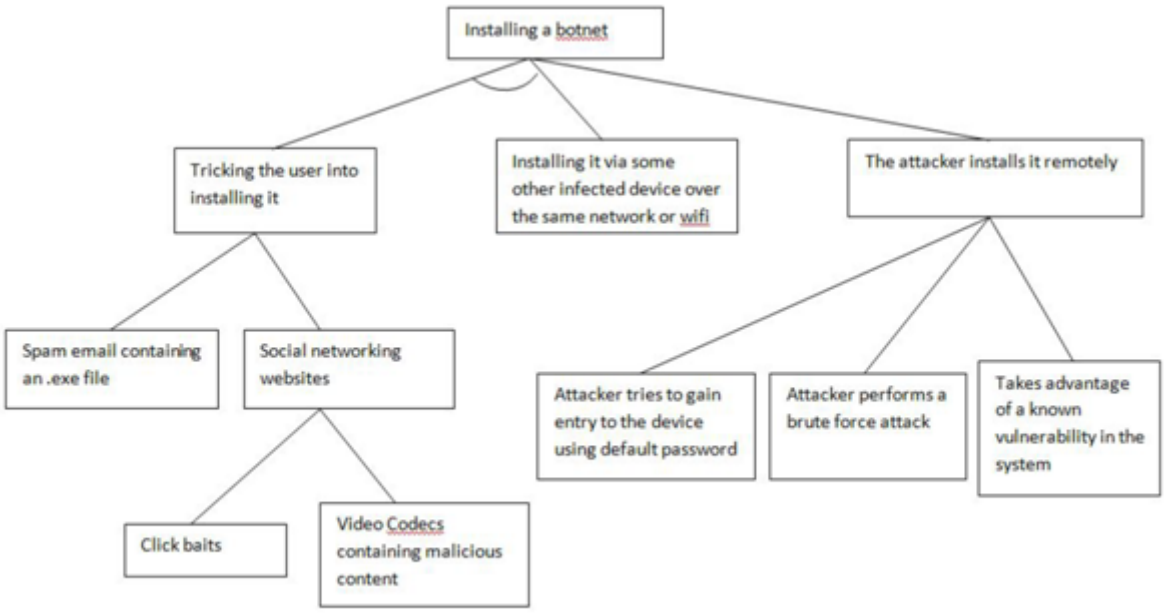

Fig. 2. Attack Tree

verify the code, we just need to generate it again to check if the same counter is used. The code is valid for few seconds or until used once, then a new one is generated.

To have a full protection with the 2FA security method, the user also has to keep the device firmware updated and change the default login credentials.

V. Implementation

In order to implement Time-based One-Time Passwords, or TOTP, a secret must be shared between the user and the IOT device. This is most commonly done using a QR code that is scanned with a user's phone. First, the user would log in to the IOT device to generate a shared secret. This would also be an opportune time to ensure the user changes the password away from the default. Once the user authenticates themselves against the IOT device, the IOT device can then display a QR code for the user to scan onto their phone or other device that supports the 2FA app. Note that both devices will also store the timestamp from which to keep track along with their shared secret.

Now assuming that both devices are synced in time, the IOT can verify that the other party has the secret. When the user needs to prove that they have the same secret as the IOT device, the user can provide a code generated by their secret plus however long ago the secret was generated. The IOT device then verifies this by comparing the given code to the code generated by the device's secret. If both parties have the same secret synced to the same starting time, then the codes will match. Note that times are often downsampled into larger ranges (commonly 30 seconds) to avoid synchronization problems.

In addition to acting as a second factor of authentication (something the user has - the secret), this form of authentication is stronger than simply authenticating with a password as the timestamp acts as a second factor. If an attacker is only able to obtain the secret, they would be unable to break into the device as they would not know what time to sync the secret to, and vice versa with obtaining only the timestamp.

Finally, the IOT device should mandate periodic updates and credential changes. A safe range is 6-12 months, as forcing the user to change passwords too frequently often leads to the user choosing weak passwords. Suitable notice should also be put out before forcing the user to change password.

VI. Evaluation

Challenges

MFA (Multi actor Authentication) does increase security but it has some challenges [11]

1) Cost: The is probably the number one challenge for multi factor authentication, but it is not a unique challenge. Most new technology deployments incur a cost increase, at least initially. MFA brings potential cost increases for things like additional support, training, maintenance, SMS Gateway or services, mobile app development, hardware and software tokens, and stipends for mobile phone expenses.[11]
2) Complexity: Some physical authenticators require additional drivers. adding another dimension of complexity for deployment, support, and maintenance. This also requires constant compatibility checking as environments change.[11]
3) Backup Options : Do you have a backup plan in place for your multi factor solution? For example, what if a user loses his or her phone or token? Is there a way for users to gain emergency access?[11]

Adaptive multi-factor authentication

Fig. 3.

Adaptive authentication means the system is flexible depending on how much risk a user presents.

For example, if an employee is working on the company premises and uses a badge to get through security to her office, Okta will recognize that she is in a trusted location, and that she has permissions to proceed. If that same employee is working from a coffee shop, the system may prompt her for an additional security factor when she goes to login remotely, since she's not in a trusted location. Or, it could present an additional MFA challenge if the user was working from a personal laptop instead of a company device.[13]

Type of MFA to be implemented

One other issue while implementing multi-factor authentication is that we have to decide which system should use which kind of multi-factor authentication.For example a phone can use Biometrics like a fingerprint Scan or laptop can use Biometrics like facial recognition but the same authentication cannot be applied to other systems like a refrigerator or DVRs. So for every System we need to optimise between cost and Security.

VII. Related Solutions

Botnets are responsible for a variety of hacking campaigns, including perpetuating Distributed Denial of Service attacks, which hit a particular network or device with so much traffic that the system is unable to work under the strain. One such program, known as Mirai, was responsible for the massive October 2016 Dyn DDoS attack, which shut down major websites such as Twitter and Netflix. The hackers took advantage of vulnerable, internet-connected DVR boxes, which had only minimal manufacturer security, and turned them into "bots". All devices are identified, authenticated and connected through servers. In order to keep this communication safe, an encryption is vital for the ecosystem.

However, even if everything is encrypted, the server might fail while everything is centralized. So, strong encryption is followed by decentralization and more specifically, the blockchain. The technology behind the blockchain is used for tracking trillions of transactions every day, which also can be used for tracking and keeping the history for billions of devices. This would enable secure exchange of information, with encrypted communication and the whole history, which would be tracked easily if necessary. Thus, better solution is the encrypted communication and data exchange between the devices.

VIII. Conclusion

In this paper we have discussed on how to secure devices from botnet attacks and have explored on how to secure the devices from botnets using multi-factor authentication.There are some limitations of MFA like cost, complexity etc.MFA also requires a periodic Synchronization So that a secret key can be maintained between the IOT device and other party.But by far MFA is the best solution that can ensure safety from remote attacks

IX. References

1) https://arcticwolf.com/blog/why-you-need-timely-patching-and-multi-factor-authentication-in-the-iot/

2. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

3. https://www.researchgate.net/publication/283257776_A_Review_Paper_on_Botnet_and_Botnet_Detection_Techniques_in_Cloud_Computing

4. https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

5. https://www.matec-conferences.org/articles/matecconf/pdf/2017/39/matecconf_cscc2017_03013.pdf

6. Dagon D., Gu G., Zou C., Grizzard J., Dwivedi S., Lee W., Lipton R.:, A Taxonomy of botnet structures – lecture: Computer Security Applications Conference, 2007. ACSAC 2007

7. Erdös P., Rényi A.: "On random graphs", Publicationes Mathematicae 6, 290-297 (1959a)

8. Erdös P., Rényi A.: "On the evolution of random graphs", Publications of the Mathematical Institute of the Hungarian Academy of Sciences 5, 17-61, (1959)

9. https://engineering.gosquared.com/building-two-factor-authentication

10. https://www.fifthdomain.com/industry/2018/01/08/the-botnet-solution-everybody-already-knows-about/
11. http://blog.identityautomation.com/the-challenges-and-benefits-of-multi-factor-authentication-mfa-101-part-2
12. https://auth0.com/blog/different-ways-to-implement-multifactor/
13. https://www.okta.com/blog/2016/12/two-factor-authentication-vs-multi-factor-authentication-what-are-the-risks/