**ITIS 6167: Network Security**

**Homework 2**

**Handout Date**: *September 5th, 2019*

**Due Date**: *Sep12th, 2019 before 5:30PM*

**Question 1 (10 points):** Read “RFC 1858 - Security Considerations for IP Fragment Filtering” at <http://www.faqs.org/rfcs/rfc1858.html> and write a half page summary to illustrate:

(1) What are the security concerns discussed in this document?

(2) What are the proposed approaches?

**Summary:**

This paper discusses IP Fragment Filtering and the possible security attacks on it. The paper discusses two types of IP Fragmentation attacks, the first one being **Tiny Fragment Attack in which** single IP datagram is broken into smaller sized multiple packets. Now, all the network links have an MTU specifying the characteristic size of messages that could be transmitted. So, if a data packet’s size is small enough to force some of a TCP packet’s TCP header fields into the second data fragment, the filter rules specifying patterns for those fields won’t match. And hence, if the filtering implementation doesn’t mandate a minimum fragment size, any disallowed packet might be passed because it didn’t hit a match in the filter.

The paper describes two proposed approaches to prevent this attack. According to the first ‘Direct Approach’, length of the transport header in each zero-offset fragment should be computed and compared against a value TMIN which is the minimum length of transport header required to contain important field values relevant to the packet filters. If the transport header length is less than the TMIN, the fragment should be discarded. The second ‘Indirect Approach’ is observation based and states that there when a TCP packet is fragmented to force significant header fields out of the zero-offset fragment, there must exist a fragment where F0==1. Conversely, if there exists a packet with F0==1, there might be a zero-offset fragment in the fragment set, with the length of the transport header being 8 octets and discarding this fragment will not allow reassembly at the receiving host.

The second attack discussed in the paper is **Overlapping Fragment attack.** The reassembly algorithm described in the current IP protocol specification results in new fragments, overwriting any overlapped portions of previously-received fragments. An attacker can leverage such a reassembly implementation to design a series of packets, with the lowest fragment containing malicious data which would be passed by administrative packet filters. In this fragment, some subsequent packet could have a non-zero offset, which would overlap the TCP header information such as destination port, and cause it to be modified. Since the second packet doesn’t have a non-zero offset, it would be passed through most of the filter implementations.

The proposed approach to prevent this attack is to make the router's filtering module enforce a minimum fragment offset for fragments that have non-zero offsets. This approach could prevent overlaps in filter parameter regions of the transport headers.

Another simple approach to prevent both Tiny Fragment attack and Overlapping Fragment Attack would be to drop any packet if the TCP fragment has F0==1.

**Question 3 (20 points):** Read “[Understanding the Mirai Botnet](https://uncc.instructure.com/courses/110077/files/6564029/download)” and write a 1-2 page (Single Spaced) summary to illustrate:

### Motivation: Not HOW they are addressing the research goal but WHAT are they trying to accomplish with this particular research goal.

### Contribution: What are they trying to provide to cybersecurity as an industry.

### Vulnerabilities:

### What are the security concerns discussed in this document?

### What are the proposed approaches to address those security concerns?

### Research Methodology: Summary of research methods used

### Results Summation and Validation

### Critique: Identify limitations in the research or methodology not identified by the authors.

### Do you feel this impacts the results?

### Opine: provide a summation of your opinion on whether you agree this research actually makes a contribution to cybersecurity.

### Summary:

### The authors of this paper have done intense research on the famous Mirai Botnet Attack. They go on to describe Mirai as a self-propagating botnet virus which came into prominence in August 31st, 2016. Mirai’s code infects poorly protected IOT devices by using telnet to discover the devices that are still using their factory default username/password. Due to its ability to infect tens of thousands of such insecure IOT devices and co-ordinate them to mount a DDOS attack against a chosen victim, Mirai was highly effective and dangerous.

### The motivation behind this research was to understand the mechanisms and motives behind Mirai-not just how it works but digging deeper to understand what were the motivations behind Mirai so they could learn something about how to combat Mirai and other botnet attacks like Mirai in the future. The researchers also see their work as a snapshot of the IOT Botnet phenomenon which could be a great reference point for future researchers. Finally, the researchers were fortunate enough to coordinate with a wide range of data partners, which resulted in a great combination of different perspectives to conduct a more nuanced and cross validated approach to understanding the Mirai Botnet.

### A deep analysis of the complete working of Mirai botnet was done by the researchers along with what classes of devices were affected the most and how the varients of Mirai evolved over time, competing for vulnerable hosts. This rearch is a great contribution to Cybersecurity as the researchers provide a proof as to how fragile the ecosystem of IOT Devices is and that learning about how a botnet attack took place and functioned, could further help in preventing another one from happening. Mirai, even through its simplicity compromised several devices creating a widespread notorious DDOS attack and threatened some of the best defended targets, thus understanding it would only give more awareness to security professionals into combating its evolved versions in future.

### There are several security vulnerabilities addressed in this paper. The first one is Lack of Security Hardening. With the Mirai Botnet attack, it was pretty clear that even a simple unsophisticated dictionary attack can successfully compromise thousands of IOT devices. Although randomizing default passwords should be the first logical step, it’s not the only secure way to prevent future attacks targeting software vulnerabilities. For this reason, IOT security should move towards default-closed ports, network configurations that limit remote address access and principles of least privilege should be adopted, ASLR, isolation boundaries should be implemented. Security hardening best practices is the key to security here.

### Patching Bugs and Vulnerabilities is another challenge mentioned in this paper which can be easily resolved by adopting Automatic Updates. However, this could be burdensome for instance where one requires building PKI infrastructure to support trusted updates. A solution to this problem could be Bug bounties. Additionally, it will require the entire IoT community to actively check itself for vulnerabilities. Furthermore, in case of a Zero-Day exploit which disables automatic updates, there has to be a fallback mechanism in pace which involves physical access and consumer intervention.

### ‘Notiﬁcations’ (such as alerting device administrators via CERT bulletins, emailing the abuse contact in WHOIS records, and in-browser warnings to site owners that a page is compromised) through out-of-band channels could be a solution to this problem. Additionally, IoT devices should be required to register an email address with a monitoring platform will then be able to can alert consumers of serious security threats in an easier way.

### Detecting even the known vulnerable device models and firmware versions on the network is difﬁcult. To resolve this issue, encoding firmware versions in a portion of MAC address is the solution. Disclosing this information at Layer 2 to local network operators would allow for blocking of remote access to known vulnerable hardware till its patched. Finally, according to the researchers, Fragmentation posed a risk to maintaining and managing IoT devices as they encountered several instances of FTP, HTTP and Telnet sacks during scans. To resolve this issue, defragmentation is required. Adoption of OSs such as RIOT OS, Tock etc. is stated to be a push towards defragmentation in this research paper.

### The researchers employ a number of different data sources to understand and research the multifaceted process of Mirai’s working. They used a network telescope of unused IP addresses (4.7 million IP address from July 18, 2016 to February 28, 2017) that allows them to observe finger-printable Mirai scan packets. Next, the researchers performed Active Scanning (136 IPv4 scans) to determine what are the infected devices, then, they used Telnet honeypots to collect around 434 binaries and supplement this malware binary collection with additional 594 binaries from Virus Total. They also used actively collected DNS data from seed lists and passively collected DNS data (collected approximately 499 Million daily RRs), generated by DNS queries at a large ISP to measure C2 domain activity and to identify DDOS targets. Additionally, the researchers utilized C2 Milkers to monitor the issuance of different attacks from the C2 centers. And finally, they were able to get a list of attack IPS for two of Mirai’s high profile targets: popular security blog called Krebs on Security and DNS hosting service- Dyn.

### Since several years, the security industry has been trying to crack the code behind working of botnets. In this research work, the researchers have meticulously utilized a lot of resources and well-established botnet measurement perspectives to disclose the IOT security concerns to the community. The researches analyzed the structure, behavior, and evolution of Mirai botnet. The researchers deduced several results such as: Theere were 46 unique passwords in the 09/30/2016 Mirai source release and that Mirai primarily targeted consumer routers, IP cameras and DVRs. Furthermore, the researchers disclose that the top vendors affected by Mirai were mainly camera, router and embedded device manufacturers and that the top 14 victims most frequently targeted by Mirai run services like political sites, online games, and even DDoS protection services. The researchers also found that Mirai launched a total of 15,194 attacks between September 27, 2016–February 28, 2017. These attacks include application-layer attacks, volumetric attacks, and TCP state exhaustion attacks.

### According to me, the only few limitations with this research are that, it does not effectively describe effective strategies to combat Mirai Attacks. Some strategies could be: Checking routers for unauthorized DNS changes, rebooting the routers (as rebooting removes infection; but not a good long term solution as they can be re-infected), CDN providers to manage traffic loads in peak hours and examining how your organization **obtains its DNS services-** Dyn customers neither used a secondary DNS provider nor configured DNS servers to use more than one of Dyn’s data centers. Hence, server reconfiguration took a lot of time, thereby creating more attack opportunities. Online companies could use both Dyn and other DNS providers, such as OpenDNS for redundant operations. This would be a good strategy in case of future DNS-based attacks. Additionally, companies should be able to capture attack traffic. This way, they can easily keep track of who could be possibly targeting their network. For instance, Since Mirai exploited TCP port 7547to connect to home routers, organizations could monitor that port by adding a detection rule. The research work is overall great but since the motivation behind this research is to prepare people in the cybersecurity community to combat future botnet attacks like Mirai, common security practices were worth mentioning. It would give more ideas to things to remember while securing their IOT devices.

### In conclusion, this paper thoroughly gives a breakdown of the motivation behind Mirai Botnet Attack, which would be a great reference point for current and future researchers to understand the working of IOT attacks and the importance of securing IOT devices.