**ITIS 6167: Network Security**

**Homework 1**

**Handout Date**: *August 30th, 2019*

**Due Date**: *Sep 5th, 2019 before 5:30PM*

**Question 1 (15 points):** The ARP protocol allows the network nodes to identify the mapping between IP address and hardware address dynamically. Now we assume that for the next generation Internet, some investigators propose to use static combination of IP address and Physical address, for example, if you know the next hop’s IP address, you can use a function Func(IP) to calculate the MAC address.

Please discuss the advantage and disadvantage of this proposal in the following aspects:

1. Do we still need ARP? Why?
2. Can we still hardcode the MAC address into the hardware when it is manufactured?
3. If a computer just boots up and it needs an IP address, how can it reach the server and how can the server send the information back?
   1. Here we assume that the computer and server are on the same Ethernet.

**Answer:**

ARP table is used to maintain a correlation between each MAC address and its corresponding IP address. Below are advantages and disadvantages if we develop a function Func(IP) to calculate the MAC address:

|  |  |  |
| --- | --- | --- |
|  | **Advantage** | **Disadvantage** |
| 1. Do we still need ARP? Why? | As the function Func(IP) calculates the MAC address, there would be no need to map the MAC address to IP address, which inturn can replace ARP and this will help avoid attacks like ARP poisoning, ARP spoofing, ARP flooding etc. | * Mac address, being a function of IP address may cause duplicate addresses or conflicts of similar IP addresses, which is easily possible when there’s communication between two different networks. * If Func(IP) is vulnerable we can still have attacks of unauthorized accesses. * Moreover, since both IP nad MAC addresses are dynamic, there are chances of IP packets getting delivered to wrong recipients. |
| 2. Can we still hardcode the MAC address into the hardware  when it is manufactured? | * Yes. We can still hardcode the MAC address into the hardware. Hardcoded MAC addresses are anyway needed for initial communication when an IP address is not assigned. Since, a unique address is always required for a new system to connect to the internet, in this case, the server would need a unique identifier/ address of the host to start the communication. Power should be assigned to the Func(IP) for a code to be generated, to get a response from the server. * NIC chip can be designed as programmable for it to calculate and alter the MAC addresses. | * Even if the MAC address is hardcoded, it will get over-written by Func(IP) when IP address is assigned. This could lead to losing device’s static identifier. * Additional computational overhead would be incurred to calculate MAC from IP when each communication begins. |

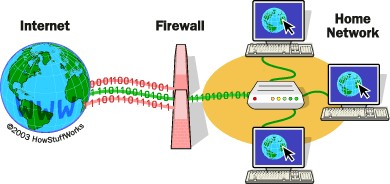
|  |  |  |
| --- | --- | --- |
| 3. If a computer just boots up and it needs an IP address, how can it reach the server and how can the server send the information back? | DHCP is the protocol which is used upon boot up; it maintains a pool of IPs and assigns IP to computers based on availability. Initially an IP is assigned randomly to a system when its booted. Using this IP, Func(IP) can calculate a temporary MAC which can then be used by DHCP to generate an actual IP address. Then, using this actual IP, Func(IP) can now generate an actual MAC address.  In order to connect to the internet (if computer and server are on the same ethernet), and for a server to respond to the machine, one must have MAC inside the hardware module or a chip. For instance, for communication to occur between the server and a computer the NIC should have another unique address, if not MAC because it would depend on IP address being assigned. | Before IP address is assigned via DHCP through principle of **DORA** (discovery, offer, request, and acknowledgement) it first talks with or identifies the host by its MAC address. Thus, having MAC dependent on acquiring IP address would create challenges in setting up initial communication when system boots up. |

**Question 2 (10 points):** A company is using IP based authentication to protect the computers behind the firewall. Only the web server and email server’s IP addresses can reach the outside world. Please use an example of ARP poisoning to illustrate how the malicious node can penetrate the firewall and reach out to surf the web pages.

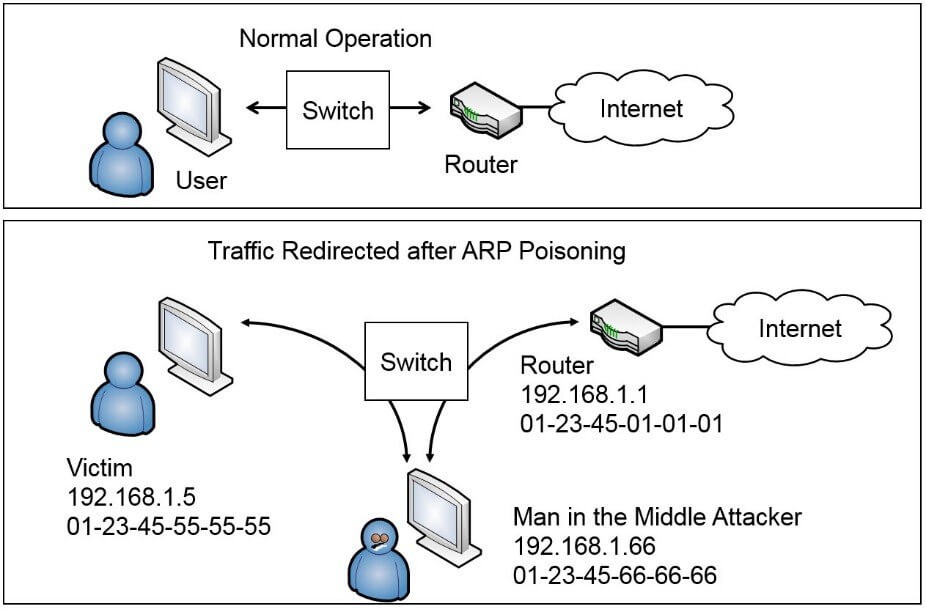
**Answer:**

* IP Address Filtering is a mechanism which determines what should be done with network data packets, based on their sender or destination addresses. In either case, the packet is inspected by a network router or firewall and then based on the rules set by an administrator, a packet is passed on to next node on the network. If the rules say that packets with a specific address should not be sent ahead, then the packet is simply ignored or dropped and is not propagated via the current network route.
* In a normal scenario if the attacker wants to access the internet, other than the allowed pages, a firewall will prevent this unauthorized access.

**Normal Scenario:**



* So, in order to gain access to the internet, the attacker will exploit the IP based filtering mechanism through ARP poisoning and spoofing.
* This is how it’s achieved: The attacker will first target understanding the communication between firewall and server and then try to poison the ARP table of firewall.
* In detail, the source IP address is checked by the firewall, originating the request. The firewall will only allow the IP addresses of the web server or email server and will discard the rest.
* Next, the attacker will determine the IP address and MAC addresse of the victim. This will be done by sniffing the network traffic eavesdropping on the internet traffic, directed towards the the server, by overriding the ARP cache.
* The ARP cache consists of the MAC address that the attacker now has along with IP address of the server.
* Now, the attacker will spoof the web server in case the firewall and web server interact directly. And when the ARP cache is updated, it will be notified, and the interception will be stopped. ARP table of server is poisoned to sniff the packets going from server to firewall, to avoid automatic update of firewall ARP cache and continue the sniffing.
* Hence, here in this attack, all the packets are directed towards the attacker rather than being transmitted from the web server to the firewall. The firewall communicates with the attacker assuming it to be the server.
* ICMP redirect functionality is disabled to avoid detection of the attack.

**ARP Poisoning Scenario:**

In this way, the attacker deceives the victim machine by spoofing the ARP tables.

Alter:

As only the web server and email server’s IP addresses can reach the outside world, the attacker can try to associate their IP address as a genuine IP address and change the MAC address by attacking the LAN with forged ARP packets. By doing this, the hacker’s MAC address takes place of the genuine MAC address and like in Man-in-the-Middle attacks, the attacker will receive the packets from the target computer and then they will forward them to the web server and the email server. This way all the information to and from the target computer and the web and email servers is intercepted by the attacker. Now that the attacker has penetrated the firewall, they have access to all the web pages that have been surfed as well as all incoming and outgoing emails.

**Question 3 (15 points):** Read “Detecting Credential Spearphishing Attacks in Enterprise Settings” at <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-ho.pdf> and write a 1-2 page 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.

**Answer:**

### In this paper, the authors have given a brief overview of what spear phishing is: a type of email spoofing attack which targets specific individuals or organizations and tricks them into leaking sensitive information for personal gain. Spear phishing has been going on for several years and has affected government systems as well as high ranking organizations and even political figures. Spear phishing does not necessarily require technical sophistication and is still very dangerous because if conducted successfully, the adversary can make a victim perform any kind of actions such as wiring money to a non-legitimate source or leaking confidential information such as SSN numbers. Hence, this security breach is a big concern because there aren’t any generally effective tools that can detect and prevent spear phishing. The authors then go on to discuss on of the most common types of spear phishing: Credential spear phishing wherein a thoughtfully handcrafted email is sent by an adversary with a malicious link which opens a web-page to fetch private credentials (username/password) of the user, the victim is tricked into believing that the email is from a trusted entity and provides his/her credentials, thereby leaking confidential data.

### According to the authors, attachment-driven spear phishing attacks are comparatively easy to capture because most organizations actively scan emails for malware, keep the machines up to date and hence the attacker will need to resort to a zero-day exploit in order to have access to confidential information. However, with credential spear phishing, an attacker just has to craft an email which appears to be legitimate and host a website! Additionally, with VPN applications, use of remote desktops, stolen credentials, the attacker already has a lot of information and attacking capabilities at hand. Because of these reasons, credential spear phishing poses a major threat to organizations and individuals and designing a practical solution to detect and prevent spear phishing is the motivation of this research. Solving this major problem would not only give Their idea of a detector which can identify both known and novel attacks with great accuracy (high true positives) without generating a huge number of alerts and manual work provides a very practical approach to detect and prevent spear phishing attacks. Not only will this idea provide safety to an organization’s valuable data but will also solve a major problem in the cybersecurity domain. This idea will probably boost DLP strategies currently in place.

### The authors have also addressed several security concerns that their detector has and what could possibly be the solutions to address these security concerns, the first security concern is the “Limited Visibility” of the detector. Their detection strategy is focused on identifying if the recipient of an email is involved in any dangerous action- To test this behavior and their detector’s abilities, the authors could make use of LBNL’s distributed network monitor (NIDS logs) which has the ability to log all HTTP GET and POST traffic that crosses its border. NIDS can remember all the URLS in the email bodies of incoming and outgoing emails at LNBL. However, emails and the network activities conducted OUTSIDE of LBNL’s network can’t be captured in the NIDS logs. Secondly, LBNL decided not to man-in-the-middle traffic served over HTTPS, thus, if there’s any spear phishing attack conducted over HTTPS, it will not be detected. However, using endpoint monitoring agents on employee machines can prevent this security issue. Finally, the detector might even miss attacks if a spear phishing email is originated from a compromised personal email account. To defend against this problem, one could adapt analyzing stylometric features to identify spear phishing.

### Other major security concerns related to the detectors design are False negatives-since the goal of the design is to set an upper-bound on the number of alerts, the detector might miss some genuine attacks if more number of attacks occur in a given day, however, this problem could be resolved by increasing the detector’s alert budget. The next concern is that the attacker can even escape detection by compromising a webpage that is visited often such as Netflix and then crafting a spear phishing attack which would in turn boost up the embedded link’s domain reputation.

### The prevention strategies discussed to solve these types of attacks are presented as future work, where efforts could be taken to make DAS more robust; such as, changing the scoring algorithm to decide on which event is more suspicious in at-least ‘k’ dimensions. The detector also requires minimum of 3 months of prior data to conduct its analysis successfully. If the detector is fed just 1 month of history, it’ll generate lots of alerts and will also fail to capture some attacks.

### The research methodology behind the detector’s design revolves around several factors, the first one being generating very less false positives (10 a day) and increased number of true positives. To make the detector robust, the authors utilized datasets such as SMTP logs which contain SMTP headers information related to all emails sent to and from the organization’s employee. NIDS logs (discussed earlier) and LDAP logs from where information such as what time did the user log in, what was the IP address and the corporate email ID used, how many times did the user attempt to login and if the login IP address actually belongs to LBNL’s network. According to the authors, while the basic detection techniques which utilize supervised and machine learning are useful, they are not necessarily effective in identifying benign behavior and hence the detector adapts additional techniques such as DAS, Real time Detection Architecture, Feature Extraction (LDAP, NIDS, SMPT Logs), Nightly Anomaly Scoring and Real Time Alert Generation.

### What I believe that the article fails to address with precision is why an event is considered less suspicious than the other. The article does mention this as a scope in the future works, but no potential attack can be less “dangerous”. How would the detector handle SSL encrypted traffic? Since due to privacy concerns, access was not granted to the URL’s webpage, what could be possible attack scenarios and how could they be handled? Let’s consider Dropbox as an example, Millions of users utilize it to back up sensitive data and share files, what if an attacker tries to lure users into providing login credentials through a fake Dropbox sign in page hosted on drop-box itself? The paper describes a great detection mechanism but does not focus on employee security awareness training, how user friendly the detector would be or how easily can it be integrated with the existing system. The paper also mentions that attacks won’t be detected if a personal G-mail account is compromised but does not describe in detail how stylometric features can be utilized along with detector’s current capabilities to achieve accurate results. I believe all of these factors are imperative to design a secure detection system and should have been addressed.

### In summary, there are a wide variety of Phishing attacks that are causing harm to the cybersecurity domain. Credential phishing is just one variety out of several more dangerous phishing schemes. I believe that this idea definitely contributes towards securing sensitive data and making a user’s life easier but at the same time, user awareness is important. Users must be discouraged from publishing sensitive corporate or personal on social media platforms and Organizations must invest in solutions, such as one described in this paper, that are capable of analyzing inbound and outbound emails for known malicious links as well as attachments. Both user awareness and a protective solution can surely help prevent or at least decrease the impact of a phishing attack.

**References:**

Image one source: <https://s.hswstatic.com/gif/firewall.gif>

Image two source: [http://gcgapremium.com/wp-](http://gcgapremium.com/wp-content/uploads/2016/01/Figure7.3-ARP-poisoning-used-to-redirect-traffic.jpg) [content/uploads/2016/01/Figure7.3-ARP-poisoning-used-to-redirect-traffic.jpg](http://gcgapremium.com/wp-content/uploads/2016/01/Figure7.3-ARP-poisoning-used-to-redirect-traffic.jpg)

<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/spear-phishing-101-what-is-spear-phishing>