Utilizing AI in the Defense against Threats in Cyber Security

Richard Gu, Ethan Hincapie, Min Kang, Kyle Khembunjong, Zachary Kohler

Nomenclature*

ARP	Address Resolution Protocol
DDoS	Distributed-Denial-of-Service
APT	Advanced Persistent Threat

*See appendix for extended nomenclature

Abstract

In this paper, the usage of AI based server is discussed to alleviate and eliminate security threats, and specifically, ARP Poisoning, DoS attacks, and APT. ARP Poisoning is the underlying infrastructural technique to many hackers which can be achieved through the forging of ARP packets in a LAN environment. Due to the stateless design of ARP and its lack of verification, networks are ultimately susceptible to malicious attacks, such as the fore mentioned DoS, MITM, and APTs. DoS attacks are performed by transporting excessive amounts of data to a device or network, causing it to temporarily malfunction. We propose a new solution based off of an ACS defense to centralize all communication within a LAN to a server. This allows for a more secure network by finding gaps in security the moment they are made.

I. Introduction

The availability of modern networking devices allow for many benefits and conveniences to our daily lives. The ability to interconnect your devices allows for accessible and effortless assistance in everyday tasks just a push of a button. However, these eases in our lives do not come without the potential to damage the devices and surrounding networks. The serviceability in today's technology leads to several methods of breaching possibilities within cyber security, and demands for greater security provisions as networks develop. Hackers have refined their malicious acts into various forms and techniques, and it has become increasingly difficult to counter and prevent such attacks. Major issues that persist in the cyber security world include ARP poisoning, DDoS attacks, and APT's.

II. Literature Review

1. ARP

ARP, or Address Resolution Protocol, is designed to convert Internet Protocol (IP) into media access control (MAC) during the interaction of devices connected through Ethernet, or local area network. Address Resolution Protocol was first introduced and defined in 1982 by RFC 826, a paper by Plummer [1]. Originally known as protocol p, this protocol was designed for the DEC/Intel/Xerox 10Mbit Ethernet [8]. Protocol p and ARP both function in similar ways; they are both executed by converting types of protocol addresses (IP) into Local Network Addresses (MAC, Ethernet). Nonetheless, protocol p still had its flaws and disadvantages. To actually transmit an Ethernet packet in a network through protocol p, an Ethernet address must be generated. This method, however, was recognized to not always be compatible between the corresponding address. Thus, Address Resolution Protocol was then developed as an alternative to resolve this reoccurring problem by David C. Plummer [2].

ARP operations are located in the DLL of the OSI model in the Transmission Control Protocol (TCP)/IP suite [5]. ARP analyzes and resolves the provided logical address (IP address) and assigns it to its corresponding physical address (MAC address) [6]. ARP is used for distinguishing MAC addresses within the network. To accomplish this in a LAN, a host must communicate with a receiving device in order to discover and resolve the conflict between addresses. The data recorded from the messages is saved in an ARP cache table.

2. IP Address

IP addresses allow for the transportation of packets from network to network through routers. IP works by specifying the format of packets (datagram) and the addressing scheme. They are typically written as four numbers separated by periods, indicating a 32-bit numeric address (IPv4). Newer versions include a 128-bit numeric address (IPv6). An IP address cannot be used to transport data packets within the network (LAN)[4].

There are two types of IP addresses: dynamic and static. Dynamic IP addresses are capable of change and assign the user a different IP every time they log onto the server. This IP can be shared by multiple people at once and brings greater security as the attacker cannot specifically pinpoint the user. Static IP addresses, on the other hand, remain constant even if the user signs out of the server. While a static IP address allows for a stable and faster connection, it also runs the risk of being easily located as the user never changes addresses. The most basic attacks on security occur with static IP [9].

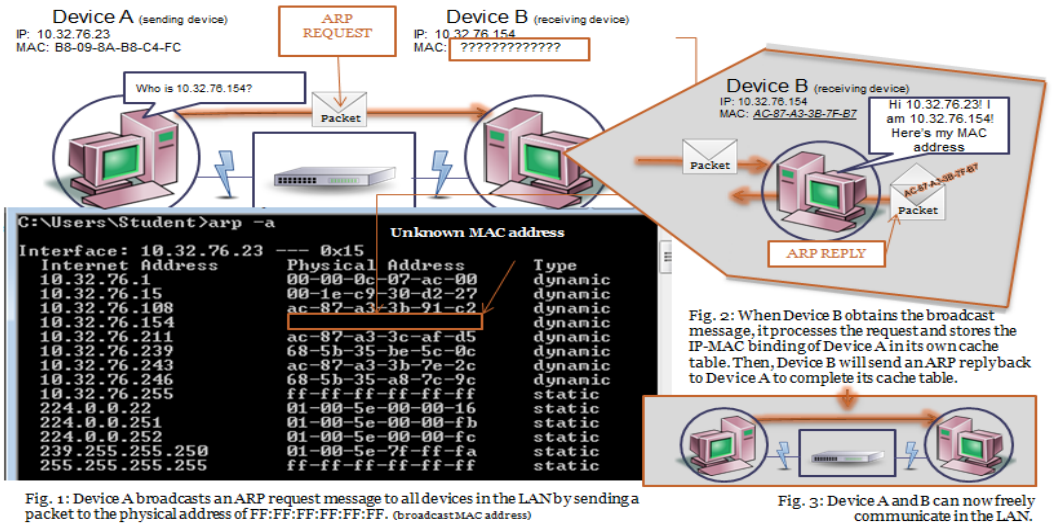


Fig. 1. Device A sends an ARP Request to Device B

3. Media Access Control Address

MAC addresses are the physical address or “hardware number” specific and exclusive to that device. The MAC address of a device is assigned and engraved into the device’s network interface card (NIC). The physical addresses allow transportation of data packets within the network.

4. Steps of ARP

First, the source device (DA) must examine its own ARP cache table to check if the receiving device's (DB) MAC address is already stored. If the MAC address is missing, the sender must acquire it and will proceed to generate a message into the network, known as an ARP request message, to find the corresponding MAC address to allow communication between the two devices on the LAN. The ARP request is broadcasted to all the devices in the LAN, and consists of both the sender and the destination's IP and MAC address. Next, the ARP request asks the network, "Who has this IP address?" Only the device with the requested IP address will respond and process the request. DB then generates an ARP reply message consisting of the IP and MAC addresses of DB along with the original message and sends it back to DA. DB will then update its ARP cache table with DA's IP and MAC address. Lastly, DA will it's ARP cache table following the ARP reply. The combining of IP addresses to MAC addresses are called IP-MAC bindings.

The protocol can be compared to giving a package to an unknown person at a party. If the package is for "Kyle", you would need to learn who he/she is first. You would begin your search by asking "Who is Kyle," to everyone in the room (the ARP request). Only individuals with the name Kyle would realize and respond by saying "I am Kyle," (the ARP reply). After hearing his reply, you now have knowledge of who Kyle is and where he is. Both individuals are now aware of each other and carry information in their memory (ARP cache table). In this example, the party represents a LAN, names represent IP addresses, while their face and location are all part of a MAC address. The connection formed between the two is representative of the IP-MAC bindings formed between devices. The protocol displays convenience in updating numerous changes in IP-MAC binding in an ARP cache table by simply repeating the ARP operation process. Despite this convenience, the exchange process of ARP lacks any form of verification, which can potentially leave the LAN vulnerable to attacks.

4. Spoofing

Spoofing is a type of attack where an attacker or malicious party intercepts the protocols between a device and a network through impersonation. This impersonation allows the device to disguise itself as another device or user in the network. Often times, these attackers gain access to various opportunities to launch more severe attacks that can cause extreme damage. Many of these attacks are against network hosts, to snatch data, spread malware, and to bypass access controls. Spoofing is a fundamental technique for attackers, as it can lead to various attacks.

5. ARP Cache Poisoning

ARP cache poisoning occurs when DA broadcasts an ARP request that the attacker can intercept to impersonate the intended receiving device (DB) and send false messages over the LAN. The result is the linkage between the attacker's MAC address and the actual recipient's IP address, creating false IP-MAC bindings in the victim device's ARP cache tables. Once the bindings between the attacker and the devices occur, the attacker will begin to receive any data or information that was intended for DB. ARP poisoning can allow attackers to intercept, change, or stop data in transit.

6. DoS

DoS attacks are amongst the oldest and most common security attacks and can be sorted into several categories. A DoS attack can be initiated by means of previous ARP poisoning, when the attacker can freely intercept communication between network devices. The purpose of a DoS attack is to backlog a server of or a network, by flooding the affected part with packets of useless data. Thus, the network is brought down, denying internet access to devices on the network. DoS attacks can be performed by groups or individuals, malicious or accidental. The majorities of attacks are done with malicious intent and have motives that range from government attacks, terrorist cells, or competitors on a market.

7. Types of DoS Attacks

The Ping of Death is one of the simplest forms of a DDoS attack, since it can be performed in a Command Window. The attack starts by sending an IP packet larger than the size allowed by standard IP protocol (65,536 bytes). It bypasses the limit by taking advantage of the TCP/IP protocol's method of fragmenting packets into smaller sizes. When the target receives the packets, the network is overloaded with packets and either crashes or freezes [18].

ICMP floods are a special type of DDoS attack that sends echo requests to devices. Echo requests are ping packets that are sent by compromised computers known as daemons or zombies. The compromised computers send an overwhelming amount of packets that slow and bring down the network, denying access to connected devices.

A TCP SYN flood, exploits Transmission Control Protocols through the process that it uses to connect a client to a server. TCPs use a three-step process, or handshake, to establish a connection. The server must partially open a port, bind to it, and "listen" for any potential connections. Afterwards, the three-step process begins. The first step is sending a SYN, or Synchronization, from the client to the server. Responding to the request, the server sends a SYN-ACK, or Synchronization Acknowledgement. The acknowledgement value is a number greater by one value than the first received number. The server attaches a second number to a sent packet, the sequence number, which the client receives. Afterwards, the client sends an ACK back to the server, along with a sequence number which is set to the value of the received number. An acknowledgement number is sent, being one value greater than the number received. During the time that the port is partially open, an attacker continuously sends SYN requests to the target. As a result, the targeted system's server's resources are consumed to the point that the affected system's unresponsive to actual traffic.Another method attackers may use when exploiting SYN is to simply make the client not respond, with an ACK, or Acknowledge, which would be the second step in the TCP's three-step handshake. Attacks may end up spoofing IP addresses, sending a SYN from a false IP. As a result, the server sends a SYN/ACK to the nonexistent address.

8. Reconnaissance Attacks

Reconnaissance attacks gather information on a target within a network; it maps out a network, finds open ports, and notes all protection the network has. This attack can intercept incoming traffic on a network and most reconnaissance attacks precede a DDoS attack such as an ICMP flood.

9. Types of Reconnaissance Attacks

A smurf attack is another type of DDoS attack that is based off of ICMP floods; the attack sends ICMP packets that contain spoofed IP addresses of a victim. The packet's header is falsely set to being sent from an endpoint device[1]. By doing so, a victim would receive a TCP reset packet from device A, despite it being from device B. Despite being effective, a forged packet requires the proper endpoint IP address, port number, etc. Once the packet's header is set to the correct values, the endpoint will close its TCP connection. To further the effectiveness of the attack, the TCP reset packet can be sent to multiple endpoints [19].

Depending on the amount of devices connected to the affected network, the amount of traffic will make the LAN impossible to work on. A fraggle Attack is a variation of the Smurf Attack, in which the affected network has UDP, or User Datagram Protocol, traffic directed to ports 7 and 19 which are linked to the targeted IP Broadcast Address. The packets intend to spoof the victim's IP, then send it back to the affected network's IP. The devices then respond in a similar way to those affected by a Smurf Attack.Another attack that utilizes a flood of ICMP packets is a twinge attack. It cripples the targeted system by using spoofed ICMP packets. However, unlike the smurf and fraggle attacks, the twinge attack uses random and fake internet source addresses, and targets computers rather than networks. With the usage of random source addresses, it may seem difficult to identify attackers, but ICMP packets have a unique signature and due to this flaw, a twinge attack is easily identified. Unlike most attacks, twinge attacks are usually meant to degrade the performance of a computer or to crash it rather than to collect information.

10. APT

An APT is a network attack where an individual with malicious intent gains access to a network and lays dormant, gathering information. APT attacks are generally targeted at organizations with high-value information such as national defense, manufacturing, and the financial industry [11]. It differs from other attacks in that an APT is a customized attack using tools and techniques developed specifically for the attack. Unlike other attacks, APTs are directed slowly to avoid detection and have specific targets such as government agencies, defense contractors, and competitors in global industries [13].

APT attacks can be divided into four phases: incursion, discovery, capture, and exfiltration. Incursion consists of reconnaissance, social engineering, zero-day vulnerabilities, and manual operations. Discovery consists of multiple vectors, research, and analysis. A phrase commonly attributed to discovery is, "run silent, run deep". Capture consists of long-term occupancy and control. After this step, the attacker has fully infiltrated the network and is now lying dormant and leeches information. Lastly, exfiltration is all about data transmission and analysis. Figure 2 shows the ongoing steps. detailed breakdown of each

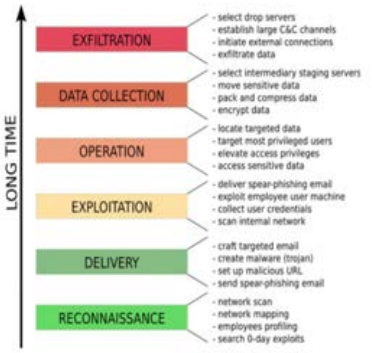


Fig. 2. Typical stages of an APT. [12]

[1] Endpoint device – an internet-capable device that can connect on a TCP/IP network

III. Project Description

This paper proposes a solution based off of many different researches designed to incorporate AI into cyber security. The solution implements a central server in the LAN to detect potential threats as well as gaps in security to defend against ARP poisoning, DoS attacks, as well as APT.

Solutions Using Secondary Cache Tables

Due to ARP and its virtually defenseless construction and its extreme availability, it has been a convenient gateway for many hackers to create malicious attacks. As a result, a variety of defenses have been proposed to prevent and protect against attacks. A solution proposed by Sumit Kumar and Shashikala Tapaswi [2] introduces an ARP Central Server (ACS). It works by having the ACS confirm the IP-MAC binding request from other nodes in the network in order to prevent potential spoofing [2]. This prevents not only potential ARP poisoning, but also other common attacks, like DoS and APT breaching. When a new node connects to the network, it will transmit a broadcast request for the ACS server and the ACS server will respond with its IP-MAC binding. The long term binding allows the client host to store it into a secondary ARP cache table, providing a method of validation when new changes are applied. Validation will only occur if the IP-MAC entry from the previous node matches the IP-MAC binding entry from the long term table produced from the ACS. If the IP-MAC entry does not match the long term IP-MAC binding, it will not be validated and will be retrieved from the ACS and stored in the long term table. The short term table will be updated with a dormant entry for 20 minutes [2]. The system is flawed in that the failure of the ACS server would leave the server unsecured [5].

Arote and Arya [1] discuss a mechanism of defense and prevention that provides backwards compatibility with existing ARPs. The solution implements the usage of a central server through a secondary cache and ICMP protocol. Their current design for the solution uses four systems connected in a wired LAN; the host contains two cache tables: a primary and a secondary cache table, while the algorithm consists of the two main modules, detection and prevention. ARPspoof and ICMP is used with the modules involving detection. Prevention relies on the usage of voting within the network. When a new node joins the network and wants to communicate with the client side for the correct IP-MAC binding, it sends out a voting request to all other available systems in the network. It then collects replies from the vote by waiting for random intervals of 0-100 msec [1]. For every MAC address collected, the node finds the polling score and the MAC address with more than 50% of the votes will be accepted. Afterwards, both the primary and secondary cache tables are updated with the new MAC address.

1. Tools and Patches

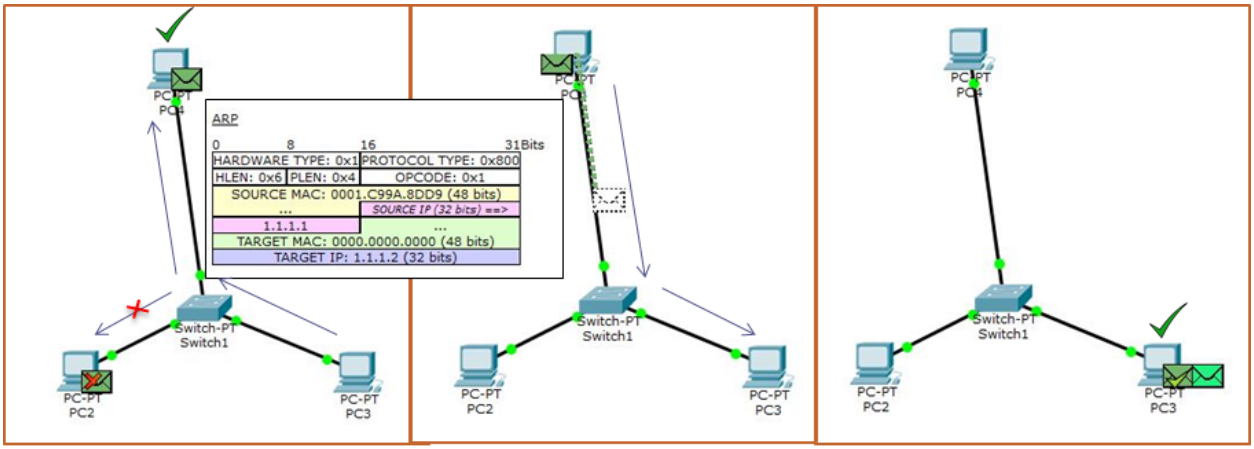
Teterin [1] proposes using a program called Antidote, which allows the host to analyze protocols, detect poisoning in its cache tables, and check for unicasting in the network. This prevents acts of spoofing in the LAN. The solution revolves around using patches and tools to detect and prevent attacks. A similar solution offered by Cisco detects poisoning and allows the host to drop packets with incorrect IP-MAC bindings. Snort-based detection introduced by Hou et al [9] uses static environments to detect and patch attacks. Although patch based solutions provide protection against cyber-attacks, they lack the ability to fully detect and patch attacks between hosts outside of a static environment.

2. Solution Using SDN

Masoud, Jannoud, and Jaradat present a SDN approach to spoofing and reconnaissance prevention. SDN is implemented to alleviate common problems of ARP poisoning with the usage of controllers and SDN characteristics. Controllers are applications that manage the flow control to allow sophisticated networking. SDN controllers are based off protocols such as OpenFlow that run on the links between a network switch and a controller server. This defines the message format, the rules of the packets, and where the packets will be sent. The proposed algorithm consists of two scenarios; the first scenario is when the hosts are designated to dynamic IP addresses using DHCP protocol (SDN_DYN), while the second scenario has the hosts designated to static IP addresses (SDN_STA). This system uses a controlled flow of packet destinations to prevent possible ARP poisoning attacks.

3. Method

To simulate the steps and protocols occurring during the interaction of devices in a network, the Cisco Packet Tracer was the primary program used. The software creates simulations of the traffic of devices in a network and tracks the processes of protocols. It reproduces a LAN environment and provides insight on the transportation of packets. Using this software, attacks such as ARP poisoning and DoS can be found easily and simulated to further our understanding of it. Figure 3 presents a visual representation of ARP, created by Cisco Packet Tracer in order to advance our proposed solution to utilize detection AI in a LAN.



The MAC address of PC_4 does not exist in the cache table. ARP request is broadcasted by PC_3. The packet is dropped by PC_2 and accepted by PC_4.

PC_4 matches the request and stores the packet information and sends an ARP reply to PC_3 (sender).

PC_3 receives the reply and stores the resolved IP-MAC binding in its cache table.

Fig. 3. A typical ARP request and reply.

4. Proposed Model:

We propose that multiple layers of AI be used in network security as internal layers can analyze big data. With the usage of learning algorithms, the AI can analyze the data and recognize access patterns of network users. When an unknown node joins, the AI compares it to the stored data and if there are any irregularities, the AI creates a note and a checkpoint deeper in the network. The AI that secures the checkpoint utilizes adversarial machine learning and with enough setup, will be able to determine if the irregularity will pose any threat by itself. If the irregularity poses

a threat, the AI informs the network host and attempts to block access. Afterwards, it works to patch the vulnerability in security as well as any data leaks.

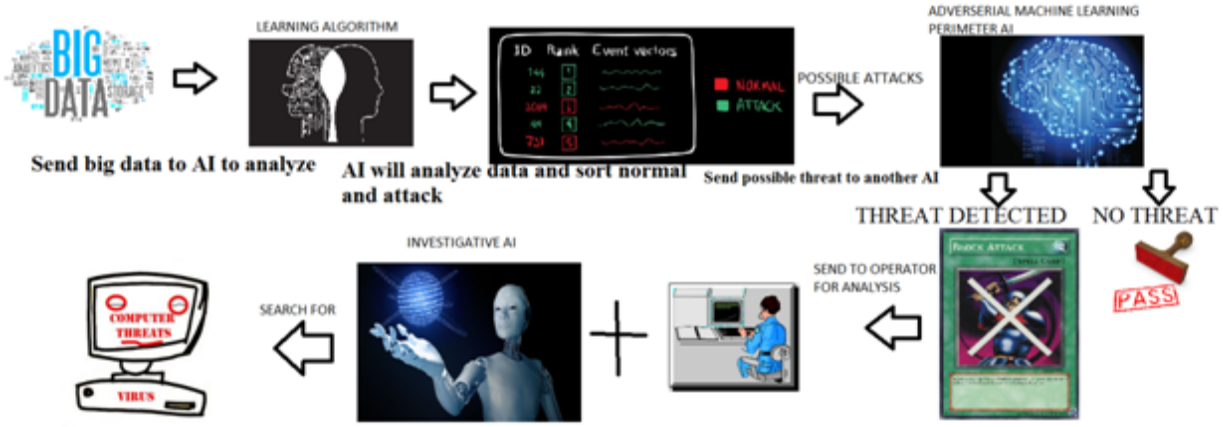


Fig. 4. The model shows the process of implementing different layers of AI and reporting back to human operators to fix security exploits.

IV. Data Results and Discussion

Despite being a theoretical model, AI-based security systems have shown to be effective in the past. AI^2, an AI developed by MIT and PatternEx was able to predict and detect more than 80% of cyber-attacks, with the input of human operators. It utilizes an active learning system to improve detection skills [16]. Since 2013, over $300 million dollars in venture capital was invested in startups that specialized AI by 2014. In IoT (internet of things), AI is being used as personal assistants (Siri, Google Now, Cortana) and these AI receive input and with the use of a learning algorithm, can adapt to tailor each user's needs. AI^2brings a promising system that when combined with the growing industry of AI, could increase network security to a point where the system will be able to sniff out as well as stop attacks before they pose a threat. As more networks begin to use AI-based security, it may be possible to reduce the amount of successful attacks, or perhaps eliminate the threat of modern attacks as a whole.

V. Conclusion

As the threat of network attacks rise and with a lack of solutions and defenses, this paper presents a theoretical framework or fundament of an AI-based security system to detect, as well as combat attacks. The solution draws from previous ideas and implementations of AI in security along with a new innovation such as the utilization of multiple layers of AI to increase security. However, we did not have the necessary resources to program these AI-based security systems to test our theory and therefore base the effectiveness of our solution off of AI2's success, which was heavily similar to ours. Future research could implement this framework to test the effectiveness and also to consider greater human-AI interactions to prevent threats and attacks.

Acknowledgements

The authors, Richard Gu, Ethan Hincapie, Min Kang, Kyle Khembunjong, and Zachary Kohler wish to thank UNLV AEOP research mentors, Mr. Shahab Tayeb and Elliot Ploutz for teaching the intricate topic of internet security in brief, but detailed lessons to further our understanding. They also guided as well as provided us with constructive criticism throughout these packed six

weeks. This research team would also like to acknowledge the U.S. Department of Defense for funding this summer program.

References

[1] P. Arote and K. V. Arya, "Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting," Computational Intelligence and Networks (CINE), 2015 International Conference on, Bhubaneshwar, 2015, pp. 136-141.)
[2] S. Kumar and S. Tapaswi, "A centralized detection and prevention technique against ARP poisoning," Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, Kuala Lumpur, 2012, pp. 259-264.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
[3] H. A. Mangut, A. Al-Nemrat, C. Benzaïd and A. R. H. Tawil, "ARP Cache Poisoning Mitigation and Forensics Investigation," Trustcom/BigDataSE/ISPA, 2015 IEEE, Helsinki, 2015, pp. 1392-1397.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
[4] M. Z. Masoud, Y. Jaradat and I. Jannoud, "On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm," Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on, Amman, 2015, pp. 1-5.
[5] N. Tripathi and B. M. Mehtre, "An ICMP based secondary cache approach for the detection and prevention of ARP poisoning," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, Enathi, 2013, pp. 1-6.
[6] P. Pandey, "Prevention of ARP spoofing: A probe packet based technique," Advance Computing Conference (IACC), 2013 IEEE 3rd International, Ghaziabad, 2013, pp. 147-153.
[7] Gao Jinhua and Xia Kejian, "ARP spoofing detection algorithm using ICMP protocol," in Computer Communication and Informatics (ICCCI), 2013 International Conference on, IEEE, Publication Year: 2013, pp. 1-6
[8] Plummer: An Ethernet address resolution protocol. RFC 826 (1982)
[9] X. Hou, Z. Jiang, and X. Tian, "The Detection and Prevention for ARP Spoofing based on SNORT," in Proc. of IEEE International Conference on Computer Application pp.V5-137.
[10] P. Bhatt, E. T. Yano and P. Gustavsson, "Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks," Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on, Oxford, 2014, pp. 390-395. doi: 10.1109/SOSE.2014.53 [11] M. Rouse, "What is advanced persistent threat (APT)? - Definition from WhatIs.com," SearchSecurity. [Online]. Available: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-apt. [Accessed: 21-Jun-2016].
[12] P. Giura and W. Wang. "A Context-Based Detection Framework for Advanced Persistent Threats," in 2012 International Conference on Cyber Security, pp.69-74
[13]*Symantec*, 2011. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf. Accessed: Jul. 12. 2016.
[14] The Economic Impact of Advanced Persistent Threats (APTs), 1st ed. Traverse City: Ponemon Institute, 2016, p. 15.
[15] N. Virvilis and D. Gritzalis, "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?," *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, Regensburg, 2013, pp. 248-254.
[16] A. Conner-Simons and CSAIL, "System predicts 85 percent of cyber-attacks using input from human experts," MIT News, 2016. [Online]. Available: https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418. Accessed: Jul. 12, 2016.
[17] J. Clark, "I'll be back: The return of artificial intelligence," Bloomberg, 2015. [Online]. Available: http://www.bloomberg.com/news/articles/2015-02-03/i-ll-be-back-the-return-of-artificial-intelligence. Accessed: Jul. 12, 2016. [18] What is ping of death? - Definition from WhatIs.com. (n.d.). Retrieved July 08, 2016, from http://searchsecurity.techtarget.com/definition/ping-of-death
[19] R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial," in *IEEE Communications Magazine*, vol. 40, no. 10, pp. 42-51, Oct 2002.

Appendix

ACK	Acknowledge

ACS	ARP Central Server
AI	Artificial Intelligence
DLL	Data Link Layer
DNS	Domain Name System
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MITM	Man in the Middle
OSI	Open Systems Interconnection
RST	Re-Structured Text
SDN	Software-Defined Networking
SYN	Synchronization
TCP	Transmission Control Protocols
UDP	User Datagram Protocol