Detecting and Combating ARP Spoofing

Chai Ming Xuan
National University of Singapore
mingxuan@u.nus.edu

Er Xue Hui
National University of Singapore
xuehuier@u.nus.edu

Wu Wenqi
National University of Singapore
wenqi.wu@u.nus.edu

Zhu Chunqi
National University of Singapore
chunqi@u.nus.edu

ABSTRACT

Our project aims to create a program for users to detect if they are victims of ARP spoofing, and offer ways to protect themselves.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General - Data Communications, Security and Protection

; D.4.6 [**Security and Protection**]: Authentication, Verification

General Terms

Network Security

Keywords

arp spoofing, network security

1. INTRODUCTION

The Address Resolution Protocol (ARP) is an important protocol in Computer Network communications. However, it is also one of the easier protocols to spoof and carry out attacks on, because of the lack of viable solutions to protect the ARP cache. The most common form of attack on the ARP is a man-in-the-middle (MITM) attack, which we will be illustrating in Section 2. Some common programs which users can use to carry out such an attack include 'Ettercap' and 'Cain and Abel'.

2. BACKGROUND

In order to understand how ARP spoofing occurs, we will need to cover the basics on how computers communicate with each other. In this section, we will be explaining how computers do so, and introduce the basic notions of how an ARP spoofing is carried out.

2.1 Computer Communications

Firstly, in a typical computer, all IP addresses are resolved dynamically through the use of the Dynamic Host Configuration Protocol (DHCP). This is carried out in the following steps:
(to include picture)
1. DHCP Discover
2. DHCP Offer
3. DHCP Request
4. DHCP Ack

After that, suppose the the user Alice wishes to send some information to Bob. The following steps are then carried out:
(to include picture)
1. ARP Request: Alice's computer sends out an ARP request to find out which MAC address has Bob's IP.
(to include picture)
2. When Bob's computer receives the request, he sends back an ARP response packet.
3. Alice gets the response and stores the corresponding IP-to-MAC entry into the ARP cache.

2.2 Poisoning the ARP Cache

(to include picture)
If an attacker, Eve, wishes to carry out an MITM attack on the ARP, this is typically what happens:
1. Alice's computer sends out an ARP request to find out what is Bob's MAC address.
2. Before Bob's computer can reply, the attacker, Eve, sends a spam of packets to Alice's computer, claiming to be Bob. The ARP cache then becomes poisoned.

3. CURRENT SOLUTIONS

There are many solutions in the market to combat ARP Spoofing, such as Agnitum Outpost Firewall. However, from Vivek's[**?**] paper, we can see that many of these solutions employ passive detection, kernal based patches, making MAC entries static, or using a secure ARP protocol.

4. GOALS

In our project, we hope to achieve the following goal:
1. To provide users with a means to actively combat ARP spoofing
2. To make any network more secure.

3. Provide a GUI for users to see what is happening in their network in real-time.

5. OUR SOLUTION

to insert stuff

6. ANALYSIS

to insert stuff

7. LIMITATIONS AND FUTURE WORK

Our project has several flaws which we were unable to resolve within a reasonable timeframe:
1. Our solution will not work on a network that employs WPA-Enterprise level of encryption. This is because the structure of WPA-Enterprise is such that only each user can see his incoming or outgoing network connections.
2. Our solution assumes that the user does not have any form of defence installed on his computer. (eg. no firewall that can prevent ARP spoofing, a network that does not use any enterprise level encryption, etc.)
We hope to improve our solution for a more varied set of systems in the future.

7.1 Citations

Citations to articles [1, 3, 2, 4], conference proceedings [3] or books [7, 5] listed in the Bibliography section of your article will occur throughout the text of your article. You should use BibTeX to automatically produce this bibliography; you simply need to insert one of several citation commands with a key of the item cited in the proper location in the `.tex` file [5]. The key is a short reference you invent to uniquely identify each work; in this sample document, the key is the first author's surname and a word from the title. This identifying key is included with each item in the `.bib` file for your article.

The details of the construction of the `.bib` file are beyond the scope of this sample document, but more information can be found in the *Author's Guide*, and exhaustive details in the *LaTeX User's Guide*[5].

This article shows only the plainest form of the citation command, using `\cite`. This is what is stipulated in the SIGS style specifications. No other citation format is endorsed.

7.2 Tables

Because tables cannot be split across pages, the best placement for them is typically the top of the page nearest their initial cite. To ensure this proper "floating" placement of tables, use the environment **table** to enclose the table's contents and the table caption. The contents of the table itself must go in the **tabular** environment, to be aligned properly in rows and columns, with the desired horizontal and vertical rules. Again, detailed instructions on **tabular** material is found in the *LaTeX User's Guide.*

Immediately following this sentence is the point at which Table 1 is included in the input file; compare the placement of the table here with the table in the printed dvi output of this document.

Table 1: Frequency of Special Characters

Non-English or Math	Frequency	Comments
Ø	1 in 1,000	For Swedish names
π	1 in 5	Common in math
$	4 in 5	Used in business
Ψ_1^2	1 in 40,000	Unexplained usage

Figure 1: A sample black and white graphic (.eps format).

To set a wider table, which takes up the whole width of the page's live area, use the environment **table*** to enclose the table's contents and the table caption. As with a single-column table, this wide table will "float" to a location deemed more desirable. Immediately following this sentence is the point at which Table 2 is included in the input file; again, it is instructive to compare the placement of the table here with the table in the printed dvi output of this document.

7.3 Figures

Like tables, figures cannot be split across pages; the best placement for them is typically the top or the bottom of the page nearest their initial cite. To ensure this proper "floating" placement of figures, use the environment **figure** to enclose the figure and its caption.

This sample document contains examples of **.eps** and **.ps** files to be displayable with LaTeX. More details on each of these is found in the *Author's Guide.*

As was the case with tables, you may want a figure that spans two columns. To do this, and still to ensure proper "floating" placement of tables, use the environment **figure*** to enclose the figure and its caption.

Note that either **.ps** or **.eps** formats are used; use the `\epsfig` or `\psfig` commands as appropriate for the different file types.

7.4 Theorem-like Constructs

Other common constructs that may occur in your article are the forms for logical constructs like theorems, axioms, corollaries and proofs. There are two forms, one produced by

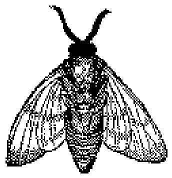

Figure 2: A sample black and white graphic (.eps format) that has been resized with the `epsfig` command.

Table 2: Some Typical Commands

Command	A Number	Comments
`\alignauthor`	100	Author alignment
`\numberofauthors`	200	Author enumeration
`\table`	300	For tables
`\table*`	400	For wider tables

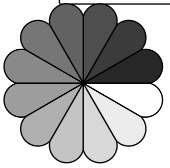

Figure 3: A sample black and white graphic (.ps format) that has been resized with the `psfig` command.

the command `\newtheorem` and the other by the command `\newdef`; perhaps the clearest and easiest way to distinguish them is to compare the two in the output of this sample document:

This uses the **theorem** environment, created by the `\newtheorem` command:

Theorem 1. *Let f be continuous on $[a, b]$. If G is an antiderivative for f on $[a, b]$, then*

$$\int_a^b f(t)dt = G(b) - G(a).$$

The other uses the **definition** environment, created by the `\newdef` command:

Definition 1. If z is irrational, then by e^z we mean the unique number which has logarithm z:

$$\log e^z = z$$

Two lists of constructs that use one of these forms is given in the *Author's Guidelines.*

and don't forget to end the environment with figure*, not figure!

There is one other similar construct environment, which is already set up for you; i.e. you must *not* use a `\newdef` command to create it: the **proof** environment. Here is a example of its use:

Proof. Suppose on the contrary there exists a real number L such that

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = L.$$

Then

$$l = \lim_{x\to c} f(x) = \lim_{x\to c} \left[gx \cdot \frac{f(x)}{g(x)} \right] = \lim_{x\to c} g(x) \cdot \lim_{x\to c} \frac{f(x)}{g(x)} = 0 \cdot L = 0,$$

which contradicts our assumption that $l \neq 0$. □

Complete rules about using these environments and using the two different creation commands are in the *Author's Guide*; please consult it for more detailed instructions. If you need to use another construct, not listed therein, which you want to have the same formatting as the Theorem or the Definition[7] shown above, use the `\newtheorem` or the `\newdef` command, respectively, to create it.

8. CONCLUSIONS

ARP spoofing is not easy to correct. etc...

9. ACKNOWLEDGMENTS

First and foremost, we would like to thank Prof. Hugh Anderson for his guidance and patience with us throughout the semester. While our initial project was to investigate the hacking of Hello Barbie, we eventually decided to change the topic for various reasons, and he very kindly allowed us to do so.

Our thanks also goes out to him for loaning us the Hello Barbie even though we eventually dropped the project.

In addition, our appreciation also goes out to our friends who loaned us various items for our project, such as a DLink Dir-825 router, so that we could work on the project in school.

10. REFERENCES

[1] Bowman.

[2] J. Braams. Babel, a multilingual style-option system for use with latex's standard document styles. *TUGboat*, 12(2):291–301, June 1991.

[3] M. Clark. Post congress tristesse. In *TeX90 Conference Proceedings*, pages 84–89. TeX Users Group, March 1991.

[4] M. Herlihy. A methodology for implementing highly concurrent data objects. *ACM Trans. Program. Lang. Syst.*, 15(5):745–770, November 1993.

[5] L. Lamport. *LaTeX User's Guide and Document Reference Manual.* Addison-Wesley Publishing Company, Reading, Massachusetts, 1986.

[6] V. Ramachandran and S. Nandi. Detecting arp spoofing: An active technique. pages 1–13.

[7] S. Salas and E. Hille. *Calculus: One and Several Variable.* John Wiley and Sons, New York, 1978.

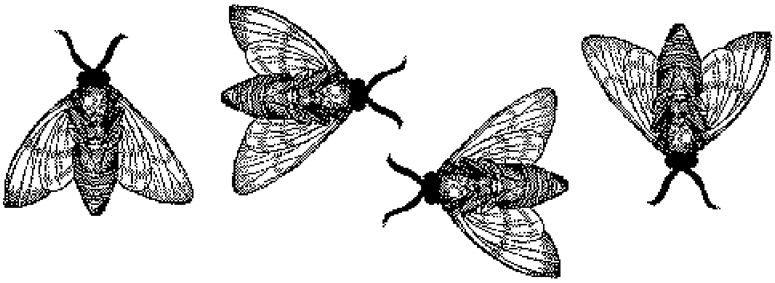

Figure 4: A sample black and white graphic (.eps format) that needs to span two columns of text.