CS 491
Assignment 4: Miscellaneous Exercises in Security and Privacy

Venkat Venkatakrishnan

Introduction

This assignment is a set of small exercises in which you may need to perform some experiments and record your observations. Some questions also involve designing (but not implementing) solutions to a security problem. You will also have to answer some questions related to each exercise.

Logistics

Submission instructions are described in a later section. Any clarifications and revisions to the assignment will be posted on the course Web page.

Use the discussion board on Piazza to discuss the homework.

Hand Out Instructions

> You are welcome to use your account on the machine sponsz.sisl.rites.uic.edu to do this homework.

Exercises

Answer the following questions. Include enough detail in your answers so we can fully understand your design / solution.

1. (Anonymity in document submission) Create a Word as well a PDF document and save them to disk. Imagine that you are required to make an anonymous submission of these two documents to a server. What steps will you take to anonymize the documents? Examine the documents closely and remove any identifying information. Describe how you found any identifying information and how you removed it. (You may want to use a hex editor to inspect the document contents as one way to do this.) In general, if your document contains other media (images, embedded objects etc), describe how these can also contain identifying information.

2. (Cloud computing) Online providers such as DropBox.com provide cloud storage service. Although they claim to encrypt the files, the master keys for unlocking files are available to the cloud providers (you can read their terms of service to see this). So, in theory, there is a chance that they can always obtain access to your file. Could you design (or identify) a solution so that such cloud provider will never be able to access your files? Your solution must share the same features of the cloud provider (e.g. automatic syncing) and must not burden the user in any additional way. There is no need to implement any solution, just discuss the design of your solution.

3. (Firewalls) Read the man page for IP tables at `https://help.ubuntu.com/community/IptablesHowTo`. IP tables is the default firewall software in GNU / Linux distributions such as Ubuntu. Now, describe, using the syntax of IP tables, the firewall rules for the following:

   - allowing FTP traffic.
   - allowing mail traffic.
   - block all telnet traffic.

   In the first two cases above, your rules must allow for (a) external traffic to any servers running FTP or SMTP within your organization that is protected by the firewall and (b) any traffic from clients within your organization above. Explain your rules clearly.

4. Bob is an end-user searching the web using a search engine, from his host `merlin.cs.uic.edu`. The DNS server corresponding to `cs.uic.edu` uses both port randomization and transaction ID checking (TXID checking). Assume that Charlie is an attacker that wishes to poison the cache of the DNS server on `cs.uic.edu`.

   (a) Construct a scenario through which Bob's requests to the search engine are made available to Charlie through DNS Cache poisoning. Explain clearly the steps required for the attack to work without being verbose.

   (b) Assuming that the UDP ports are 32 bits, construct an analysis of the number of DNS records Charlie has to forge in order to successfully poison the cache of the DNS server.

5. (Gmail image inling) By default, inlining of images is turned off in Gmail. That is, when rich text that contains inline images are present in a user's image, the Gmail web application suppresses the display of these images, and instead presents a hyperlink to turn them on. Explain how automatic inlining of images may be a threat. In what circumstances, would automatic inlining could be turned on as a reasonable option? You can experiment with a Gmail account if you wish.

6. (Denial of service) Design a scheme such that a website can distinguish between lack of capacity and denial of service. For example, websites often experience a tremendous increase in the volume of traffic right after an advertisement with the site's URL shown on television during the broadcasting of a popular sporting event. That spike in usage is the result of a normal access that happens to occur at the same time. How can a site determine if the traffic

is reasonable? This is a design question, so list your assumptions, and try to cover many possible scenarios.

Submission Instructions

Your submission will consist of all answers to question above. Submit your work as a PDF document on BlackBoard under the HW4 folder.