School of Computing and Information Technology

CSCI262 System Security
SIM-2015-S4
Tutorial Set C

Part One: Mostly DoS

1. Explain `RBAC.jpg` (taken from Wikipedia) and Figure 1 in `3a_SandhuET1996.pdf`, in the context of Role Based Access Control. In particular, explain what is meant by the constraints and role hierarchies.

2. What is a zombie in the context of denial of service?

3. What is the default size of a ping.

4. Find some examples of typical bandwidth or link capacities by searching on the Internet.

5. The classical DoS flood attack overwhelms the bandwidth of a link, to effectively shut that link down. Consider that we use ICMP pings of size 500 bytes. How many packets do we need to send per second to flood links with the following capacities?

   (a) 0.5–Mbps.

   (b) 2–Mbps.

   (c) 10–Mbps.

6. More problematic than the DoS attack is the distributed DoS attack. Assume each captured system has an upload capacity of 128–kbps. Assuming the same sized pings are used in the previous questions, how many such captured systems would be required to flood links with the following capacities?

   (a) 0.5–Mbps.

   (b) 2–Mbps.

   (c) 10–Mbps.

7. What is a DNS?

8. Describe DNS amplification.

   (a) What implication does it have for the resources required by an attacker?

(b) How is DNS amplification different from general amplification, and how do they relate to reflection attacks?

(c) Amplification, DNS amplification and reflection attacks do not generate backscatter traffic. Explain what backscatter traffic is and why this is the case.

9. `NuCaptcha`: What is it? You should go to the website of the company and have a look at some examples. Look at the article in the lab directory too and see what claims they make.

10. `DeCaptcha`: What is it?

11. In groups of size greater than one, discuss alternative forms of Captcha.

12. Look at `http://www.cloudflare.com/ddos` and out something about the classes of DOS and the mechanism Cloudflare uses to provide protection.

Part Two: Client Puzzles

1. What is the expected cost of calculating a puzzle consisting of m k–bit puzzles, in the Client Puzzle Protocol of Juels and Brainard (1999)?

2. Using the above formula, draw up a table demonstrating the cost for $1 \leq m \leq 20$, $1 \leq k \leq 60$.

3. Assume a uniform distribution of hash values for the hash function used.

   (a) What is the probability of a single guess by an attacker solving the puzzle, as a function of m and k?

   (b) Using the above formula, draw up a table demonstrating the probability for $1 \leq m \leq 20$, $1 \leq k \leq 60$.

   (c) What if the distribution of hash values wasn't uniform? Would it increase or descrease the probabilities determined above?

4. Why use multiple puzzles rather than one single large one?

Part Three: If you have time

1. Explain `RBAC.jpg` (taken from Wikipedia) and Figure 1 in `3a_SandhuET1996.pdf`, in the context of Role Based Access Control. In particular, explain what is meant by the constraints and role hierarchies. You won't have time to read all of `3_SandhuET1996.pdf` in the lab but you can look through it later.

2. Implement two versions of calculating the Fibonacci sequence. They should have demonstratably different levels of performance. Provide some timing evidence regarding the performance.

3. Construct a client puzzle that consists of two sub–puzzles and involves no hashing in the generation of the puzzle.