Student Name: Federico Watkins

CSIS 1800: Introduction to Computer Science and Information Systems

Chapter number: 17 Networks Computer Security

Assignment number: 13

1. Describe the purpose and processing of CAPTCHA software

A CAPTCHA is a way to prevent automated web form submissions. User is shown an image with a confirmation code, and submission is accepted only if the user enters the code correctly.

* Works with any web programming language and framework
* Works on any server and shared hosting account and does not require extensions or special software
* Can be implemented in just a few lines of code and it is easy to integrate with existing apps/websites

To display the captcha image on a website an image tag is created and linked Captchator server as follows:

**<img src="http://captchator.com/captcha/image/$sessionID />**

* Session ID could simply be a part of the PHP session ID or something similar.
* Create or modify an existing form with a text field to send the captcha answer to a script.
* The script check the submitted captcha answer for correctness and then loads the following URL from the Captchator server:

<http://captchator.com/captcha/check_answer/$yoursessionid/$answer>

* If the answer is correct, the result is "1", if not, it is "0".

1. Compare and contrast a computer virus and a computer worm

Both are computer programs that attempt to bypass appropriate authorization and/or perform unauthorized functions

* **Worms** are characterized by their stand-alone nature and usually target network resources
* **Viruses** are characterized by their ability to self-replicate.

1. What is a logic bomb?

A **logical bomb** is a computer program that is set up to execute at system event and attempts to bypass appropriate authorization and/or perform unauthorized functions

1. What are the two ways antivirus software detects malicious code?

Antivirus Software detects and remove malicious code by use of the following:

* **Signature detection** which recognizes known malware and removes them.
* **Heuristics** which are strategies used to identify general patterns of malicious code.

1. Describe a specific scenario that someone launching a phishing attack might use

**Phishing is the act of attempting to** Trick users into revealing security information. Example:

In the email representation below (third paragraph) the user is intimidated into and urged to click on a link that would take them to a suspect server that would collect the user’s information

Stanford University Email Account  
Security info replacement

Someone started a process to replace all of the security info for your Email Account.

If this was you, you can safely ignore this email. Your security info will be replaced with 15623535981 when the 5-day waiting period is up.

If this wasn't you, someone else might be trying to take over your email account. Click here to fill in details and verify your current information in our servers and we'll help you protect this account.

Thanks,  
Barker Ashton

For: Stanford University Email Team  
Phone: 650-723-2300  
Email: alert@stanford.edu

1. What is a denial of service (DoS) attack? Give couple of examples.

A [Denial of Service](http://www.webopedia.com/TERM/D/DoS_attack.html) is a malicious attack on a [network](http://www.webopedia.com/TERM/N/network.html) essentially designed to bring a network to its knees by flooding or crashing it with useless traffic. Many such attacks work by exploiting limitations in the [TCP/IP](http://www.webopedia.com/TERM/T/TCP.html) [protocols](http://www.webopedia.com/TERM/P/protocol.html). The most serious attacks are distributed and in most cases involve forging of IP sender addresses ([IP address spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing)) so that the location of the attacking machines cannot easily be identified, nor can filtering be done based on the source address.

* **(S)SYN flood**
  + Occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address.
  + Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet).
  + Because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server can make, keeping it from responding to legitimate requests until after the attack ends.

### Peer-to-peer attacks

### The most aggressive of these peer-to-peer-DDoS attacks exploits [DC++](https://en.wikipedia.org/wiki/DC%2B%2B).

### With peer-to-peer there is no botnet and the attacker does not have to communicate with the clients it subverts. Instead, the attacker acts as a "puppet master," instructing clients of large [peer-to-peer file sharing](https://en.wikipedia.org/wiki/File_sharing) hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead.

1. How does a transposition cipher work? Is it effective?

**Transposition ciphers** is a cipher that rearranges the order of existing characters in a message in a certain way (e.g., a route cipher)

* Write the letters in a row of five, using '+' as a blank. Encrypt by starting spiraling inward from the top left moving counter clockwise
* Decrypt by recreating the grid and reading the letters across the row
* The key are the **dimensions** of the grid and the **route** used to encrypt the data

Encrypt: “CRAZY IN BRAZIL” 🡪 C+RAZILBYZARIN+

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | R | A | Z | Y |  |  |  |  |  |  |  |  |
| + | I | N | + | B |  |  |  |  |  |  |  |  |
| R | A | Z | I | L |  |  |  |  |  |  |  |  |

**Cryptanalysis** is the process of decrypting a message without knowing the cipher or the key used to encrypt it. Substitution and transposition ciphers are easy for modern computers to break hence they are **ineffective** in the modern world.

1. What are some of the reasons a person makes mistakes when it comes to keeping their online information secure?

* The Internet creates a false sense of anonymity
* People make assumptions about how securely their information is being treated
* People don’t think about the ramifications of sharing information

1. A Caesar cipher that shifts characters 4 positions to the right would encode the word LADDER as which of the following?
2. ERLADD ☺ Correct option missing from Assignment-Set.
3. DDALRE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Alphabet shift = 4

LADDER = PEHHIV

1. Provide a brief description of each encryption, first; then determine to which category of encryption belongs a route cipher?
   1. Caesar cipher

|  |
| --- |
| A substitution cipher that shifts characters a certain number of positions in the alphabet |

* 1. Public-key encryption

|  |
| --- |
| An approach in which each user has two related keys, one public and one private. A person encrypts an outgoing message, using the receiver's public key. Only the receiver's private key can decrypt the message |

* 1. Transposition cipher

|  |
| --- |
| A cipher that rearranges the order of existing characters in a message in a certain way |

* 1. Electronic signature

|  |
| --- |
| Data that is appended to a message, made from the message itself and the sender's private key, to ensure the authenticity of the message |

|  |
| --- |
| The Route Cipher is a **transposition cipher** where the key is which route to follow when reading the cipher-text from the block created with the plaintext. The plaintext is written in a grid, and then read off following the route chosen |

Reference:

1. Dr. Szabo Tutorials: ch17\_Computer\_Security(1).ppt.
2. <https://itservices.stanford.edu/phishing>
3. <https://en.wikipedia.org/wiki/Denial-of-service_attack>
4. https://en.wikipedia.org/wiki/Electronic\_signature
5. <http://www.webopedia.com/DidYouKnow/Internet/DoS_attack.asp>
6. http://crypto.interactive-maths.com/route-cipher.html