Topic 2 Activity Guide

Ryan Coon

CST-407

Professor Ty Howard

December 17, 2023

Part 1: Authentication and Encryption

Identity and Authentication

1.What is the difference between the terms identify and authenticate?

Identification is the act of identifying a particular user through username or email. Authentication is the proof of the users identity commonly managed with a password.

2.In what situations should each of these be used or not used?

Authentication Methods

Name three types of authentication other than a password. Explain the advantages and disadvantages of each.

1. Multi-Factor authentication -advantages are that MFA enhances security, reduces risk of fraud and improve user accountability. Disadvantages are increased complexity causing user frustration, cost for implementation and maintenance and MFA is not foolproof.

2. SSO – Advantages of SSO is that it reduces the load of memorizing passwords and its easy to implement and connect to new data sources. Disadvantages are that when SSO fails access to related systems is lost and there is an increased risk of identity spoofing and phishing in user-external accesses.

3.Token Authentication – Advantages of Token authentication would be that it is more scalable and efficient, robust security, and the flexibility and performance. Disadvantages would be compromised secret key, data overhead, and shorter lifespan.

Caesar Encryption

1.Give at least two examples of a type of encryption that is in the Caesar model.

Reverse Caesar Cypher and the Vigenère Cipher

2.Explain the process of deciphering a Caesar shift.

Firstly you would need the shift key. For instance if the key is 3, you would simply shift the letters back by 3 places. Hello encrypted with a shift of 3 is Khoor. When you take each letter and move it back 3 spaces you get back to the decrypted hello.

AES and DES. Two Modern Encryption Standards

1.How are AES and DES both different than the Caesar encryption model?

2.Explain the differences between AES and DES, and why one is superior to the other.

With DES the block is slit into halves before being processed, but in AES the entirety of the block is processed to get cyphertext. DES has a key size of 56 bits whereas AES has a size of 128, 192, or 256. AES is comparatively faster than DES. DES uses the Feistel Cipher principle and AES uses the substitution and permutation principle.

3.Explain how the XOR operator works and how it relates to encryption algorithms.

XOR is called modulus 2 addition. The output is true when the inputs are different. XOR basically means either one not both or none.

4.The AES algorithm uses as block cypher. What alternatives are there to block cypher? What are the advantages and disadvantages of a block cypher?

Alternatives to block cypher are Blowfish, TwoFish, Serpent, Threefish, Camellia, and RC6.

Advantages of block cypher are they have immunity to tampering and are high diffusion. Disadvantages are encryption is slow and error propagation is bad.(one error may corrupt the entire block)

Symmetric vs Asymmetric Encryption

1.Explain the differences between symmetric and asymmetric encryption.

The main difference between the two are speed and security preferences. Symmetric is fater due to shorter key lengths whereas asymmetric bogs down networks due to it longer key lengths.

2.What are the advantages and disadvantages of each method?

Symmetric advantages are security as it uses AES algorithm that can take billions of years to crack, speed due to shorter key lengths, and industry adaption and acceptance as it uses the AES algorithm which is considered the gold standard. Symmetric disadvantages are that it uses a single secret cryptographic key to encrypt and decrypt. As it uses one key, if two locations are encrypting and decrypting simultaneously, the key would need to be transmitted leaving it vulnerable to interception.

Advantages of asymmetric are that key distribution is not necessary, private key exchange not necessary, and a digital signature/message authentication is used. Disadvantages are that it is slow because of the longer key lengths and there are security risks.

Private Key vs Public Key

1.Explain the difference between a public and private key.

A public key is truly public and can be shared, private key should only be known by the author.

2.Research “RSA Algorithm Step by Step Example.” How do prime numbers relate to the RSA algorithm used in creating a public and private key?

It is said that prime numbers keep encrypted messages safe. When you multiply two together you get a number that can be only broken down into those primes.

3.Explain how quantum computing relates to cryptography.

As most of todays cryptography is related to mathematical algorithms, attacks on these encryption methods that would normally take years could theoretically take days with quantum computers.

Hashing vs. Encryption

1.Explain the purpose of a hashing algorithm. Explain how it is different than encryption.

Hashing algorithms are used to authenticate data. It is used as sort of a seal of approval.

They differ because encryption is a two way function where information is scrambled to be unscrambled later. Hashing is a one way function where data is mapped to a fixed length value.

2.Explain how a computer system can use hashing to ensure passwords are private.

When a user creates a password, the computer system hashes the password and stores the hash value, not the actual password.

3.Explain how hackers use a rainbow table and how you can defeat them.

Hackers use a rainbow table to cracked hashed passwords by using a database. This can be defeated by using salting techniques. This means it randomizes the data before it is passed onto the hashing stage.

4.Explain the impact that hashing and encryption have had in relation to historical, social, professional, ethical, and legal aspects of computing. To support your statement, provide at least one historical example of how encryption relates to ethics in computing.

Hashing can be seen that it creates a unique fingerprint for your data making sure it isn’t tampered with. Encryption scrambles your data to make it unreadable without the key.

Through history encryption helped win WWII. Encryption was used by both sides and the most famous one used was called the enigma machine.

Part 2: Gnu PGP Tutorial

A screenshot of a computer

Description automatically generated

Here you see the screenshot of the encrypted message using symmetric encryption.

A screenshot of a computer

Description automatically generated

Here is the message encrypted using the armor option to show only ASCII.

A screenshot of a computer program

Description automatically generated

Here is the message.txt.asc decrypted as shown in the terminal.

A screenshot of a computer

Description automatically generated

Here is the message.txt.gpg decrypted as shown in the terminal.

A screenshot of a computer

Description automatically generated

This shows that it created the decrypted messages as text files.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Here are both messages decrypted into their own text files.

A screenshot of a computer

Description automatically generated

Both file hashes match one another.

A screenshot of a computer screen

Description automatically generated

Here we generated a public key file.

A screenshot of a computer

Description automatically generated

Here is the public key submitted into the website.

I had no friends to send a message to at this point in time.

Part 3:

A screen shot of a computer

Description automatically generated

Here is the initial website with the username and password shown in the address bar. This is unsecure as described.

A screenshot of a computer

Description automatically generated

Here is an attempted login with bad credentials.

A screen shot of a computer

Description automatically generated

Here is a successful login using admin credentials.

A screenshot of a computer

Description automatically generated

Here is the http packet stream while attempting a successful login.

A screenshot of a computer

Description automatically generated

This is the view when you select to follow the stream of one of the GET forms.

A screen shot of a computer

Description automatically generated

Here is the view when we filter for only http POST requests.

A screenshot of a computer

Description automatically generated

Here you can see the username and password entered when following the process\_login post stream.

**Table 1. Table of Common Internet Communication Protocols**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Protocol Initials** | **Full Name** | **Purpose** | **Type of Application Likely to Utilize the Protocol** | **Security Vulnerability to Wireshark** |
| **SMTP** | Simple Mail Transfer Protocol | Used by mail servers to send, receive, and relay outgoing email between senders and receivers. | AmazonSES SendGrid Mailgun Postmark Google | Denial of service |
| **IMAP** | Internet Message Access Protocol | An internet standard protocol used by email clients to retrieve email messages from a mail server. | Microsoft Outlook Windows Mail  Apple Mail  Mozilla Thunderbird | IMAP Dissector could crash triggered by packet injection |
| **DNS** | Domain Name Service | Turns domain names into ip addresses | Primary Website  Marketing campaign websites  Email servers  Customer support websites | Wireshark is not validated |
| **SSH** | Secure Shell Protocol | Cryptographic network protocol for operating network services securely over an unsecured network. | Putty  SolarPutty  Putty tray  MRemoteNG  MobaXterm | Vulnerable to Denial of service error |
| **POP** | Post Office Protocol | Application-layer internet standard protocol used by e-mail clients to retrieve e-mail from a mail server. | Gmail | Can allow attacker to send a malicious packet file that can result in DoS |
| **FTP** | File Transfer Protocol | A way to download, upload, and transfer files from one location to another on the internet and between computer systems. | Cyberduck  FileZilla  WinSCP  SmartFTP | It’s a plaintext protocol that can allow anonymous authentication |
| **TELNET** | Teletype Network | Provides a command line interface for communication with a remote device or server. | Absolute Telnet  RUMBA  Line Mode Browser  TeraTerm | Open as there are no encryption mechanisms |

**References:**

“Cryptography: What Are the Advantages and Disadvantages of Block Ciphers over Stream Ciphers? - Quora.” Www.quora.com, www.quora.com/Cryptography-What-are-the-advantages-and-disadvantages-of-block-ciphers-over-stream-ciphers.

Daniel, Brett. “Symmetric vs. Asymmetric Encryption: What’s the Difference?” Www.trentonsystems.com, 4 May 2021, www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption.

“Difference between DES (Data Encryption Standard) and AES (Advanced Encryption Standard) - Javatpoint.” Www.javatpoint.com, www.javatpoint.com/des-vs-aes#:~:text=The%20main%20difference%20between%20DES.

“Explore the Impact of Quantum Computing on Cryptography | TechTarget.” Data Center, www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography#:~:text=Much%20of%20today.

Frąckiewicz, Marcin. “The Pros and Cons of Implementing Multifactor Authentication.” TS2 SPACE, 18 June 2023, ts2.space/en/the-pros-and-cons-of-implementing-multifactor-authentication/#gsc.tab=0.

GeeksforGeeks. “Caesar Cipher in Cryptography - GeeksforGeeks.” GeeksforGeeks, 2 June 2016, www.geeksforgeeks.org/caesar-cipher-in-cryptography/.

---. “Difference between Private Key and Public Key - GeeksforGeeks.” GeeksforGeeks, 13 May 2019, www.geeksforgeeks.org/difference-between-private-key-and-public-key/.

“Identification vs. Authentication: What’s the Difference?” Blog.hypr.com, blog.hypr.com/identification-vs-authentication. Accessed 17 Dec. 2023.

Nohe, Patrick. “The Difference between Encryption, Hashing and Salting.” Hashed out by the SSL StoreTM, 19 Dec. 2018, www.thesslstore.com/blog/difference-encryption-hashing-salting/#:~:text=Encryption%20is%20a%20two%2Dway%20function%20where%20information%20is%20scrambled.

“Pros and Cons of Using Token-Based Authentication | LoginRadius Blog.” Www.loginradius.com, www.loginradius.com/blog/identity/pros-cons-token-authentication/.

Smith, Belinda. “This Is How Prime Numbers Keep Your Online Shopping Secure.” ABC News, 19 Jan. 2018, www.abc.net.au/news/science/2018-01-20/how-prime-numbers-rsa-encryption-works/9338876.

“What Is Single Sign on (SSO)? Characteristics and Advantages.” Chakray, 30 May 2017, www.chakray.com/what-is-single-sign-on-sso-definition-characteristics-and-advantages/.

“What Is the Best Alternative to Advanced Encryption Standard (AES) for Symmetric Key Cryptography?” Quora, www.quora.com/What-is-the-best-alternative-to-Advanced-Encryption-Standard-AES-for-symmetric-key-cryptography. Accessed 17 Dec. 2023.