2023

Class #5 – Domain 3

Christophe Foulon

Christophe Foulon - CPF Coaching, Founder & Coach

CISSP® MENTOR PROGRAM – SESSION SIX

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- Do not copy or share copy of copyrighted materials.

DAD JOKE TIME

CISSP® MENTOR PROGRAM – SESSION SIX

WHO I AM?

I love Baby Yoda

Outside of being a security practitioner focused on helping businesses tackle their cybersecurity risks while minimizing friction resulting in increased resiliency and helping to secure people and processes with a solid understanding of the technology involved.

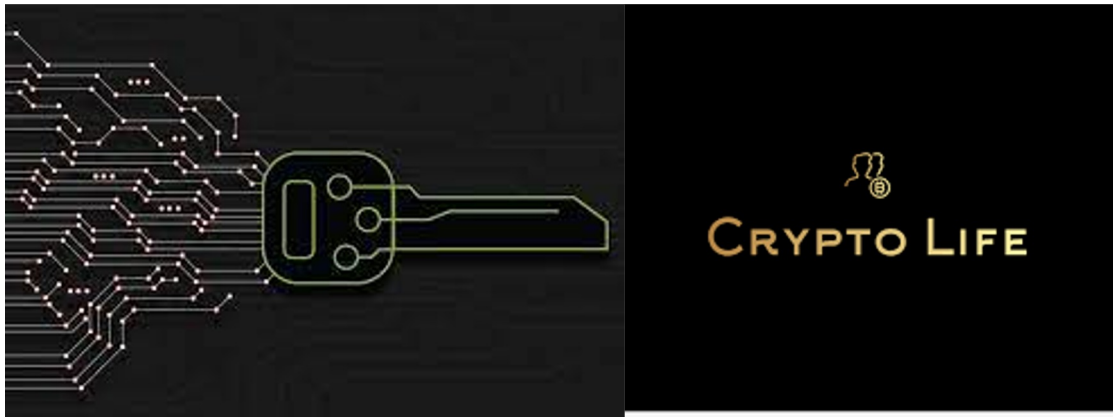
I am a dad, dog dad and career coach. I love helping other to achieve their best. Through this channel, I help veterans with their transitions and others via non-profits like Whole Cyber Human Initiative, Boots2Books and others.

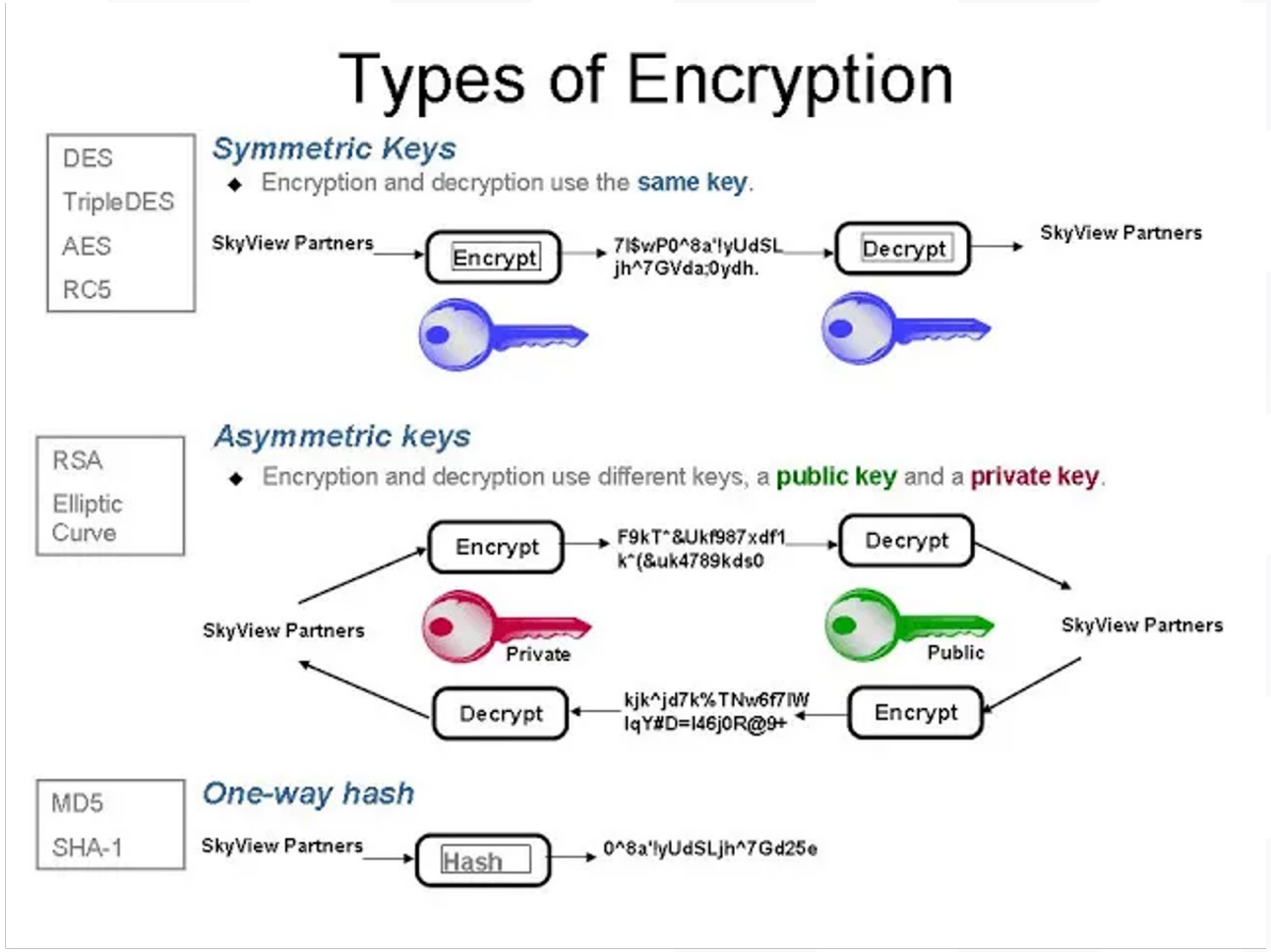
I give back by producing a podcast focused on helping people who are "Breaking into Cybersecurity" by sharing the stories of those who have done it in the past 5 years to inspire those looking to do it now.

Co-authored:
"Develop Your Cybersecurity Career Path: How to Break into Cybersecurity at Any Level"
"Hack the Cybersecurity Interview: A complete interview preparation guide for jumpstarting your cybersecurity career"
And advised on "Understand, Manage, and Measure Cyber Risk"

LET'S DO THIS!

Picking up where we left off.





DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

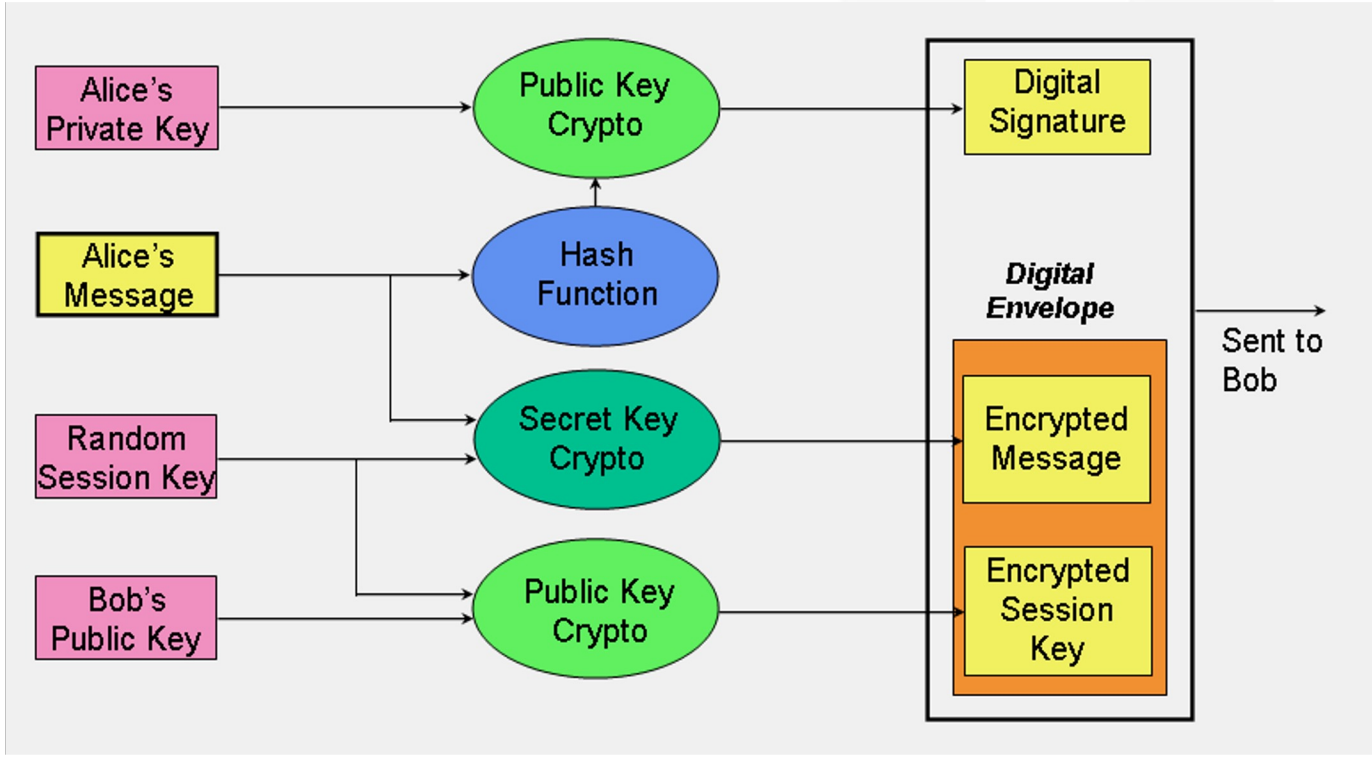
Cryptographic Methods

USE CASE	TYPE OF CRYPTOGRAPHY
Protect confidentiality of stored data	Symmetric
Protect confidentiality of data in transit	Symmetric (possibly aided by asymmetric)
Verify identity	Public key infrastructure
Protect integrity (detect tampering)	Hashing (e.g., Message Authentication Code)
Protect passwords	Hashing (with salt and pepper)
Nonrepudiation	Digital signature

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

- Uses **one key** to encrypt and decrypt
- Also called "**Secret key**" encryption
- Strengths include **speed** and cryptographic **strength** per bit of key
- Major weakness is that the **key must be securely shared** before two parties may communicate securely
- Keys are often shared via an out-of-band method

Stream and Block Ciphers

- Stream mode means each bit is independently encrypted in a "stream."
- Block mode ciphers encrypt blocks of data each round:
- 56 bits for the Data Encryption Standard (DES)
- 128, 192, or 256 bits for AES
- Some block ciphers can emulate stream ciphers by setting the block size to 1 bit; they are still considered block ciphers.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

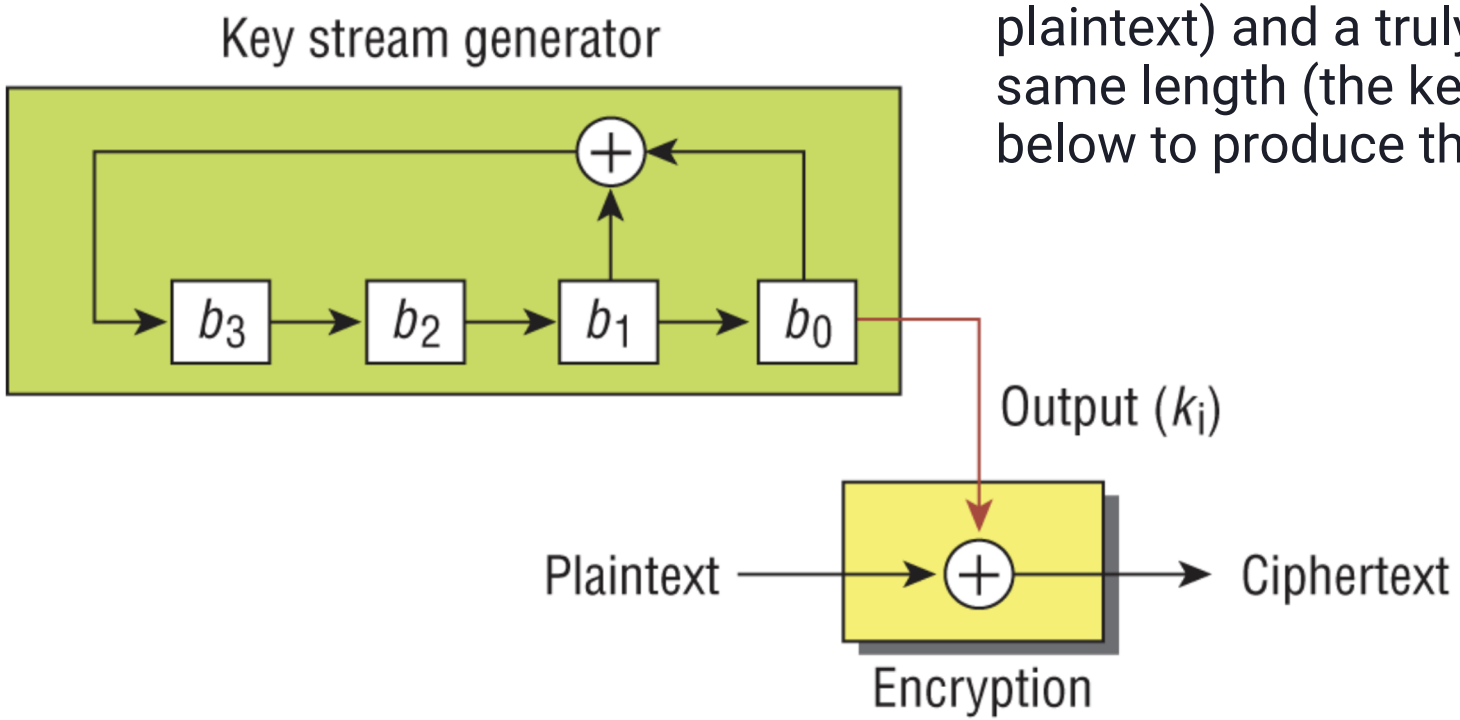
Select and Determine Cryptographic Solutions

Cryptographic Methods

Symmetric Encryption

Stream Ciphers

An example of a simple and provably unbreakable stream cipher is to take a message of length n (the plaintext) and a truly random string of digits of the same length (the key) and combine them as shown in below to produce the ciphertext.



A stream cipher is an encryption algorithm that works one character or bit at a time (instead of a block)

An Exclusive OR (XOR) function is a binary operation applied to two input bits. If the two inputs are equal to one another, the result is zero. If the two bits are different, the result is 1.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

Quiz time -

What is this?

What is it important?

What is its weakness?

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

Quiz time -
What is this?
One Time Pad

What is it important?
Stream Cipher on paper used to encode message

What is its weakness?
If you reuse it, threat actors can use pattern commonality to find cipher

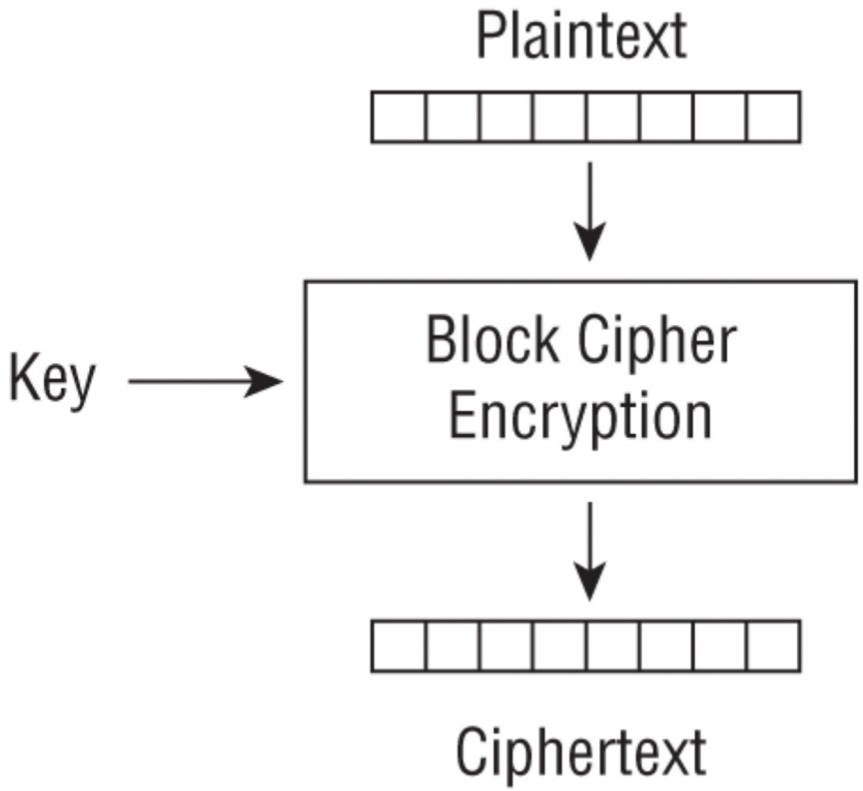
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods

Symmetric Encryption - Block Ciphers

Block ciphers use a deterministic algorithm that takes a fixed-sized block of bits (the plaintext) and a key value, and produces an encrypted block (the ciphertext) of the same size as the plaintext block. *Different key values will produce different ciphertexts from the same plaintext.*



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption - Block Ciphers

BLOCK CIPHER	BLOCK SIZE (*N*)	KEY SIZE (*K*)	ROUNDS
DES	64	56	16
AES-128	128	128	10
AES-192	128	192	12
AES-256	128	256	14

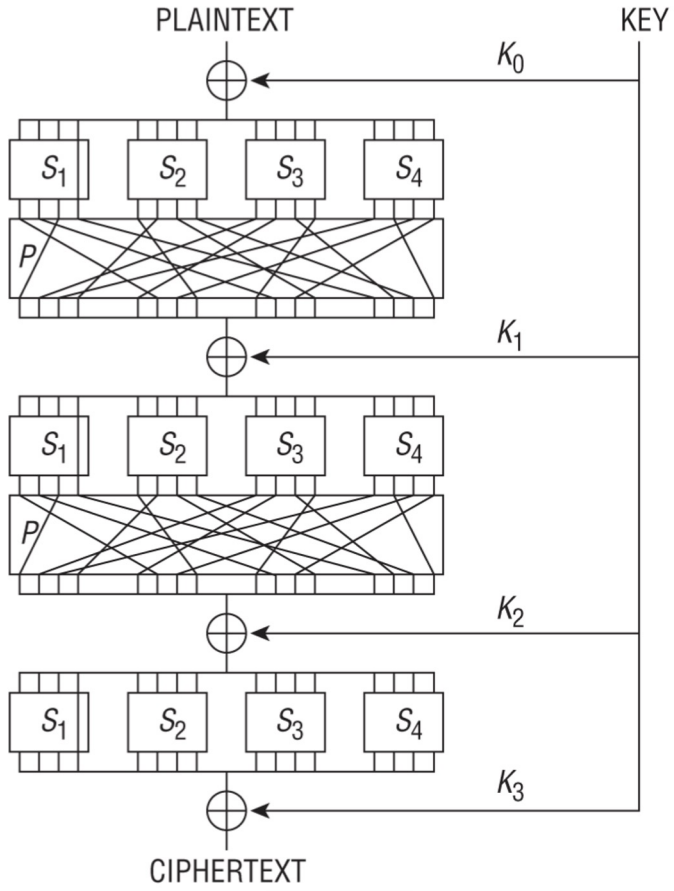
The **DES cipher is no longer considered secure** because of its short keysize
AES was selected as the replacement for DES
Triple DES (3DES) is an important evolution of DES

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption - Block Ciphers

Most block ciphers, including **DES and AES**, are built from **multiple rounds of mathematical functions**. While *more rounds mean greater security*, it also slows down the algorithmic process, so the choice is a **trade-off between security and speed**.



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

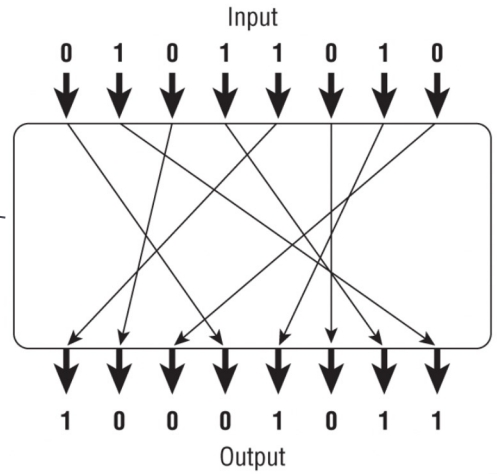
Cryptographic Methods - Symmetric Encryption - Bloc

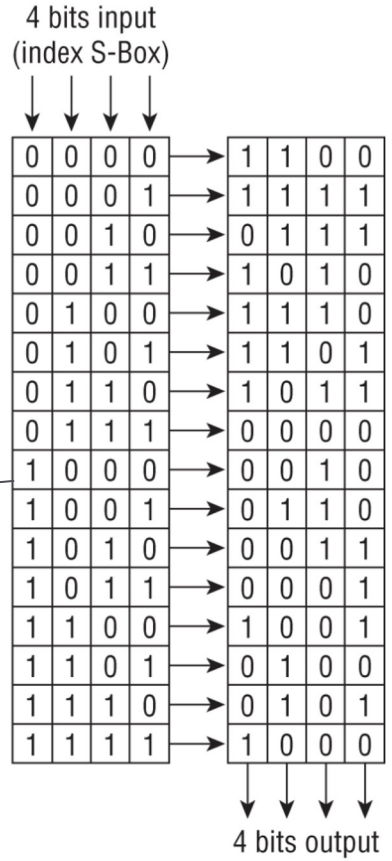
The differences between different block ciphers are in the transformations performed during each round, and the manner in which the encryption key is stretched and then divided to provide a unique key for each round.

There are a couple of standard building blocks used to construct block ciphers:

Substitution or S-boxes

Permutations or P-boxes

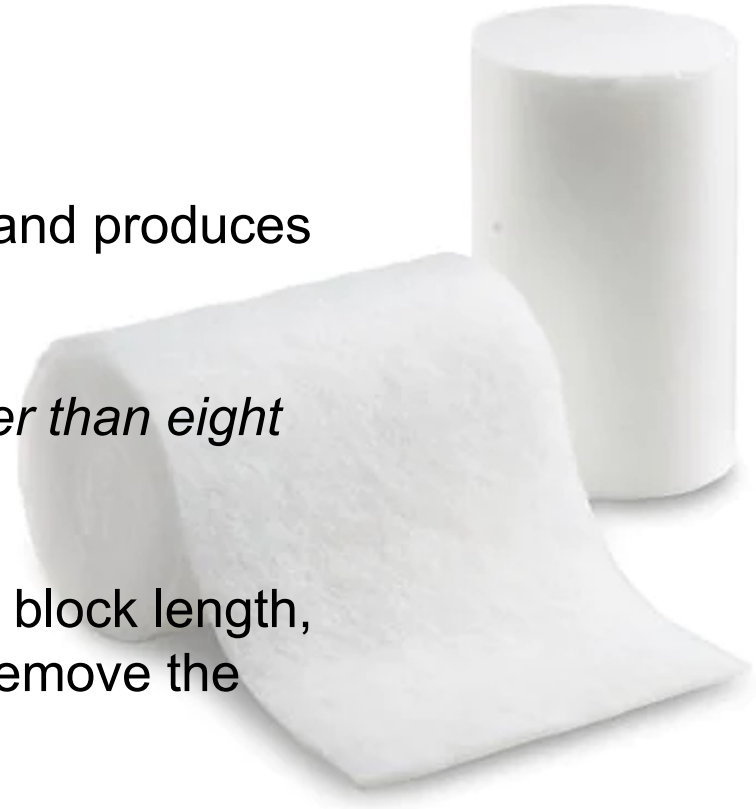




DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption – Block Ciphers



Block Cipher Modes of Operation

A block cipher such as AES takes eight bytes of plaintext and produces eight bytes of ciphertext.

But what if your message is shorter than eight bytes, longer than eight bytes, or not a multiple of eight bytes?

To handle messages that are not a multiple of the cipher's block length, one mechanism is to add padding before encryption and remove the padding after encryption.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

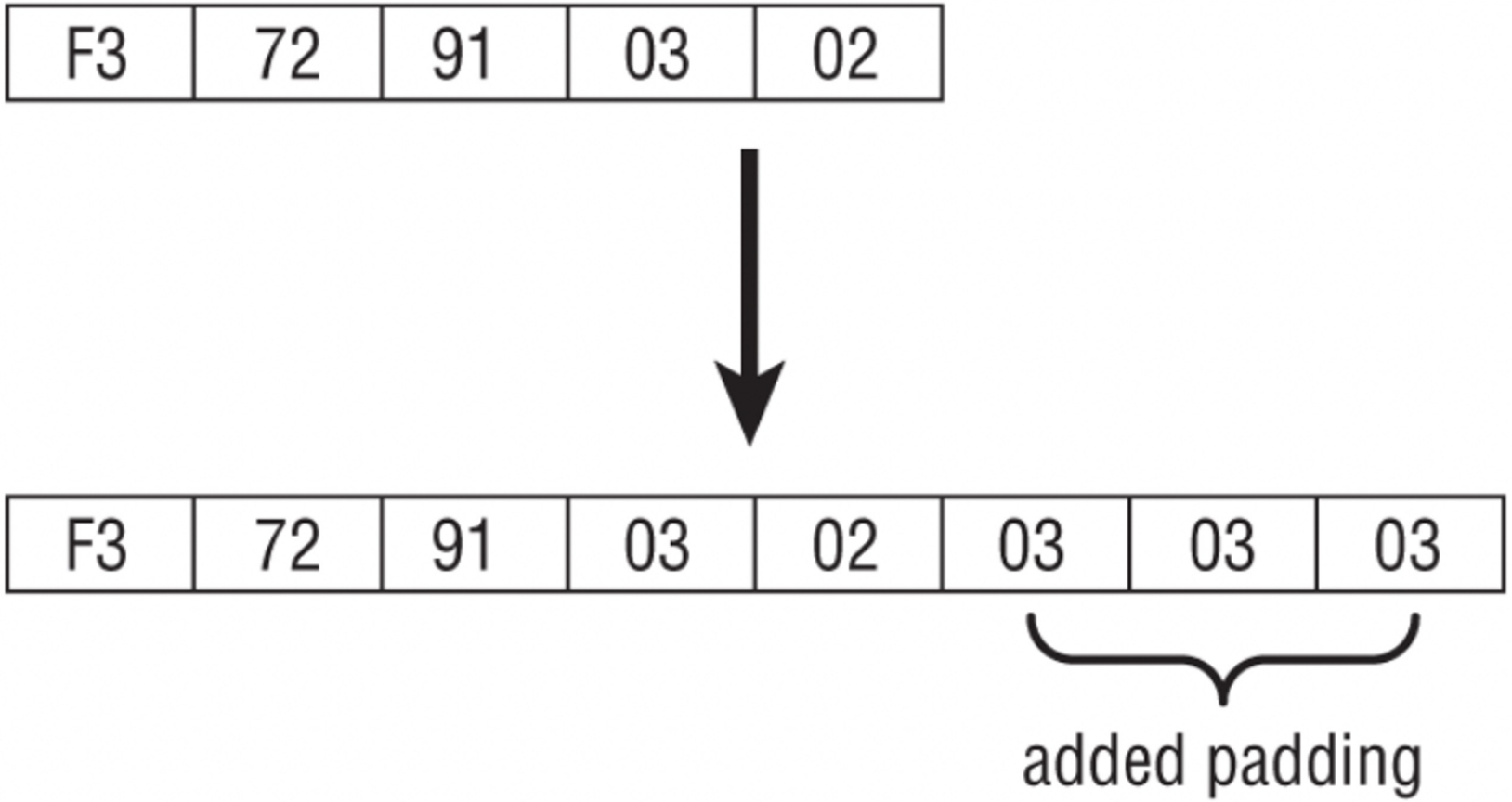
Select and Determine Cryptographic Solutions

Cryptog – Block C

Block Cipher
A block cipher
eight bytes of

But what if you
bytes, or not a

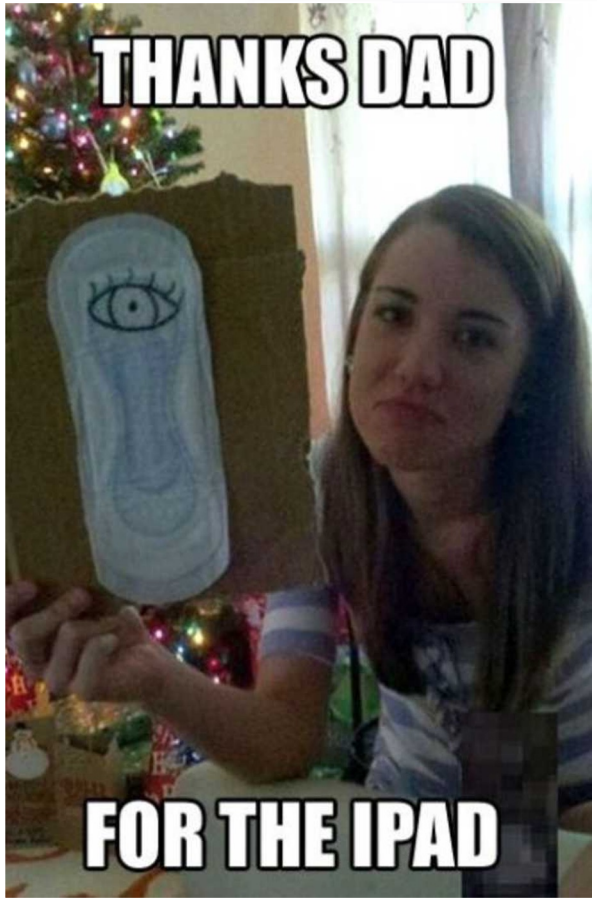
To handle mes
one mechanisr
padding after e



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

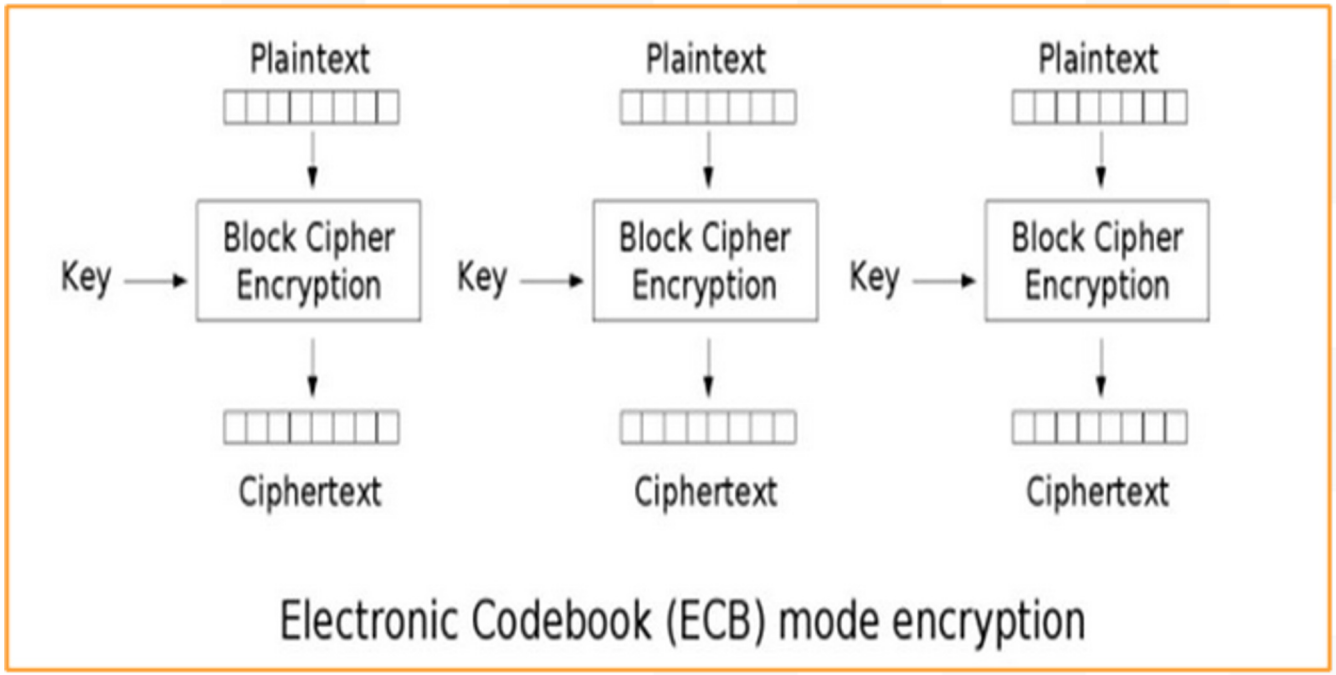
Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

Data Encryption Standard (DES) - Electronic Code Book (ECB)

- The simplest and **weakest** form of DES
- No initialization vector or chaining
- *Identical plaintexts with identical keys encrypt to identical ciphertexts*

As a trivial example, if one were to use ECB to encrypt the birthdate field, then one could easily determine all the people in the database born on the same day, and if one could determine the birthdate of one of those individuals, you would know the birthdate of all (with the same encrypted birthdate).



Electronic Codebook (ECB) mode encryption

DOMAIN 3: SECURITY ARCHIT

Select and Determine Cryptographic Solutions

Cryptographic Methods - Sym

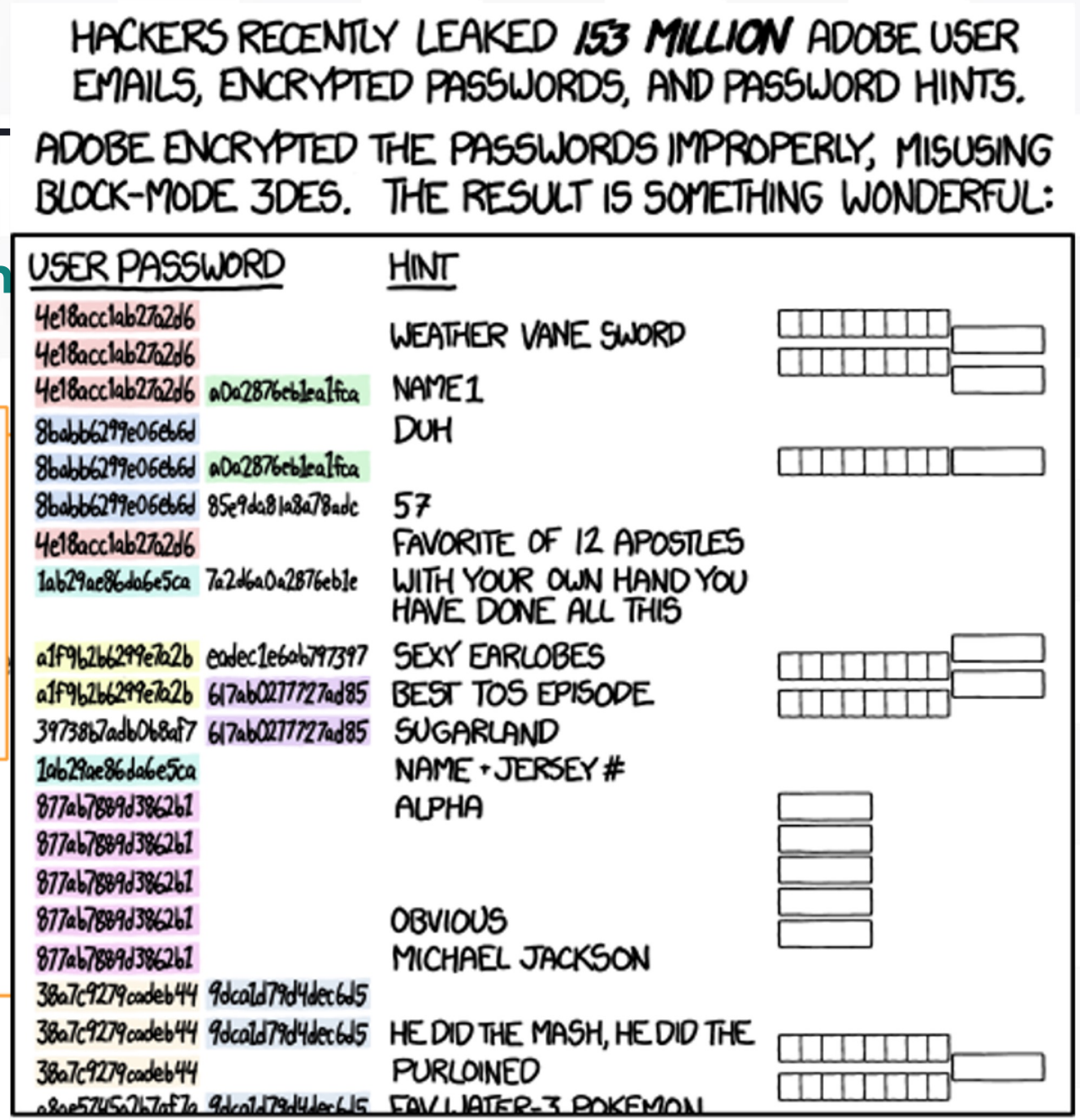
Data Encryption Standard (DES) -

Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder

04 NOV 2013 65

Adobe, Cryptography, Data loss, Privacy

As a trivial example, if one were to use ECB to encrypt the birthdate field, then one could easily determine all the people in the database born on the same day, and if one could determine the birthdate of one of those individuals, you would know the birthdate of all (with the same encrypted birthdate).



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

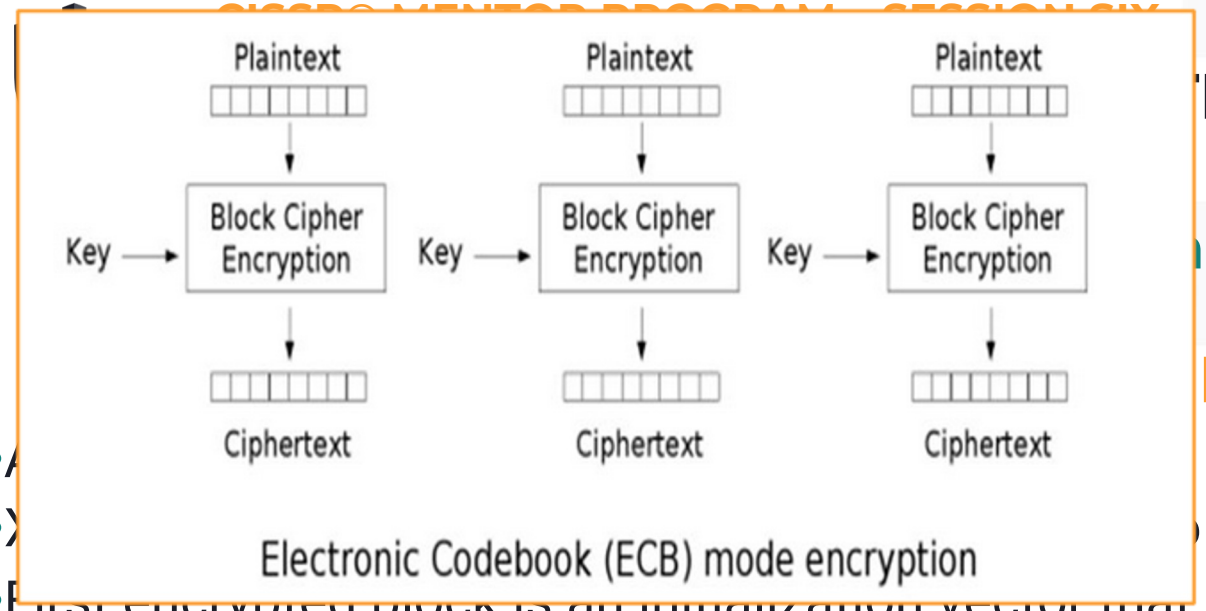
Data Encryption Standard (DES) - Cipher Block Chaining (CBC)

- A block mode of DES
- XORs the previous encrypted block of ciphertext to the next block of plaintext to be encrypted
- First encrypted block is an initialization vector that contains random data
- The “chaining” destroys patterns
- One limitation of CBC mode is that encryption **errors will propagate**: *an encryption error in one block will cascade through subsequent blocks due to the chaining, destroying their integrity.*

ECTURE AND ENGINEERING

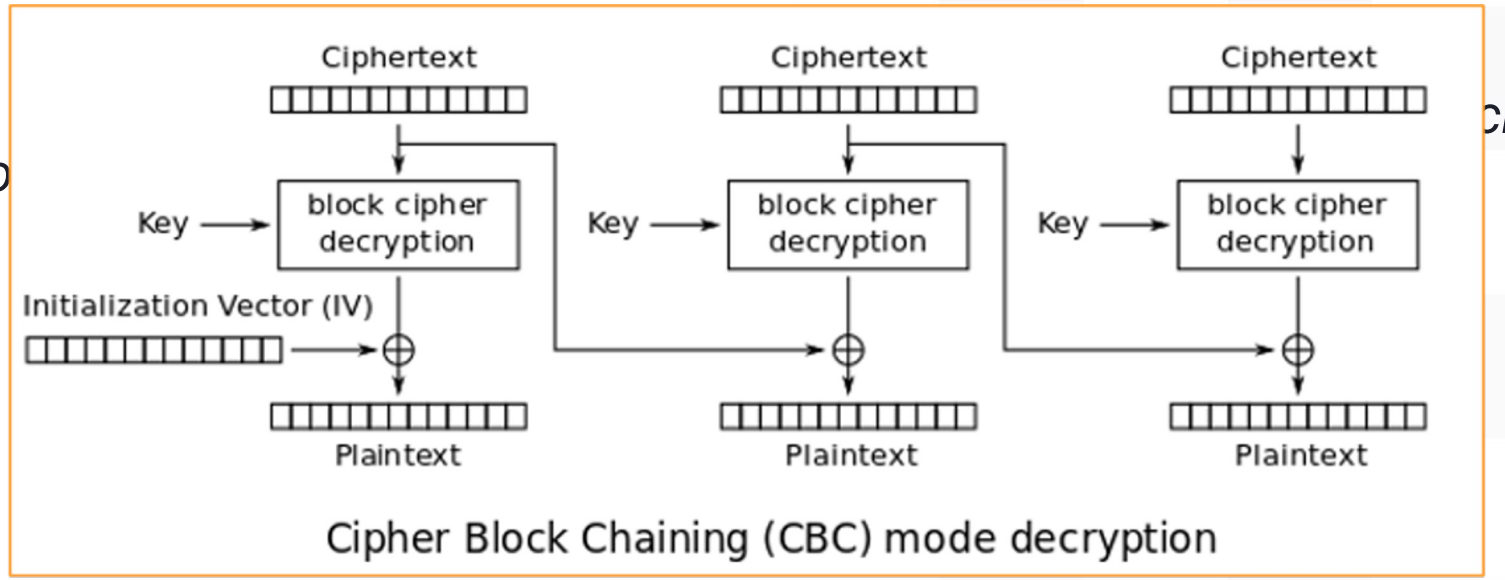
metric Encryption

Block Chaining (CBC)



Electronic Codebook (ECB) mode encryption

- A
- X the next block of plaintext to be encrypted
- First encrypted block is an initialization vector that contains random data
- The “chaining” destroys patterns
- One limitation of CBC mode is that ck *will cascade through subsequent blo*



Cipher Block Chaining (CBC) mode decryption

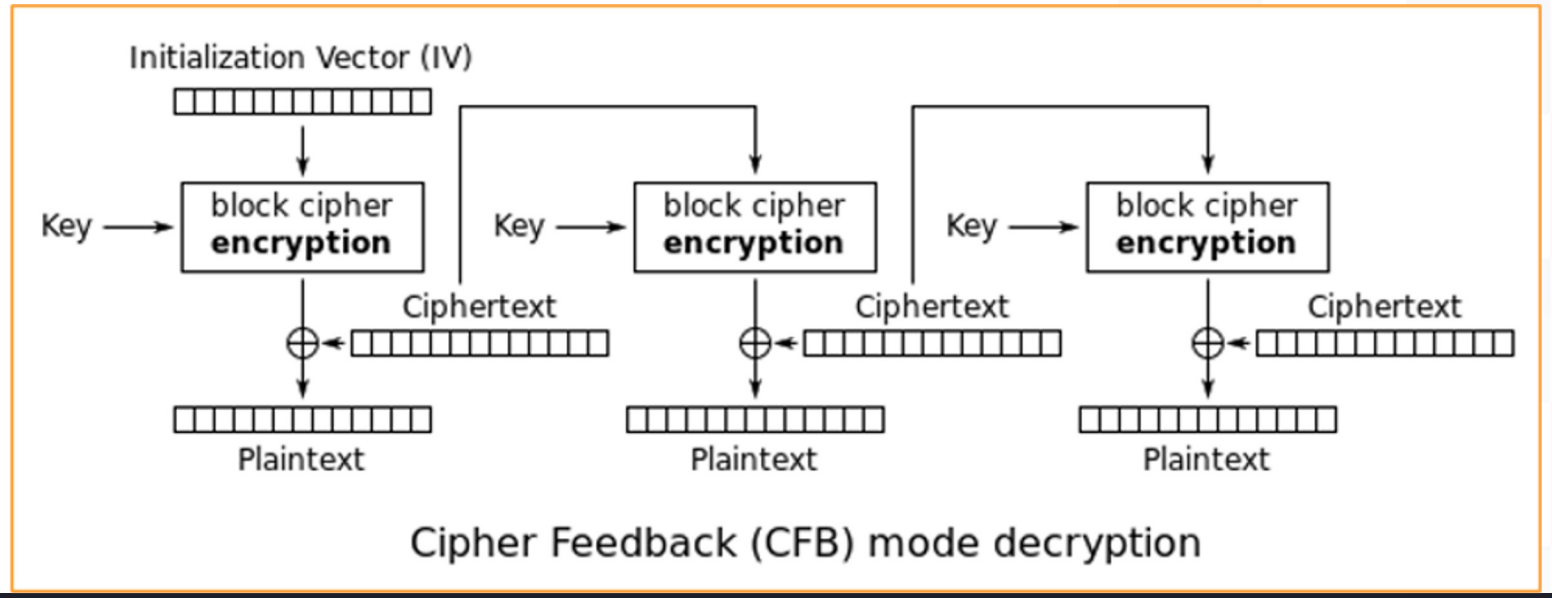
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

Data Encryption Standard (DES) - Cipher Feedback (CFB)

- Very similar to CBC; the primary difference is CFB is a stream mode
- Uses feedback (the name for chaining when used in stream modes) to destroy patterns
- Like CBC, CFB uses an initialization vector and destroys patterns, and **errors propagate**



Cipher Feedback (CFB) mode decryption

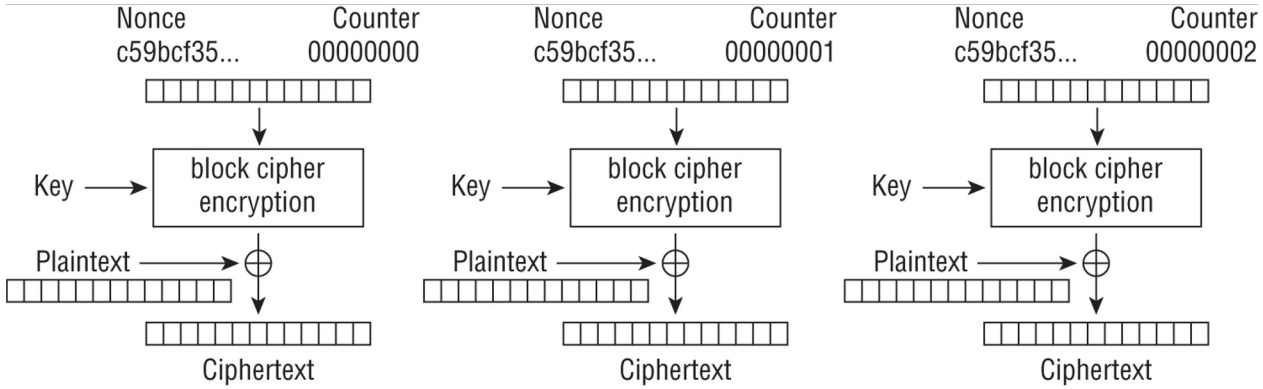
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

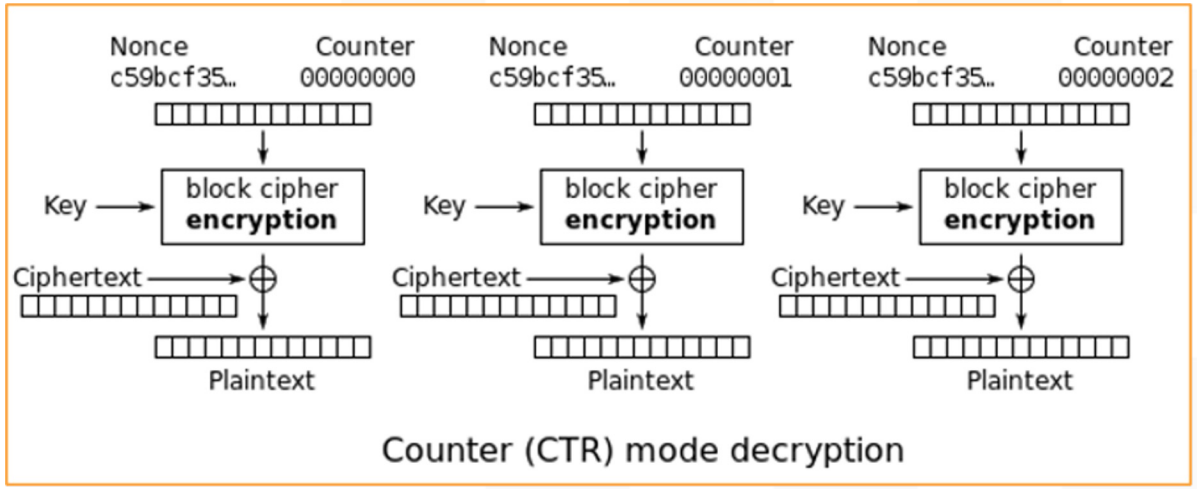
Cryptographic Methods - Symmetric Encryption

Data Encryption Standard (DES) - Counter (CTR)

- Like OFB; the difference again is the feedback: CTRmode uses a counter
- Shares the same advantages as OFB (patterns are destroyed and errors do not propagate) with an additional advantage: since the feedback can be as simple as an ascending number, CTR mode encryption can be done in parallel



Counter (CTR) mode encryption



Counter (CTR) mode decryption

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

The following are the main differences between CBC and CFB:

- With CBC, a one-bit change in the IV will result in the same change in the same bit in the first block of decrypted ciphertext.
  - Depending on the application, this could permit an attacker who can tamper with the IV to introduce changes to the first block of the message.
  - This means with CBC it is necessary to ensure the integrity of the IV.
- With CFB, a one-bit change in the IV will result in random errors in the decrypted message;
  - thus, this is not a method of effectively tampering with the message.
- With CBC, the decryption of messages requires the use of the block cipher in decryption mode.
  - With CFB, the block cipher is used in the encryption mode for both encryption and decryption, which can result in a simpler implementation.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

Data Encryption Standard (DES) – Triple DES encryption order and keying options

- Applies DES encryption three times per block
- FIPS 46-3 describes "Encrypt, Decrypt, Encrypt" (EDE) order using three keying options: one, two, or three unique keys (called 1TDES EDE, 2TDES EDE, and 3TDES EDE, respectively)
- Applying triple DES EDE with the same key each time results in the same ciphertext as single DES
- 2TDES EDE uses key 1 to encrypt, key 2 to "decrypt," and key 1 to encrypt. This results in 112 bits of key length. It is commonly used for legacy hardware applications with limited memory
- 3TDES EDE (three different keys) is the strongest form, with 168 bits of key length
- Two- and three-key TDES EDE remain a FIPS-approved standard until 2030 (sort of)

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

Advanced Encryption Standard (AES)

- Current United States standard symmetric block cipher
- Federal Information Processing Standard (FIPS) 197 (see: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)
- Uses 128-bit (with 10 rounds of encryption), 192-bit (12 rounds of encryption), or 256-bit (14 rounds of encryption) keys to encrypt 128-bit blocks of data
- Open algorithm, free to use, and free of any intellectual property restrictions Designed to replace DES

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Symmetric Encryption

Rivest Ciphers

Dr. Ron Rivest (the "R" in the RSA algorithm discussed in the next section) developed a number of symmetric-key algorithms, collectively known as the Rivest ciphers. These algorithms are annotated RCn, and you should be familiar with these four:

- **RC2** is a block cipher that uses a 64-bit block size and a variable-length key. *RC2 is vulnerable to chosen-plaintext attacks and should not be used.*
- **RC4** is a stream cipher used in internet protocols such as TLS and SSH, with variable length, ranging from 40 to 2048 bits. *RC4 is not considered secure and should not be used, although it still is in many places.*
- **RC5** is similar to the RC2 block cipher, but with a variable block size (32, 64, or 128 bits) and variable key size (0 to 2040 bits). **RC5 is considered secure with sufficient rounds of encryption.**
- **RC6** is a derivative of RC5 that uses a 128-bit block size and variable length keys (128, 192, or 256 bits). **RC6 is an improvement upon RC5 and is considered to be a secure algorithm.**

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

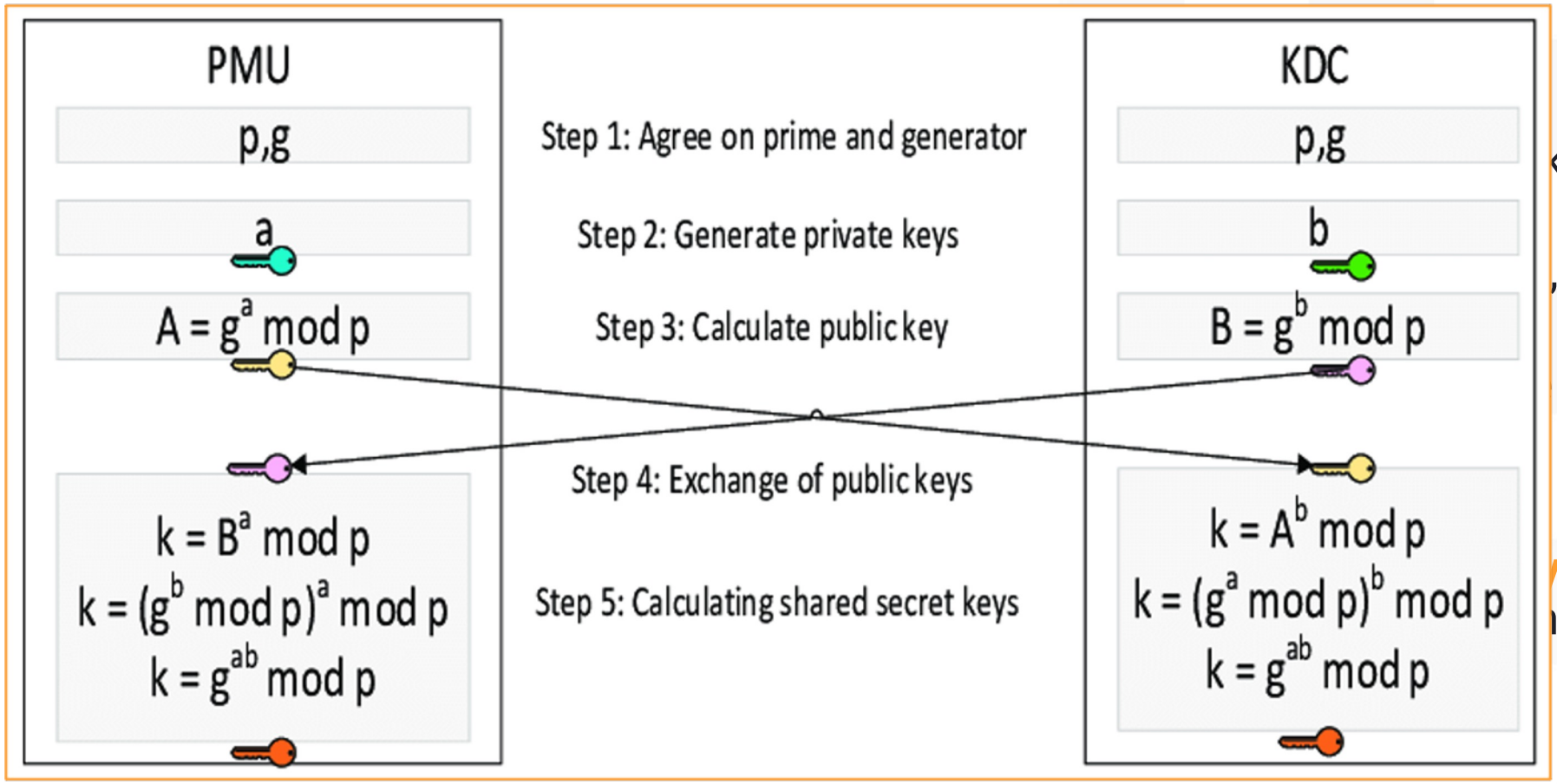
Cryptographic Methods - Asymmetric Encryption

- Solves the age-old challenge of preshared keys
- Whitfield Diffie and Martin Hellman, who created the Diffie-Hellman key exchange in 1976
- RSA algorithm was invented in 1977 (RSA stands for "Rivest, Shamir, and Adleman," the authors' names)
- Uses **two keys**: if you encrypt with one key, you may decrypt with the other
- Also called public key encryption
- Public – Private key pair
- Math lies behind the asymmetric encryption - methods use "**one-way functions**," which are easy to compute "one way," and difficult to compute in the reverse direction.

DOMAIN 3: SECURITY ARCHITECTURE AN

Select and Determine Cryptographic Solutions

Cryptographic Methods - Asymmetric Encry



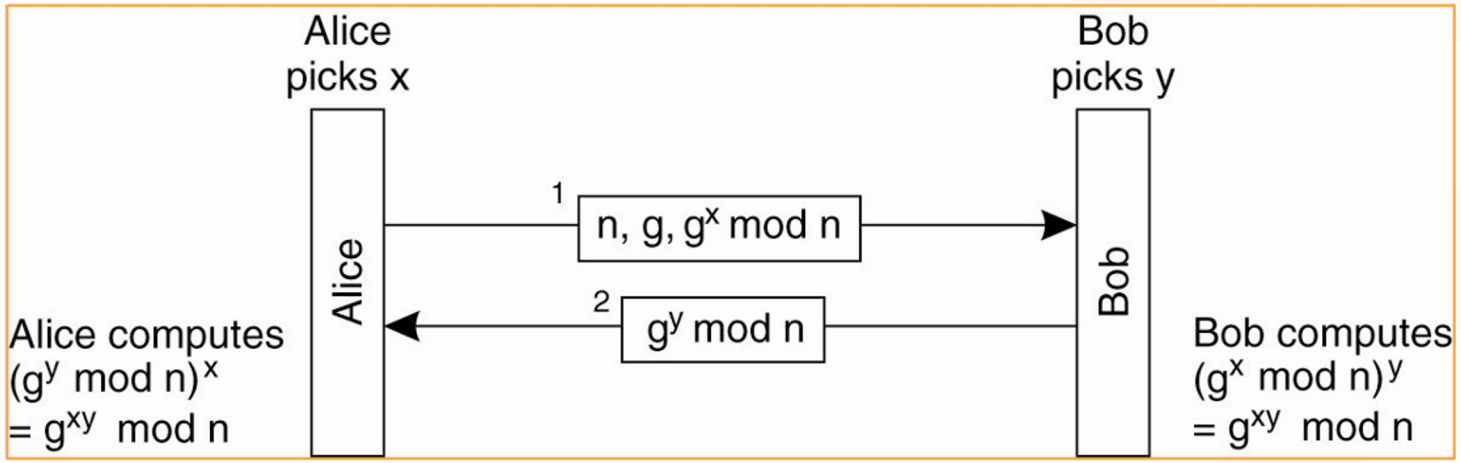
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Asymmetric Encryption

Diffie-Hellman key agreement protocol

- Allows two parties to securely agree on a symmetric key via a public channel
- Also called the Diffie-Hellman Key Exchange



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

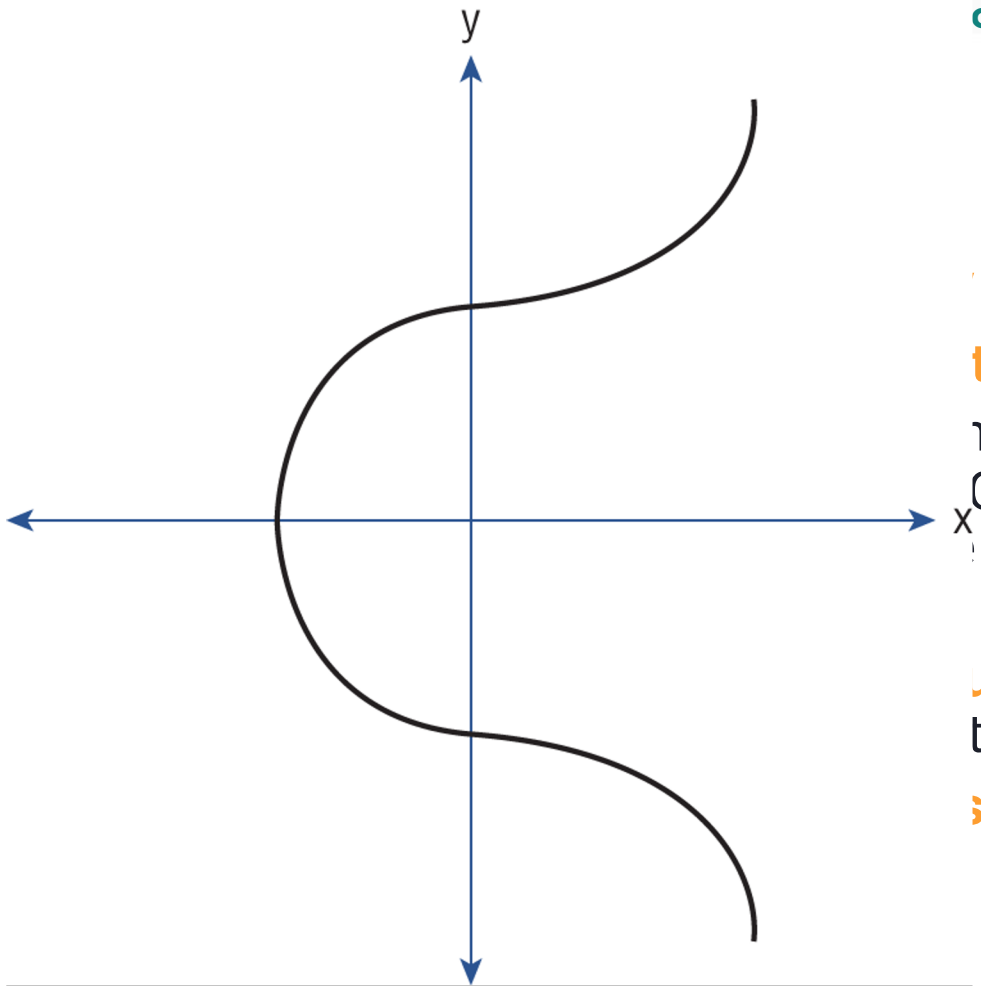
Select and Determine Cryptographic Solutions

Cryptographic Methods - Asymmetric Encryption

Elliptic Curve Cryptography (ECC)

- One-way function that uses **discrete logarithms as applied to elliptic curves**
- Solving this problem is harder than solving discrete logarithms, so algorithms based on Elliptic Curve Cryptography (ECC) are **much stronger** per bit than systems using discrete logarithms (and also stronger than factoring prime numbers)
- Requires **less computational resources** because shorter keys can be used compared to other asymmetric methods
- Often **used in lower power devices**

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING



ons

Asymmetric Encryption

(ECC)

te logarithms as applied to elliptic curves

n solving discrete logarithms, so
Cryptography (ECC) are **much stronger**
logarithms (and also stronger than

urces because shorter keys can be used
thods

s

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

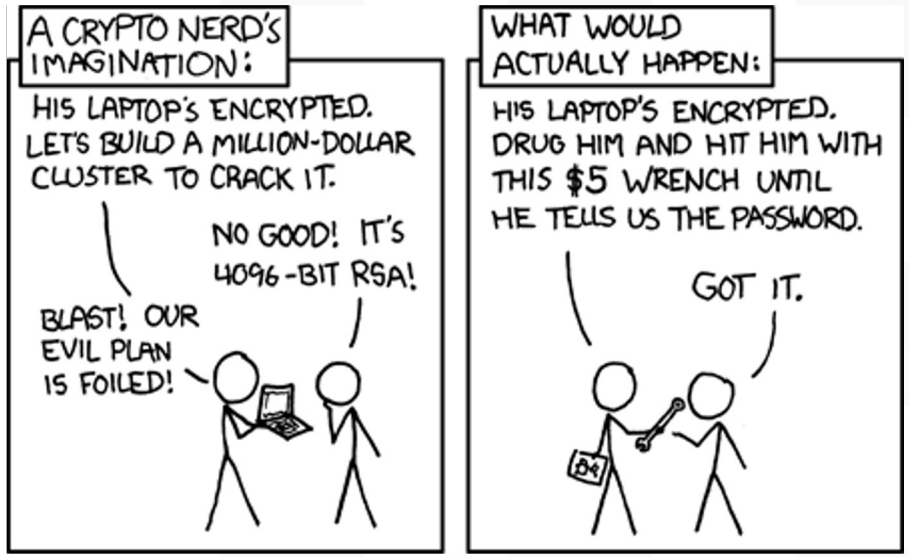
Select and Determine Cryptographic Solutions

Cryptographic Methods - Quantum Cryptography

One property of quantum mechanics that lends itself to cryptography is that any attempt to observe or measure a quantum system will disturb it. This provides a basis to transmit a secret encryption key such that if it is intercepted by an eavesdropper, it can be detected.

So, Alice first sends Bob a secret key using quantum key distribution (QKD), and Bob checks to see if it has been intercepted. If it has, he asks for another key. If it hasn't, he signals Alice to start sending messages encrypted using a symmetric cipher or a one-time pad and the key, knowing that only Alice and he have access to the key and therefore the communications will remain secret.

Quantum Encryption



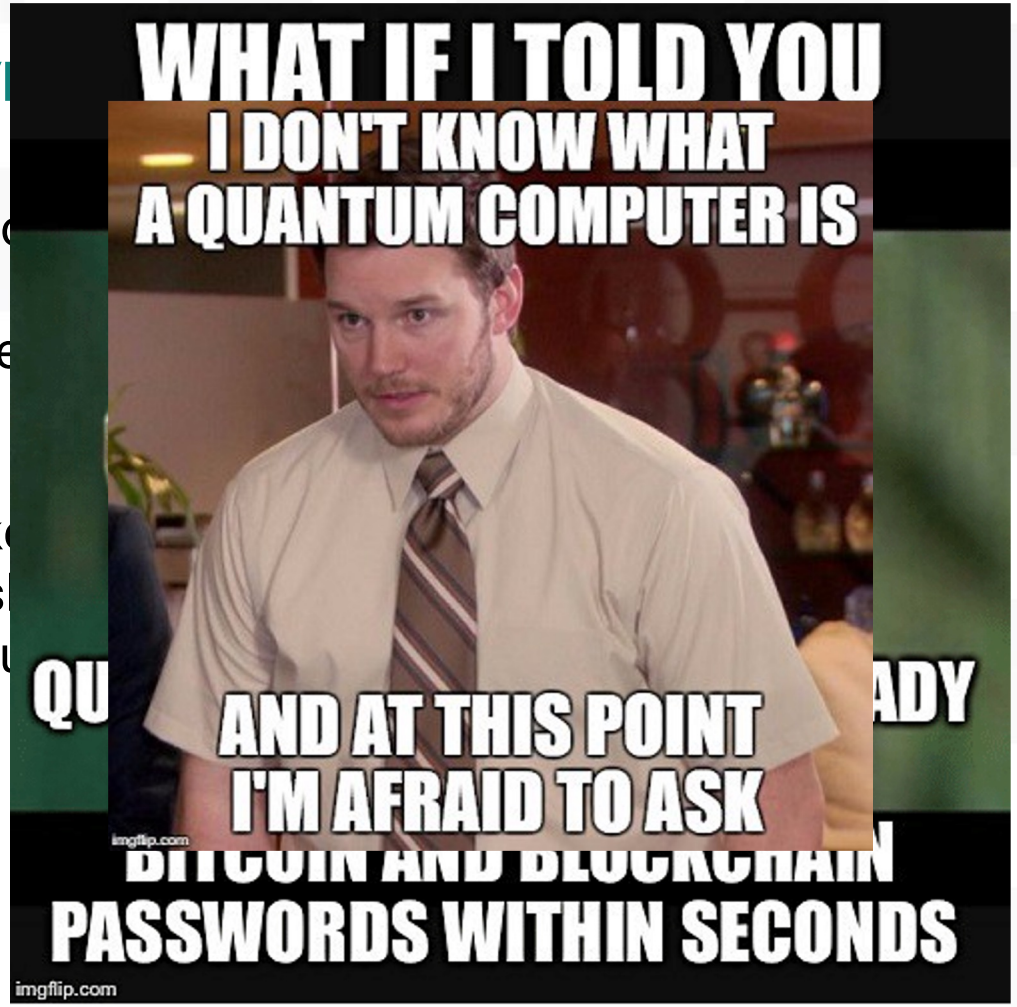
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Quantum Cry

One property of quantum mechanics that lends itself t
attempt to observe or measure a quantum system will
to transmit a secret encryption key such that if it is inte
can be detected.

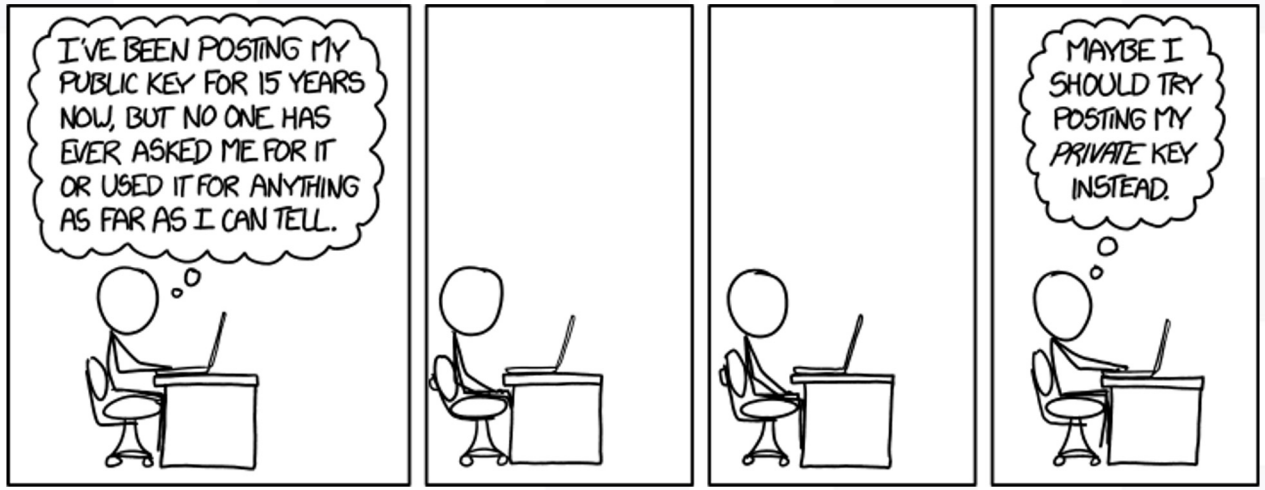
So, Alice first sends Bob a secret key using quantum k
checks to see if it has been intercepted. If it has, he as
he signals Alice to start sending messages encrypted u
one-time pad and the key, knowing that only Alice and
therefore the communications will remain secret.



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Asymmetric Encryption



Public Key Infrastructure (PKI)

- Leverages all three forms of encryption to provide and manage digital certificates
- A digital certificate is a public key signed with a digital signature
- Digital certificates may be server-based (used for SSL Web sites such as https://www.ebay.com, for example) or client-based (bound to a person).
- If the two are used together, they provide mutual authentication and encryption.
- The standard digital certificate format is X.509.

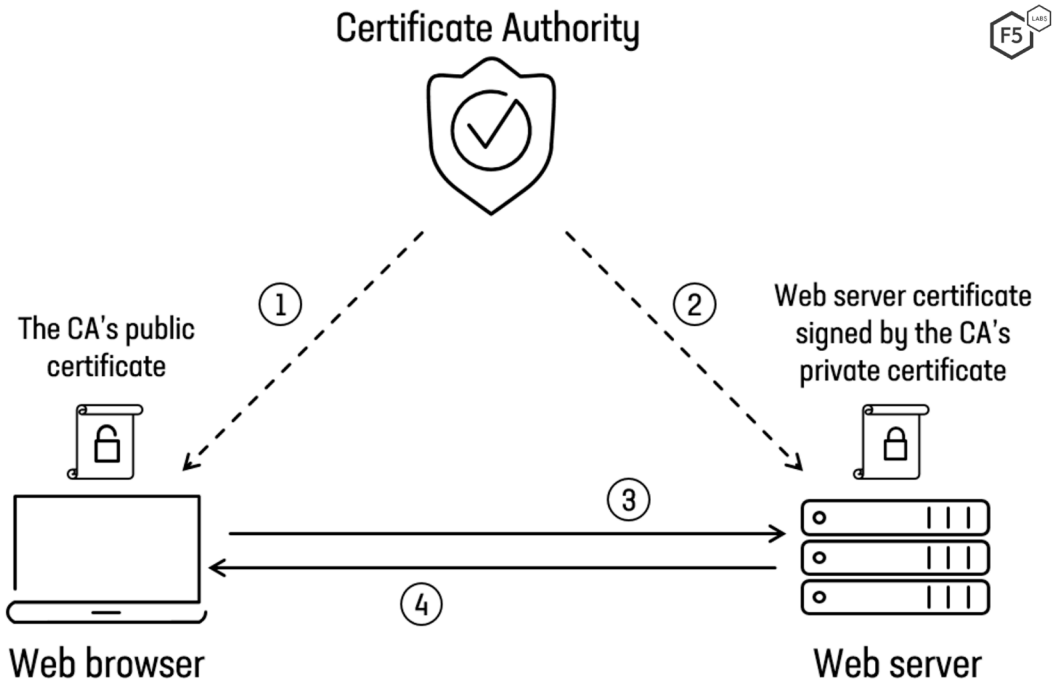
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Asymmetric Encryption - PKI

The standard for public key certificates (also known as digital certificates) is X.509, defined by the International Telecommunications Union (ITU). An X.509 certificate contains the following:

- Version number
- Serial number
- Signature algorithm ID
- Issuer (CA) name
- Validity period (not before, not after)
- Subject name
- Subject public key (algorithm, public key)
- Key usage
- Optional extensions
- Certificate signature (algorithm, signature)



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI

Public Key Infrastructure (PKI)

Certificate Authorities

- Digital certificates are issued by Certificate Authorities (CAs)
- Authenticate the identity of a person or organization before issuing a certificate to them
- CAs may be private (run internally) or public (such as Verisign or Thawte)

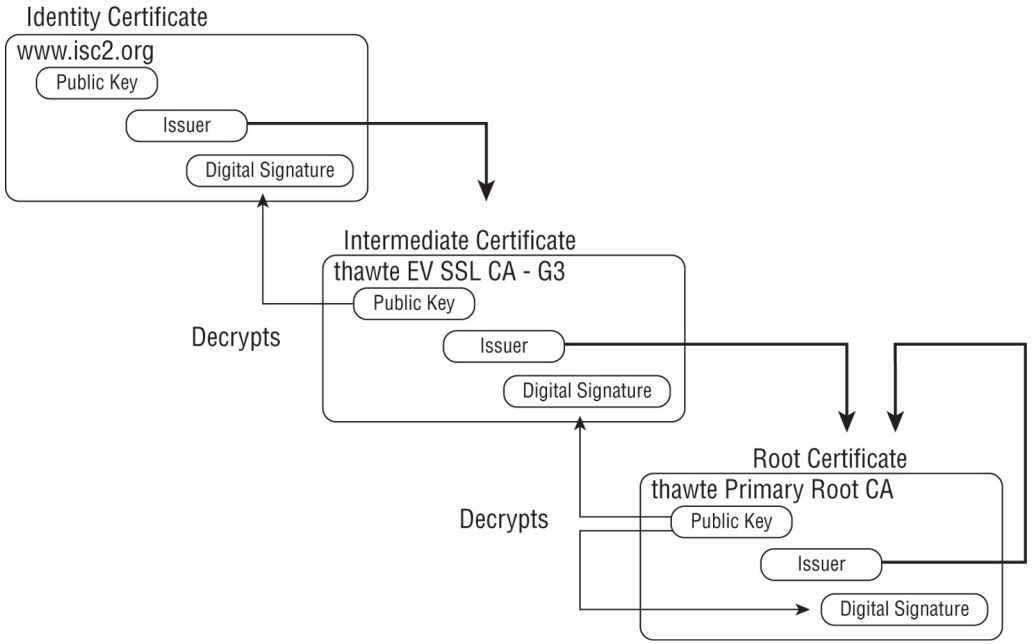
Certificate Revocation Lists

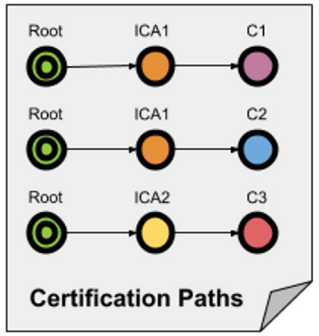
- Certificate Authorities maintain Certificate Revocation Lists (CRL)
- List certificates that have been revoked

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI

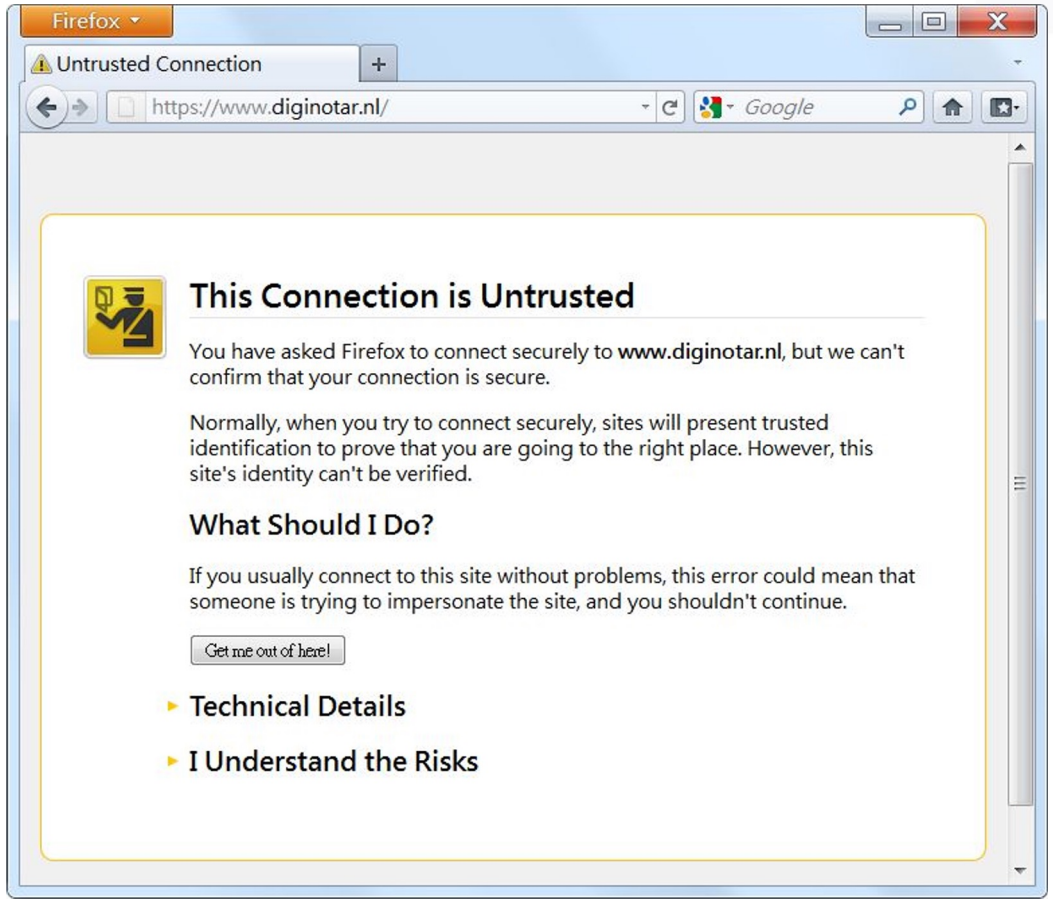




DOMAIN 3: SECURITY ARCHITECT EERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI



Date	Incident	Target	Reason
Jan 25 2011	**Stuxnet** Stuxnet driver is discovered to be signed with a valid certificate belonging to Realtek Semiconductor Corps. On July 16 2011, Verisign revokes Realtek Semiconductor Corps certificate.[1]	Realtek	Stolen Certificate
Mar 24 2011	**Comodo** As a revenge for Stuxnet, an Iranian Hacker forges fake certificates for google email services.[2]	Comodo	Vulnerability in Enrollment
Aug 29 2011	**Diginotar** A user named finds a certificate warning about a revoked SSL certificate Google services. The certificate was issued on July 10th by Dutch DigiNotar. The fake certificate was forged by Comodo Hacker, and revoked immediately.[3]	DigiNotar	Non Disclosed Web Vulnerability
Sep 6 2011	**Diginotar, Globalsign and StartCom** The real extent of the Diginotar breach becomes clear: 531 bogus certificates issued including Google, CIA, Mossad, Tor. Comodo Hacker also claims to own four more CAs, among which GlobalSign which precautionally suspends issuance of certificates. Another one StartCom was able to avoid the hack since its CEO was sitting in front of HSM, although the attacker claims to own emails, DB and Customer data.[4]	DigiNotar GlobalSign StartCOM	N/A
Sep 7 2011	**Symantec** As a consequence of Comodo Hackler's claims, Symantec releases a statement to reassure their customers their infrastructure has been audited and it is not compromised.[5]	Symantec	N/A
Sep 7 2011	**Thawte** Panic is spreading on the Certification Authority industry. Thawte publishes a similar announcement than Symantec after an erroneous report from a Dutch Government agency according to which the Security firm had been breached.[6]	thawte	N/A
Sep 9 2011	**GlobalSign** After suspending issuing certificates, GlobalSign finds evidence of a breach to the web server hosting the www website. The breached web server has always been isolated from all other infrastructure and is used only to serve the www.globalsign.com website.[7]	GlobalSign	Breach on Web Site
Oct 19 2011	**Duqu** Researchers discover that Duqu, the son of Stuxnet, masks itself as legitimate code using a driver file signed with a valid digital certificate. The certificate belongs to a company headquartered in Taipei, identified by F-Secure, as C-Media Electronics Incorporation. The certificate was set to expire on August 2, 2012, but authorities revoked it on Oct. 14, shortly after Symantec began examining the malware.[8]	Cmedia	Stolen Certificate?
Nov 3 2011	**Digicert Malaysia (not to be confused with US based Digicert)** Mozilla announces to revoke another intermediate signing certificate used by a registrar in Malaysia, DigiCert Sdn. Bhd. (not to be confused with US based DigiCert) which had issued 22 weak certificates (RSA 512) to the Malaysian government that could lead to abuse or compromise. Entrust stated that two of the certificates issued were used to sign malware used in a spear phishing attack against another Asian certificate authority. Three other certificates were also involved, but were not issued by DigiCert Sdn. Bhd.[9]	digicert	N/A
Nov 4 2011	**Getronics (KPN Certification Authority)** After Diginotar, another Dutch certificate authority, KPN, stops issuing digital certificates as a precaution after finding an attack DDoS tool during an audit on a server in its Web infrastructure. The tool may have been there for as long as four years.[10]	kpn	DDoS Tool on the a Web Server
Nov 14 2011	**Malaysian Agricultural Research and Development Institute** F-Secure detects a malware signed with a Governmental Signing Key belonging to mardi.gov.my which is part of the Government of Malaysia: Malaysian Agricultural Research and Development Institute. According the information received from the Malaysian authorities, this certificate has been stolen "quite some time ago".[11]		Stolen Certificate
Dec 8 2011	**Gemnet** Another Dutch Certification Authority breached: security firm Gemnet suffers a data breach including administrative credentials. Parent company KPN has suspended sister company Gemnet CSP's certificate signing operations.[12]	Gemnet	No Password on the phpMyAdmin portal

paulsparrows.wordpress.com

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

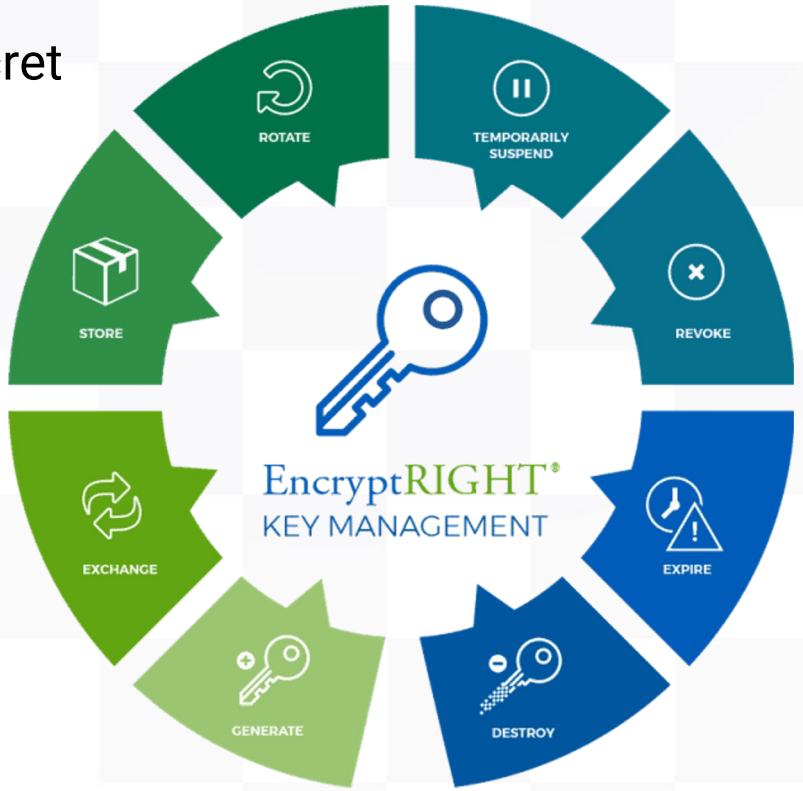
Cryptographic Methods - PKI

Key Management Practices

Secure use of cryptography depends on keeping symmetric and private keys confidential. Attackers who can obtain or guess a secret key can compromise the confidentiality and integrity of the data protected by that key.

Proper cryptographic key management includes the following:

- Secure key generation
- Secure key storage and use
- Separation of duties, dual control, and split knowledge
- Timely key rotation and key change
- Key destruction



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI

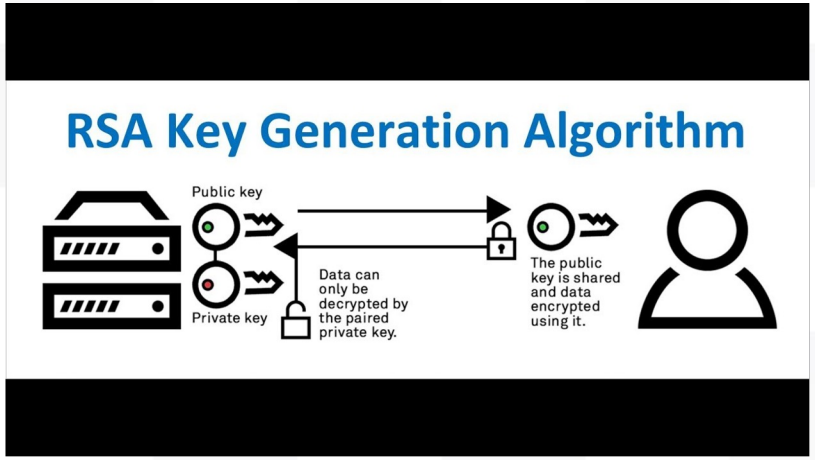
There are two factors that make for a secure cryptographic key:

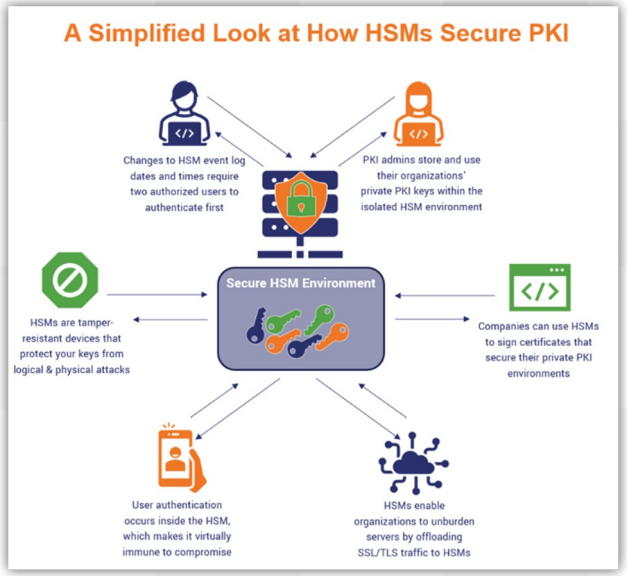
- length
- randomness

The strength of a symmetric key also depends on its being unpredictable (i.e., unguessable).

Using a mechanism that will generate high-quality (i.e., cryptographically secure) random numbers is essential for key generation.

The best method is to use hardware-based true random number generators that rely on physical phenomena known to be truly random. (TPMs and HSMs, as well as some microprocessors)

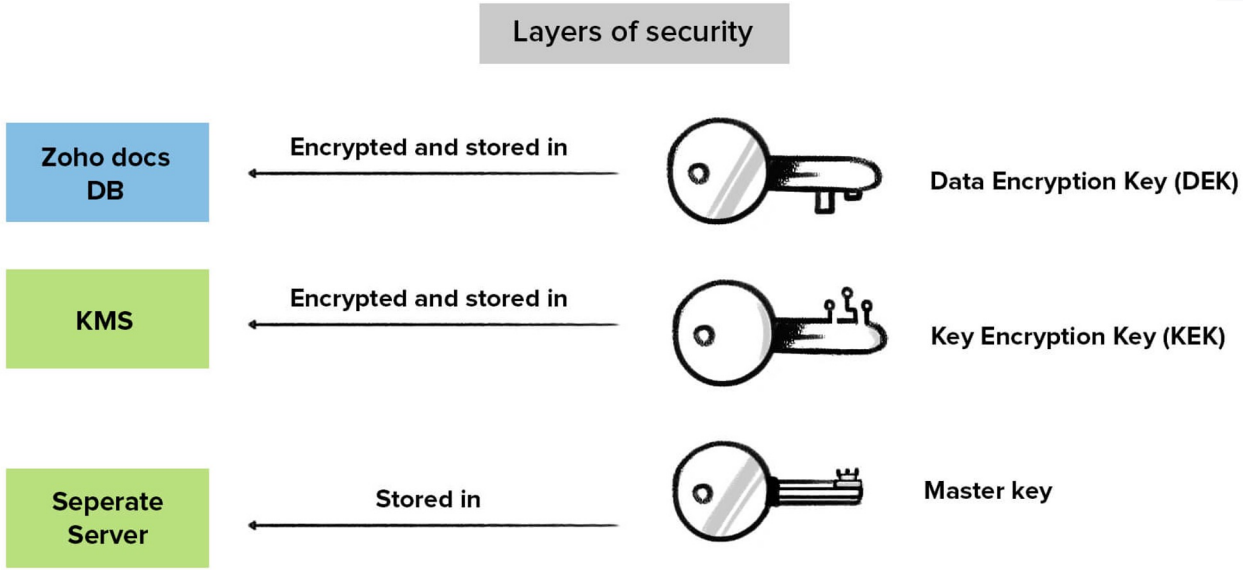


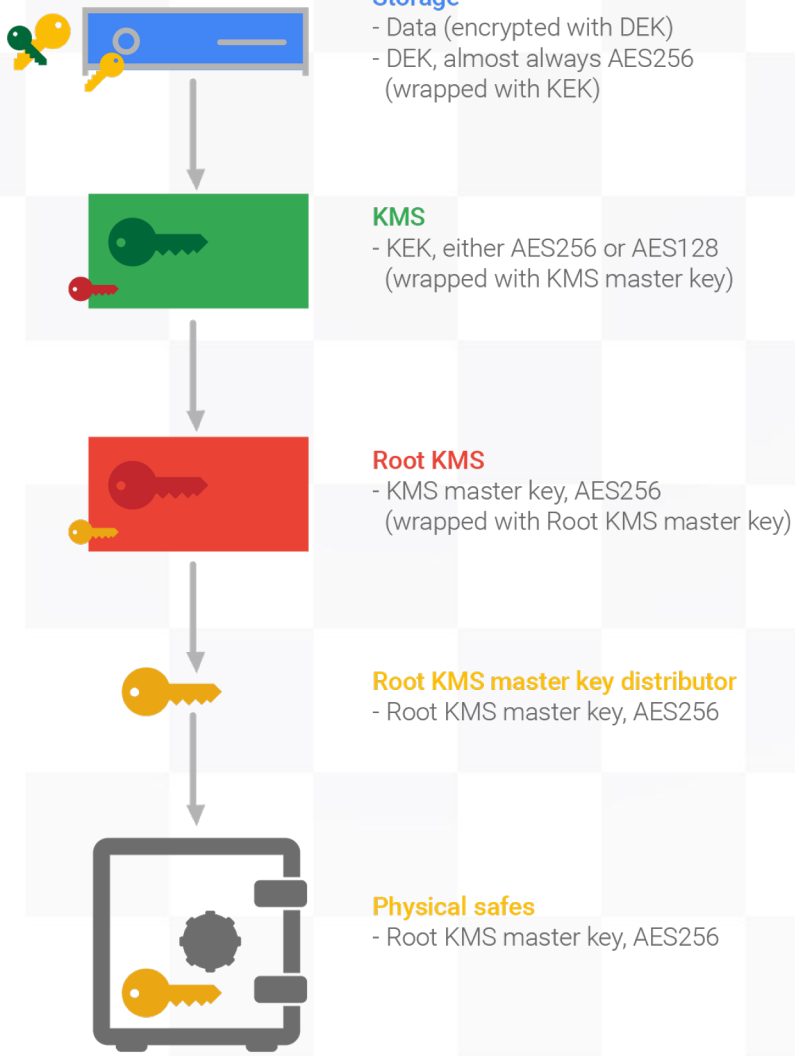


DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI





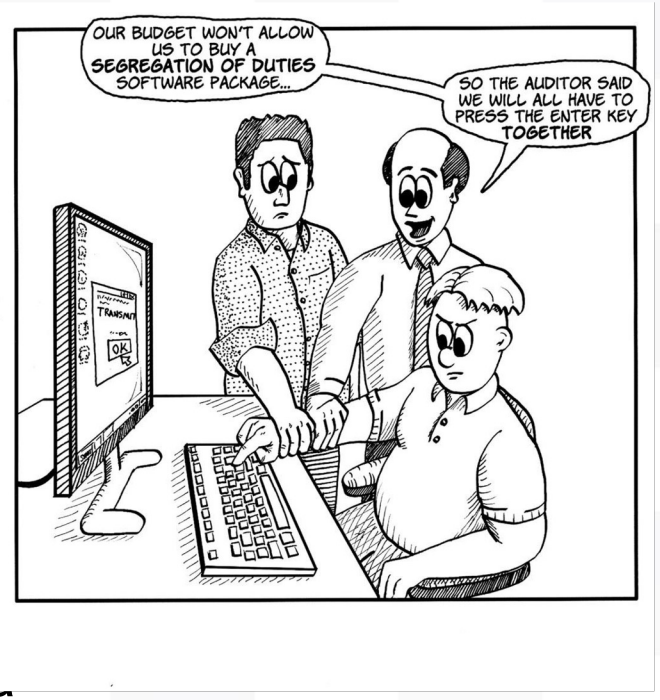
One could store the **master key** in any of the following:

- A hardware-encrypted USB key
- A password management app
- A secrets management package

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI



Separation of Duties, Dual Control, and Split Knowledge

These are three types of controls used to mitigate the risk of a rogue employee:

- Separation of duties - certain processes should require at least two different individuals to complete from beginning to end.
- Dual control - specific step in a process requires two or more individuals.
- Split knowledge - a key (or password) is split into two or more pieces such that each piece is unusable by itself, and it requires that two (or more) pieces be brought together to decrypt the data (or access the system)

These three concepts are related but different.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

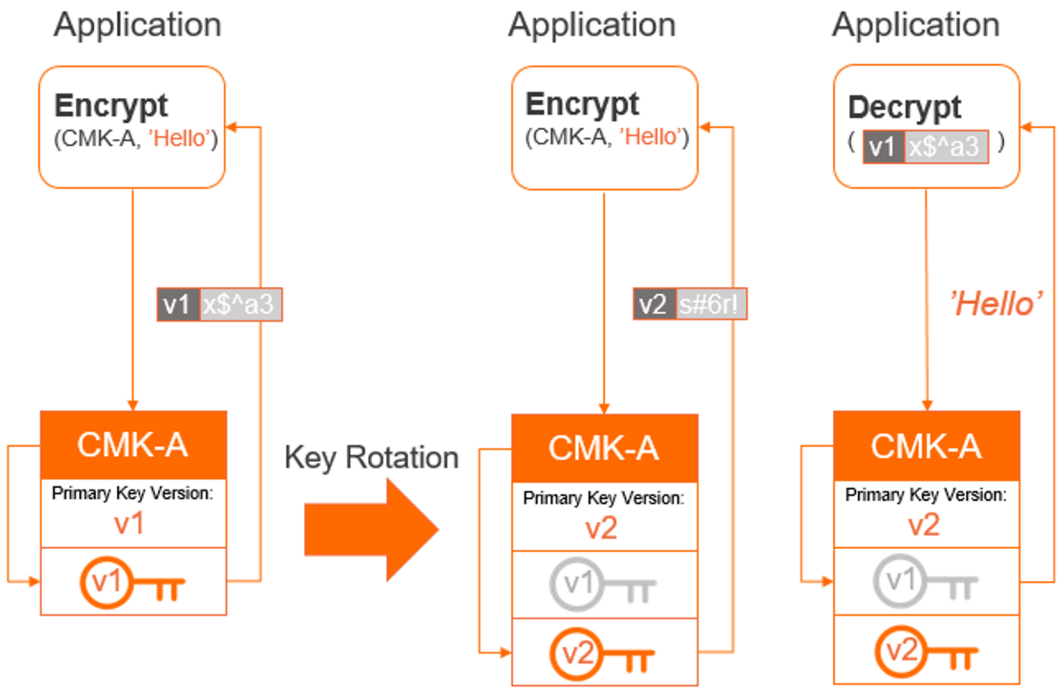
Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI - Key Rotation

Timely Key Rotation and Key Change

Why rotate keys?

- **To limit the damage should the key be discovered by an attacker**
- **To limit the amount of data encrypted by the same key** (the more data encrypted using the same key, the easier it is to crack the encryption)
- **To limit the time available to the attacker to crack the cipher** (if none of your data is encrypted with the same key for longer than one year, then any brute-force attack must be able to be completed within a year of the key's generation)

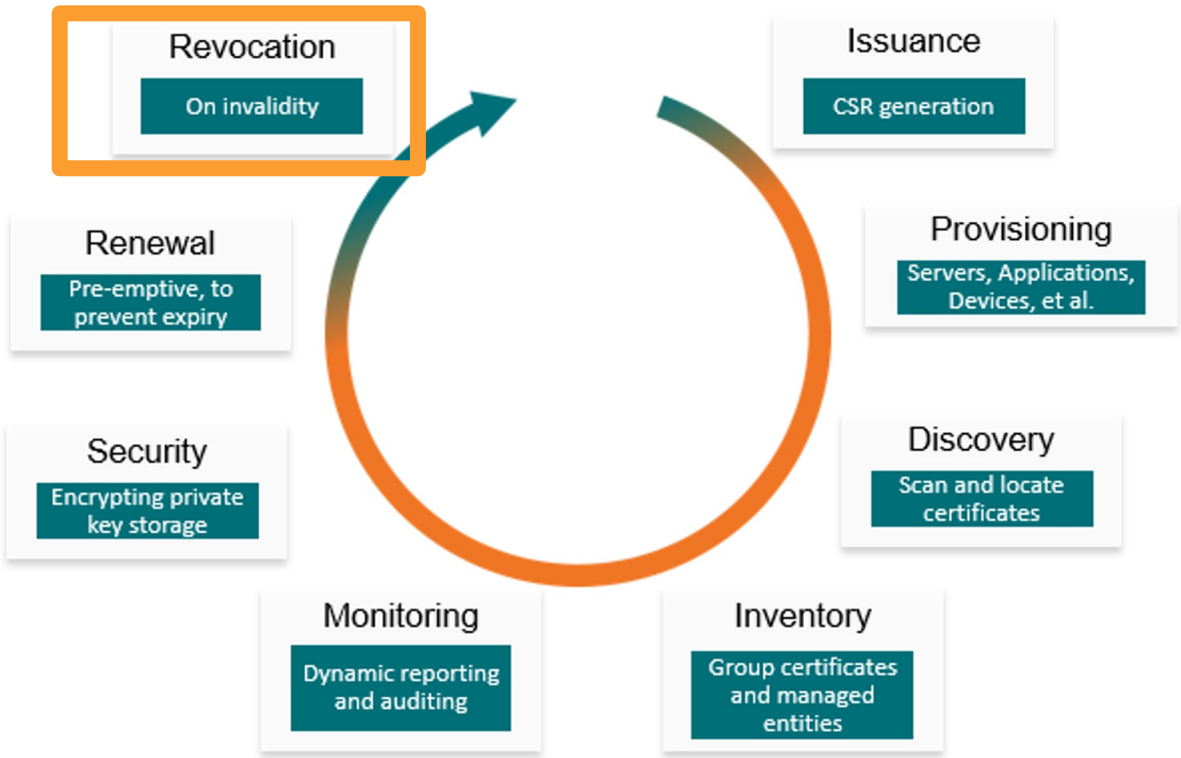


DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - PKI - Key Destruction

- Once a key has been retired and it has been determined that there is no data that has been encrypted using that key that will need to be decrypted, then the key must be securely destroyed.
  - This involves locating every copy of the key and deleting it in a manner appropriate for the media on which it was stored to ensure that it cannot be recovered.
- Depending on the media and the risk of it becoming accessible to unauthorized individuals, this may require overwriting the storage, degaussing of the media, or physical destruction of the media or device containing the media.
- Records ought to be kept that document the locations of the destroyed keys and the means used to ensure secure destruction.



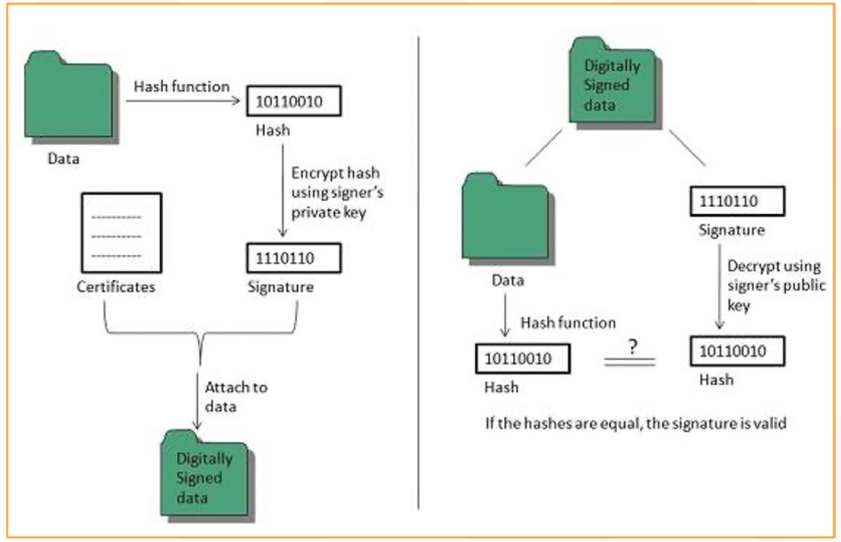
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Digital Signatures and Digital Certificates

Digital Signatures

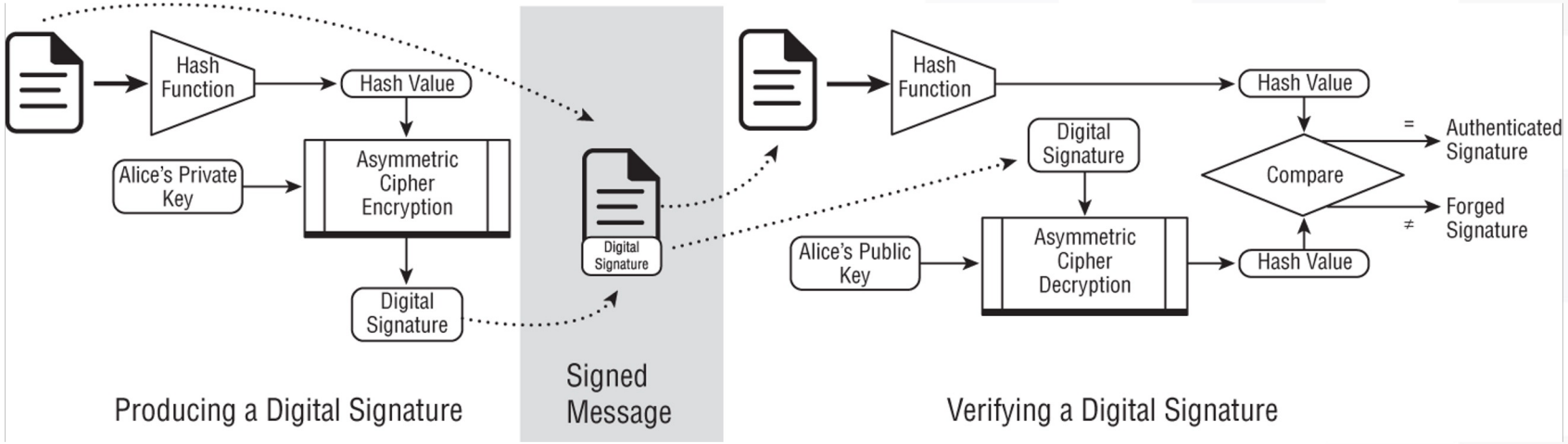
- Used to cryptographically sign documents
- Provide **nonrepudiation**, which includes authentication of the identity of the signer, and proof of the document's integrity (proving the document did not change)
- Use a hash function to generate a hash value of the plaintext
- Create the digital signature by encrypting the hash with a private key
- Digital signatures provide authentication and integrity, which forms nonrepudiation. They do not provide confidentiality: the plaintext remains unencrypted.



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Digital Signatures and Digital Certificates



There are a number of possible vulnerabilities with digital signatures:

- Hash collision
- Private key disclosure
- CA compromise

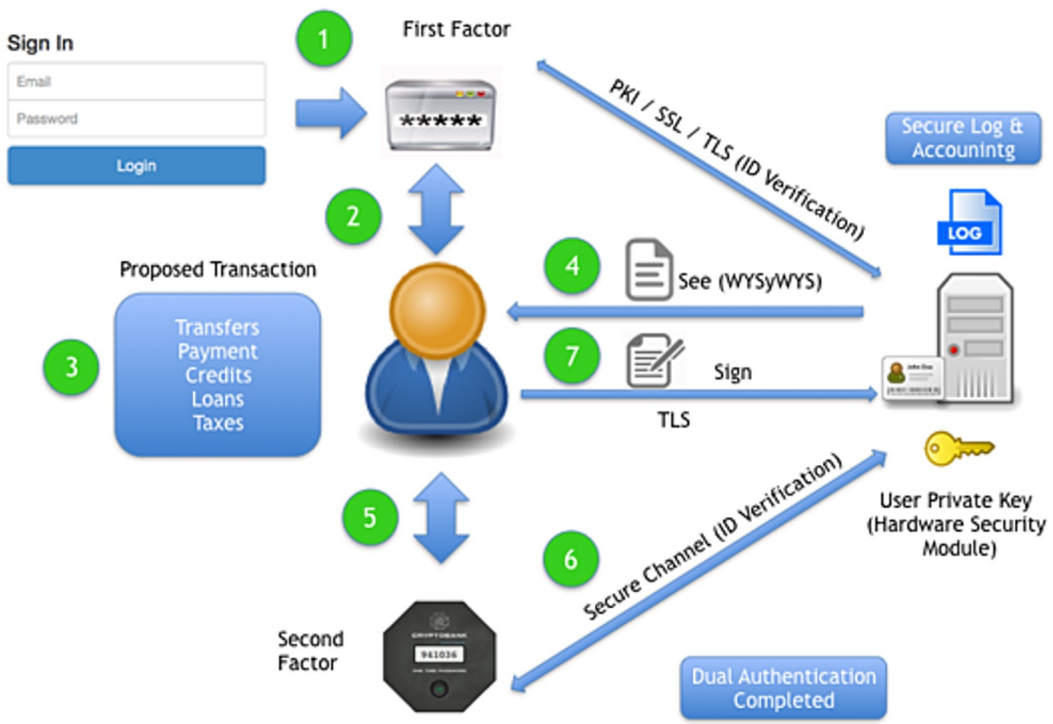
A digital signature, in and of itself, does not protect the confidentiality of the message. If that is required, the sender must also encrypt the message itself.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Digital Signatures and Digital Certificates

- Nonrepudiation is the ability to prove that a message must have originated from a specific entity.
- This can be critically important, for example, with contracts or other legal documents, as well as instructions to banks or orders to suppliers.
- Only with the ability to demonstrate nonrepudiation of the received communication can the recipient act on the message with confidence that the originator is accountable for the content of the message.

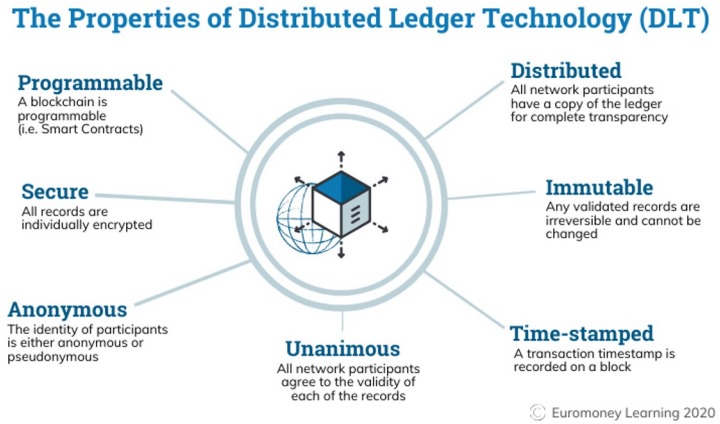


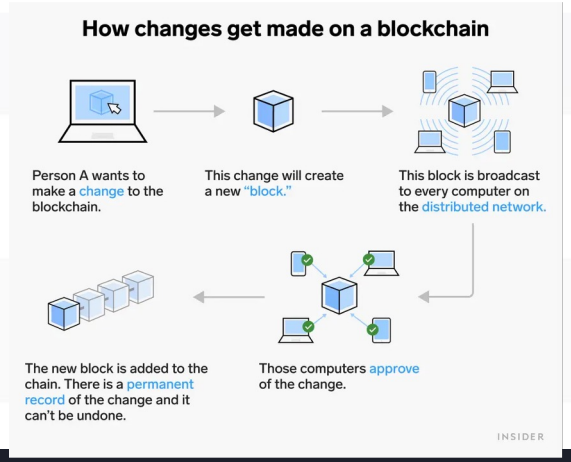
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Digital Signatures and Digital Certificates

- Blockchain and Nonrepudiation
- Another approach to nonrepudiation is to use a blockchain. Blockchain is a form of a decentralized and distributed ledger in which records are recorded and linked together, using cryptographic hashes, meaning that to change any record in the blockchain, one must change every subsequent block.
- Since the blockchain is distributed (i.e., stored by multiple systems), it requires the collusion of a majority of the blockchain participants. For a sufficiently widely (and independently) operated blockchain, this is infeasible. For example, Bitcoin currently (early 2021) has approximately 12,000 nodes across 100 countries.
- NOTE Not all distributed ledgers require blockchain, and not all blockchains need to be “coin-based” like Bitcoin and Ethereum.



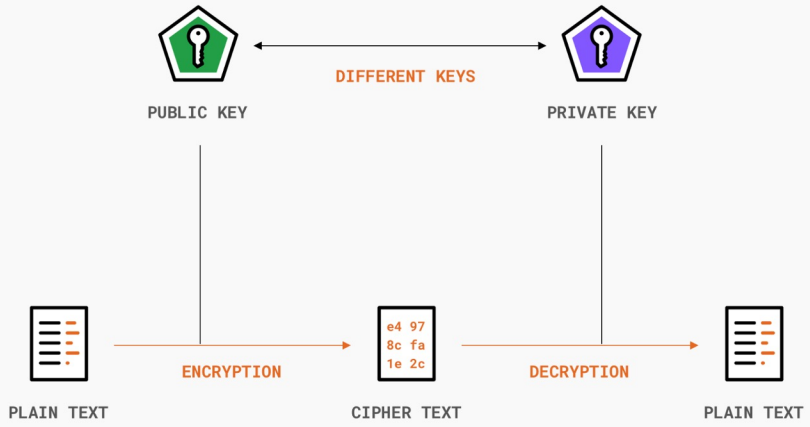


DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Integrity

Cryptographic methods can do more than just protect the confidentiality of messages and **help prove the identity of the originator.**

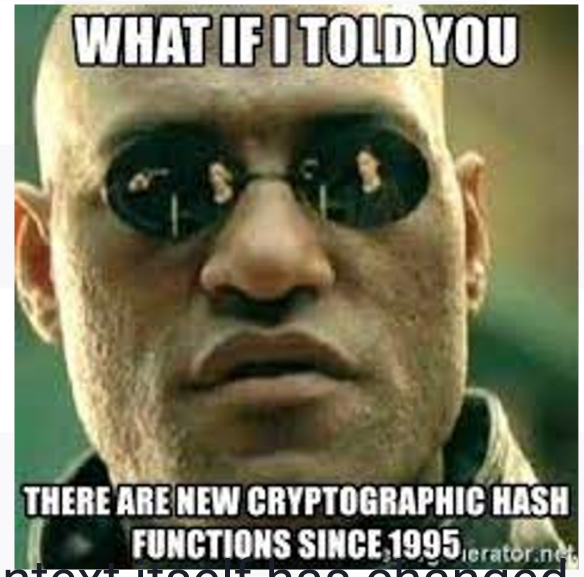


DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Integrity

A **hash function** is an algorithm that takes a block of data (i.e., a message or file) and computes a derived value such that any change to the data will result in a change to the hash value.

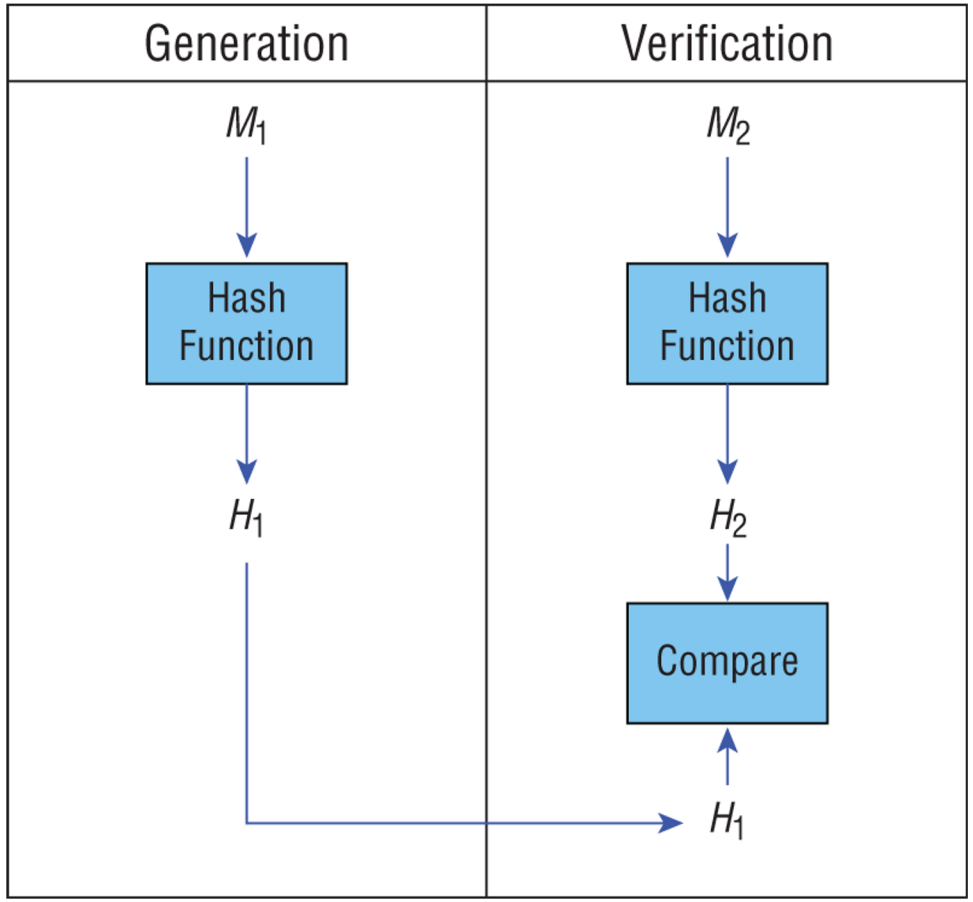


- Provides encryption using an algorithm and **no key**
- Called "**one-way** hash functions" because there is no way to reverse the encryption
- A **variable-length plaintext is "hashed" into a fixed-length hash value** (often called a "message digest" or a "hash")
- Primarily used to provide integrity: if the hash of a plaintext changes, the plaintext itself has changed
- Older hash functions include Secure Hash Algorithm 1 (SHA-1), which creates a 160-bit hash and Message Digest 5 (MD5), which creates a 128-bit hash
- Newer alternatives such as SHA-2 are recommended

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Integrity



A **checksum** is a mathematical function that takes a block of data and calculates a number (*the checksum*) in a manner such that any single change to the block of data will cause the checksum number to change.

- As the name implies, a checksum is typically calculated by taking the sum of each byte in the message, as an unsigned integer, and ignoring any overflow.

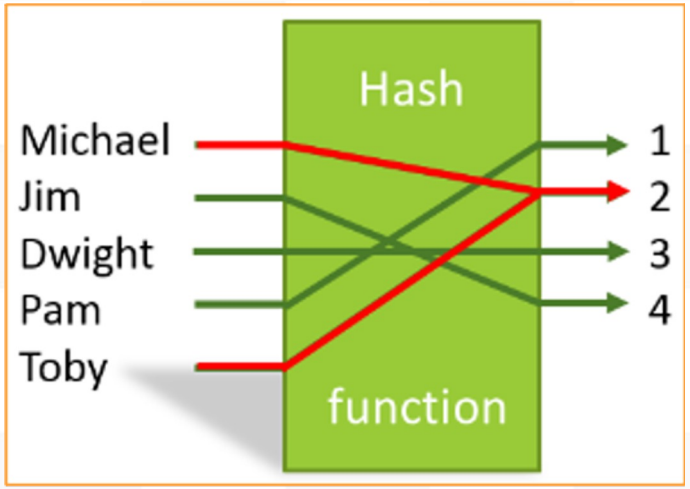
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

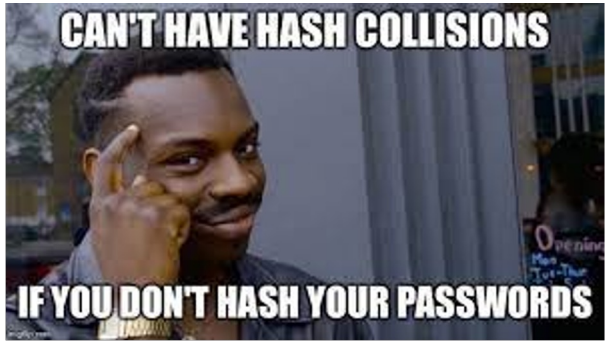
Select and Determine Cryptographic Solutions

Cryptographic Methods - Integrity

Collisions

- Hashes are not unique, because the number of possible plaintexts is far larger than the number of possible hashes
- More than one document could have the same hash: this is called a collision
- Collisions are always possible (assuming the plaintext is longer than the hash), they should be very difficult to find





DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - Integrity

MD5

- Message Digest algorithm 5, created by Ronald Rivest
- Creates a 128-bit hash value based on any input length
- Weaknesses have been discovered where collisions could be found in a practical amount of time
- MD6 is the newest version of the MD family of hash algorithms, first published in 2008

NOTE **Message Digest 5 (MD5)** is a very well-known and widely used algorithm as a hashing function.
It was later discovered to be susceptible to collisions. Now considered "**cryptographically broken**"
Despite its flaws, MD5 can still be safely used as a checksum — however, it is not suitable for use in hashing applications

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

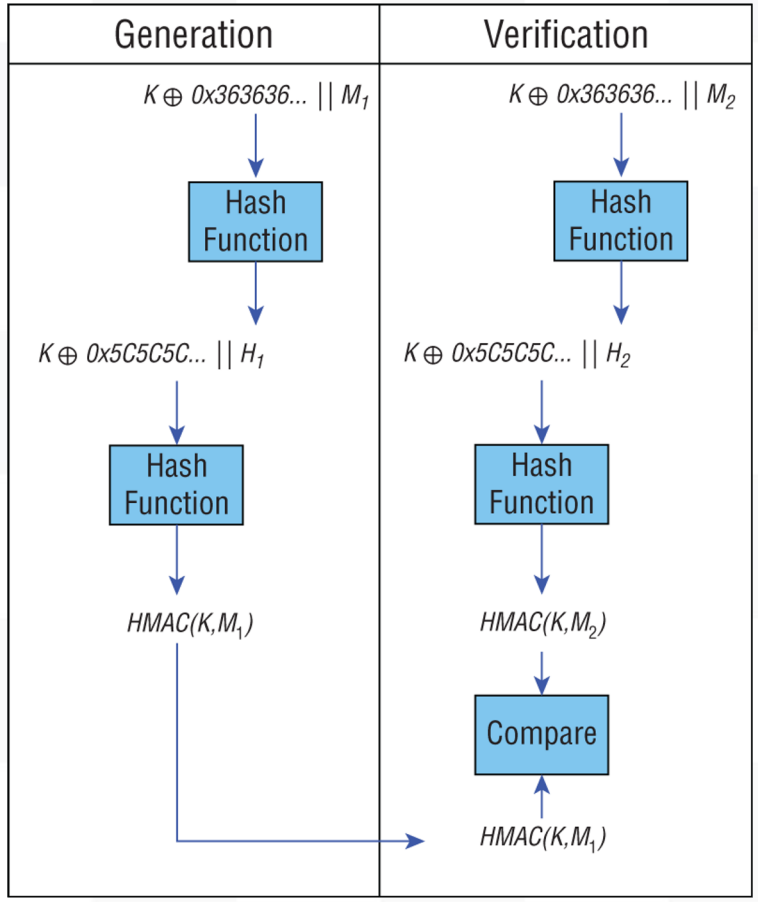
Select and Determine Cryptographic Solutions

Cryptographic Methods - Integrity

Hash-based Message Authentication Code (HMAC), concatenates a secret key (which has been XORed with a string to pad it to a fixed length) and hashes that. It then takes that hash, combines it with the key again, and hashes it a second time, producing the HMAC value.

HMAC is a less complex method of ensuring message integrity and authentication, but with the overhead of sharing a symmetric cipher key.

Digital signatures eliminate the need to share a secret but require the overhead of PKI.



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

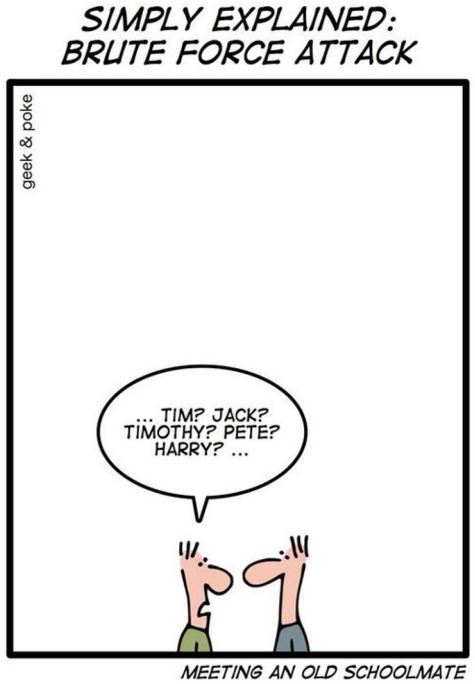
Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Brute Force

- Generates the entire keyspace, which is every possible key
- Given enough time, the plaintext will be recovered
- Effective attack against all key-based ciphers, except for the one-time pad



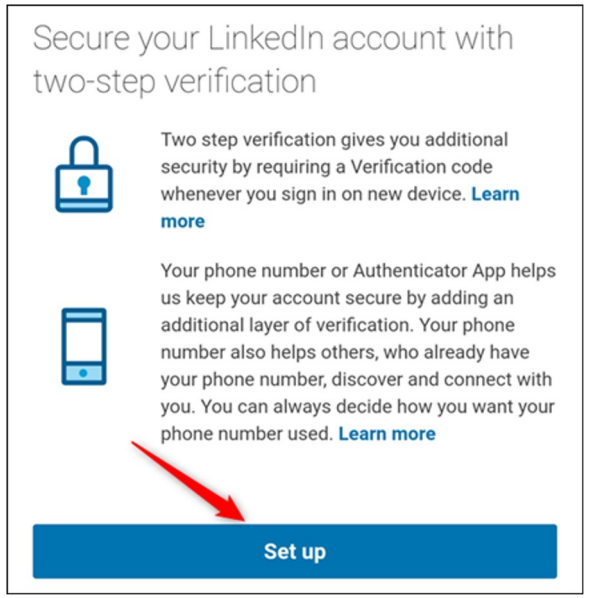
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

Defenses against a stolen password list used for Brute Forcing:

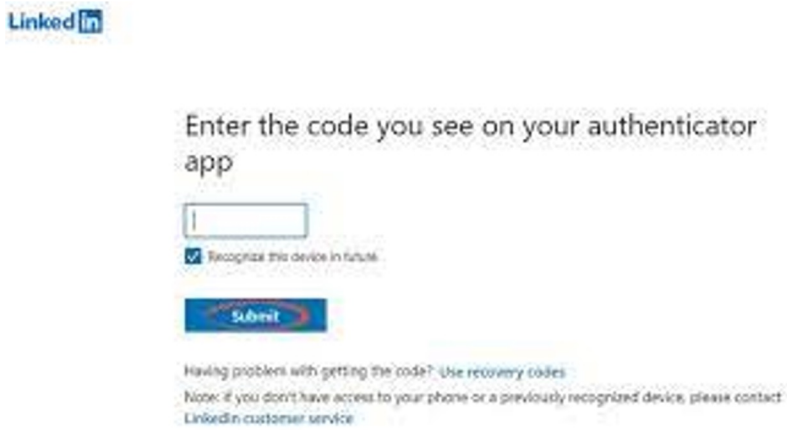
- Hashing complexity
- Salting



SECURITY May 19, 2016

117 million hacked LinkedIn accounts sold on Dark Web

In 2012, LinkedIn was hacked and now a data set filled with user credentials has appeared



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

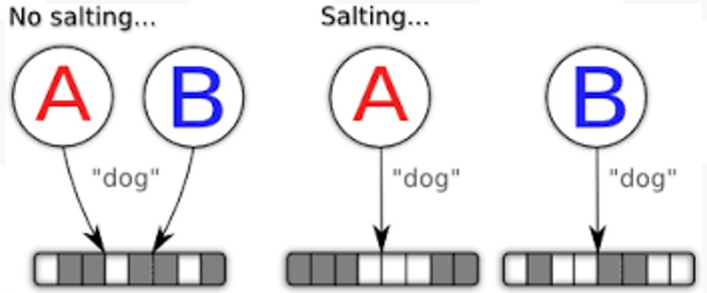
Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

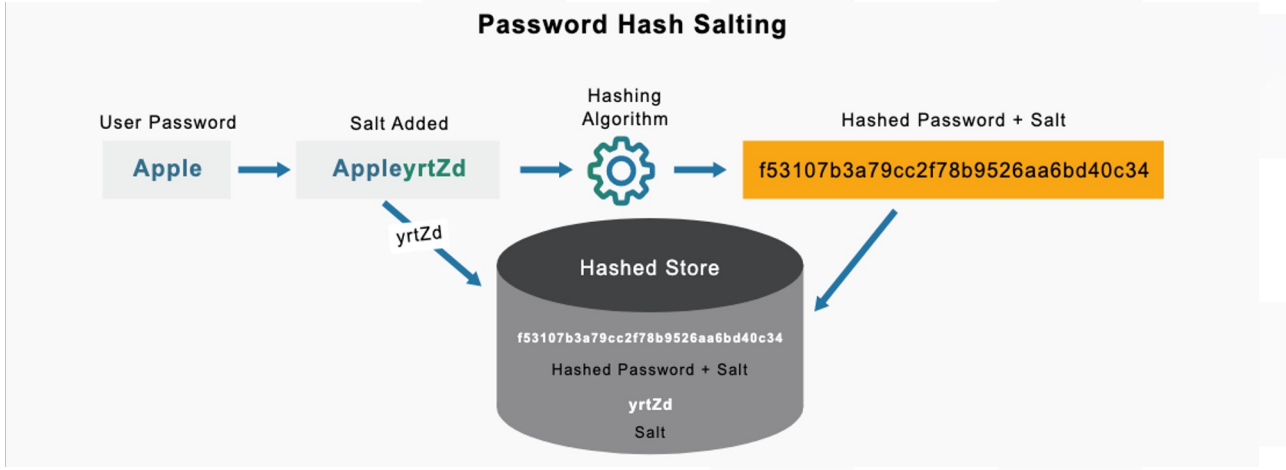
Salted Password file contains two fields (in addition to the user's login
name and other metadata):

- The salt
- The output of HASH (salt + password)

To be secure, the salt must be the following:

- Long (at least 16 bytes, and preferably 32 or 64 bytes)
- Random (i.e., the output of a cryptographically secure pseudo-random number generator)
- Unique (calculate a new salt for every user's password, and a new salt every time the password is changed)





DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

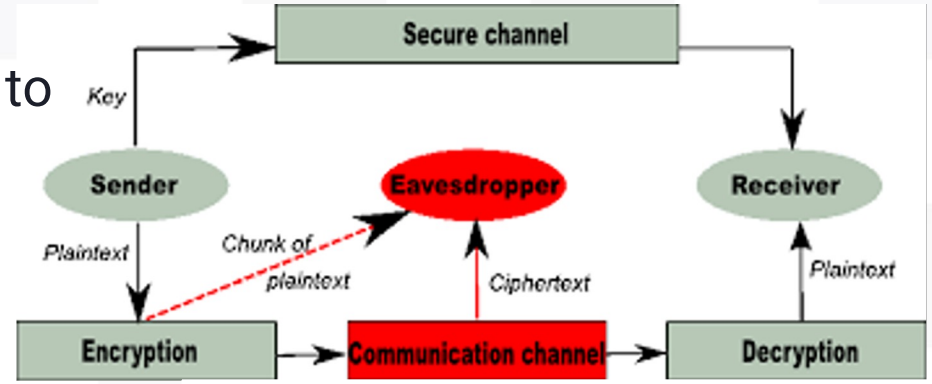
Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Known Plaintext

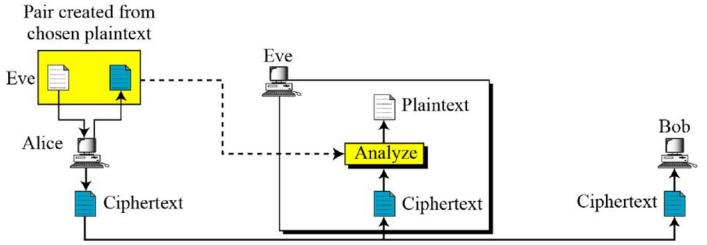
- Relies on recovering and analyzing a matching plaintext and ciphertext pair
- The goal is to derive the key which was used



Chosen-plaintext attack

Chosen Plaintext and Adaptive Chosen Plaintext

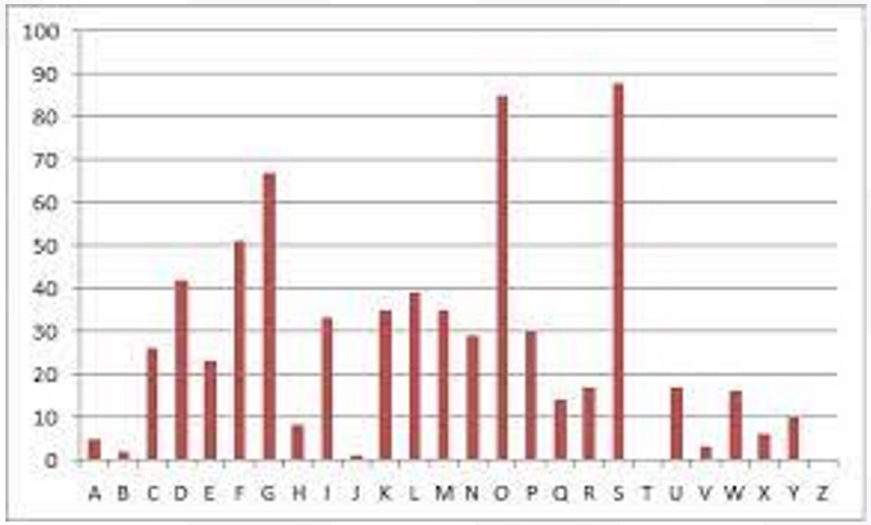
- Cryptanalyst chooses the plaintext to be encrypted
- Goal is to derive the key
- Adaptive-chosen plaintext begins with a chosen plaintext attack in round 1. The cryptanalyst then "adapts" further rounds of encryption based on the previous round



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS



Frequency analysis is the study of the frequency of characters (letters, numbers, or groups of either) in ciphertext. This attack works best against rudimentary cryptographic approaches such as substitution ciphers that map each character in a given set (e.g., alphabet) to another character (for example, a = z, b = y, and so on).

- By understanding the typical distribution of characters in a given language, frequency analysis can help a cryptanalyst deduce plaintext equivalents of commonly occurring ciphertext characters.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

Linear Cryptanalysis

- A known plaintext attack where the cryptanalyst finds large amounts of plaintext/ciphertext pairs created with the same key
- The pairs are studied to derive information about the key used to create them

Side-channel Attacks

Use physical data to break a cryptosystem, such as monitoring CPU cycles or power consumption used while encrypting or decrypting

Implementation Attacks

Implementation attack is a broad term used to describe any attack that exploits implementation weaknesses, such as in software, hardware, or the encryption algorithm itself.

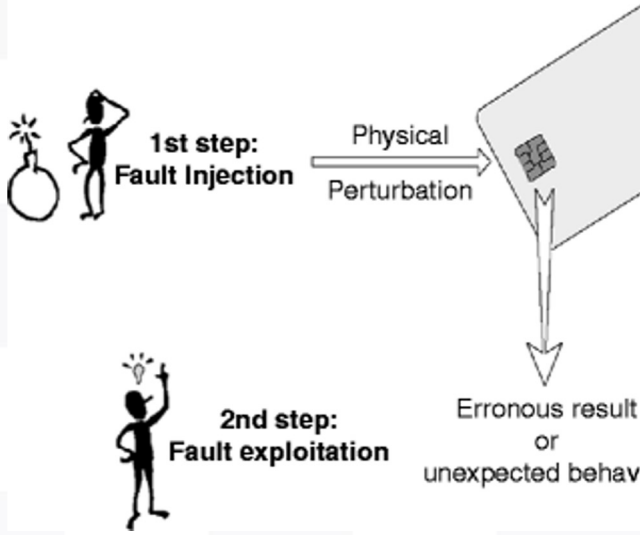
DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

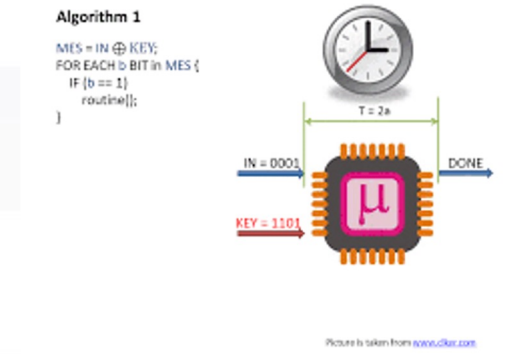
Fault Injection

Fault injection attacks are side-channel attacks that involve deliberately injecting faulty or erroneous inputs and observing the errors and outputs.



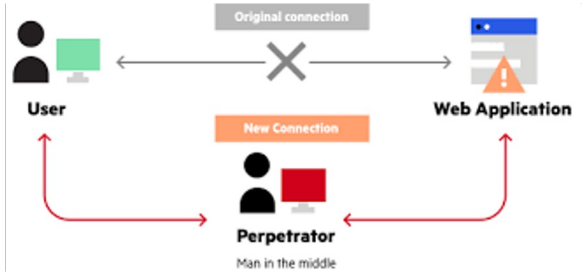
Timing Attacks

A timing attack is a side-channel attack that involves the attacker attempting to compromise a cryptosystem by monitoring the time taken to execute algorithmic functions.



Man-in-the-Middle

An MITM attack requires that the attacker be able to intercept and relay messages between two parties.



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

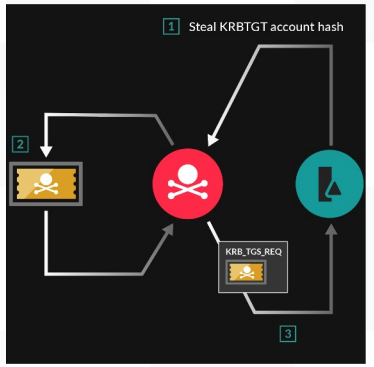
Pass the Hash

Pass the hash is an attack that occurs when an attacker obtains a password hash and passes it through for authentication. With this type of attack, the attacker does not need to decrypt the hash or otherwise obtain the plaintext password. This type of attack targets the authentication protocol, as opposed to the hash or any other cryptographic elements.

A least privilege security model can help limit the likelihood and impact of a potential pass-the-hash attack by reducing an attacker's ability to gain and use elevated privileges. Password management processes and tools that rotate passwords (preferably automatically) can also help fight against this attack.

Kerberos Exploitation

Kerberos is a network authentication protocol that uses symmetric-key encryption to provide strong authentication for client/server environments. The protocol operates on the basis of tickets that allow nodes (systems) on a network to prove their identity to one another.



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Select and Determine Cryptographic Solutions

Cryptographic Methods - UNDERSTAND METHODS OF CRYPTANALYTIC ATTACKS

Ransomware

Ransomware is malicious software that infects a system, encrypts the victim's files, and renders them unavailable until a ransom is paid.

- the victim is given instructions on how to pay a fee to get the decryption key required to recover their data.
  - Attackers will often request payment in Bitcoin, due to its anonymity.

Protection best practices:

- Keep your operating systems and applications patched and up-to-date, limit use of administrative privileges (i.e., least privilege)
- Use trusted antimalware software with updated signatures, among the other system hardening best practices.
- Maintaining overall good security hygiene, backing up your data frequently

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Introduction

- Physical assets: people, buildings, systems, and data
- CISSP® exam considers **human safety** as the most critical concern of this domain - trumps all other concerns
- Physical security protects against threats such as unauthorized access and disasters, both man-made and natural

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

The general security principles outlined earlier for information security also have application to site and facility design.

Confidentiality and Integrity: The primary physical threat to confidentiality and integrity is unauthorized access (e.g., intruders and theft).

Availability: In addition to the threat to availability from unauthorized access, availability can also be compromised intentionally or accidentally by a range of events:

- Environmental events such as fire, floods, storms, or earthquakes
- Infrastructure events such as power outages, cooling (HVAC) failure, floods (from burst water pipes)

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Wiring Closets/Intermediate Distribution Facilities

Vulnerabilities related to networking distribution differ slightly between a data center and an office.

- Data center owned and managed for a single company (or cloud-hosting provider), the network distribution will be within the same perimeter as the servers themselves, so the physical and environmental security controls will apply to both.
- Colocation facility, different clients will have access to different areas of the facility (to access the equipment owned by or assigned to them for their exclusive use).
  - Wiring closets are managed by the hosting provider and must not be accessible to clients, as it would permit even authorized clients to access or affect service to other clients.
- Office, intermediate distribution facilities need to be protected from both malicious outsiders and insider threats, not to mention environmental risks.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Location

- Avoid keeping combining wiring closets with other building services, as they often lack sufficient circulation and security
  - Small wiring closet full of network switches with poor (or no) ventilation can overheat, at a minimum shortening the life of your equipment, causing random resets, errors, and even total failure in the worst case.
  - Wiring closets can also be at risk from threats such as burst or leaking pipes that pass through or near the space or overflowing washrooms on the floors above

Consider compensating controls to secure access, add circuiation as well as plan for worse case scenarios like floods and power outages and the effect on equipment

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

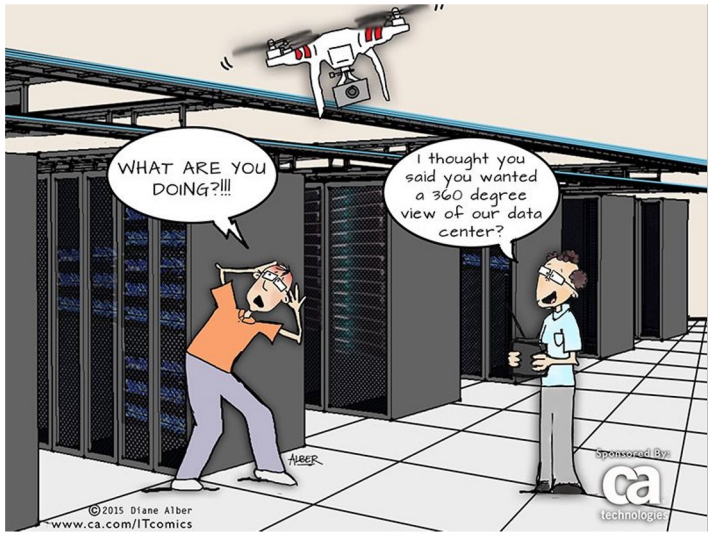
Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Server Rooms/Data Centers

Security controls need to be selected to address the following:

- **Physical access risks**
- **HVAC**
- **Environmental risks**
- **Fire risks**



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

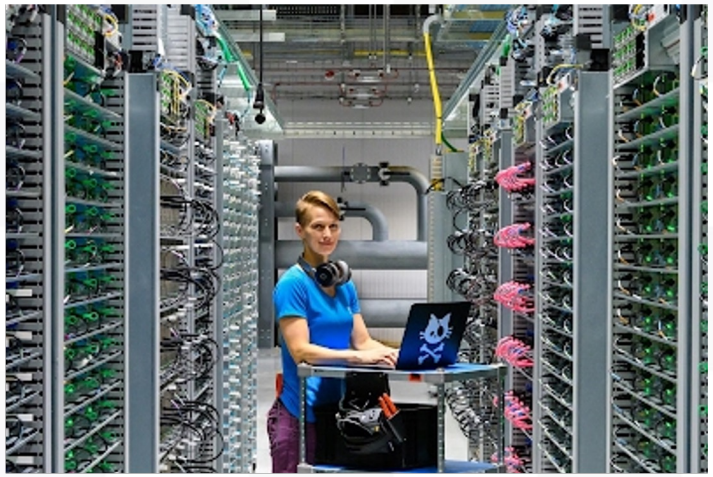
Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Server Rooms/Data Centers

These controls should cover, at a minimum, the following:

- **Personnel** (e.g., background checks, training, or access procedures)
- **Maintenance**
- **Logging, monitoring, and alerting**
- **Control testing and auditing**



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Server Rooms/Data Centers

Review the guidance available from organizations such as the following:

- American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)
- ANSI / BICSI: ANSI/BICSI 002-2014, Data Center Design and Implementation Best Practices
- Electronic Industries Association and Telecommunications Industries Association (EIA/TIA): ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers
- European Union (EU): EN 50600 series of standards
- International Organization for Standardization (ISO): ISO/IEC 30134 series, “Information technology – Data centres – Key performance indicators”
- Uptime Institute: Tier Standards

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Media Storage Facilities

Recommended Controls:

- Controlled and stable temperature and humidity
- Air filtration and positive air pressure to minimize infiltration by airborne dust and microfine particulate matter or contaminants (such as corrosive fumes and engine exhaust from diesel generators or nearby vehicles)
- Appropriate floor covering to minimize static electricity
- Careful siting of the media storage facilities to avoid magnetic fields that might arise from electrical equipment (e.g., transformers or motors)

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Media Storage Facilities

Other considerations with respect to media storage include the following:

- If the environment of the media storage facility is different (in temperature or humidity) than the production environment in which the tape will be read, then time must be allowed for the tape to acclimate to the different environment before being processed.
- Some tape media needs to be “retensioned” (i.e., unspooled and respooled), depending on the tape manufacturer's recommendations (e.g., every three years).
- For longer archival storage, it is advisable to read the data from the stored media and rerecord on new media. Again, the tape manufacturer's recommendations ought to be followed with respect to the appropriate frequency (e.g., every six years).
- Appropriate procedures are necessary for the tracking of media that are placed in, and removed from, storage. This may include bar code scanning and separation-of-duties controls requiring two people to sign in and sign out media items.
- Fire detection and suppression systems may need to be installed.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Media Storage Facilities

Other considerations with respect to media storage include the following:

- Proper housekeeping is required to reduce the possibility of fire and to reduce the fuel available should a fire break out. On a related note, media storage facilities ought to be used only to store media and should not be shared with other general storage.
- Depending on the risk analysis and costs associated with managing on- premises media storage, it may be appropriate to retain the services of an off-site media storage service that will handle the physical security and environmental concerns related to secure long-term storage of media. This can be used for all media, or a portion, in order to provide disaster recovery should the primary media storage facility be damaged by fire or other calamity.
- Appropriate media end-of-life procedures must be enforced to sanitize (e.g., by degaussing magnetic media) and securely destroy media before disposal so that sensitive information cannot be extracted from the media once it leaves the control of the organization.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

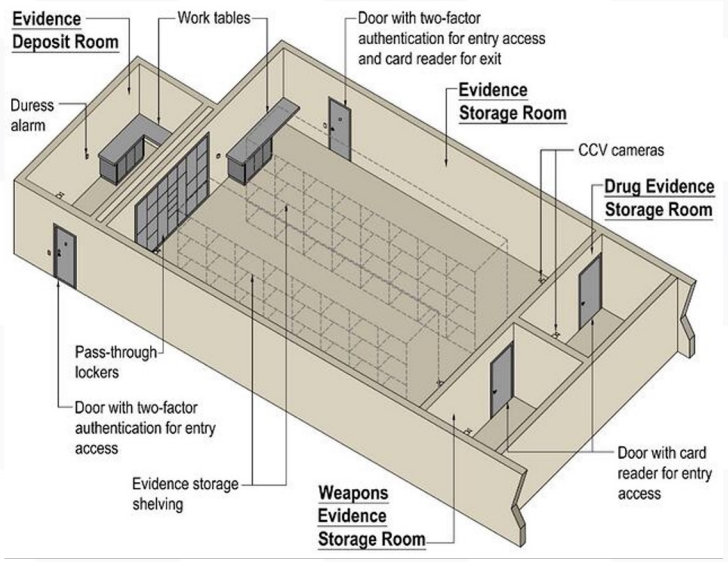
Apply Security Principles to Site and Facility Design

Design Site and Facility Security Controls

Evidence Storage

The evidence storage room include the following:

- **Strict policies surrounding who is permitted access** to the evidence storage room, the information that is to be entered into the log, and procedures governing the management of the access keys to the evidence storage room
- **Video monitoring**
- **Double locks on the evidence storage room doors**, or a locked storage cabinet inside the locked evidence storage room, with separation of duties surrounding the control of the keys, so that two people are required to access the evidence storage



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Work area security must be designed in response:

- **Risk assessment** (including threat modeling)
- **Security principles** and the appropriate controls to mitigate risk.
  The considerations to be addressed include:
  - **least privilege**
  - **need-to-know**
  - **separation of duties**
  - **dual control**
  - **defense in depth**
  - **compliance obligations**

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Least Privilege and Need-to-Know

- Access to restricted and secure areas must be granted only to the extent necessary for individuals to carry out their responsibilities, in accordance with formally approved policies and procedures.
- Access also must be periodically reviewed to ensure that the justification for access has not changed.
- Detailed auditable records attesting to the previous must be maintained.

Separation of Duties and/or Dual Control

- Depending on the risk assessment, it may be appropriate to require more than one authenticated staff member to be present in order to obtain access to the secure work area.
- Administrative control, verified through guard records or video surveillance, or it can be enforced through multiple locks or electronic access controls.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Defense in Depth

Mantrap - A preventive physical control with two doors. Each door requires a separate form of authentication to open

Bollard—A post designed to stop a car, typically deployed in front of building entrances

Smart card—A physical access control device containing an integrated circuit

Tailgating—Following an authorized person into a building without providing credentials

Perimeter Defenses - Help prevent, detect, and correct unauthorized physical access. Should employ defense-in-depth Fences, doors, walls, locks, etc.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Defense in Depth

Mantrap - A preventive physical control with two doors. Each door requires a separate form of authentication to open

Bollard—A post designed to stop a car, typically deployed in front of building entrances

Smart card—A physical access control device containing an integrated circuit

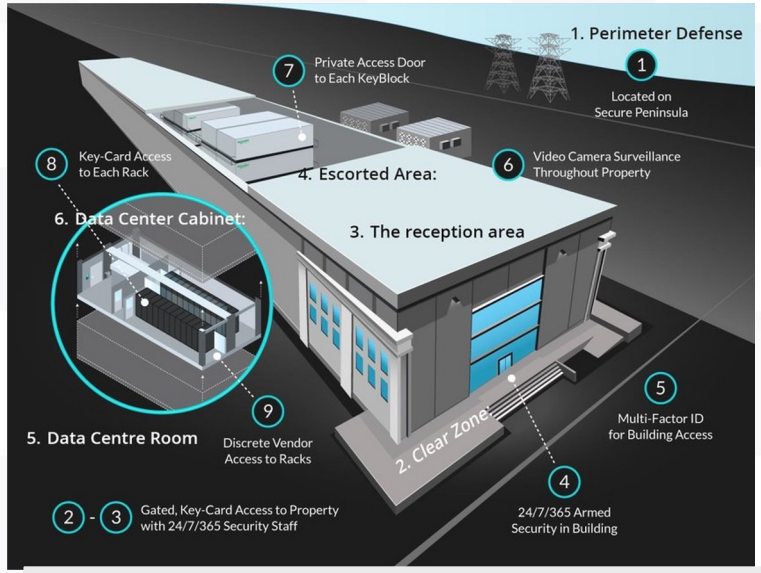
Tailgating—Following an authorized person into a building without providing credentials

Perimeter Defenses - Help prevent, detect, and correct unauthorized physical access. Should employ defense-in-depth Fences, doors, walls, locks, etc.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

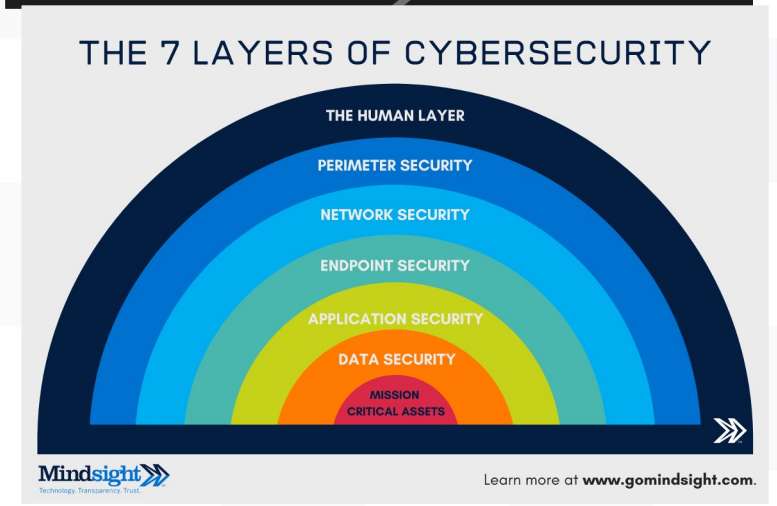
Restricted and Work Area Security



Defense in Depth

Different types of security controls ought to be considered for the higher security zones. In addition to preventive controls such as door locks, detective controls such as video monitoring and corrective controls such as motion detectors and alarms can be used as compensating controls should the primary preventive control (e.g., the door lock) fail or be compromised.

Multifactor authentication techniques are as valuable for physical access as for logical (e.g., login) access. Requiring a user to have an access card as well as enter a personal identification number (PIN) to unlock the door to higher security zones protects against loss of the access card and its use by an impostor. Requiring the card (and not the PIN alone) protects against shoulder-surfing by a threat actor observing staff enter their PINs.



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Restricted and Work Area Security

Compliance Obligations

Requirements for the following:

- Personnel identification Guards
- Electronic access control Electronic intrusion detection Video monitoring
- Interior access controls

One solution for having confidential discussions is the Sensitive Compartmented Information Facility (**SCIF**). SCIF is a common term among U.S. and British military and governmental agencies with a need for isolated space to preserve confidentiality.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Controls

- Designed to provide a safe environment for personnel and equipment
- Power, HVAC, and fire safety are considered environmental controls

Electricity

- Reliable electricity is critical for any data center
- One of the top priorities when selecting, building, and designing a site

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Types of Electrical Faults

- All types of electrical faults can impact availability and integrity
- The following are common types of electrical faults:
  - **Blackout: prolonged loss of power**
  - **Brownout: prolonged low voltage**
  - **Fault: short loss of power**
  - **Surge: prolonged high voltage**
  - **Spike: temporary high voltage**
  - **Sag: temporary low voltage**

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Battery UPS systems can differ in a number of important aspects:

- **Load**: The capacity of the unit to deliver a specified level of continuous power
- **Capacity**: The time during which the unit can maintain the load
- **Filtering**: The ability of the unit to isolate the equipment from noise,surges, and other problems with the utility power Reliability: Some designs trade low cost for reliability

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

With both power (UPS and generator) and HVAC systems, due consideration has to be made for the following:

- **Regularly scheduled maintenance**
- **Regular testing under full load** (of UPS and generators, and backup HVAC equipment if not used in production)
- **System fault detection and alerting** (and regular tests of those subsystems)
- **Periodic checks and audits** to ensure all of the above are being properly and regularly performed

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Surge Protectors, UPSs, and Generators

Provide protection against electrical failures

Surge Protectors

- Protect equipment from damage due to electrical surges
- Contain a circuit or fuse which is tripped during a power spike or surge, shorting the power or regulating it down to acceptable levels

Uninterruptible Power Supplies

- Provide temporary backup power in the event of a power outage
- May also “clean” the power, protecting against surges, spikes, and other forms of electrical faults
- Backup power is provided via batteries or fuel cells
- Provide power for a limited period of time, and can be used as a bridge to generator power; generators typically take a short period of time to start up and begin providing power

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Generators

- Designed to provide power for longer periods of times than UPSs
- Will run as long as fuel is available
- Sufficient fuel should be stored onsite for the period the generator is expected to provide power
- Refueling strategies should consider a disaster's effect on fuel supply and delivery
- Generators should not be placed in areas which may flood or otherwise be impacted by weather events
- Should be tested and serviced regularly.
- http://www.cumminspower.com/www/literature/technicalpapers/PT-7006-Standby-Katrina-en.pdf

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

TIER LEVEL	AVAILABILITY %	REDUNDANCY
1	99.671	None. Multiple single points of failure.
2	99.741	Some. Nonredundant (e.g., N) UPS.
3	99.982	N+1 UPS. Able to take equipment out of service for maintenance without affecting operation.
4	99.995	2N UPS. No single point of failure, able to automatically compensate for any single failure.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

With both power (UPS and generator) and HVAC systems, due consideration has to be made for the following:

- Regularly scheduled maintenance
- Regular testing under full load (of UPS and generators, and backup HVAC equipment if not used in production)
- System fault detection and alerting (and regular tests of those subsystems)
- Periodic checks and audits to ensure all of the above are being properly and regularly performed

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Issues

Environmental issues that need to be considered include the likelihood of the following:

- Major storms (hurricanes, lightning, blizzards, ice storms, typhoons, tornadoes, blizzards, etc.)
- Earthquakes
- Floods and tsunamis Forest fires
- Internal building risks Vermin and wildlife
- Volcanoes

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Issues

Environmental issues that need to be considered include the likelihood of the following:

- Major storms (hurricanes, lightning, blizzards, ice storms, typhoons, tornadoes, blizzards, etc.)
- Earthquakes
- Floods and tsunamis Forest fires
- Internal building risks Vermin and wildlife
- Volcanoes

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Environmental Issues

Mitigations include the following:

- Monitoring announcements from public health authorities
- Having a sick-leave policy that does not incentivize employees to come to work ill
- Developing a plan to operate with: a reduced workforce; employees working from home; or work shifted to office locations less affected (in the case of larger companies with multiple offices)

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Utilities and Heating, Ventilation, and Air Conditioning

Cloud Computing and Availability

- **Organizations that want to take availability a step further use hybrid/multicloud deployments** so that they don't rely on a single CSP for their operations.

- The **availability increases that highly redundant data centers** can provide are impressive, with cloud providers claiming 99.99 percent or higher availability. That number is useful only if organizations also ensure that they will be able to access cloud providers that are highly available.
- **Redundant network routes and hardware that can stay online** through a local or regional disaster are a necessary part of cloud hosting availability designs that can take full advantage of these highly available remote infrastructures.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Human safety is paramount, and any fire safety system must be designed first and foremost to protect the lives and health of those who work in the facility. Enabling occupants to safely exit the building and ensuring that fire suppression systems are unlikely to compromise health or safety are more important than protecting systems and buildings.

Balance the costs of the following:

- Downtime
- Restoration costs
- Fire suppression system costs (capital and ongoing maintenance)

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Most jurisdictions have standards and guidelines for the fire protection systems for IT equipment:

- **Canada and the United States: NFPA 75, "Standard for the Fire Protection of Information Technology Equipment," and NFPA 76, "Fire Protection of Telecommunications Facilities."**
- **UK: BS 6266:2011, "Fire protection for electronic equipment installations." Code of practice.**
- **Germany: The VdS series of guidelines for fire protection and suppression.**

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Heat, Flame, and Smoke Detectors

- Three methods for detecting fire
- Typically alert locally, and may also be centrally monitored by a fire alarm system
- An audible alarm and flashing lights should be used, so that both deaf and blind personnel will be aware of the alarm

Heat Detectors

- Alert when temperature exceeds an established safe baseline
- May trigger when a specific temperature is exceeded or when temperature changes at a specific rate (such as “10 °F in less than 5 minutes”)

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Smoke Detectors

- Work through two primary methods: ionization and photoelectric
- Ionization-based smoke detectors contain a small radioactive source which creates a small electric charge
- Photoelectric sensors work in a similar fashion, except that they contain an LED (Light Emitting Diode) and a photoelectric sensor that generates a small charge while receiving light
- Both types of alarm alert when smoke interrupts the radioactivity or light, lowering or blocking the electric charge
- Dust should always be avoided in data centers. Small airborne dust particles can trigger smoke detectors just as smoke does, leading to false alarms.

Flame Detectors

- Detect infrared or ultraviolet light emitted in fire
- One drawback to this type of detection is that the detector usually requires line-of-site to detect the flame; smoke detectors do not have this limitation

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Safety Training and Awareness

- Training provides a skill set such as learning to operate an emergency power system
- Awareness changes user behavior (“Don't let anyone follow you into the building after you swipe your access card”)

Evacuation Routes

- Evacuation routes should be prominently posted
- All personnel should be advised of the quickest evacuation route from their areas
- Guests should be advised of evacuation routes as well
- All sites should use a meeting point, where all personnel will meet in the event of emergency

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Evacuation Roles and Procedures

- The two primary evacuation roles are safety warden and meeting point leader
- The safety warden ensures that all personnel safely evacuate the building in the event of an emergency or drill
- The meeting point leader assures that all personnel are accounted for at the emergency meeting point
- Special care should be given to any personnel with handicaps, which could affect egress during an emergency
- Elevators should never be used during a fire
- All sites should have mitigating controls to allow safe egress for all personnel

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

ABCD Fires and Suppression

- Fire suppression systems are used to extinguish fires
- Different types of fires require different suppressive agents
- Class K fires are kitchen fires, such as burning oil or grease. Wet chemicals are used to extinguish class K fires.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Fires are categorized by the type of fuel:

- **Class A**: Ordinary solid combustibles (e.g., paper, wood, and plastic) Class B: Flammable liquids and gases (e.g., gasoline)
- **Class C**: Energized electrical equipment
- **Class D**: Combustible metals (e.g., lithium metal, but not lithium-ion batteries, which are considered Class B, although water will also work well with Li-ion battery fires)
- **Class F or K**: Cooking oils and greases

BusinessWatch Type Fire Type / Extinguisher Type	Class A Organic Materials (e.g Paper & Coal)	Class B Flammable Liquids (e.g Petrol & Paint)	Class C Flammable Gases (e.g Butane & Methane)	Class D Flammable Metals (e.g Lithium & Magnesium)	Electrical Electrical Equipment (e.g Computers & Servers)	Class F Cooking Oils (e.g Olive Oil & Fat)	Businesses that may need this type of Extinguisher
Water	✓	✗	✗	✗	✗	✗	- Schools - Hospitals - Offices - Shops
Foam	✓	✓	✗	✗	✗	✗	- Apartments - Hospitals - Offices - Shops
Dry Powder	✓	✓	✓	✓	✓	✗	- Garages - Welding - Boiler Rooms - LPG Plants
CO2	✗	✓	✗	✗	✓	✗	- Server Rooms - Offices
Wet Chemical	✓	✗	✗	✗	✗	✓	- Kitchens - Canteens

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

Make sure they know the following information:

- Where all the exits are (so they know the closest, and if blocked, the alternates)
- Where all the fire extinguishers are located as well as how and when to use them (different types of fire extinguishers are appropriate for different types of fires)
- How to disable (or delay the discharge of) the fire suppression system should a false fire detection be suspected
- How to manually trip the fire suppression system (in the case of gaseous suppression and some sprinkler systems) should early signs of fire be detected by staff before the fire detectors are triggered
- Where the fire alarm pull stations or call points are How to manually shut off power to the data center

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Apply Security Principles to Site and Facility Design

Fire Prevention, Detection, and Suppression

HOLY MOLY! That was a long Domain with a lot of information!

We are ½ way for todays session!

LET'S DO THIS!

Picking up where we left off.

CHAPTER

5

Domain 4: Communication and Network Security (Designing and Protecting Network Security)

WHAT ARE WE GOING TO COVER?

Agenda – Domain 4: Communication and Network Security

- Network Architecture and Design
- Secure Network Devices and Protocols
- Secure Communications

Starting on page 283 this evening

Great domain for the techies. A little more challenging for the “normal” people…

LECTURE

Network Architecture and Design

Network Defense-in-Depth

- Assume that an attacker has already compromised your perimeter.
- Network segmentation, isolation, etc.
- NSA Methodology for Adversary Obstruction (not testable, but great guidance) - https://www.cdse.edu/documents/cdse/nsa-methodology-for-adversary-obstruction.pdf

LECTURE

Network Architecture and Design

Network Defense-in-Depth

- Assume that an attacker has already compromised your perimeter.
- Network segmentation, isolation, etc.
- NSA Methodology for Adversary Obstruction (not testable, but great guidance) - https://www.cdse.edu/documents/cdse/nsa-methodology-for-adversary-obstruction.pdf

LECT

Networl

Networl

- Ass
  per
- Net
- NS
  gre
  me

National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

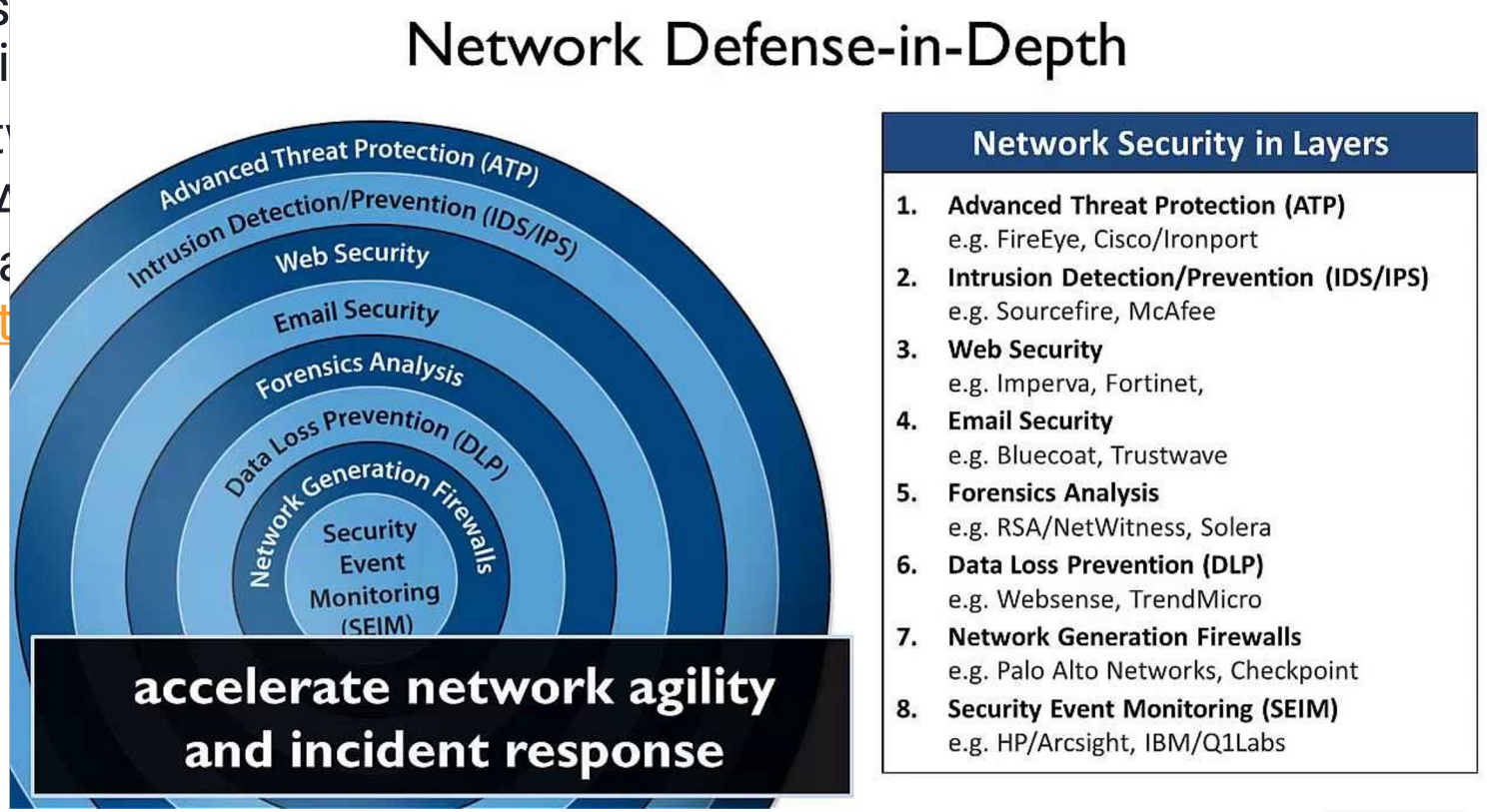
NSA Methodology for Adversary Obstruction

LECTURE

Network Architecture and Design

Network Defense-in-Depth

- Ass
  peri
- Net
- NSA
  grea
  met



Network Security in Layers

1. **Advanced Threat Protection (ATP)**
   e.g. FireEye, Cisco/Ironport
2. **Intrusion Detection/Prevention (IDS/IPS)**
   e.g. Sourcefire, McAfee
3. **Web Security**
   e.g. Imperva, Fortinet,
4. **Email Security**
   e.g. Bluecoat, Trustwave
5. **Forensics Analysis**
   e.g. RSA/NetWitness, Solera
6. **Data Loss Prevention (DLP)**
   e.g. Websense, TrendMicro
7. **Network Generation Firewalls**
   e.g. Palo Alto Networks, Checkpoint
8. **Security Event Monitoring (SEIM)**
   e.g. HP/Arcsight, IBM/Q1Labs

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

LANs, WANs, MANs, GANs, PANs…

- **PAN**s are Personal Area Networks
  - Typically, a range of 100 meters or much less
  - Low-power wireless technologies such as Bluetooth use PANs.
- **LAN** is a Local Area Network
  - A comparatively small network
  - Typically confined to a building or an area within one
- **MAN** is a Metropolitan Area Network
  - Typically confined to a city, a zip code, a campus, or office park
- **WAN** is a Wide Area Network
  - Typically covering cities, states, or countries
- **GAN** is a Global Area Network; a global collection of WANs.
  - Also called the **internet**

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

… Internet, intranet, extranet, DMZ, VLAN, SDN

- **Internet** is a globally connected WAN
  - enables communication over vast geographical regions
- **Intranet** is a local or restricted network
  - Enables users to store or share information across their organizations
- **Extranet** is an externally facing web portal
  - Allows organizations to share select information with others
- ***Demilitarized zone*** (DMZ) a partially controlled area between the internet and a fully protected intranet
  - Used when a section of your intranet is public-facing
- **VLAN** are Virtual Area Networks
  - Isolated broadcast zones to segment a network
- **SDN** is a Software Defined Network
  - Software instances of a physical network
  - Used in virtualization

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Packet-Switched Networks

- Instead of using dedicated circuits, **data is broken into packets**, each sent individually
- If multiple routes are available between two points on a network, packet switching can choose the **best route**, and fall back to secondary routes in case of failure
- Packets may take any path (and different paths) across a network, and are then reassembled by the receiving node
- Missing packets can be retransmitted, and out of-order packets can be re-sequenced.
- Unlike circuit-switched networks, packet-switched networks make unused bandwidth available for other connections

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Packet-Switched Networks

- Instead of using dedicated circuits, data is broken into packets, each s
- If mult work, packe seco
- Packe netwo
- Missi kets can be
- Unlike make

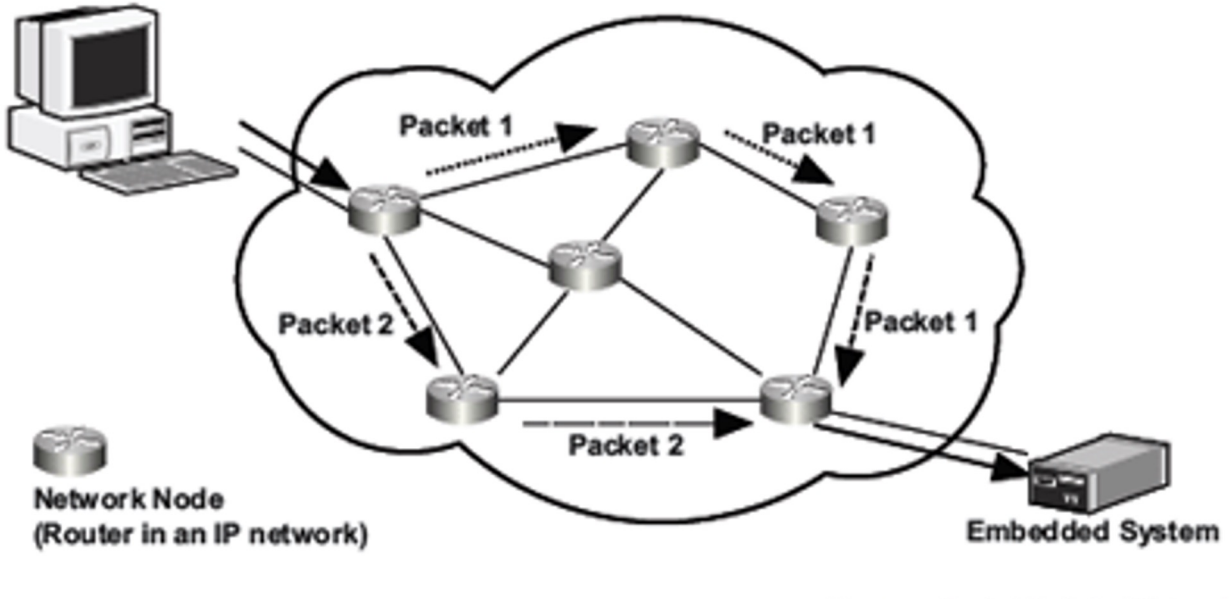


Figure 2-2 Packet Switched Network

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

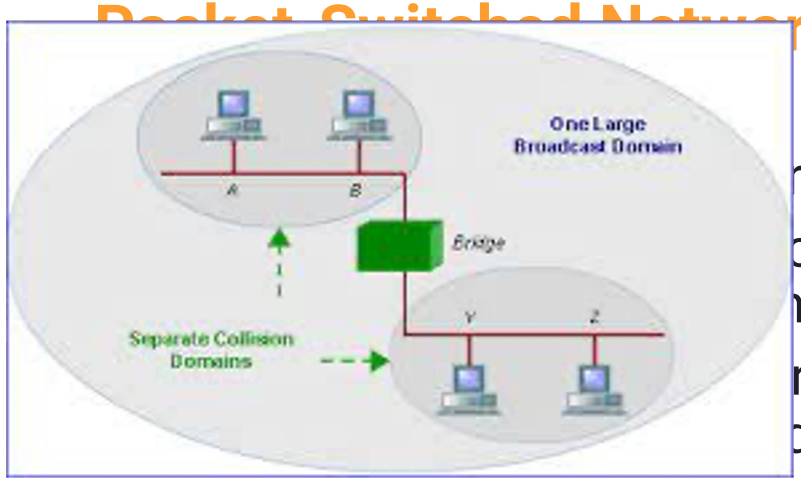
Packet-Switched Networks

- *Collision domain*
  - A part of the network where packet collisions can occur
  - Network collisions can occur when two deices send packets at the same time on the shared network
  - The packets interfere with each other (or "*collide*"), and both devices are required to resend their packets
    - Causing reduced network efficiency
  - On each port on a bridge, switch, or router is a separate collision domain, but all ports on a hub share the same collision domain

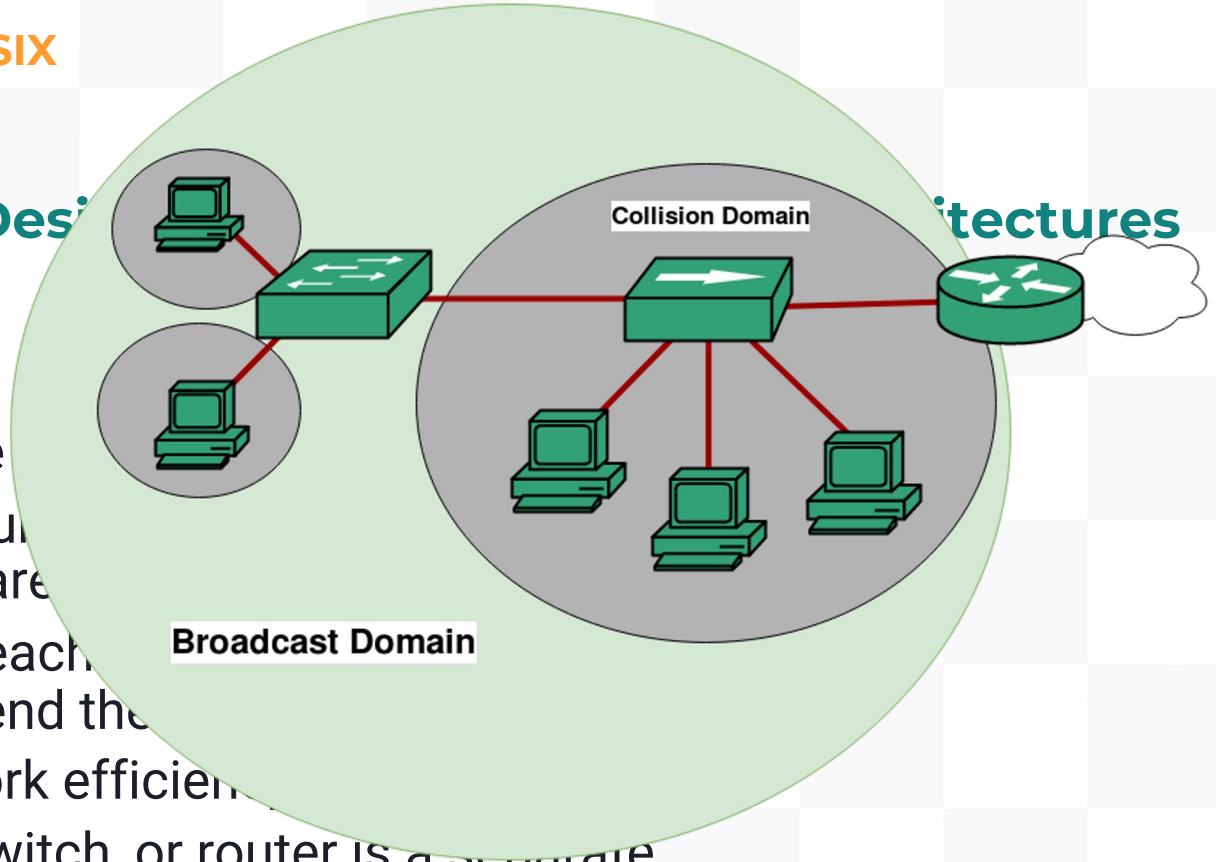
LECTURE

Assess and Implement Secure Desi… …itectures

…Packet-Switched Networks…rks



- …rk where …
  - …can occu…
  - …n the share…
  - …re with each…
  - …d to resend the…
  - Causing reduced network efficien…
- On each port on a bridge, switch, or router is a separate collision domain, but all ports on a hub share the same collision domain



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Layered Design

- Models such as OSI and TCP/IP
- Each layer performs a specific function
- The complexity of each layer's functionality is contained within its layer
- Changes in one layer do not directly affect another: changing your physical network connection from wired to wireless (at Layer 1) has no effect on your Web browser (at Layer 7)

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Models and Stacks

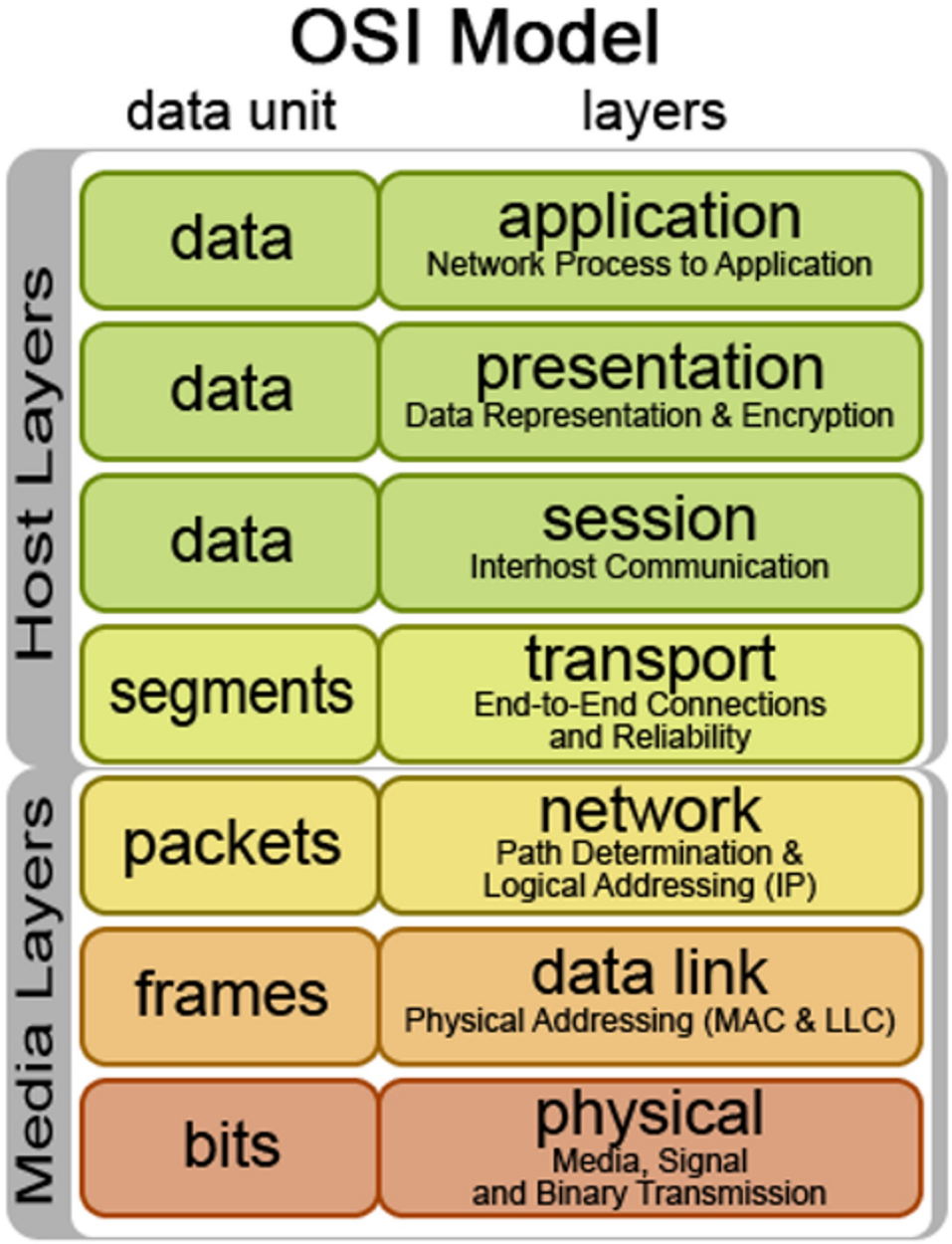
- A **network model is a description of how a network protocol suite operates**
- A **network stack is a network protocol suite** programmed in software or hardware
- **Protocol** - set of **rules** that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model

- OSI (Open System Interconnection) Reference Model is a layered network model
- The model is abstract: we do not directly run the OSI model in our systems
- Used as a reference point, so “Layer 1” (physical) is universally understood
- Has seven layers
- Developed by International Organization for Standardization (ISO)
- Formally called “X.200: Information technology—Open Systems Interconnection—Basic Reference Model.” - downloaded for free at: http://www.itu.int/rec/T-REC-X.200-199407-I/en



esign Principles in Network Architectures

on

t d

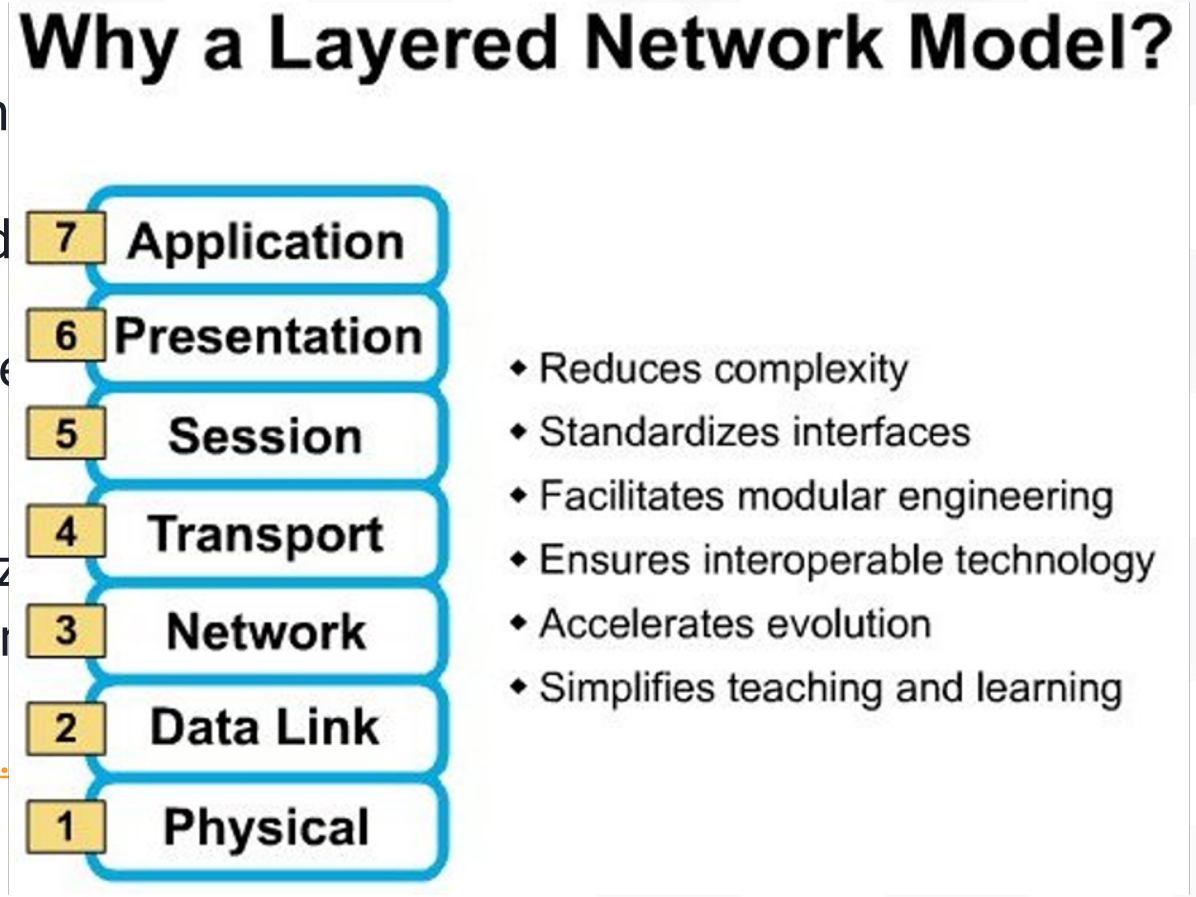
aye

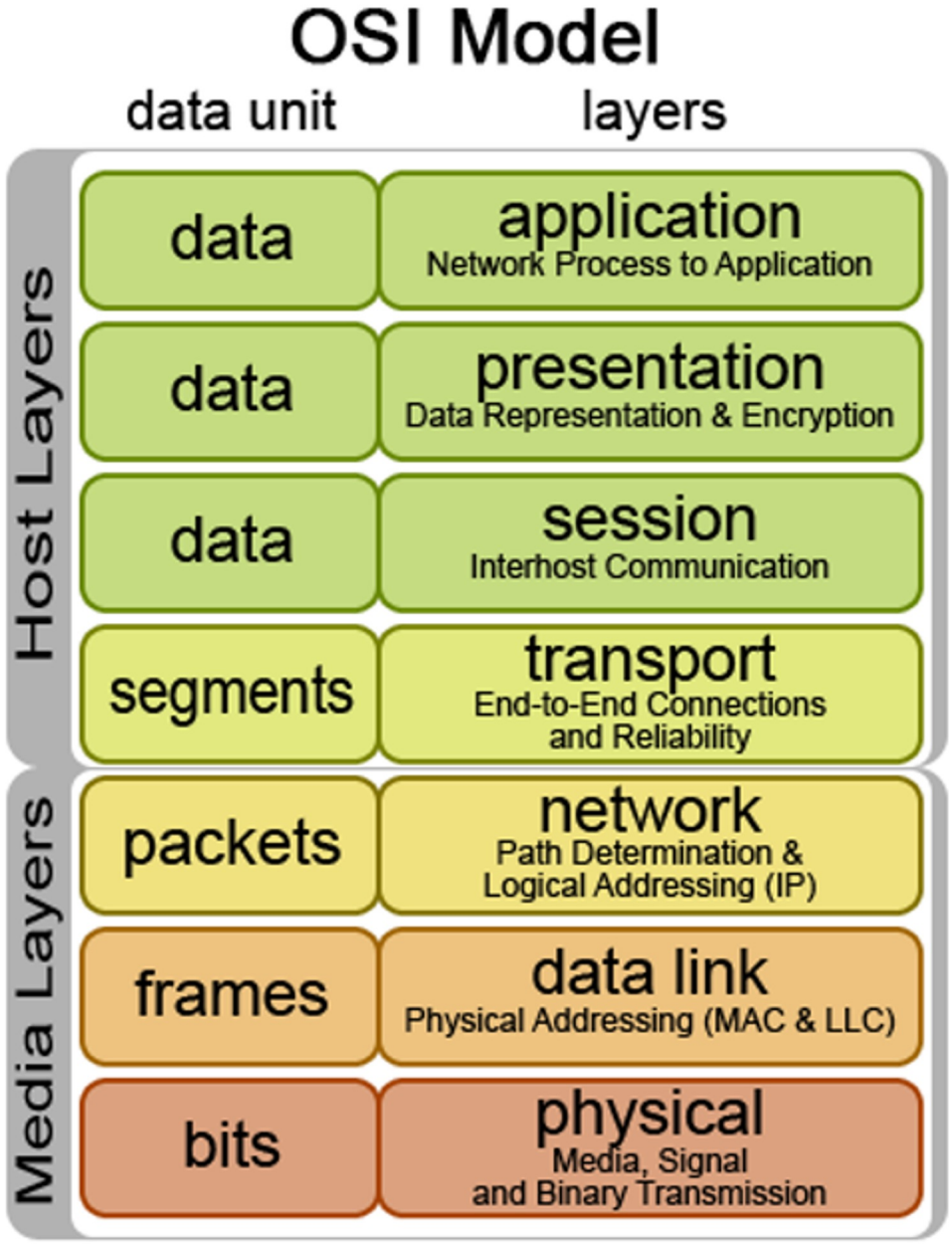
niz

ion

ce

-X.





esign Principles in Network Architectures

on) Reference Model is a layered

t directly run the OSI model in our

ay

n

ion technology—Open Systems
:e Model." - downloaded for free
-X.200-199407-I/en

People don't need to see Paula Abdul

People don't need those stupid packets anyway.

Please Do Not Teach Students Pointless Acronyms

Please Do Not Take Sales People's Advice.

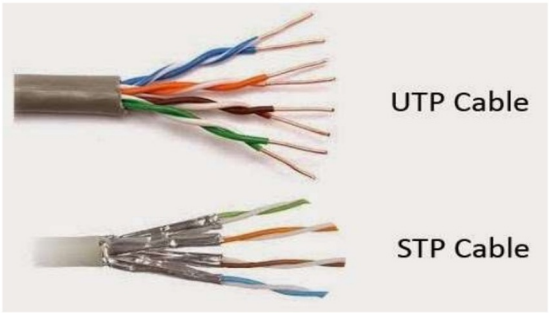
LECTURE

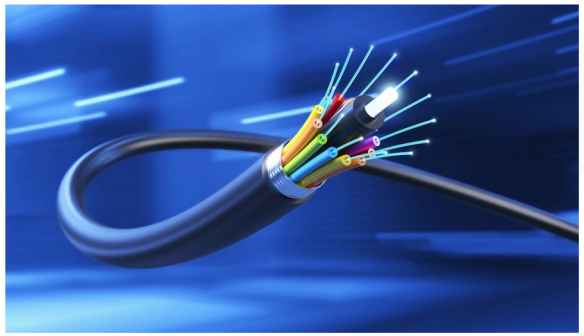
Assess and Implement Secure Design Principles in Networl

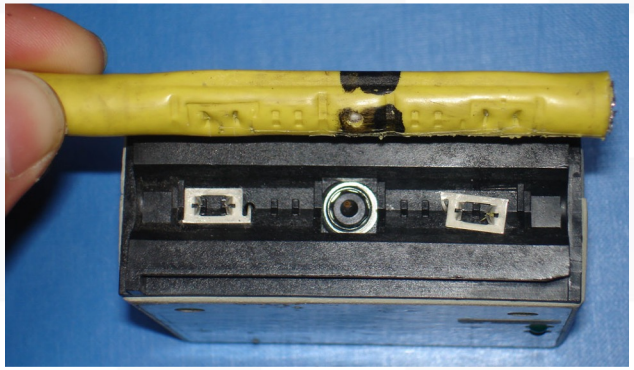
The OSI Model - Layer 1: Physical

- Describes units of data such as bits represented by energy (such as light, electricity, or radio waves) and the medium used to carry them (such as copper or fiber optic cables)
- Cabling standards such as Thinnet, Thicknet, and Unshielded Twisted Pair (UTP) exist at layer 1, among many others
- **Layer 1 devices include hubs and repeaters**

"Dumb" devices (no logic)





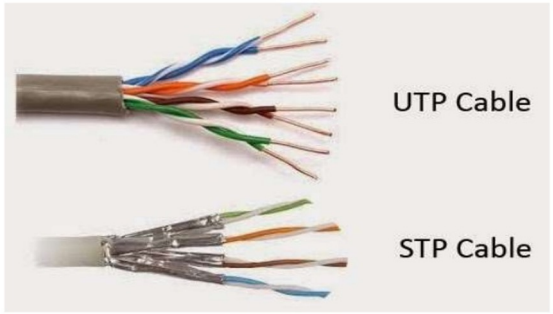


LECTURE

Assess and Implement Secure Design Principles in Networl

The OSI Mo

- Describ ch as light, rry them (s
- Cabling Twisted
- **Layer 1**



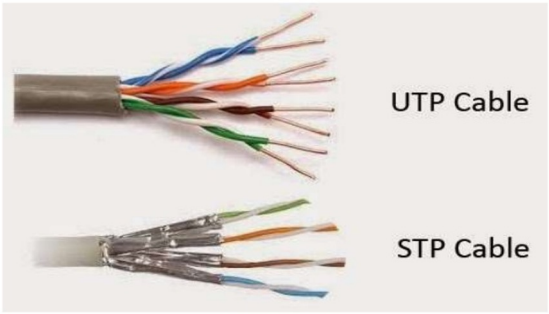
7	Application	Network Processes to Applications
6	Presentation	Data Representation
5	Session	Interhost Communication
4	Transport	End-to-end Connections
3	Network	Address and Best Path
2	Data Link	Access to Media
1	Physical	Binary Transmission • Wires, connectors, voltages, data rates

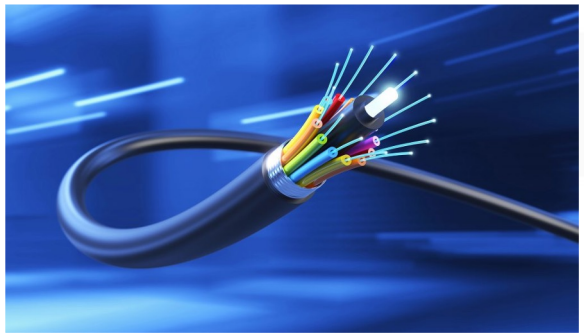
LECTURE

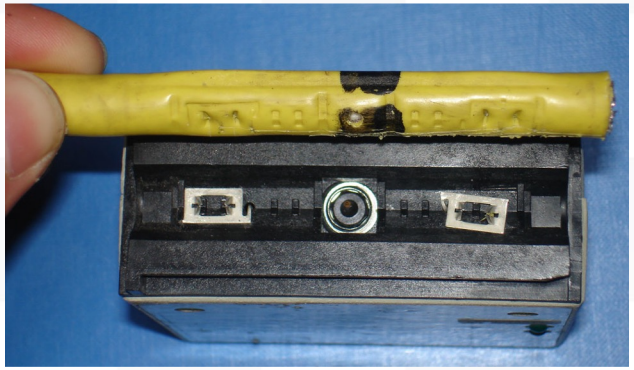
Assess and Implement Secure Design Principles in Networl

The OSI Model - Layer 1: Physical Attack Vectors

- Attackers might want to penetrate devices or connection media or interfere with operations
  - Passive sniffing either over the cable or wireless
  - Cause excessive electrical interreference
    - Jamming
  - Cutting the cable







LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 2: Data link

- Handles access to the physical layer as well as local area network communication
- An Ethernet card and its MAC (Media Access Control) address are at Layer 2, as are switches and bridges.
- Divided into two sub-layers:
  - Media Access Control (MAC) - transfers data to and from the physical layer - touches Layer 1
    - 12-digit long number – prefix or first 6 assigned to manufacturers by IEEE, second half represent serial number
  - Logical Link Control (LLC) -handles LAN communications - touches Layer 3
    - Facilitates node-to-node flow control and error management
      - ARQ – Automatic Repeat Request

Also called a "hardware address"

Switches and bridges work here. A little less dumb.

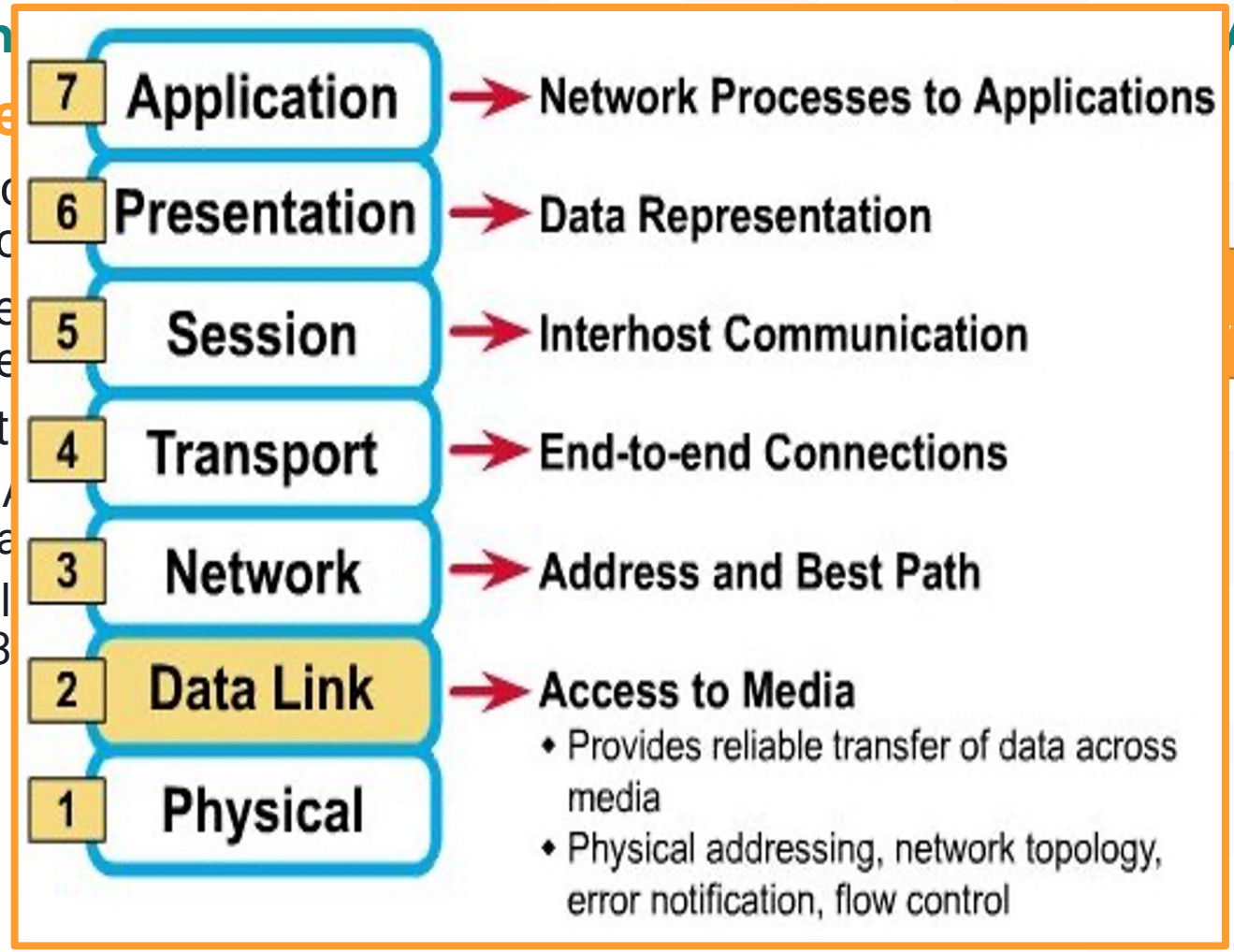
LECTURE

Assess and Im

Architecture

The OSI Mode

- Handles ac
  network cc
- An Etherne
  are at Laye
- Divided int
  - Media A
    physica
  - Logical
    Layer 3



Also called a "hardware address"

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 2: Data link Attack Vectors

- Forging MAC addresses (aka *Address Resolution Protocol [ARP] spoofing*)
  - By forging ARP requests or replies, an attacker can fool data layer switching to redirect network traffic intended for legitimate hosts to an attacker's machine
  - ARP spoofing is a common precursor to man-in-the-middle (MITM) [can also be called machine-in-the-middle] attacks and session hijacking

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network

- Describes routing: moving data from a system on one LAN to a system on another
- IP addresses and **routers**
- Protocols include IPv4 and IPv6, among others.

Also called a “logical address”

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network

- **Internet Protocol (IP)** – is a set of requirements for addressing and routing data across networks, including the internet
- **Addressing** – IP facilitates transmission of data from host to destination IP address, traversing the network until the destination is located and reached
- **Host addressing** – each host has a unique address to provide its logical location on the internet; its IP address
- **Message Forwarding** – gateways or routers are special-purpose devices or hosts on the network that forward data between networks that are segmented
- **Fragmentation** – packet sizes can be large and complex; the network layer facilitates the subdivision of a packet into a manageable or allowable size without the loss of integrity
- **Internet Protocol Security (IPSec)** – when implemented, secure communication using virtual private networks (VPNs) and encryption is made possible by this set of protocols that provides for IP.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network

- Border Gateway Protocol
  - *Autonomous System* (AS) is a large network or group of networks managed or controlled by a single entity or organization
  - BGP is a path-vector routing protocol used between separate ASs; external BGP (eBGP) used between ASs (eg. ISPs), internal BGP (iBGP) used within a single autonomous system
  - Chooses the shortest path through the internet by navigating the least number of ASs along the route;
  - Routing Information Base (RIB) stores multiple paths across the internet, and can silently update/remove routes without notifying peers

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network

- Routing Information Protocol Versions 1 and 2 (RIP)
  - Early routing protocol; first to use distance-vector routing mothed
  - Uses counts of hop that a signal makes along the network path (max 15)
  - In addition to hop count, RIP considers the below to prevent route looping
    - Split horizon – prevents a route being directed backwards
    - Route poisoning – sets the hop count to at 16 for failed routes
    - Hold-down timers – if a bad route is received it will pause advertising or accepting new routes during this time

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network

- Open shortest path first v 1 & v2 (OSPF)
  - A link-state protocol, one of the interior gateway protocols (IGPs)
  - Gathers information from nearby routing devices and creates a network topology, making changes when detect and automatically rerouting
  - Computes traffic load and seeks to balance it
  - Encapsulates data directly in IP packets at protocol number 89 , so does not use UDP/TCP

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network

- Internet Control Message Protocol (ICMP)
  - 3 field that distinguish the type and code of the ICMP packet and those values never change in transit.
  - Uses include manual troubleshooting (ping utility), network diagnostics (traceroute utility) and system-generated error messages during IP transmissions

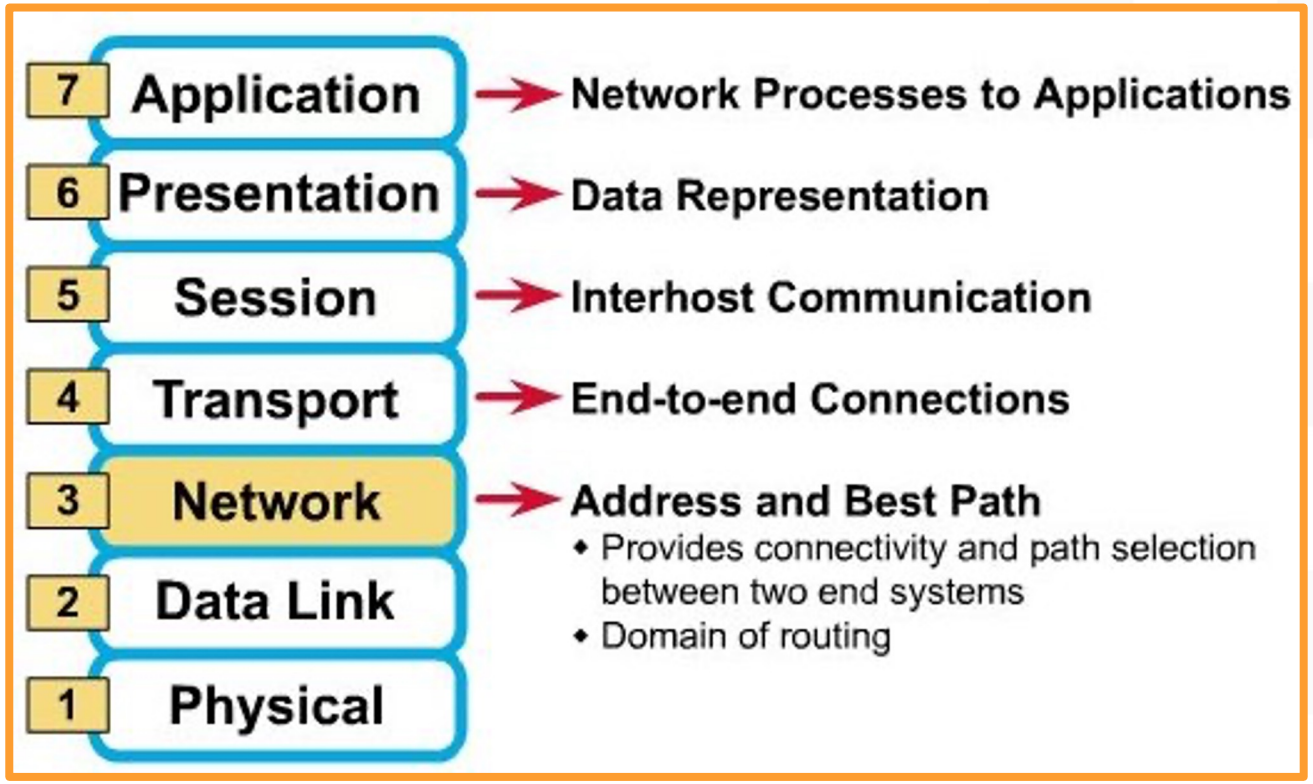
- Internet Group Management Protocol (IGMP)
  - Operates at the network layer, but specific to a host or a router in a group
  - Key protocol for multicasts protocol

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network

Also called a “logical address”



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 3: Network Attack Vectors

- MITM attacks involving traffic being redirects to a malicious actors
- Spoofing or forging network addresses
- Denial of service (DoS) by overwhelming target with resources

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 4: Transport

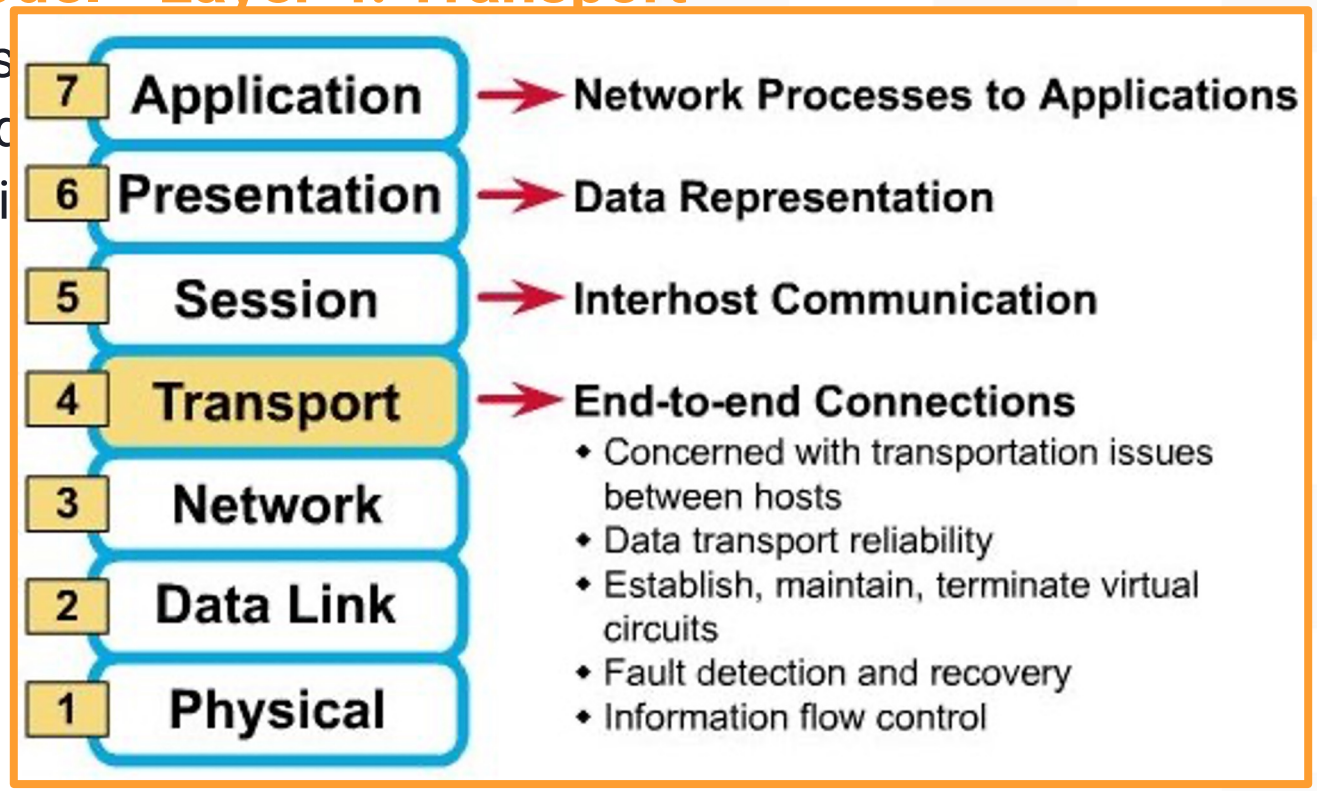
- Handles packet sequencing, flow control, and error detection
- TCP and UDP are Layer 4 protocols
- Resending or re-sequencing packets

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 4: Transport

- Handles
- TCP and
- Resendi



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 4: Transport Attack Vectors

- SYN Floods that drains resources by initiating TCP connections, creating a DoS
- Trojans and malware target specific TCP/UDP ports
- Session hijacking

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 5: Session

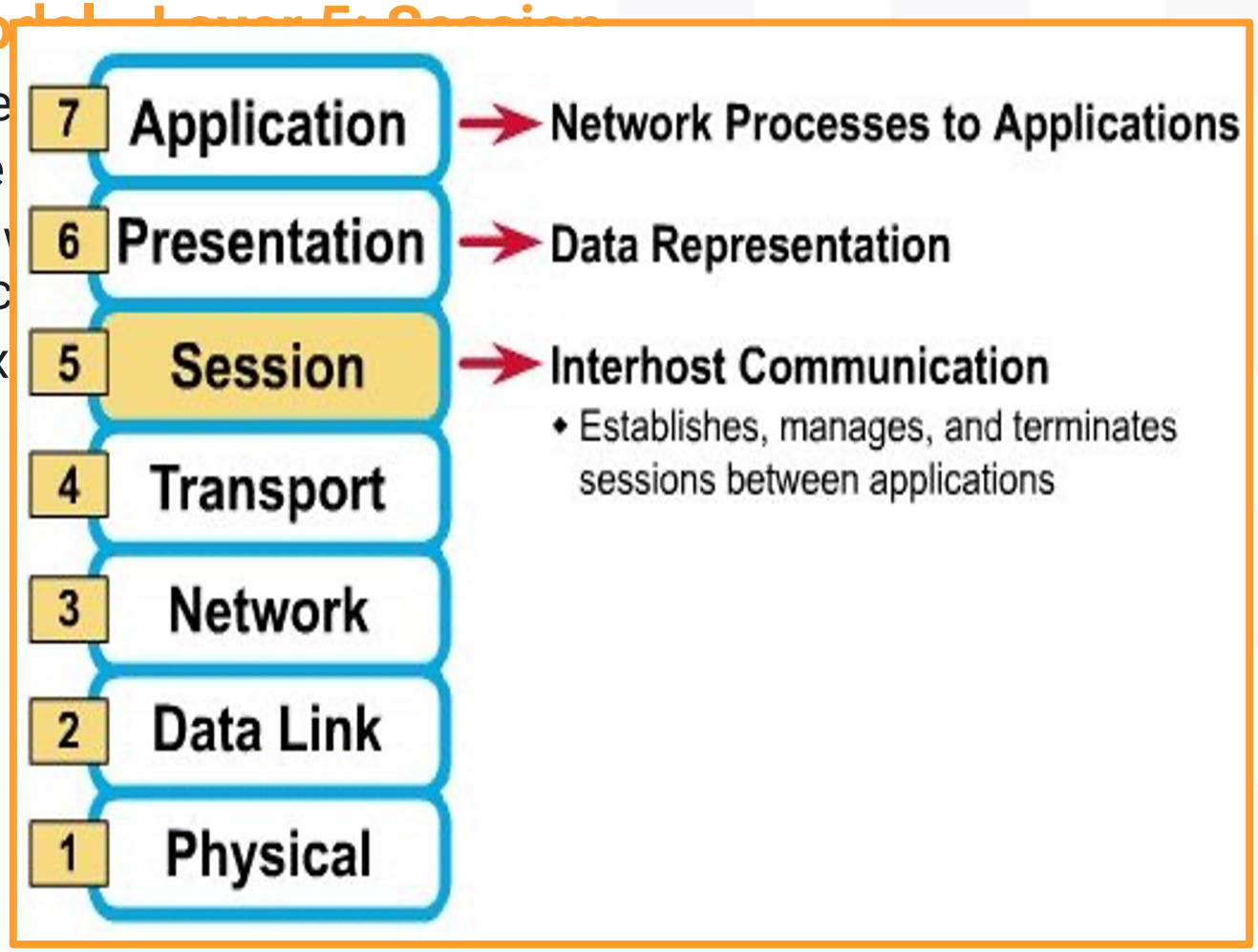
- Manages sessions, providing maintenance on connections
- Remote Procedure Calls (RPCs)
- A good way to remember the session layer's function is "connections between applications"
- Simplex, half-duplex, and full-duplex communication.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Mo… Layer 5: Session

- Manage…
- Remote…
- A good … "connec…
- Simplex…



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 5: Session Attack vectors

- Not a common target for attacks
- Weakness in the deprecated Secure Socket Layer (SSL) or less secure versions of Transport Layer Security (TLS) could be target

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 6: Presentation

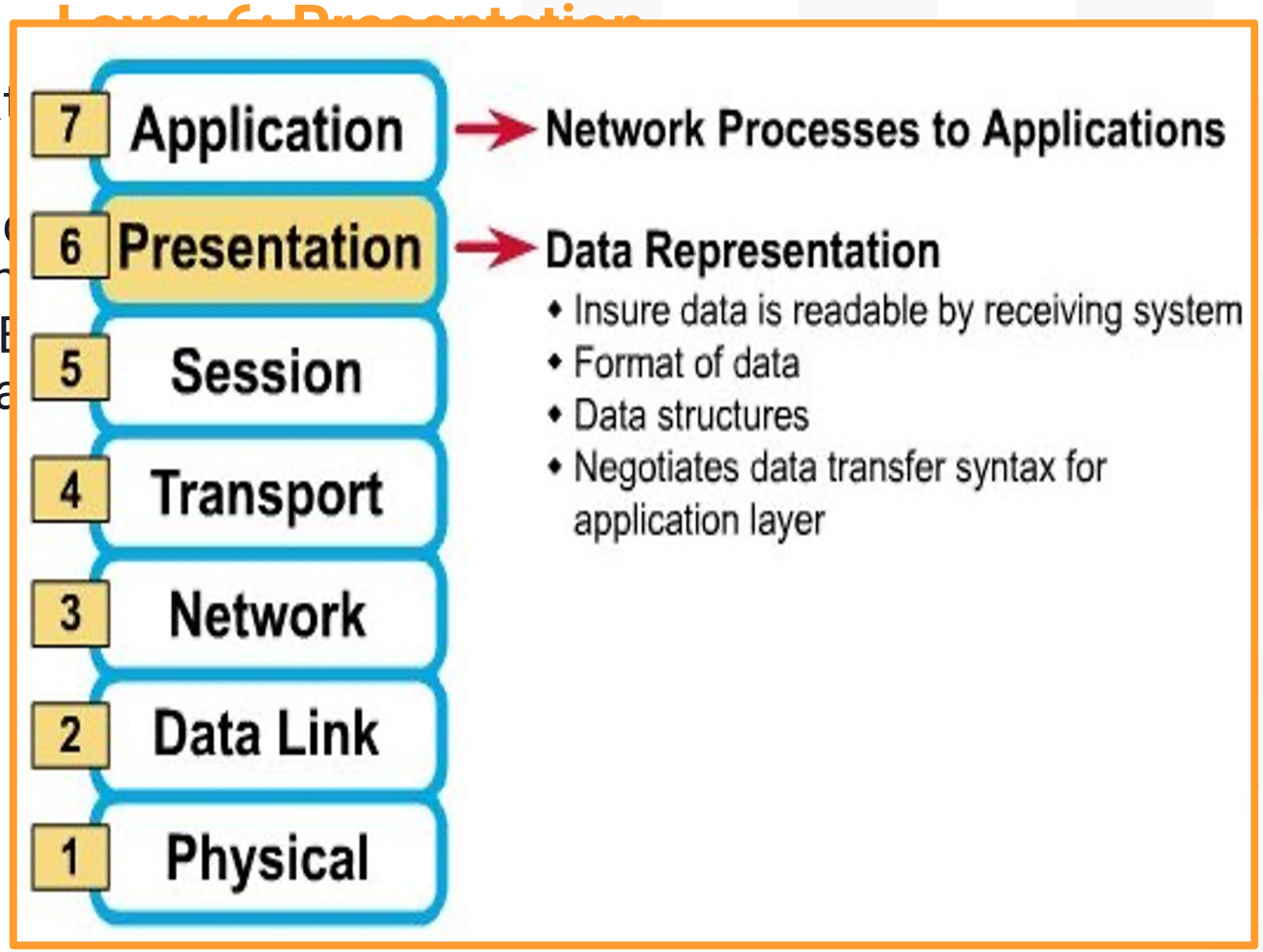
- Presents data to the application (and user) in a comprehensible way
- Concepts include data conversion, characters sets such as ASCII, and image formats such as GIF (Graphics Interchange Format), JPEG (Joint Photographic Experts Group), and TIFF (Tagged Image File Format)

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model – Layer 6: Presentation

- Presents dat
  way
- Concepts in
  ASCII, and in
  Format), JPE
  (Tagged Ima



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 6: Presentation Attack Vectors

- most common attacks involve encryption schemes using cryptographic and cryptanalytic attacks covered in Chapter 3

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 7: Application

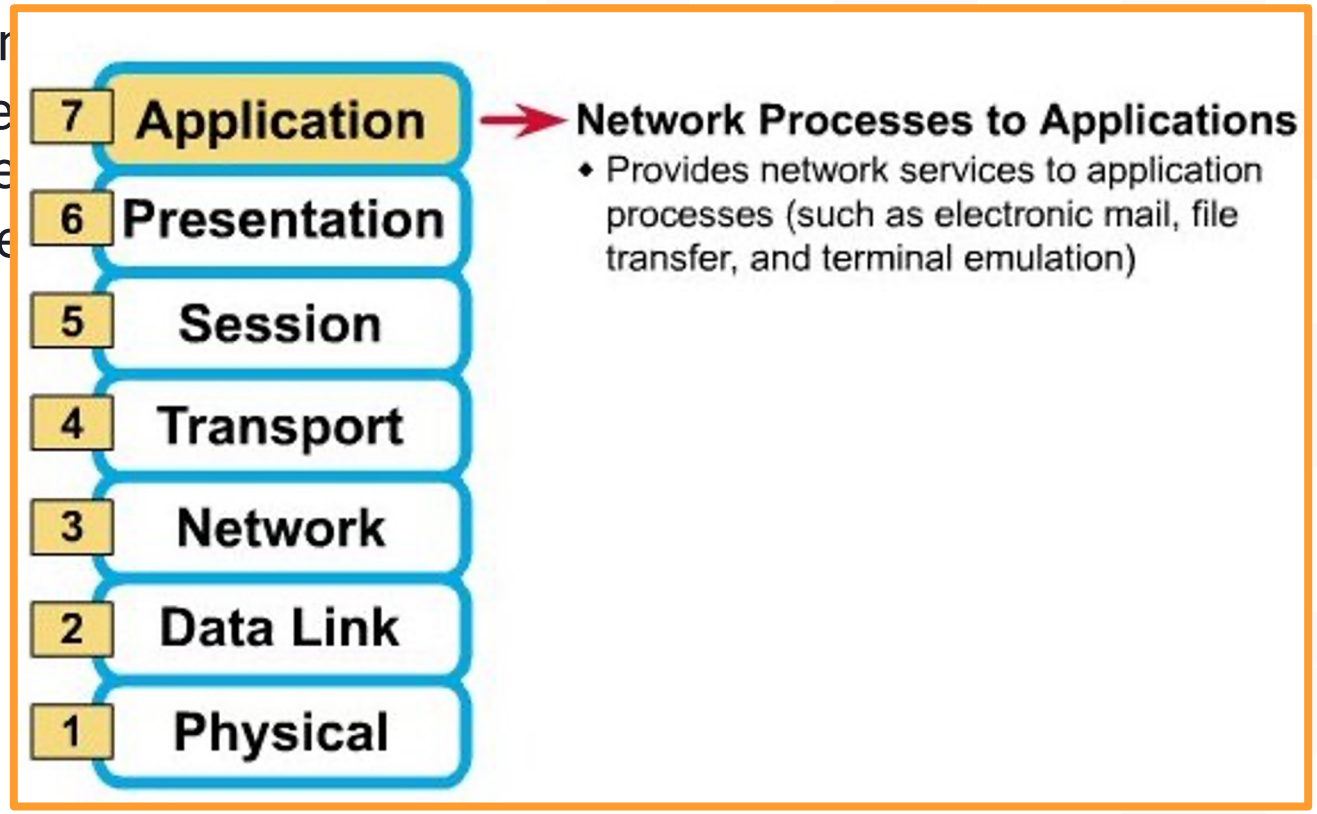
- Where you interface with your computer application
- Web browser, word processor, and instant messaging clients exist at Layer 7
- Protocols Telnet and FTP

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 7: Application

- Where you ir
- Web browse
  exist at Laye
- Protocols Te



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model - Layer 7: Application Attack Vectors

- Weakness in HTTP, FTP, Simple Mail Transfer Protocol (SMPT), SNMP
- Other attacks like HTTP Flooding or input validation, SQL Injection, cross-site scripting (XXS), Authentication weakness

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The OSI Model

Many mnemonics exist to help remember the OSI model:

- "Please Do Not Throw Sausage Pizza Away" (Physical Data-Link Network Transport Session Presentation Application)
- "Please Do Not Tell Sales People Anything."
- "All People Seem to Need Data Processing"

CISSI

LE

Asse

The

Ma

•

•

•

itectures

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model

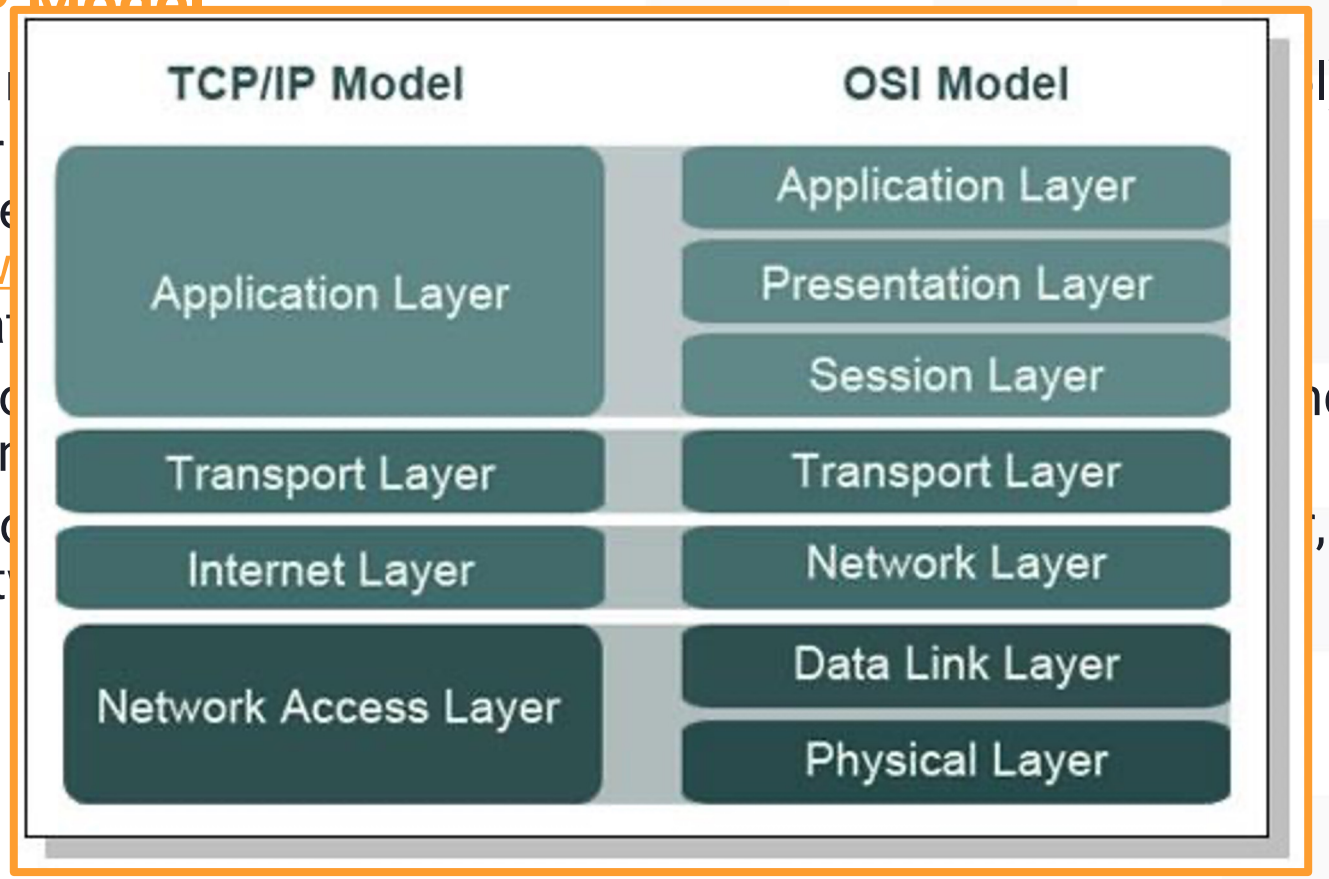
- TCP/IP model (Transmission Control Protocol/Internet Protocol)
- Popular network model created by the United States Defense Advanced Research Projects Agency in the 1970s (see: http://www.isoc.org/internet/history/brief.shtml for more information)
- A suite of protocols including UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol), among many others
- Some sources use Link Layer in place of Network Access Layer, and Network layer in place of Internet Layer

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model

- TCP/IP
- Popular
  Advance
  http://w
  informa
- A suite
  ICMP (Ir
- Some s
  and Net



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model - Network Access Layer

- Combines layers 1 (Physical) and 2 (Data Link) of the OSI model
- Describes Layer 1 issues such as energy, bits, and the medium used to carry them (copper, fiber, wireless, etc.)
- Also describes Layer 2 issues such as converting bits into protocol units such as Ethernet frames, MAC (Media Access Control) addresses, and Network Interface Cards (NICs)
- Networks include:
  - WAN - Wide Area Network
  - LAN - Local Area Network
  - Internet

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model - Internet Layer

- Aligns with the Layer 3 (Network) layer of the OSI model
- IP addresses and routing
- IPv4, IPv6, ICMP, and routing protocols (among others)
- IP (Internet Protocol) governs the Internet layer. (All packets go through IP!)
- Best path determination and packet switching occur at this layer

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP handshake

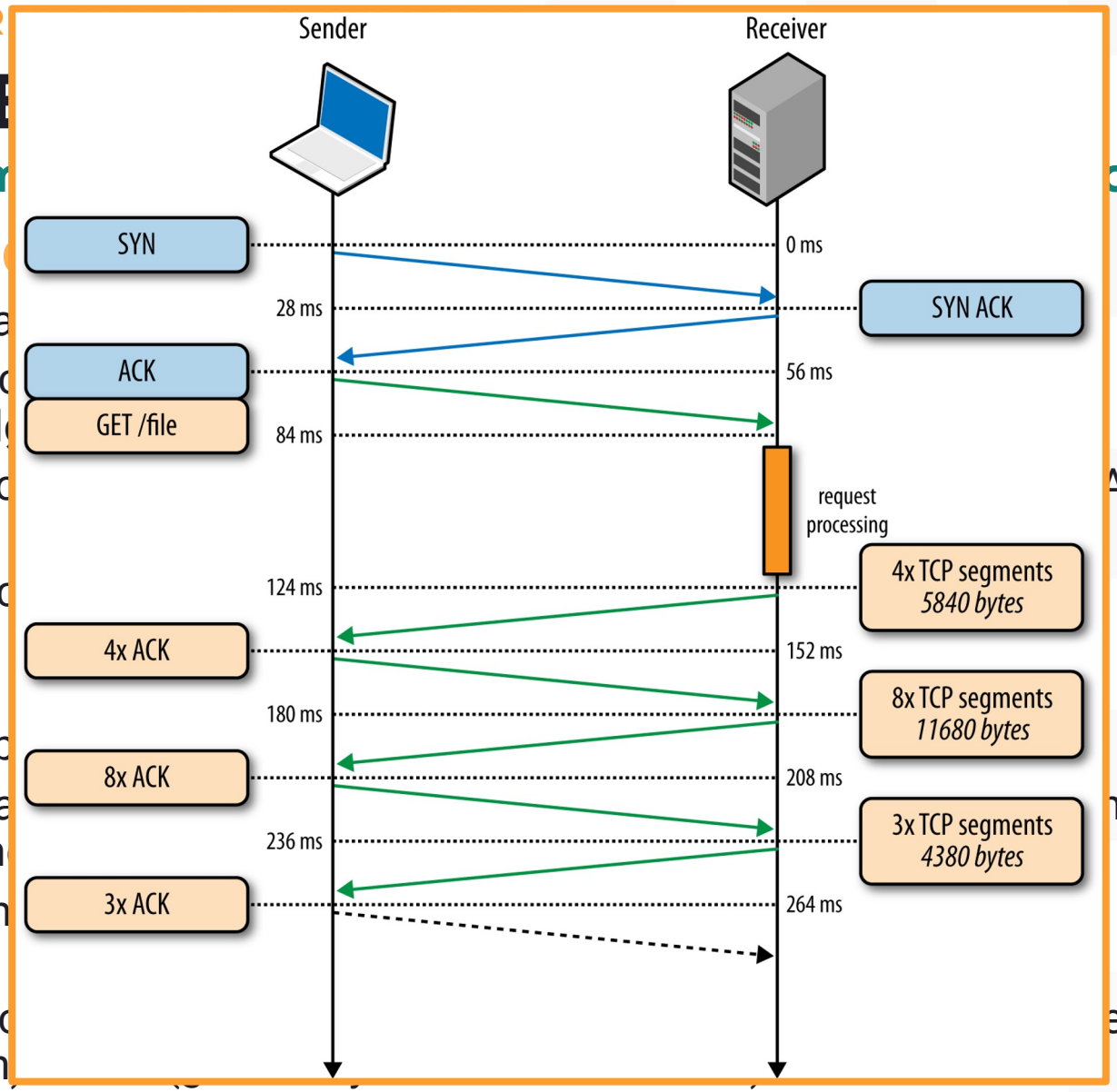
- TCP uses a three-way handshake to establish a reliable connection
- The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other
- Exchange of these four flags is performed in three steps: SYN, SYN-ACK, ACK
- The client chooses an initial sequence number, set in the first SYN packet
- The server also chooses its own initial sequence number, set in the SYN/ACK packet
- Each side acknowledges each other's sequence number by incrementing it: this is the acknowledgement number
- Once a connection is established, ACKs typically follow for each segment
- The connection will eventually end with a RST (reset or tear down the connection) or FIN (gracefully end the connection)

LECTURE

Assess and Im ork Architectures

The TCP han

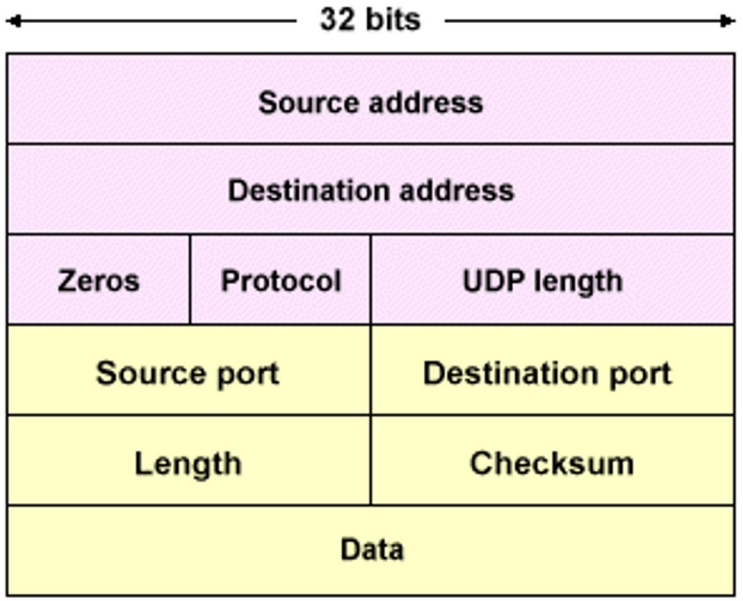
- TCP uses a
- The connec acknowledg
- Exchange c ACK, ACK
- The client c packet
- The server SYN/ACK p
- Each side a nting it: this is th
- Once a con segment
- The connec e connection



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

UDP



- User Datagram Protocol
- A simpler and faster cousin to TCP
- No handshake, session, or reliability
- Informally called “Send and Pray”
- Has a simpler and shorter 8-byte header
- Fields include:
  - Source IP
  - Destination IP
  - Packet length (header and data)
  - Simple (and optional) checksum - if used, the checksum provides limited integrity to the UDP header and data
- Operates at Layer 4
- Commonly used for applications that are “lossy” (can handle some packet loss), such as streaming audio and video
- Also used for query-response applications, such as DNS queries.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model - Host-to-host Transport Layer

- Sometimes called either “Host-to-Host” or, more commonly, “Transport” alone
- Connects the Internet Layer to the Application Layer
- Where applications are addressed on a network, via ports
- TCP and UDP are the two Transport Layer protocols

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model - Host-to-host Transport Layer

TCP - Transmission Control Protocol:

- Connection-oriented protocol.
- supports dialogues between source and destination.
- packages application information into segments.
- provides reliable full-duplex transmission.
- supports flow control that exchanges packets.
- windowing, acknowledgements.
- retransmission - resends anything not received.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model - Host-to-host Transport Layer

UDP - User Datagram Protocol:

- Connectionless protocol that exchanges datagrams.
- does not provide flow control.
- does not support windowing, acknowledgments or guaranteed delivery.
- error processing and retransmission must be handled by other protocols.
- unreliable.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model - Application Layer

- Combines Layers 5 though 7 (Session, Presentation, and Application) of the OSI mode
- Most of these protocols use a client-server architecture, where a client (such as ssh) connects to a listening server (called a daemon on UNIX systems) such as sshd
- Clients and servers use either TCP or UDP (and sometimes both) as a Transport Layer protocol
- Protocols include SSH, Telnet and FTP, among many others

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

The TCP/IP Model - Application Layer

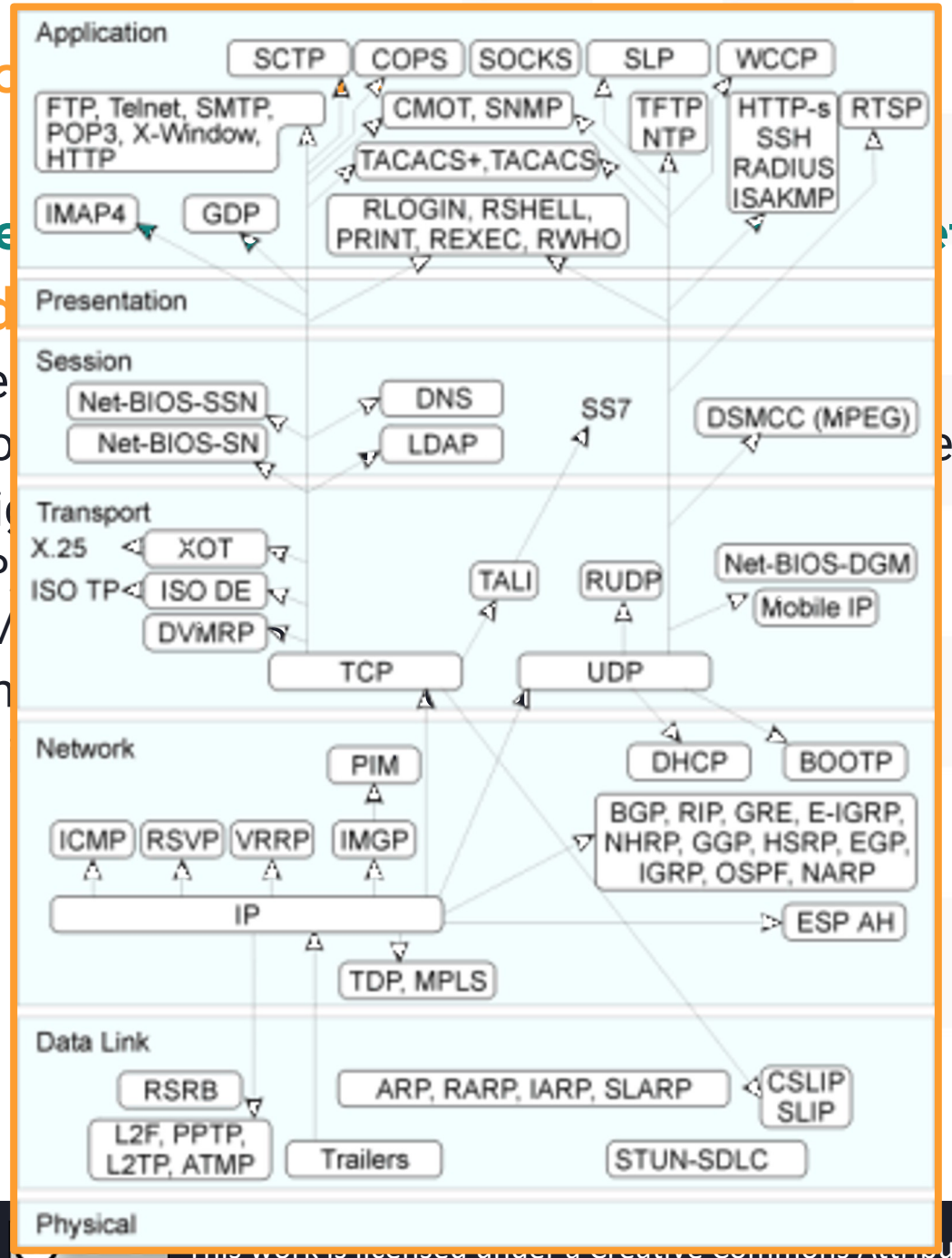
- aka the Process Layer:
- Emphasis is on maximum flexibility for software developers.
- Handles all high-level protocols:
  - FTP, HTTP, SMTP [TCP examples]
  - TFTP, SNMP, DHCP, DNS, BOOTP [UDP examples]
- Data representation, encoding and dialog control.
- Ensures data is properly packaged for the next layer.

LECTURE

Assess and Imple

The TCP/IP Mod

- aka the Proce
- Emphasis is o
- Handles all hi
  - FTP, HTTP
  - TFTP, SNM
- Data represen
- Ensures data



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Encapsulation

- Takes information from a higher layer and adds a header to it, treating the higher layer information as data
- "One layer's header is another layer's data."
- As the data moves down the stack in the TCP/IP model, application layer data is encapsulated in a layer 4 TCP segment. That TCP segment is encapsulated in a Layer 3 IP packet. That IP packet is encapsulated in a Layer 2 Ethernet frame. The frame is then converted into bits at Layer 1 and sent across the local network.
- Data, segments, packets, frames, and bits are examples of Protocol Data Units (PDUs)
- Reverse of encapsulation is called de-multiplexing (sometimes called de-encapsulation)

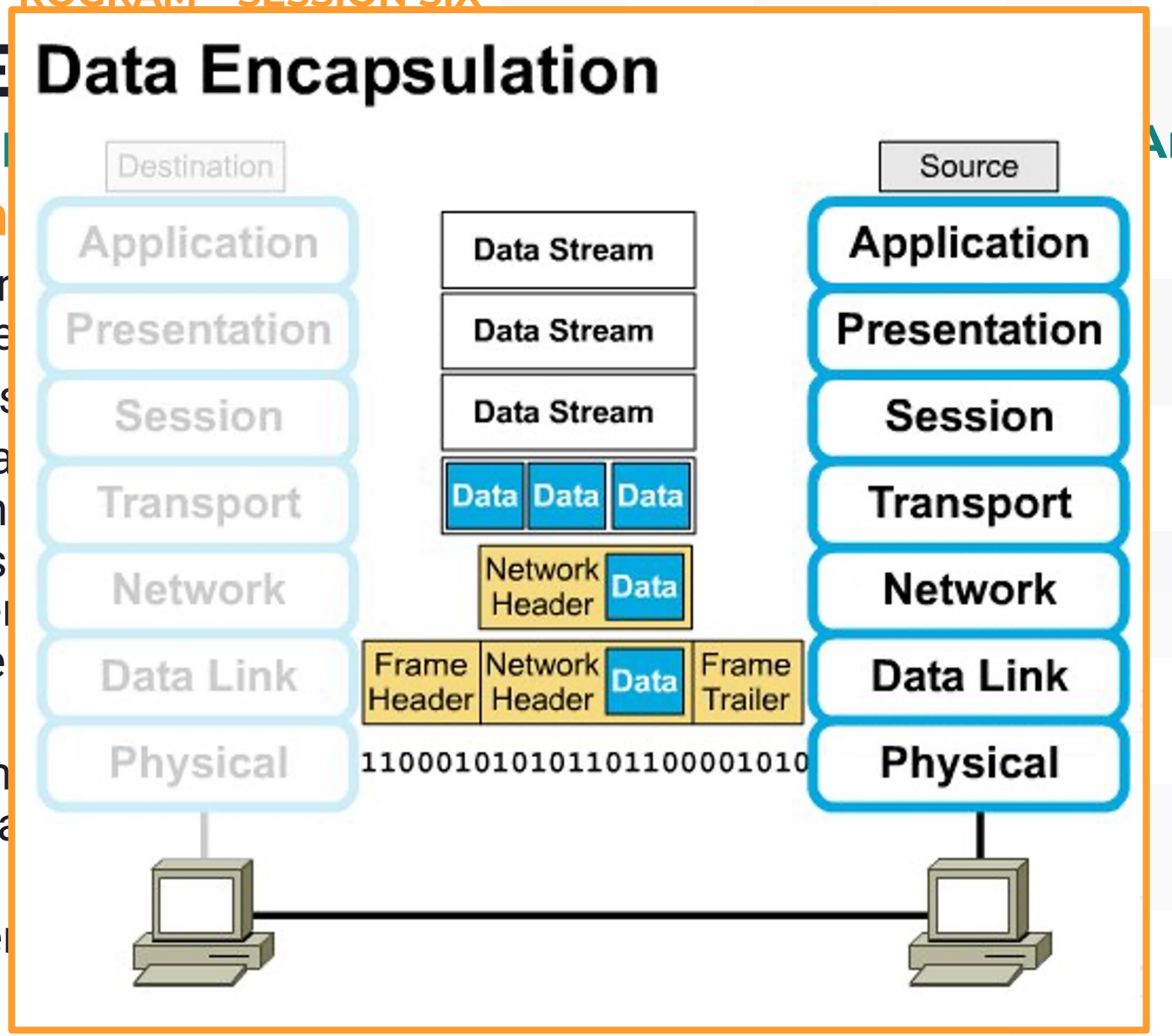
LECTURE

Assess and Imp

Architectures

Encapsulation

- Takes infor
  treating the
- "One layer's
- As the data
  application
  That TCP s
  packet is e
  then conve
  network.
- Data, segm
  Protocol Da
- Reverse of
  called de-e

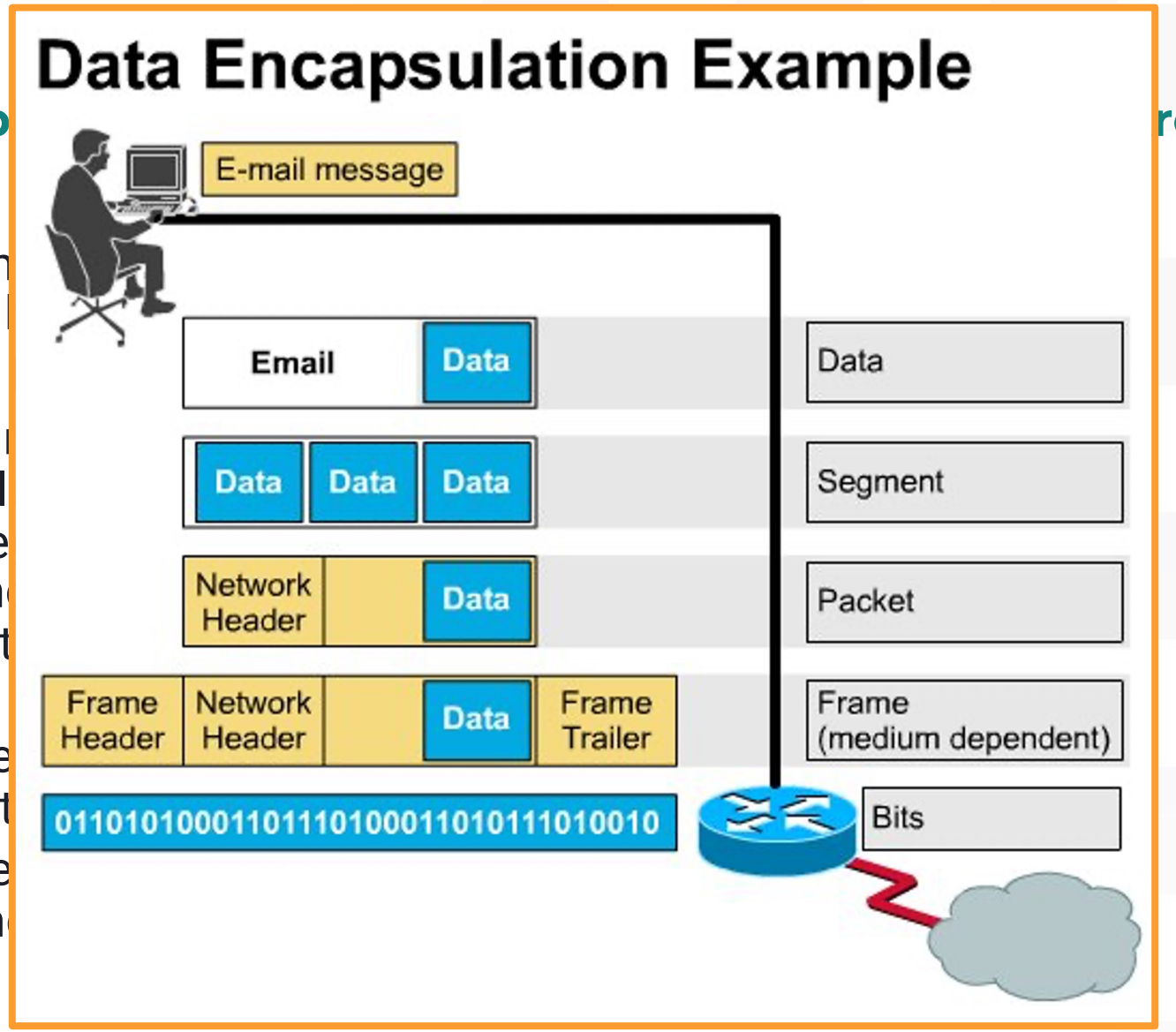


LECTURE

Assess and Imp rchitectures

Encapsulation

- Takes inform
  treating the
- "One layer's
- As the data
  application l
  That TCP se
  packet is en
  then convert
  network.
- Data, segme
  Protocol Dat
- Reverse of e
  called de-en



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Network Access, Internet and Transport Layer Protocols and Concepts

- TCP/IP is a protocol suite: including (but not limited to):
  - IPv4 and IPv6 at Layer 3
  - TCP and UDP at Layer 4
  - A multitude of protocols at layers 5-7, including Telnet, FTP, SSH, and many others
  - Some protocols, such as IP, fit neatly into one layer (Internet). Others, such as Address Resolution Protocol (ARP), help connect one layer to another (Network Access to Internet in ARP's case)

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

MAC Addresses

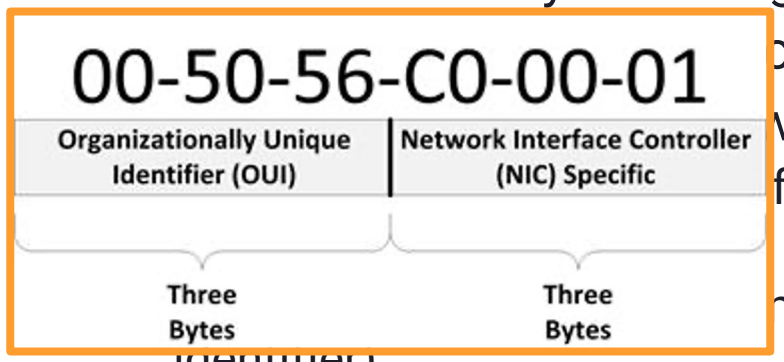
- Unique hardware address of an Ethernet network interface card (NIC)
- Typically, “burned in” at the factory
- MAC addresses may be changed in software
- Burned-in MAC addresses should be unique
- Historically, MAC addresses were 48 bits long:
  - Two halves: the first 24 bits form the Organizationally Unique Identifier (OUI)
  - Last 24 bits form a serial number (formally called an extension identifier)
- Organizations that manufacture NICs, such as Cisco, Juniper, HP, IBM, and many others, purchase 24-bit OUIs from the Institute of Electrical and Electronics Engineers (IEEE), Incorporated Registration Authority. A List of registered OUIs is available at http://standards.ieee.org/regauth/oui/oui.txt

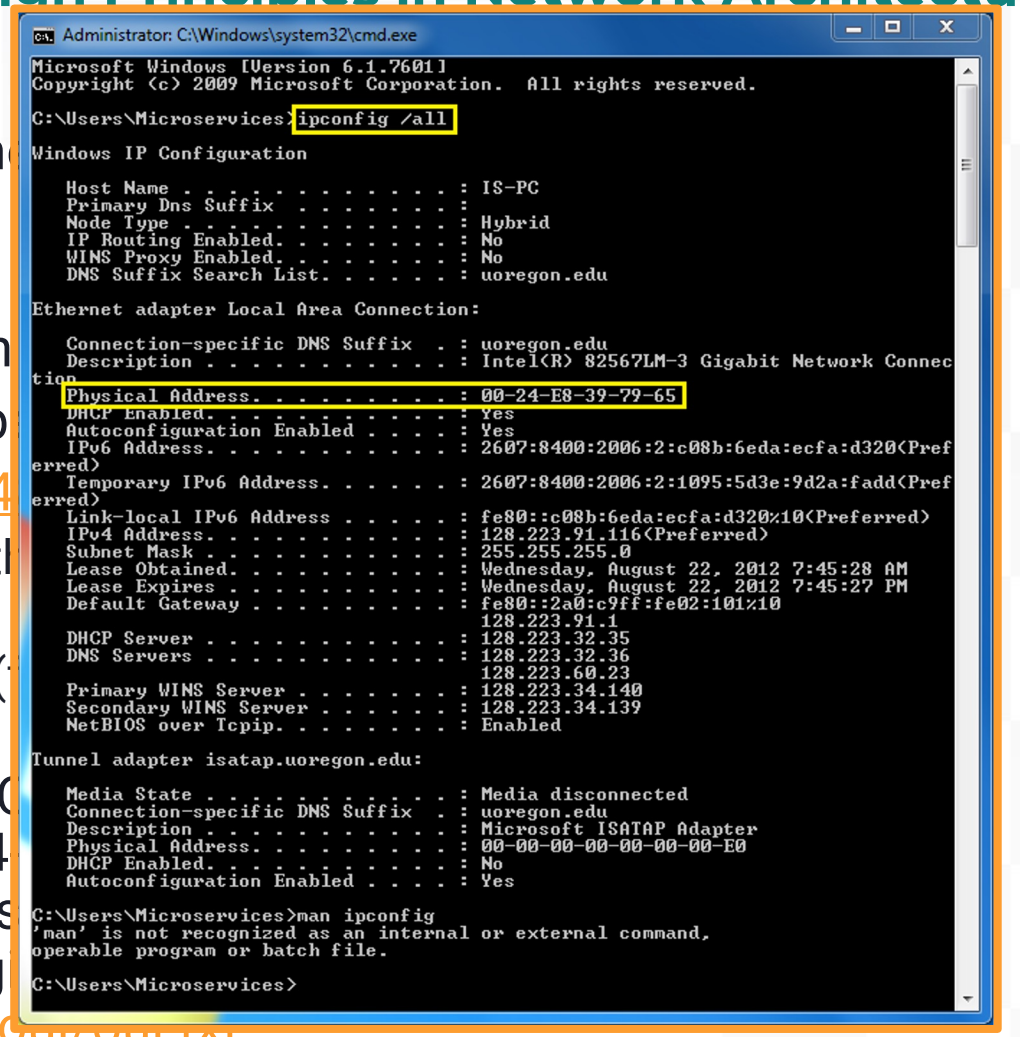
LECTURE

Assess and Implement Secure Design Principles in Network Architectures

MAC Addresses

- Unique hardware address of an Eth
(NIC)
- Typically, “burned in” at the factory
- MAC addresses may be changed in
ould b
vere 4
form t
mber (
identifier)
- Organizations that manufacture NI
IBM, and many others, purchase 24
Electrical and Electronics Engineers
Registration Authority. A List of reg
http://standards.ieee.org/regauth/oui/oui.txt





LECTURE

Assess and Implement Secure Design Principles in Network Architectures

EUI-64 MAC addresses

- IEEE created the EUI-64 (Extended Unique Identifier) standard for 64-bit MAC addresses
- OUI is still 24 bits, but the serial number is 40 bits
- Allows far more MAC addresses, compared with 48-bit addresses

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv4

- Internet Protocol version 4, commonly called “IP”
- Fundamental protocol of the Internet
- Designed in the 1970s to support packet-switched networking
- Used for the ARPAnet, which later became the Internet
- IP is a simple protocol, designed to carry data across networks

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv4

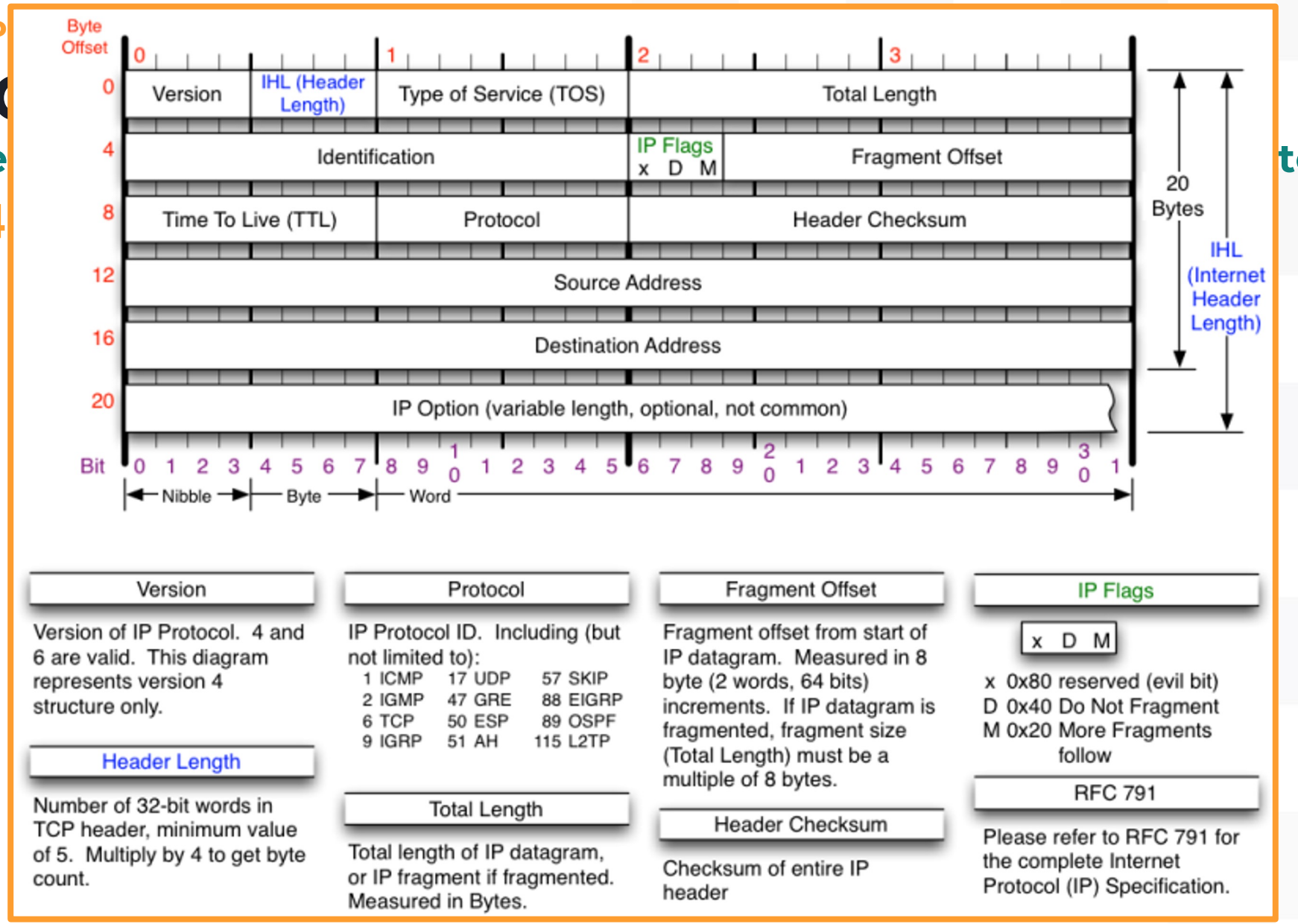
- Requires a “helper protocol” called ICMP
- IP is connectionless and unreliable: it provides “best effort” delivery of packets
- If connections or reliability are required, they must be provided by a higher-level protocol carried by IP, such as TCP
- Uses 32-bit source and destination addresses, usually shown in “dotted quad” format, such as “192.168.2.4”
- 32-bit address field allows 2_{32}, or nearly 4.3 billion addresses
- Lack of IPv4 addresses is a fundamental problem: one of the factors leading to the creation of IPv6, which uses 128-bit addresses

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv4 - Key IPv4 Header Fields

- An IP header is 20 bytes long (with no options)
- Key fields are:
  - Version: IP version (4 for IPv4)
  - IHL: Length of the IP header
  - Type of Service: sets the precedence of the packet
  - Identification, Flags, Offset: used for IP fragmentation
  - Time To Live: to end routing loops
  - Protocol: embedded protocol (TCP, UDP, etc.)
  - Source and Destination IP addresses
  - (Optional) Options and padding



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv4 - IP Fragmentation

- If a packet exceeds the Maximum Transmission Unit (MTU) of a network
- May be fragmented by a router along the path
- MTU is the maximum PDU size on a network
- Fragmentation breaks a large packet into multiple smaller packets
- Typical MTU size for an IP packet is 1500 bytes
- IP Identification field (IPID) is used to re-associate fragmented packets (they will have the same IPID)
- Flags are used to determine if fragmentation is allowed, and whether more fragments are coming
- Fragment offset gives the data offset the current fragment carries: “Copy this data beginning at offset 1480”
- Path MTU discovery uses fragmentation to discover the largest size packet allowed across a network path
- If a large packet is sent with the DF (do not fragment) flag sent and a router with a smaller MTU than the packet size will drop it, sending a “Fragmentation needed and DF set” ICMP message

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv6

- Successor to IPv4
- Larger address space (128-bit addresses compared to IPv4's 32 bits)
- Simpler routing
- Simpler address assignment
- Lack of IPv4 addresses was the primary factor that led to the creation of IPv6

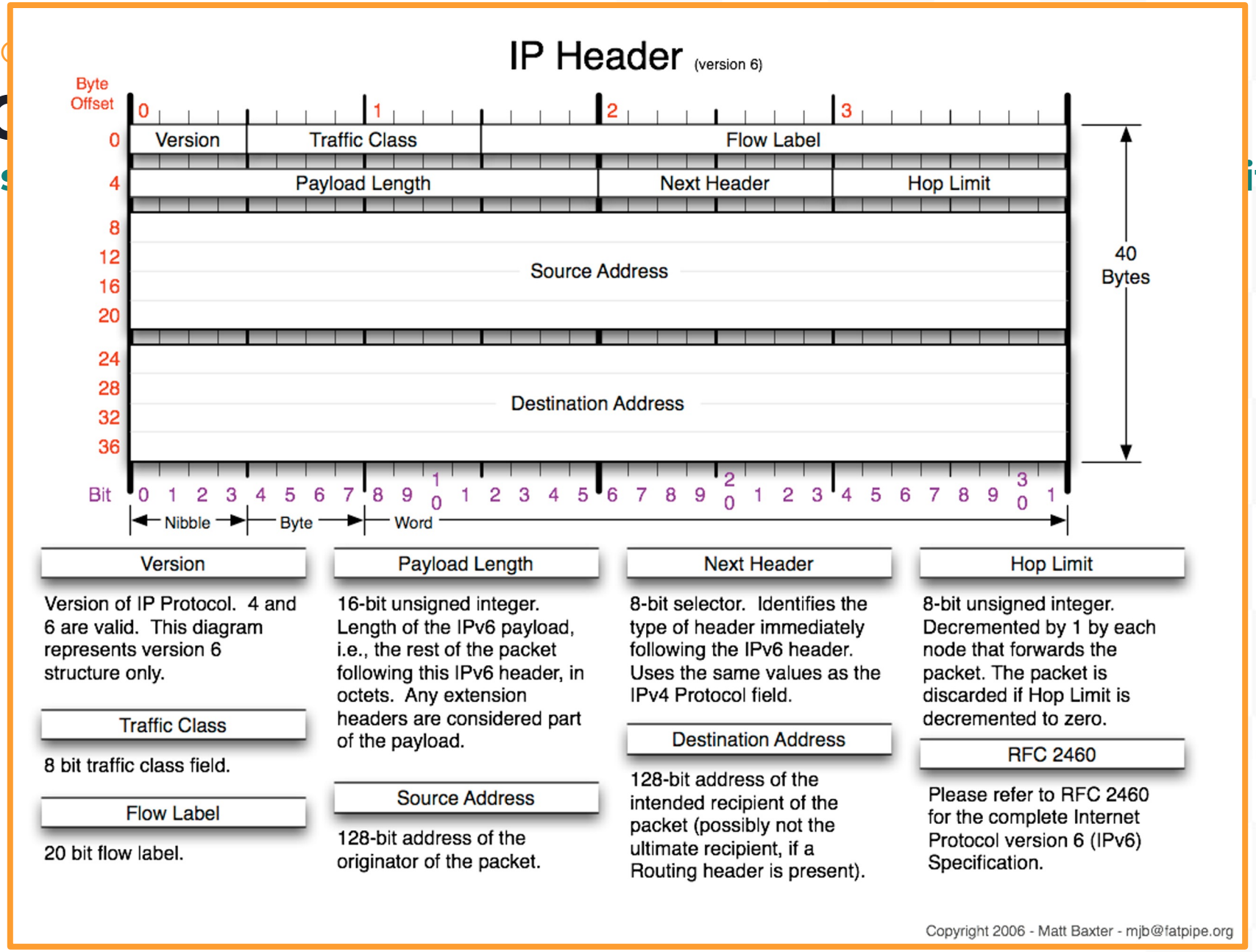
Note - IPv6 address space is 2_{128}; there are over 340 undecillion (called 340 sextillion) total addresses, which is a 39-digit number in decimal: 340,282,366, 920,938,463,463,374,607,431,768,211,456.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv6

- The IPv6 header is larger (40 bytes vs. 20 bytes) and simpler than IPv4
- Fields include:
  - Version: IP version (6 for IPv6)
  - Traffic Class and Flow Label: used for QoS (Quality of Service)
  - Payload Length: length of IPv6 data (not including the IPv6 header)
  - Next header: next embedded protocol header
  - Hop Limit: to end routing loops



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv6 Addresses and Autoconfiguration

- IPv6 hosts can statelessly autoconfigure a unique address, omitting the need for static addressing or DHCP
- Stateless autoconfiguration takes the host's MAC address and uses it to configure the IPv6 address
- IPv6 addresses are 128 bits long, and use colons instead of periods to delineate section
- One series of zeroes may be condensed into two colons ("::").
- Stateless autoconfiguration removes the requirement for DHCP (Dynamic Host Configuration Protocol)
- DHCP may be used with IPv6: this called "stateful autoconfiguration"

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv6 Addresses and Autoconfiguration

- The “ifconfig” (left) shows two IPv6 addresses:
  - fc01::20c:29ff:feef:1136/64 (Scope:Global)
  - fe80::20c:29ff:feef:1136/64 (Scope:Link)
  - The first address (fc01::…) is a “global” (routable) address, used for communication beyond the local network
  - IPv6 hosts rely on IPv6 routing advertisements to assign the global address
  - The second address (fe80::…) is a link-local address, used for local network communication only
  - Systems assign link-local addresses independently, without the need for an IPv6 router advertisement
  - /64 is the network size in CIDR format; means the network prefix is 64 bits long: the full global prefix is fc01:0000:0000:0000

IPv4 is noted in binary (1 bit) and numerical (8 bits) form.
IPv6 is noted in hexadecimal (4 bits) form.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv6 Addresses and Autoconfiguration

- The host uses the following process to statelessly configure its global address:
  - Take the MAC address: 00:0c:29:ef:11:36
  - Embed the “ffee” constant in the middle two bytes: 00:0c:29:ff:fe:ef:11:36
  - Set the “Universal Bit”: 02:0c:29:ff:fe:ef:11:36
  - Prepend the network prefix & convert to “:” format: fc01:0000:0000:0000:020c:29ff:feef:1136
  - Convert one string of repeating zeroes to “::”: fc01::20c:29ff:feef:1136

Remember, stateless means the system assigned its own address If DHCP is used, it’s stateful.

Note: systems may be “dual stack” and use both IPv4 and IPv6 simultaneously

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

IPv6 Security Challenges

- An IPv6-enabled system will automatically configure a link-local address (beginning with fe80:…) without the need for any other ipv6-enabled infrastructure. The host can communicate with other link-local addresses on the same LAN. This is true even if the administrators are unaware that IPv6 is now flowing on their network.
- ISPs are also enabling IPv6 service, sometimes without the customer's knowledge. Modern network tools, such as networked intrusion detection systems, can "see" IPv6, but are often not configured to do so.
- Many network professionals have limited experience or understanding of IPv6. From an attacker's perspective, this can offer a golden opportunity to launch attacks or exfiltrate data via IPv6.
- All network services that are not required should be disabled: this is a fundamental part of system hardening. If IPv6 is not required, it should be disabled

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Classful Networks (back to IPv4)

- Original IPv4 networks (before 1993) were “classful”
- Classified in classes A through E
- Class A through C were used for normal network use. Class D was multicast, and Class E was reserved

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

LECTURE

Assess and Implement Secure Design Principles

Network Address Translation

NAT Type	Example
Static	192.168.1.47 -> 192.0.2.252
Pool	192.168.1.17 -> 192.0.2.10 192.168.1.21 -> 192.0.2.11 192.168.1.56 -> 192.0.2.12
PAT	192.168.1.* -> 192.0.2.20

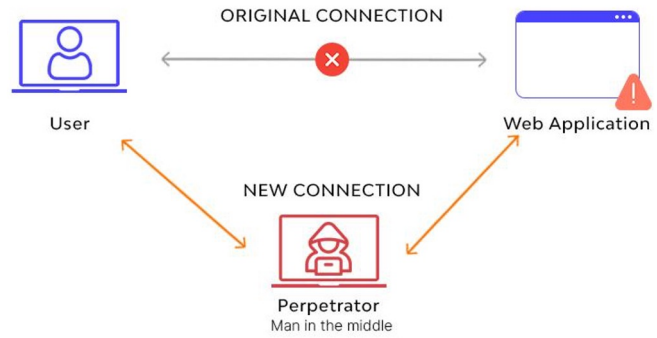
- Used to translate IP addresses
- Frequently used to translate RFC1918 addresses as they pass from intranets to the Internet
- Three types of NAT are:
  - Static NAT
    - Makes a one-to-one translation between addresses, such as 192.168.1.47→192.0.2.252
  - Pool NAT (also known as dynamic NAT)
    - Reserves a number of public IP addresses in a pool
    - Addresses can be assigned from the pool, and then returned.
  - Port Address Translation (PAT, also known as NAT overloading)
    - Typically makes a many-to-one translation from multiple private addresses to one public IP address
    - Common solution for homes and small offices: multiple internal devices such as laptops, desktops and mobile devices share one public IP address

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Network attacks

- **Distributed Denial of Service (DDoS) Attacks** e.g. using large numbers of distributed systems like IoT devices to flood the target with UDP traffic
- **SYN Flooding** – overwhelming target with SYN connections. Increasing backlog queue by leaving half opened connections, recycling the oldest half-opened TCP connection, acting on SYN cookies to recreate the SYN backlog
- **IoT devices** – since there are increasing numbers of IoT devices on networks that remained increasingly unpatched or unable to be patched, attackers can easily attack these devices with simply code and bring them into their botnets
- **Man-In-the-Middle (MITM) attack** – Signal intercepts /signal relays; impersonation attacks
  - **Authentication** – to prevent MITM attacks cryptographic Protocols are used to authenticate endpoint or transmission
  - **Tamper detection** - to prevent MITM attacks detect changes in latency and hashes vs expected base lines



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Network attacks

- **Packet sniffing** – any unencrypted protocols are subject to passive attacks where an attacker has been able to place a packet sniffing tool on the network to monitor traffic. This can be used to monitor traffic types and patterns to map out the network
- **Hijacking Attacks** – another type of MITM attack which involves the exploitation of an active session, where an attack can intercept or eavesdrop on the session token or cookie, and connect to the server in parallel with the victim or send a specifically formed packet to the victim to terminate the session
- **TIP –** promiscuous mode is a setting that packet sniffers enable to stop a device from discarding or filtering data unintended for it. The packet sniffers can gain access to the additional traffic and data packets that otherwise have been unfiltered.
- **MITRE ATT&CK Framework -** More about MITRE ATT&CK at attack.mitre.org

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Secure Protocols

- **Secure Shell** – replacement for Telenet, supports a cryptographic tunnel to protect the integrity of the communications, limiting MITM and session hijacking. SSH-1 deemed insecure, SSH-2 protects better against ease dropping, DNS & IP spoofing and MITM attacks
- **Transport Layer Security (TLS)** – is a secure protocol that replaces SSL for web traffic. It's a session-oriented protocol used for web, email, FTP and even Telenet traffic. Easier that IPSec for VPN as it doesn't need pre-installed client certificates. Provides One-way, Two-way authentication using digital certificates. Can operate at network layer for VPN (eg. Open VPN)
- **Kerberos** – communication protocol for logon credentials using ticketing systems to allow communication over an unsecured network

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

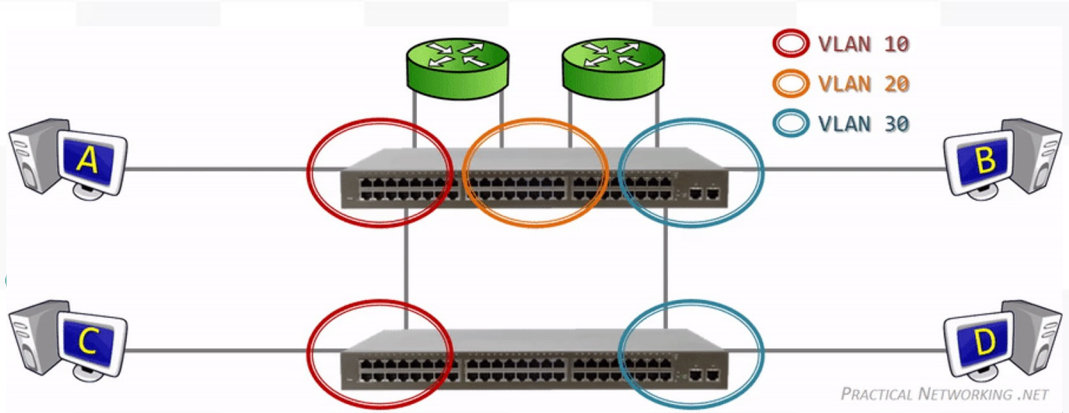
Secure Protocols

- **Internet Protocol Security (IPSec)** – a suite of protocols design to provide confidentiality, integrity and authentication of data sent over an IP network. It uses Authentication Headers (AH), Encapsulation security payload (ESP), Security Associations (SAs) via Transport or Tunnel Mode

- **Internet Key Exchange (IKE)** – part of the IPSec suite used to establish a secure, authenticated communication channel between two identities usually using X.509 PKI certificates. IKEv1 is consider vulnerable. IKEv2 addresses issues in v1. IPSec VPN configs using both IKEv1/IKEv2 can be vulnerable to downgrade attacks; mitigate by segregating systems that need IKEv1 from IKEv2

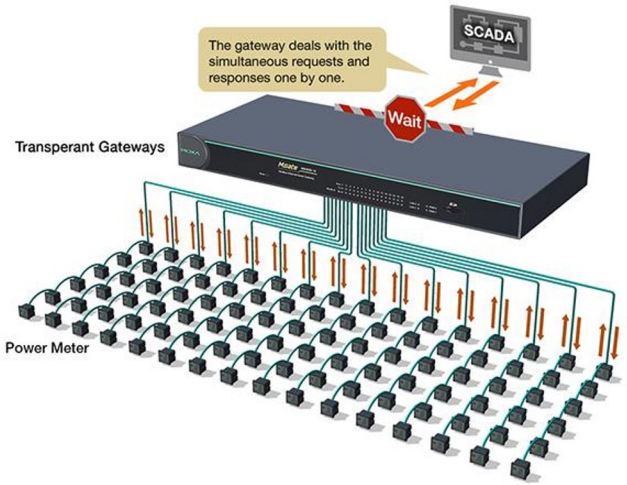
LECTURE

Assess and Implement Secure Design Prin



Implications of multilayer protocols

- adversaries can use multiple layers of encapsulation to hide their activities, eg. Hiding FTP traffic in HTTP packet
- **Virtual Local Area Networks (VLAN)–** attackers can use multilayer protocol encapsulation to fool interior switching devices to gain access to a VLAN. VLANs are used to isolate network traffic to its own separated broadcast domains, and the switch know what VLAN traffic is supposed to go based on its VLAN ID per IEEE 802.1Q encapsulates each packet. To hop VLANs an attack is *double encapsulating* a packet.
- **Supervisory Control and Data Acquisition Systems (SCADA)** – use a legacy protocol *Distributed Network Protocol (DNP3)* which has many similarities to TCP/IP. In order to communicate over public networks they used encapsulating DNP3 over TCP/IP
  - *NOTE:* many systems use another legacy protocol Modbus, defacto standard of application layer protocol, variants include Modbus+ and Modbus/TCP; which allows a modbus client to send requests to a modbus server with function code that specifies actions take and a data field with additional information



LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Converged Protocols

- Differ from encapsulated or multiprotocol, as they merge specialty or proprietary protocols with standard protocols like TCP/IP
- **Fibre Channel over Ethernet (FCoE)** – supports Fibre Channels that are usually need over fiber-optic cables for SANs or NAS to achieve of 128 - 256 Gbps over 10 Gbps Ethernet. FCoE uses Ethernet frames to support the Fibre Channel communications.
- **Internet Small Computer System Interface (iSCSI)** – viewed as a low cost alternative to fiber, transmits SCSI commands over IP
- **Multiprotocol Label Switching (MPLS)** – high-throughput, high performance network technology using short path labels rather than long addresses. MPLS networks can handle T1/E1, ATM, Frame Relay, SONET, and DSL, not just TCP/IP. Often creates dedicated circuits between two stations. Commonly called 2.5 protocol operates between layer 2 and 3
- **Voice over Internet Protocol (VoIP)** – encapsulates voices communications and multimedia sessions over IP networks. Popular way to operate telephony solutions

Uses Fibre spelling to separate from fiber optic implementations form.

iSCSI acts like a virtual SATA cable

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Micosegmentation

- is a method of creating zone within a network to isolate resources from one another and secure each segment individually. Requires re-authentication with viewing or accessing resources across zones.
- **Software-Defined Networking (SDN)** – allows networks to be centrally managed/programmed. Allows dynamic network configurations/management and improves network performance, plus gives orgs a centralized view of network architecture.
  - **Infrastructure layer (data plane)** – network switches and routers and the data itself as well as the process of forwarding data to destination
  - **Control layer** – the intelligence in devices that determine how traffic should flow based on the status of the infrastructure layer as needed by application layer
  - **Application layer** – Network services, utilities, and applications that interface with the control layer to specify needs and requirements

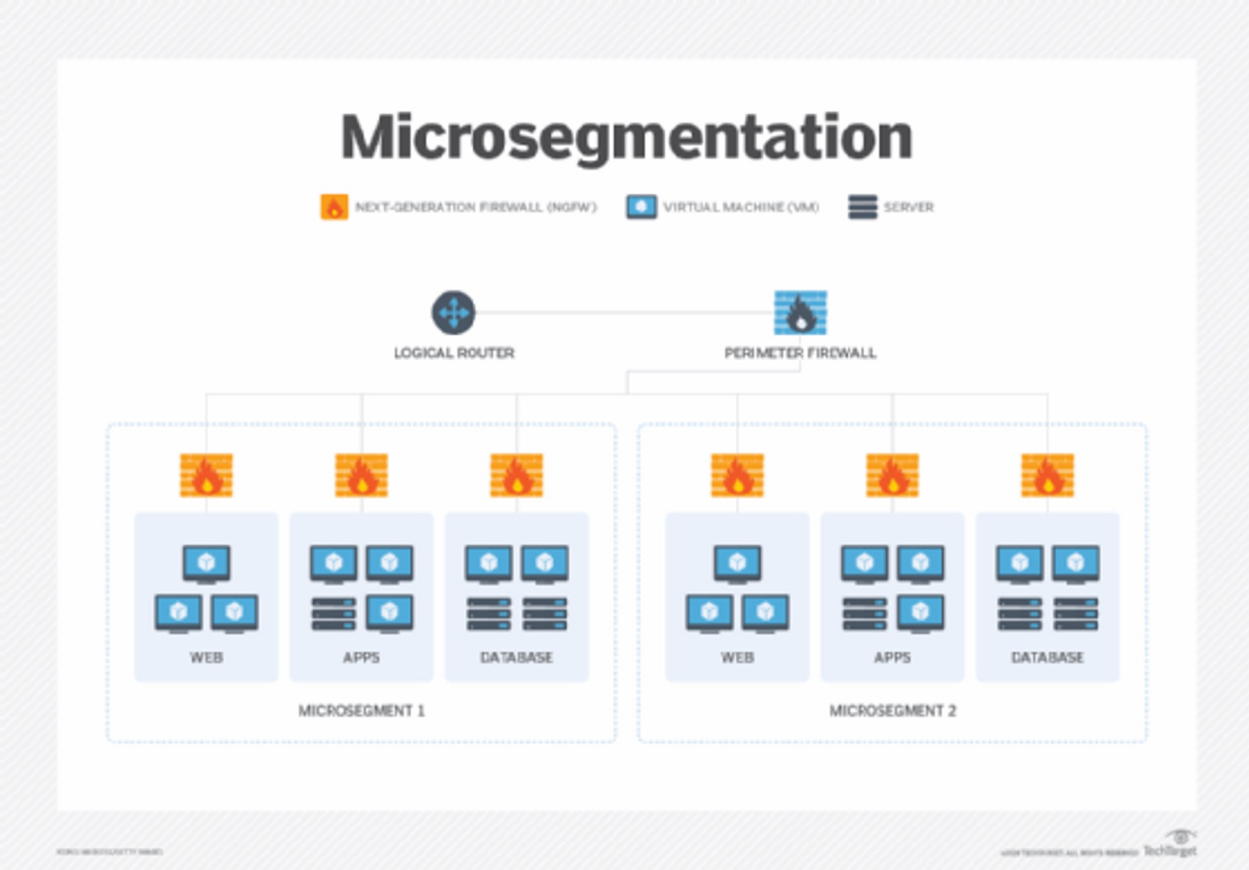
TIP: East-West is usually traffic flow within data center or network. North (outside)- South(inside) data flow.
3 layers of SDN are closed related to network engineer view of data/control/management planes for circuit and network management

LECTURE

Assess and Implement Secure Desi

Microsegmentation

- is a method of creating zone within a networ and secure each segment individually. Requir accessing resources across zones.
- **Software-Defined Networking (SDN)** – allows managed/programmed. Allows dynamic netw improves network performance, plus gives or architecture.
  - **Infrastructure layer (data plane)** – netwo itself as well as the process of forwardin
  - **Control layer** – the intelligence in device based on the status of the infrastructure
  - **Application layer** – Network services, uti with the control layer to specify needs and requirements



TIP: East-West is usually traffic flow within data center or network. North (outside)- South(inside) data flow.
3 layers of SDN are closed related to network engineer view of data/control/management planes for circuit and network management

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Microsegmentation

- **Software-Defined Security (SDS)** – a security model in which security mechanisms are controlled and managed by security software. Policy-driven security that consists of network segmentation, intrusion detection and prevention, user and device identification, application controls
- **Software-Defined Wide Area Network (SD-WAN)** – use software to control connectivity and management services between data centers and remote networks such a cloud service providers (CSPs). Must support multiple connection types (internet, MPLS, LTE, etc); perform dynamic path selection to support load sharing across WAN connections; provides simple interface for managing the WAN; Must support VPN and 3rd party services
- **Virtual eXtensible Local Area Network (VXLAN)** – encapsulates layer 2 ethernet frames within layer 4 UDP datagrams. Allows networks to segment large networks with scale that VLANs can't support. 16 million VXLANs vs 4096 VLANS
- **Encapsulation** – the wrapping of one protocol around the contents (or payload) of a subsequent protocol. Logically separating functions from their underlaying physical structures

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Wireless Networks

- Wireless networks face the same vulnerabilities without the strings attached, some additional items may include insecure defaults, increased MITM types of eaves dropping, DDoS or interference, signal capture and recreation, RF mapping
- Wi-Fi (wireless fidelity) is the most common family of wireless protocol, with Wi-Fi governed by IEEE 802.11 family of standards. 802.11x is used to refer to the all of the specific implementations.
- **Do not confuse 802.11x with 802.1x which is used for authentication**

STANDARD		DATE	FREQUENCY (GHZ)	MAXIMUM DATA RATE
WiFi 1	802.11b	1999	2.4	11 Mbps
WiFi 2	802.11a	1999	5.0	54 Mbps
WiFi 3	802.11g	2003	2.4	54 Mbps
WiFi 4	802.11n	2009	2.4 / 5.0	600 Mbps
WiFi 5	802.11ac (Wave 1)	2013	5.0	1.73 Gbps
	802.11ac (Wave 2)	2015	5.0	3.46 Gbps
WiFi 6	802.11ax	2020	2.4 / 5.0/ 6.0	9.60 Gbps

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Wireless Networks

- **Wired Equivalent Privacy (WEP) and Wi-Fi Protected Area (WPA)** – are the two more used encryption standards for Wi-Fi. WEP is considered Highly insecure and should not be used. WPA continues to evolve with WPA3 being the current standard. 802.11 standard defines 2 methods to authenticate to a Wireless Access Point (WAP) using Open system authentication (OSA) and shared key authentication (SKA).
  - OSA is open and unencrypted. SKA enforces authentication or blocks access
- **WEP** implements Rivest Cipher 4 (RC4) and was instantly cracked
- **WPA** was designed as an interim solution for 802.11i and implement Lightweight Extensible Authentication Protocol (LEAP) and Temporal Key Integrity Protocol (TKIP) which implemented a per packet 128 bit encryption key, added cyclic redundancy check (CRC) to validate integrity. Both options now crackable
- **WPA2 (IEEE 802.11i)** – FIPS 140-2 compliant AES encryption and counter mode cipher block chaining message authentication code protocol (CCMP). The name WPA2 was selected since WPA was so widely published.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Wireless Networks

- **WPA3** – adds 192 bit encryption and individualized encryption for each user
- **IEEE 802.1X** – WPA, WPA2, WPA3 support enterprise authentication know as 802.1X/EAP a standard NAC that is port-based to ensure client access control to network resources. Checking system that allows wireless network to leverage the existing network infrastructure's authentication services
- **Extensible Authentication Protocol** – authentication framework vs mechanisms
- **Protected Extensible Authentication Protocol** - using TLS tunnel PEAP encapsulates EAP methods to provide authentication and potentially encryption
- **Lightweight Extensible Authentication Protocol** – Cisco alternative to Temporal Key Integrity Protocol for WPA
- **Temporal Key Integrity Protocol** – TKIP designed as replacement for WEP without replacement of legacy hardware which added key mixing function and message integrity checks

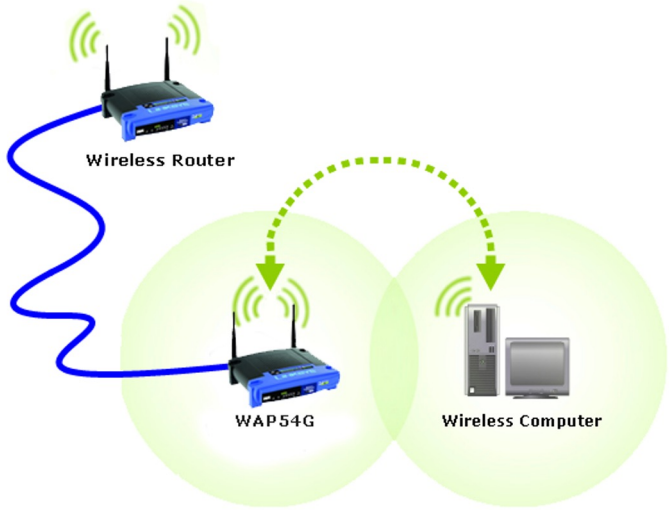
LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Securing Wireless Access Points

- **Wireless Access Point (WAP or AP) –** allows a networking devices that allows wireless-enabled devices to connect to a wired network. Aps connect directly to the LAN or other wireless technologies

- To set up a secure wireless environment, there is more than booting it up, configuring a funny SSID (*service set identifiers*) and choosing which hardware modes and speeds you will be supporting

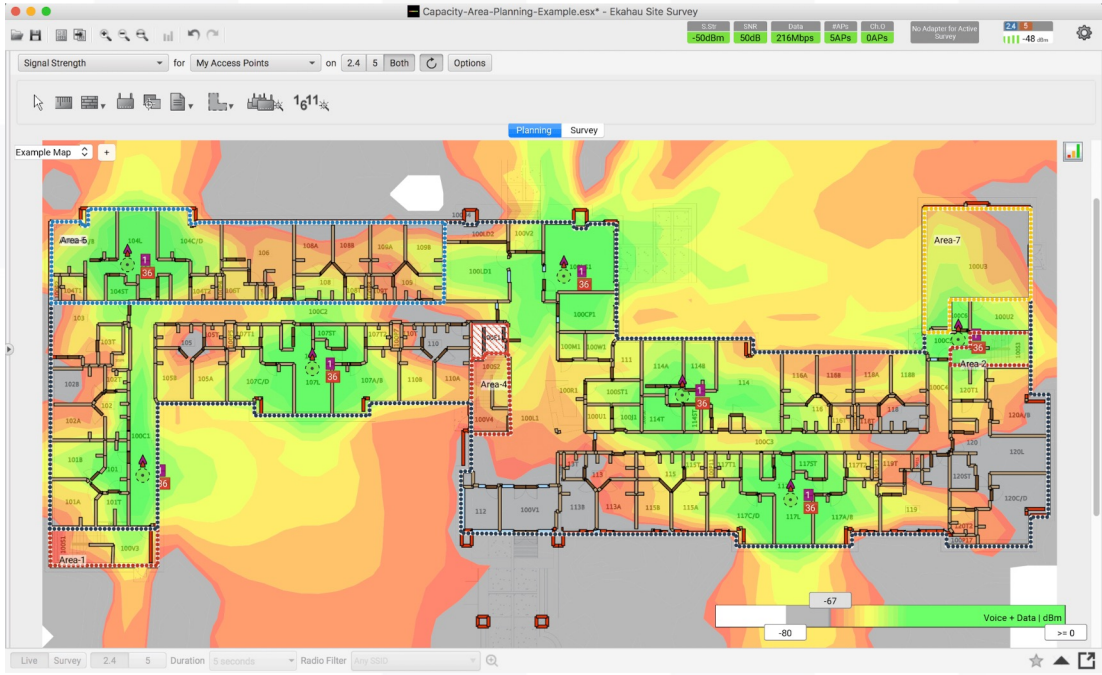


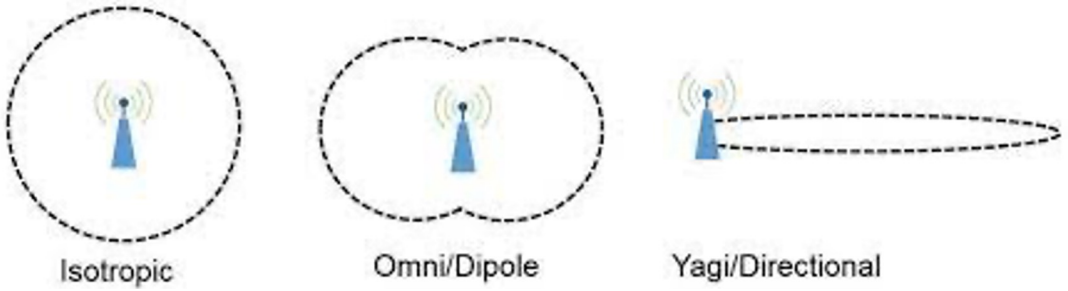
LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Securing Wireless Access Points

- **Conducting a Site Survey** – used to identify rouge Aps as well as define the placement, configuration and documentation of the Aps
- **Determining Wireless Access Placement** – use visualization software to help you determine the best placement. Use central locations, avoid solid structures, avoid reflective or flat metal surfaces or electrical equipment. Position external omnidirectional antennas pointing vertically, point directional antennas towards the desired direction. Consider the environmental impact of the environment on the signal.
- **Antenna types** -





LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Securing Wireless Access Points

- **Wireless Channels –** wireless signals are subdivided into channels within a frequency called channels. Channels have no implications on security, just on limiting interference, choose the least congested ones
- **Infrastructure Mode and Ad Hoc Mode:**
  - **Standalone** – APs connects to wireless clients but not wired resources
  - **Wired Extension** – APs act as a connection point, or hub to link to wired resources
  - **Enterprise Extended** – multiple APs with the same ESSID are used to connect a large physical area to the same wired network
  - **Bridge** – a wireless connection used to link two wired networks
- **Service Set Identifiers (SSID)** – the network name. ESSID is when its used in infrastructure mode or BSSID when in ad-hoc or peer-to-peer mode. BSSID is the MAC of the hosting base station
- Disable the broadcast of the SSID by disabling the *beacon frame*

To BSSID or not to BSSID, that is the question.

LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Securing Wireless Access Points

- **Captive Portals –** used as authentic safeguards. Note that a captive portals are compromised they can be used to serve malicious scripts to everyone that connects
- **Mac Filters** – a list of authorized devices based on a defined list of MAC addresses of the devices
- **Wireless attacks** – War driving similar to war dialing where they can use tools in a moving vehicle to infiltrate wireless networks

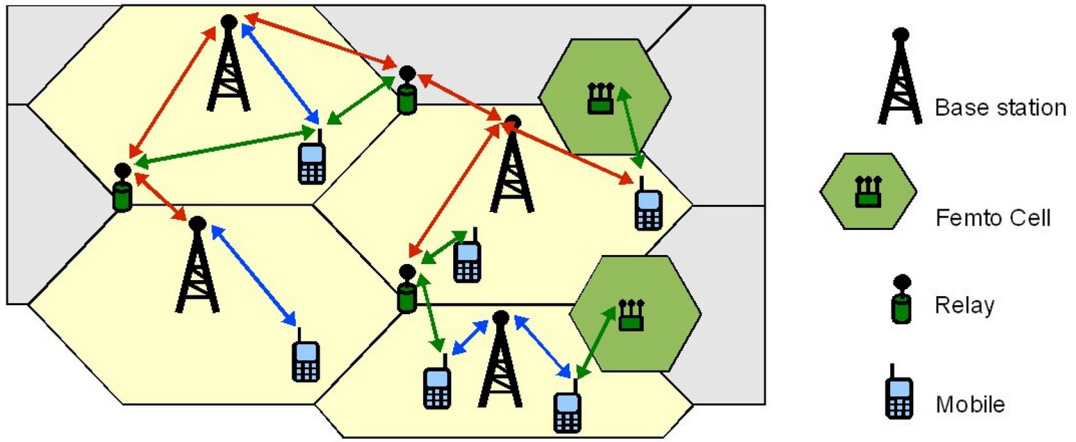
- **Li-fi** – uses ultraviolet or infrared light to transmit data
- **Bluetooth** – wireless technology that supports point to point transmission from 30-300 feet. Create a personal area network (PAN)
- **ZigBee** – IEEE 802.15.4 low-cost, low-power and low-latency communication, used in applications with short range with low data transfers. used within many IoT devices

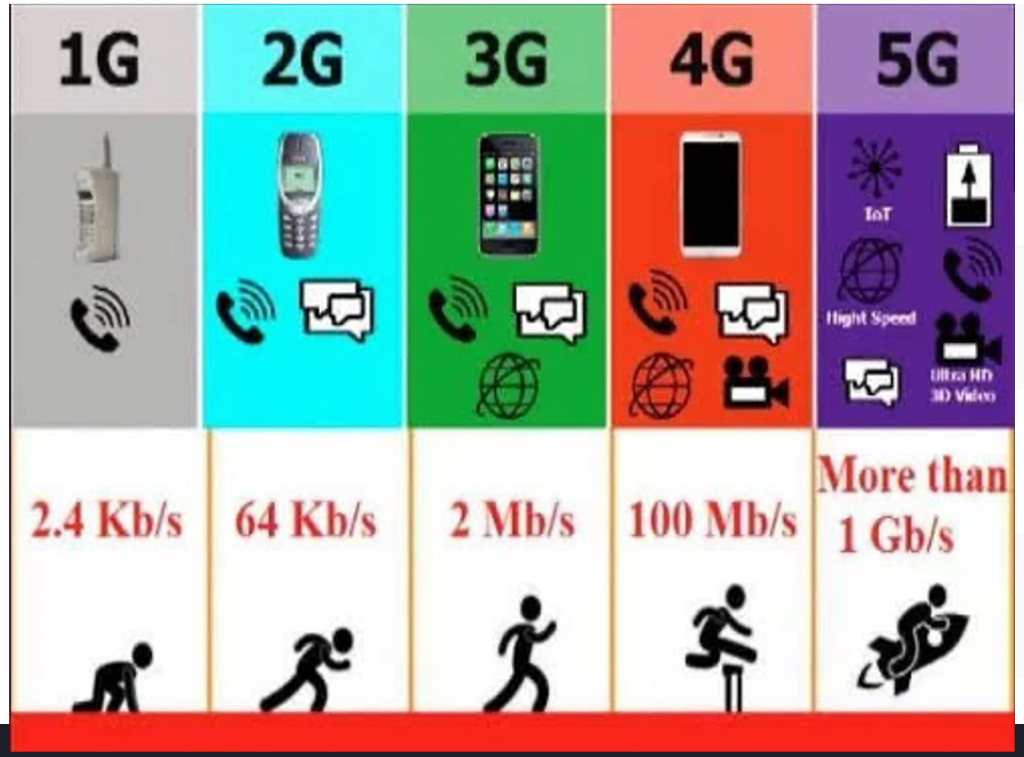
LECTURE

Assess and Implement Secure Design P

Cellular networks

- wireless networks that traverse across cells. The cells are geographically dispersed areas that may consist of one or more cell sites or base stations
- Cellular transmission are not inherently secure and are susceptible to MITM traffic capture
- As the speed of cellular technology advances so does the application to more sensitive applications





LECTURE

Assess and Implement Secure Design Principles in Network Architectures

Content Distribution Networks (CDN)

- also called a Content Delivery Network
- Collection of resources services, proxy services, and data storage centers that a geographically dispersed to provide low-latency access to high availability data such as multimedia, ecommerce, social media, etc

WE MADE IT THROUGH SESSION #6!

Technical, but not too technical.

Please try to catch up in your reading.

- We left off on page 334 in the book.
- Wednesday (5/4) we'll finish this chapter and domain.
- Come with questions!

Have a great evening, talk to you Wednesday!