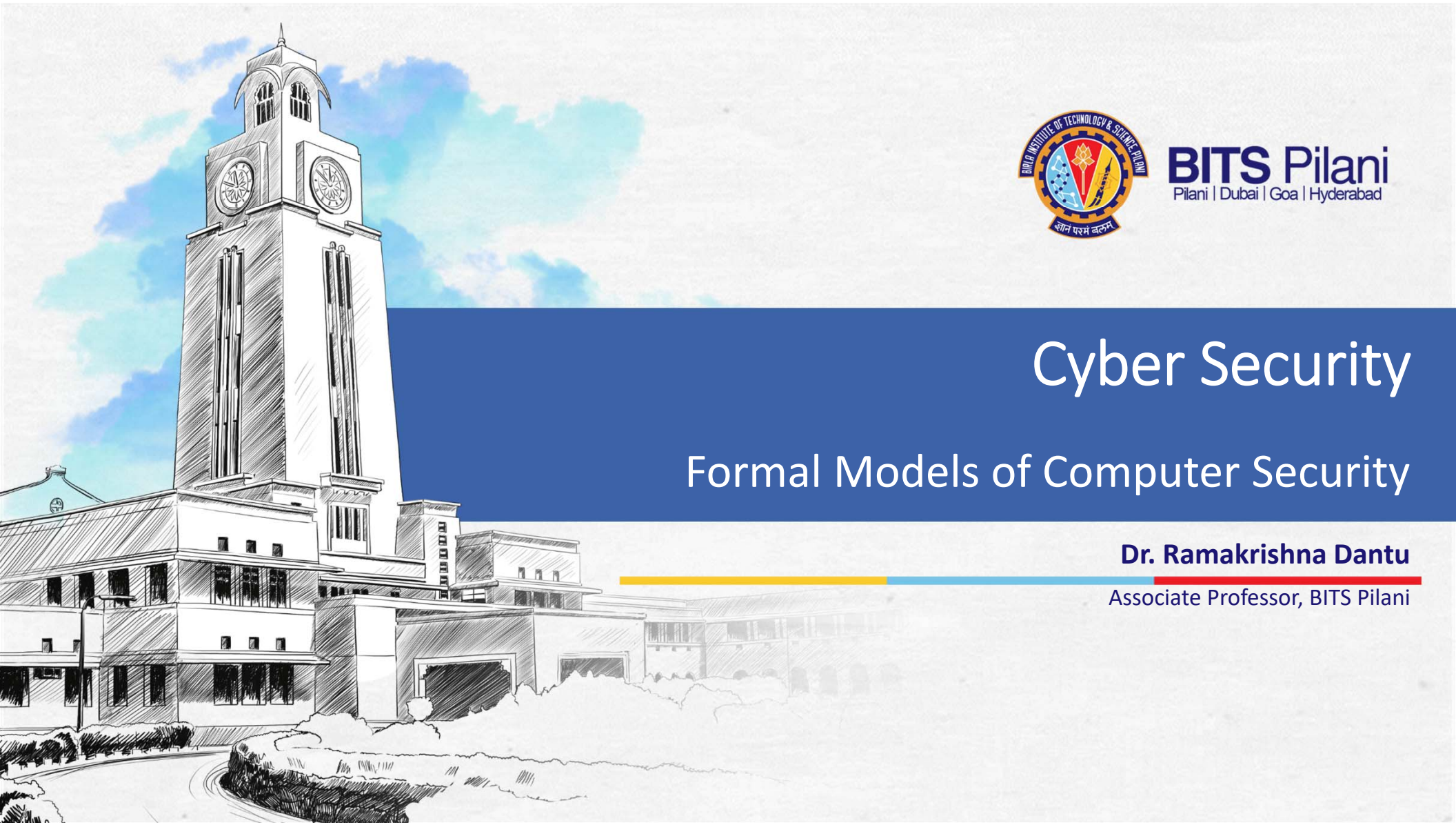


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Formal Models of Computer Security

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

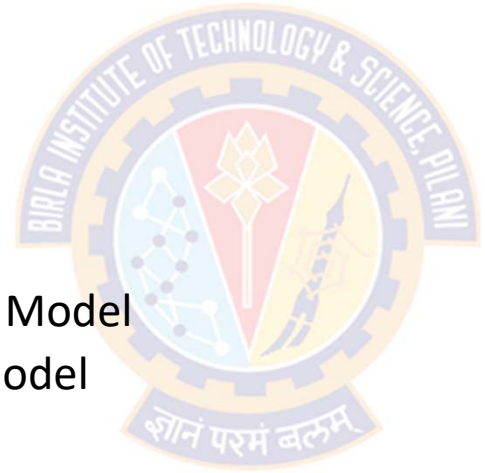
Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Formal Models of Computer Security

Agenda

- The CIA Classification:
  - Confidentiality Policies:
    - Bell-LaPadula Model
  - Integrity Policies:
    - The Biba Model
    - Lipner's Integrity Matrix Model
    - Clark-Wilson Integrity Model
    - Trust Models
  - Availability Policies:
    - Deadlock
    - Denial of Service Models



Confidentiality Policies

Overview

- A confidentiality policy, also called an information flow policy
- Goal: prevent the unauthorized disclosure of information
  - Deals with the flow of information
  - Unauthorized alteration (integrity) of information is secondary
- Multi-level security models are best-known examples
  - Bell-LaPadula Model basis for many, or most, of these
- Example
  - In the United States, the Privacy Act requires that certain personal data be kept confidential
  - Income tax returns are legally confidential and are available only to the Internal Revenue Service or to legal authorities with a court order
  - Governmental models represent the policies that satisfy these requirements

Bell LaPadula Model

Bell LaPadula Model

Overview

- David Bell and Leonard LaPadula first described the DoD multilevel military security policy in 1973 in abstract, formal mathematical terms
- Each subject and each object is assigned a security class
- Security classes form a strict hierarchy and are referred to as security levels
- Example: The U.S. military classification scheme:
  - top secret > secret > confidential > restricted > unclassified
- Example: Commercial classification scheme
  - strategic > sensitive > confidential > public

Bell LaPadula Model

innovate achieve lead

Overview

- Levels consist are:
  - *Security clearance L(s)* for subjects
    - A subject is said to have a security clearance of a given level
  - *Security classification L(o)* for objects
    - An object is said to have a security classification of a given level
- A subject's (usually a user's) access to an object (usually a file) is allowed or disallowed by
  - comparing the object's security classification with the subject's security clearance
- BPL model uses mathematical notation and set theory to define the concepts of:
  - a secure state, the modes of access, and the rules for granting access

Bell LaPadula Model

innovate achieve lead

Example

security level	*subject*	*object*
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	Ulaley	Telephone Lists

- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- Ulaley can only read Telephone Lists

Bell LaPadula Model

innovate achieve lead

Access Modes

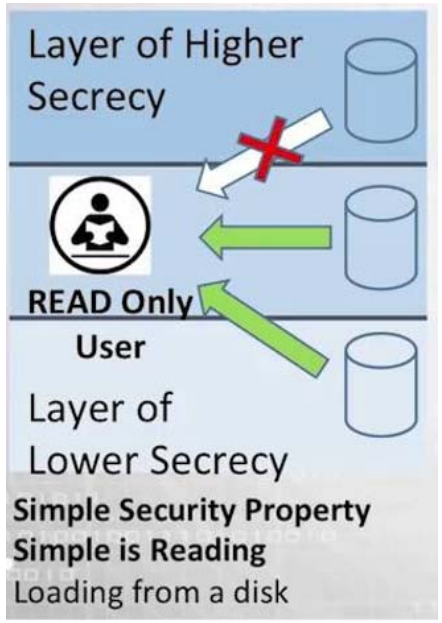
- Multilevel Security (MLS)
  - When multiple categories or levels of data are defined, the requirement is referred to as multilevel security (MLS)
- The BLP model defined four access modes
  - read:
    - The subject is allowed only read access to the object
  - append:
    - The subject is allowed only write access to the object
  - write:
    - The subject is allowed both read and write access to the object.
  - execute:
    - The subject is allowed neither read nor write access to the object but may invoke the object for execution.

Bell LaPadula Model

innovate achieve lead

Reading Information

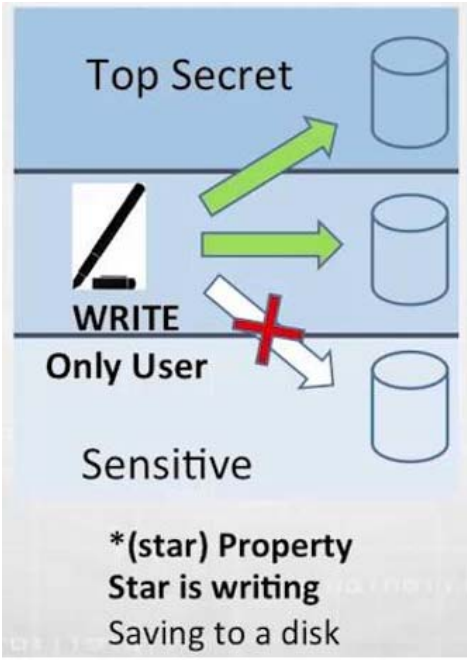
- Information flows up, not down
  - "Reads up" disallowed, "reads down" allowed
- Simple Security Condition (Step 1)
  - A subject may only read an object if she has a clearance level equal to or greater than the security level of the file
  - Subject s can read object o iff, $L(o) \leq L(s)$ and s has permission to read o
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called "no reads up" rule



Bell LaPadula Model

Writing Information

- Information flows up, not down
  - "Writes up" allowed, "writes down" disallowed
- *-Property (Step 1)
  - A subject is allowed write access to an object (a file) only if the security level of the object is greater than or equal to the clearance level of the subject
  - Subject s can write object o iff $L(s) \leq L(o)$ and s has permission to write o
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called "no writes down" rule



Bell LaPadula Model

innovate achieve lead

Three Basic Rules

- The *-property (star property) (Step-1)
  - This makes it impossible for data from a highly cleared subject to become available to users with a lower security clearance in an object (file/directory) with a low security level
  - Without this rule, a user with a high security clearance could copy sensitive data into a low security clearance document—thus allowing "confidential" data to be written down, or to flow from a "top secret" to an "unclassified" level

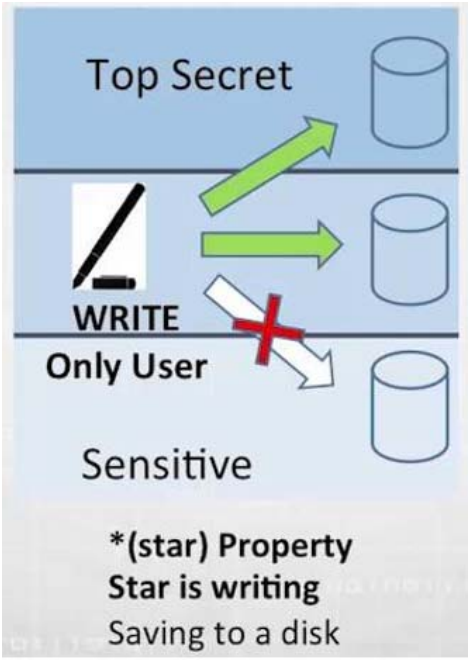


Image Source: Skillset.com

Bell LaPadula Model

Three Basic Rules

- The simple security condition (Step-1)
  - someone with a "secret" security level cannot read a file with a "top secret" security level, but can read a file with a "secret" or "confidential" security level
- The tranquility property
  - It states that the security level of an object cannot be changed while it is being processed by a computer system
  - This keeps a program or attack from modifying the sensitivity of a file while it is open and vulnerable

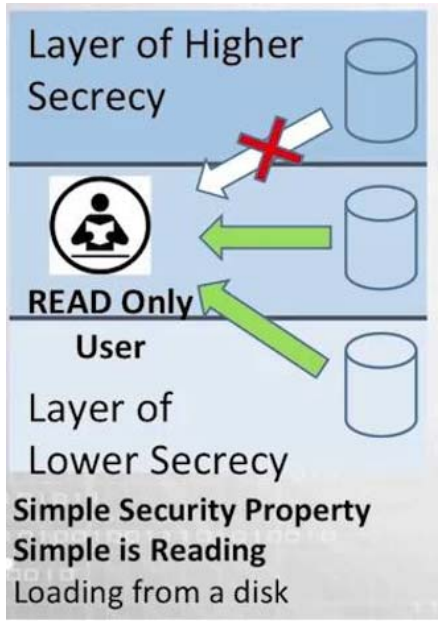
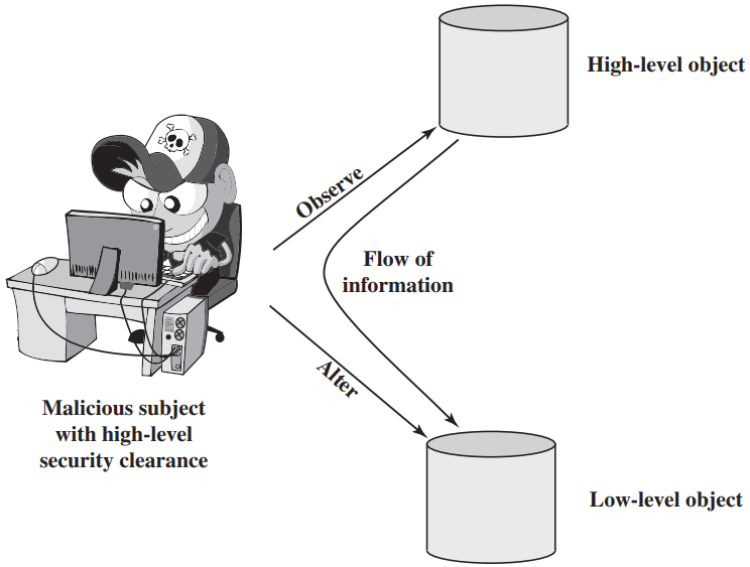


Image Source: Skillset.com

Bell LaPadula Model

Three Basic Rules

- What is the need for the *-property?
- Here, a malicious subject passes classified information along by putting it into an information container labeled at a lower security classification than the information itself
- This will allow a subsequent read access to this information by a subject at the lower clearance level



Bell LaPadula Model

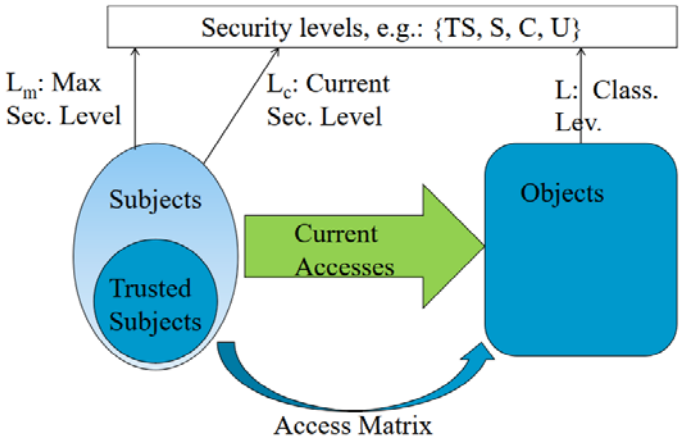
Approach

- Use state-transition systems to describe computer systems
- Define a system as secure iff. every reachable state satisfies 3 properties
  - simple-security property
  - *-property
  - discretionary security property

Bell LaPadula Model

Approach

- A computer system is modeled as a state transition system
  - There is a set of subjects; some are designated as trusted
  - Each state has objects, an access matrix, and the current access information
  - There are state transition rules describing how a system can go from one state to another
  - Each subject s has a maximal sec level $L_m(s)$ and a current sec level $L_c(s)$
  - Each object has a classification level



Bell LaPadula Model

Approach

- A state is considered secure if it satisfies
  - Simple Security Condition (no read up):
    - S can read O iff $L_m(S) \geq L(O)$
  - The Star Property (no write down): for any S that is not trusted
    - S can read O iff $L_c(S) \geq L(O)$
    - S can write O iff $L_c(S) \leq L(O)$
  - Discretionary-security property
    - every access is allowed by the access matrix
- A system is secure if and only if every reachable state is secure

Bell LaPadula Model

Is BLP Notion of Security Good?

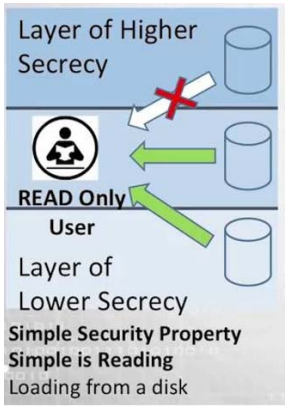
- The objective of BLP security is to ensure
  - a subject cleared at a low level should never read information classified high
  - The ss-property and the *-property are sufficient to stop such information flow at any given state
  - What about information flow across states?

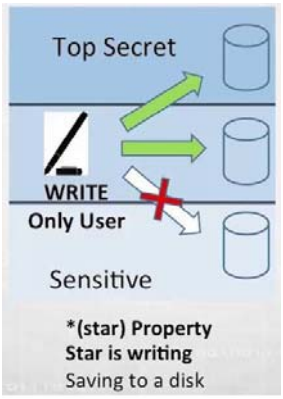
Bell LaPadula Model

innovate achieve lead

Is BLP Notion of Security Good?

- Consider a system with s_1, s_2, o_1, o_2
- And the following execution
  - s_1 gets access to o_1, read something, release access, then change current level to low, get write access to o2, write to o2
- Every state is secure, yet illegal information exists
- Solution:
  - Tranquility principle: subject cannot change current levels



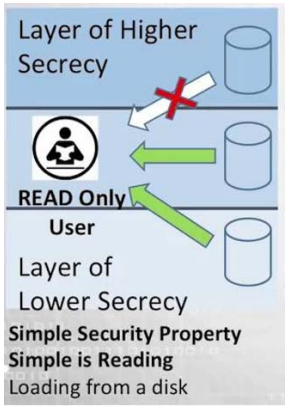


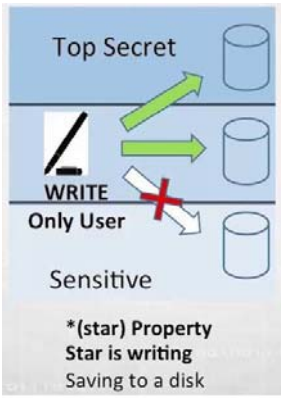
Bell LaPadula Model

innovate achieve lead

Principle of Tranquility

- Strong Tranquility
  - The clearances of subjects, and the classifications of objects, do not change during the lifetime of the system
- Weak Tranquility
  - The clearances of subjects, and the classifications of objects, do not change in a way that violates
    - the simple security condition or the *-property during the lifetime of the system





Bell LaPadula Model

innovate achieve lead

Extension

- Why Extension is needed?
  - Since all information is not meant for all people, we need to classify the information too into categories
  - Categories also known as compartments
- Typical military security categories
  - Nuclear Defense (abbreviated: NUC)
  - European Politics (EUR)
  - US Governmental issues (US)
  - army, navy, air force
  - nato, nasa, noforn
- Typical commercial security categories
  - Sales, , R&D, HR
  - Dept A, Dept B, Dept C
- But how these categories can go with security classification levels:
  - Top Secret (TS), Secret (S), Confidential (c) and Unclassified (UC)

Bell LaPadula Model

Attaching Category with i) User and ii) Info. Security Levels

- Example:
  - William may be cleared into the level:
    - (SECRET, {EUR}) and
  - George may be cleared into the level
    - (TOP SECRET,{NUC,US})
- A document may be classified as
  - (CONFIDENTIAL, {EUR})
- How can we compare the security levels of user with that of documents?
- This is needed to satisfy the Bell-LaPadula model

Bell LaPadula Model

innovate achieve lead

Security Categories and Dominance

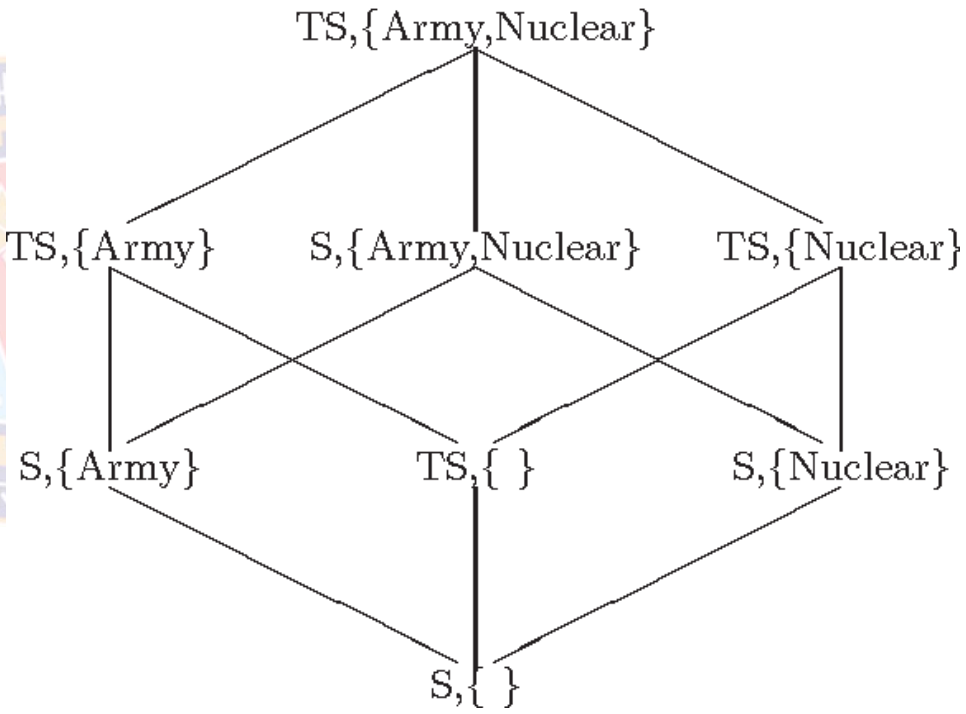
- Security Level = {Security Classification, {Set of Categories})
  - E.g., (top-secret, {Nuclear, NATO})
- Security level A dominates B if and only if:
  - A's classification level > B's classification level, and
  - A's category set contains B's
- That is,
  - $(SC_1, C_1) \geq (SC_2, C_2)$ iff. $SC_1 \geq SC_2$ and $C_2 \subseteq C_1$
- For instance
  - (top-secret, {Nuclear, NATO}) dominates (secret, {NATO})
- because
  - top-secret > secret, and
  - the set {Nuclear, NATO} contains {NATO}

Bell LaPadula Model

innovate achieve lead

Lattice of Categories

- (TS, {Army, Nuclear}) dominates (S, {Army})
- (TS, {Army, Nuclear}) dominates (TS, {Nuclear})
- (S, {Army, Nuclear}) dominates (S, {Nuclear})
- (S, {Army}) dominates (S, {})



Integrity Policies

Integrity Policies

Overview

- Requirements
  - Very different than confidentiality policies
- Biba's models
  - Strict Integrity policy
- Lipner's model
  - Combines Bell-LaPadula, Biba
- Clark-Wilson model
- Trust models
  - Policy-based
  - Reputation-based

Integrity Policies

Requirements

- Users will not write their own programs, but will use existing production programs and databases.
- Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
- A special process must be followed to install a program from the development system onto the production system.
- The special process in requirement 3 must be controlled and audited.
- The managers and auditors must have access to both the system state and the system logs that are generated.

Integrity Policies

innovate achieve lead

Principles of Operation

- *Separation of duty*:
  - if two or more steps are required to perform a critical function, at least two different people should perform the steps
- *Separation of function*:
  - different entities should perform different functions
- *Auditing*:
  - recording enough information to ensure the abilities to both recover and determine accountability

The Biba Model

Overview

- The Biba Model or Biba Integrity Model developed by Kenneth J. Biba in 1975
- The model is based on information flow, and the objects and subjects are grouped into ordered levels of integrity
- The Biba model was designed after the BLP model
  - sometimes called the Bell-LaPadula upside down model
- Where the BLP model addresses confidentiality, the Biba model addresses integrity
- The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.
- The model is also built on state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity

The Biba Model

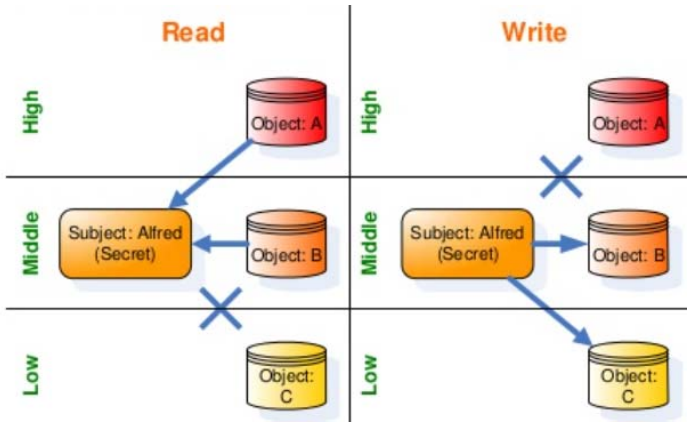
Overview

- Like other models, the Biba model supports the access control of both subjects and objects.
  - Subjects:
    - are the active elements in the system that can access information (processes acting on behalf of the users).
  - Objects:
    - are the passive system elements for which access can be requested (files, programs, etc.).
- Each subject and object will have a integrity level associated with it
  - denoted as I(S) and I(O) for subject S and object O, respectively
- A simple hierarchical classification uses a strict ordering of levels from lowest to highest
- Biba was designed to address three integrity issues:
  - Prevent modification of objects by unauthorized subjects.
  - Prevent unauthorized modification of objects by authorized subjects.
  - Protect internal and external object consistency

The Biba Model

Properties

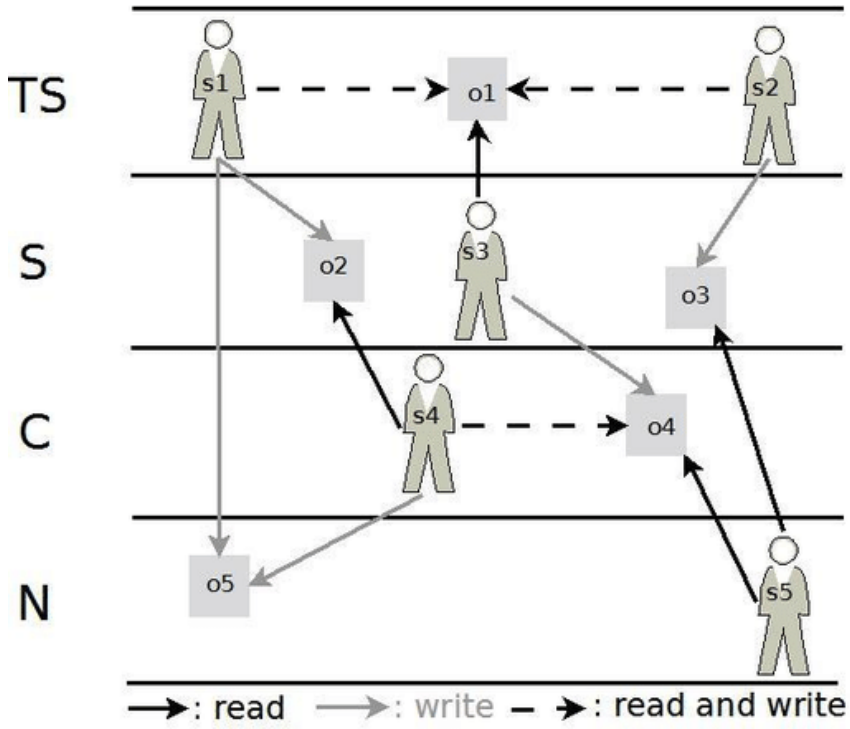
- Basic properties or axioms of the Biba model state machine:
  - The Simple Integrity Property
    - A subject cannot read an object at a lower integrity level (no read-down).
  - The * (star) Integrity Property
    - A subject cannot modify an object at a higher integrity level (no write-up)
  - Invocation Property
    - A subject cannot send messages (logical request for service) to object of higher integrity



Biba Model

innovate achieve lead

Properties



	o1	o2	o3	o4	o5
s1	read write	write			write
s2	read write		write		
s3	read			write	
s4		read		read write	write
s5			read	read	

Image Source: https://www.researchgate.net/figure/Two-Laws-of-Biba-Model-The-satisfaction-of-both-Biba-laws-prevents-the-information-flow_fig3_273706233

The Biba Model

Access Modes

- The Biba model consists of the following access modes:
- Modify:
  - The modify mode allows a subject to write to an object. This mode is similar to the write mode in other models.
- Observe:
  - The observe mode allows a subject to read an object. This command is synonyms with the read command of most other models.
- Invoke:
  - The invoke mode allows a subject to communicate with another subject.
- Execute:
  - The execute mode allows a subject to execute an object. The command essentially allows a subject to execute a program which is the object.

The Biba Model

Integrity Levels

- Each integrity level will be represented as L = (C, S) where:
  - L is the integrity level
  - C is the classification
  - S is the set of categories.
- The integrity levels then form a dominance relationship.
- Integrity level $L_1 = (C_1, S_1)$ dominates ($\geq$) integrity level $L_2 = (C_2, S_2)$ if and only if this relationship is satisfied:
  - $C_1 \geq C_2$ and $S_2 \subseteq S_1$

The Biba Model

Biba Policies

- The Biba model is actually a family of different policies that can be used.
- The goal of the model is to prevent the contamination of "clean" high level entities from "dirty" low level entities
- The model supports both mandatory and discretionary policies.
- The Mandatory Policies:
  - Strict Integrity Policy
  - Low-Watermark Policy for Subjects
  - Low-Watermark Policy for Objects
  - Low-Watermark Integrity Audit Policy
  - Ring Policy
- The Discretionary Policies:
  - Access Control Lists
  - Object Hierarchy
  - Ring

The Biba Model

Strict Integrity Policy

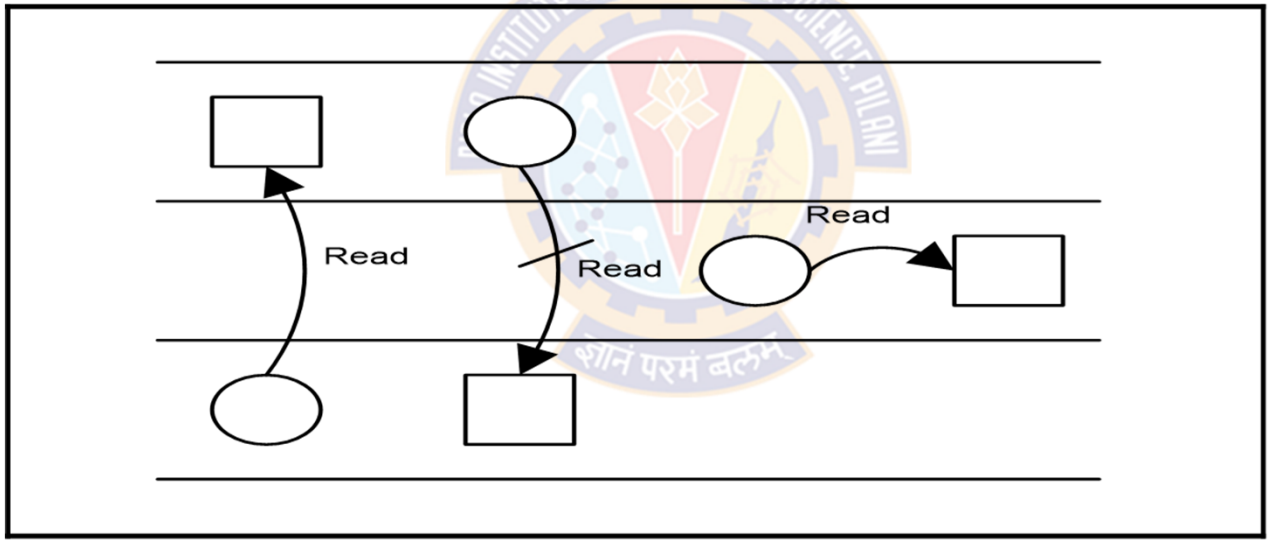
- Simple Integrity Condition ("no read-down"):
  - A subject can read an object only if : $I(S) \leq I(O)$.
  - $s \in S$ can observe $o \in O$ if and only if $i(s) \leq i(o)$
- Integrity Star Property ("no write-up"):
  - A subject can modify an object only if : $I(S) \geq I(O)$.
  - $s \in S$ can modify $o \in O$ if and only if $i(o) \leq i(s)$
- Invocation Property:
  - A subject can invoke/comm with another subject only if : $I(S1) \geq I(S2)$.
  - $s_1 \in S$ can invoke $s_2 \in S$ if and only if $i(s_2) \leq i(s_1)$

The Biba Model

innovate achieve lead

Strict Integrity Policy

- Simple Integrity Condition ("no read-down"):



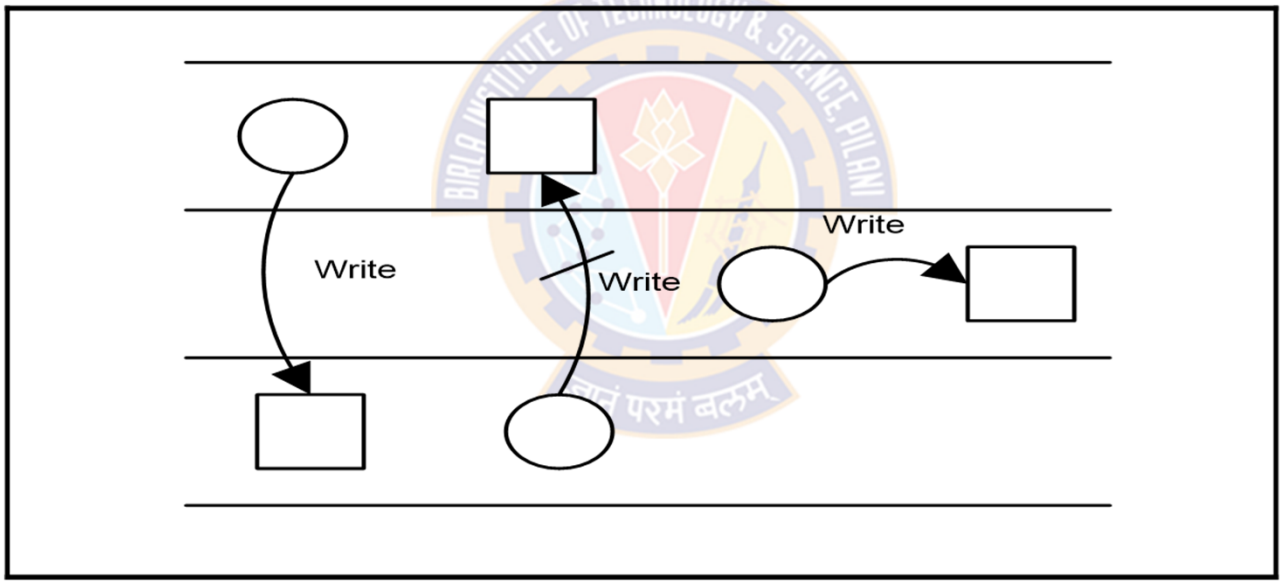
circle = subject, square = object

The Biba Model

innovate achieve lead

Strict Integrity Policy

- Integrity Star Property (“no write-up”):



circle = subject, square =object

The Biba Model

Strict Integrity Policy

- The "no write-up" is essential because it limits the damage that can be done by malicious objects in the system
- For instance:
  - "no write-up" limits the amount of damage that can be done by a trojan horse in the system
  - The trojan horse would only be able to write to objects at it integrity level or lower
  - This is important because it limits the damage that can be done to the operating system.
- The "no read-down" prevents a trust subject from being contaminated by a less trusted object

The Biba Model

Low-Water-Mark Policy

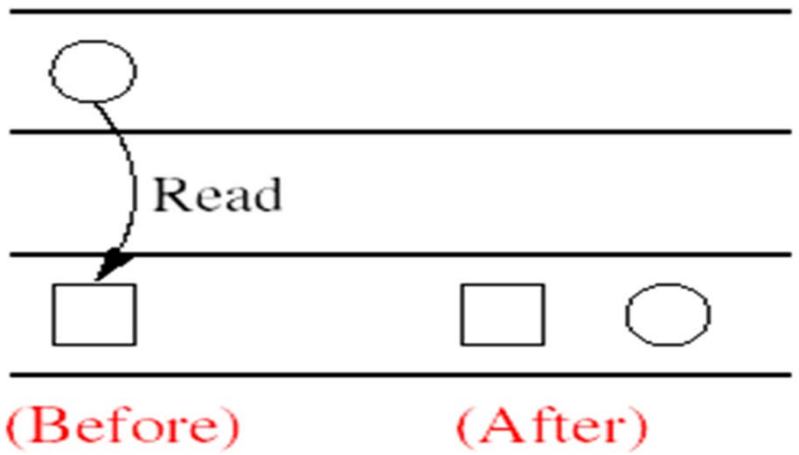
- The low-watermark policy for subjects
  - Is a relaxed "no read-down"
  - Contains these following rules:
    - Integrity Star Property:
      - s ∈ S can modify o∈ O if and only if i(o) ≤ i(s) (“no write-up”).
    - A subject may examine any object:
      - If s ∈ S examines o ∈ O then i’(s) = min(i(s),i(o)), where i’(s) is the subjects integrity level after the read.
    - Invocation Property:
      - s_1∈ S can invoke s_2 ∈ S if and only if i(s_2) ≤ i(s_1).

The Biba Model

innovate achieve lead

Low-Water-Mark Policy

- The low-watermark policy for subjects



circle = subject, square = object

The Biba Model

Low-Water-Mark Policy

- The low-watermark policy for subjects
  - Does nothing to restrict a subject from reading objects.
  - Is a dynamic policy, because it lowers the integrity level of a subject based on what objects are observed.
  - Drawback
    - One problem with this policy is that if a subject observes a less trusted object, it will drop the subjects integrity level to that of the object
    - Then later, if the subject needs to legitimately observe other objects, it may not be able to do so because the subjects integrity level has been lowered
    - The effect of this would be denial of service depending on the timing of the submissions.

The Biba Model

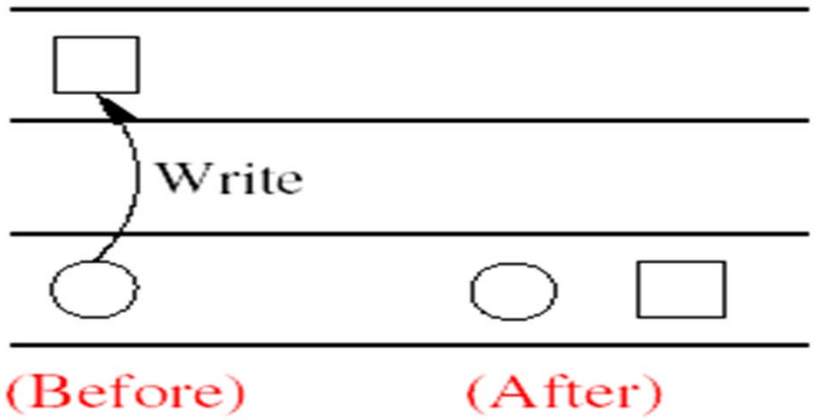
Low-Water-Mark Policy

- The low-watermark policy for objects
  - Is a relaxed "no write-down"
  - Contains the following rules:
    - s ∈ S can modify any o ∈ O regardless of integrity level.
    - If s ∈ S modifies o ∈ O then
      - i'(o) = min(i(s),i(o)), where i'(o) is the objects integrity level after it is modified.

The Biba Model

Low-Water-Mark Policy

- The low-watermark policy for objects



circle = subject, square = object

The Biba Model

innovate achieve lead

Low-Water-Mark Policy

- The low-watermark policy for objects
  - Is also a dynamic policy, similar to the low-watermark policy for subjects.
  - It does nothing to prevent an un-trusted subject from modifying a trusted object
    - In reality policy is not very practical.
  - The policy provides no real protection in a system
  - The policy simply lowers in the trust placed in the objects
  - If a malicious program was inserted into the computer system it could modify any object in the system
  - This model would just lower the integrity level of objects that have become contaminated

The Biba Model

Low-Water-Mark Policy

- The low-watermark Integrity Audit Policy
  - The policy consists of the following rules:
    - Any subject may modify any object, regardless of integrity levels.
    - If a subject modifies an object at higher integrity level (a more trusted object), it results in the transaction being recorded in an audit log.
  - The drawback to this policy is it does nothing to prevent an improper modifications of an object
  - This policy is similar to the low-watermark for objects policy, except in this case the objects integrity level is not lowered, it is recorded.
  - This policy simply records that an improper modification took place.

The Biba Model

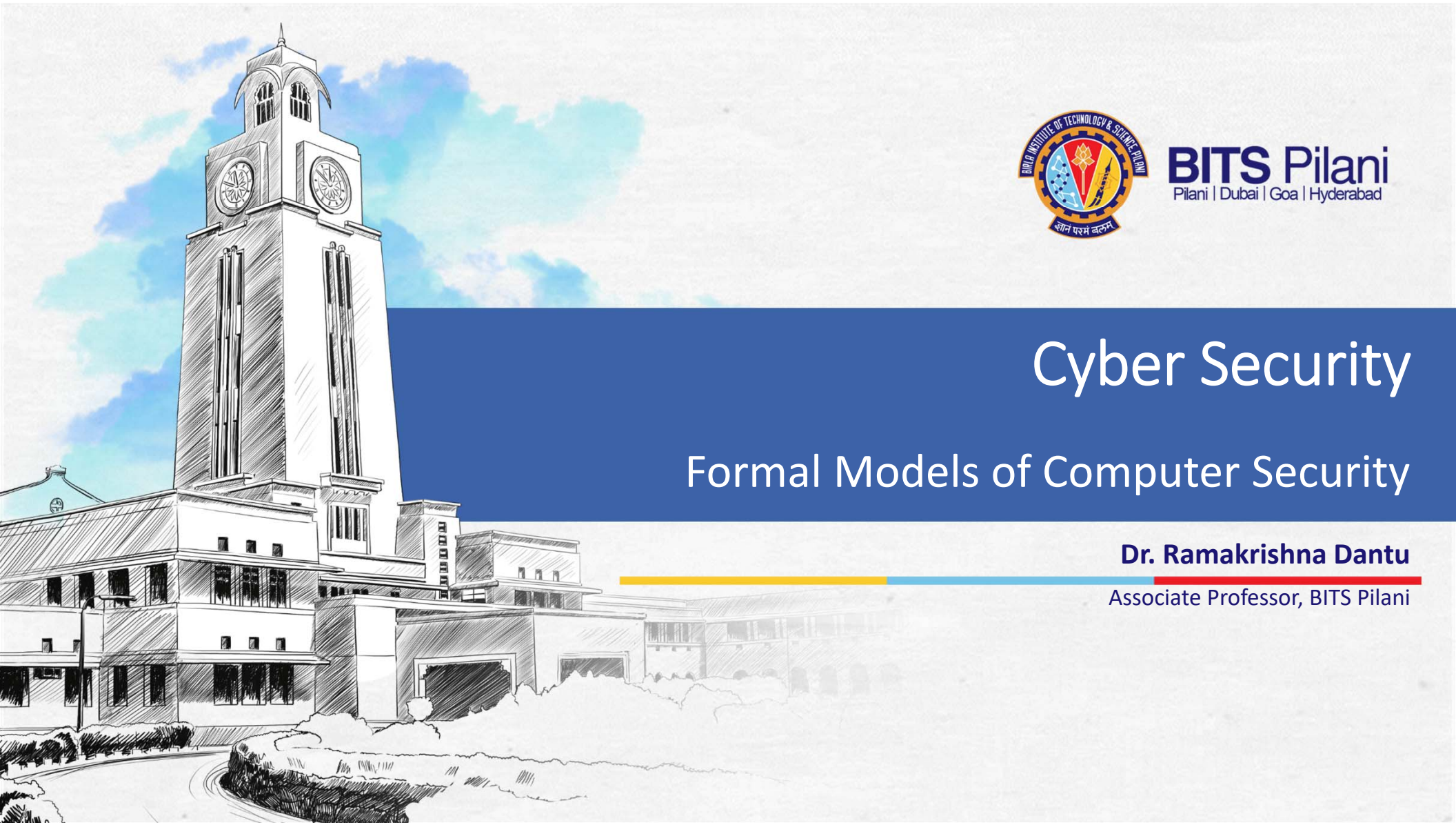
Drawbacks

- Advantages:
  - The Biba model is it simple and easy to implement.
  - The Biba model provides a number of different policies that can be selected based on need.
- Disadvantages:
  - The model does nothing to enforce confidentiality.
  - The Biba model doesn't support the granting and revocation of authorization.
  - To use this model all computers in the system must support the labeling of integrity for both subjects and objects
  - To date, there is no network protocol that supports this labeling. So there are problems with using the Biba model in a network environment.


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Formal Models of Computer Security

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

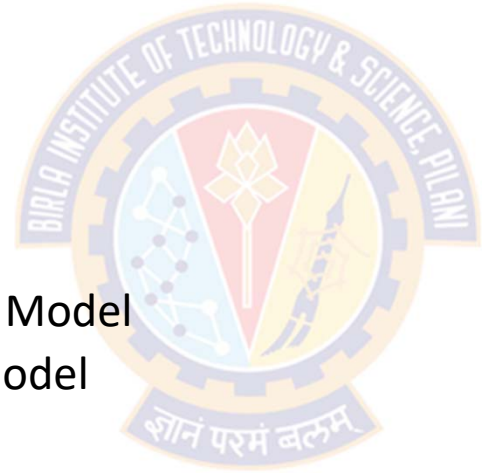
Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Formal Models of Computer Security

Agenda

- The CIA Classification:
  - Confidentiality Policies:
    - Bell-LaPadula Model
  - Integrity Policies:
    - The Biba Model
    - Lipner's Integrity Matrix Model
    - Clark-Wilson Integrity Model
    - Trust Models
  - Availability Policies:
    - Deadlock
    - Denial of Service Models



Lipner's Integrity Matrix

Integrity Policies - Recap

Commercial Integrity Constraints

- Users will not write their own programs, but use existing production software and databases
- Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
- A special process must be followed to install a program from the development system onto the production system.
- The special process in requirement 3 must be controlled and audited.
- The managers and auditors must have access to both the system state and the system logs that are generated.

Lipner's Integrity Matrix

Overview

- Lipner devised his Integrity Matrix Model specifically to handle those concerns/constraints in a commercial environment
- Liper's model accomplishes this by combining the elements of Bell La-Padula and Biba models to provide confidentiality and integrity
- Does it in two steps
  - Bell-LaPadula component first (Confidentiality)
  - Add in Biba component (Integrity)

Lipner's Integrity Matrix

Lipner's Use of Bell-LaPaluda Model

- There are two confidentiality levels (higher to lower):
  - Audit Manager (AM):
    - system audit and management functions are at this level.
  - System Low (SL):
    - any process can read information at this level
- In addition there are five confidentiality categories:
  - Development (D):
    - production programs under development and testing, but not yet in production use
  - Production Code (PC):
    - production processes and programs
  - Production Data (PD):
    - data covered by the integrity policy
  - System Development (SD):
    - system programs under development, but not yet in production use
  - Software Tools (T):
    - programs provided on the production system not related to the sensitive or protected data

Lipner's Integrity Matrix

User/Subject Properties

- Lipner then assigned users to security levels based on their jobs.
- Ordinary users
  - can execute (read) production code but cannot alter it
  - can alter and read production data
  - cannot execute category T (Software Tools), so they cannot write their own programs
- Application Developers
  - need access to tools for developing their programs
  - do not have read/write access to PD (Production Data), so cannot access production data
  - If they need production data, the data must first be downgraded to D (this requires sys admins)

Lipner's Integrity Matrix

User/Subject Properties

- Lipner then assigned users to security levels based on their jobs.
- System Programmers
  - System programmers develop system programs and, like application programmers, use tools to do so
- System managers and Auditors
  - need access to all logs but cannot change levels of objects
- System controllers
  - need to install code
  - must have the ability to downgrade code once it is certified for production, so other entities cannot write to it;
- Etc.

Lipner's Integrity Matrix

Users and Security Levels

- Lipner then assigned users to security levels based on their jobs

Subjects	Description	Security Level
Ordinary users	Will use production code to modify production data	(SL, { PC, PD })
Application developers	Develop programs and need access to tools for developing their programs	(SL, { D, T })
System programmers	Develop system programs and, use tools to do so	(SL, { SD, T })
System managers and auditors	Need high clearance to be able to access all logs	(AM, { D, PC, PD, SD, T })
System controllers	Must have the ability to downgrade code once it is certified for production, so other entities cannot write to it	(SL, {D, PC, PD, SD, T}) and downgrade privilege

- E.g.: Ordinary users have security level of System Low (SL) under the categories of Production Code and Production Data
- E.g.: System Programmers have security level of System Low (SL) under the categories of System Development and Software Tools

Lipner's Integrity Matrix

Users and Security Levels

- Lipner then assigned users to security levels based on their jobs

Security Level → Categories↓	**Audit Manager (AM)**	**System Low (SL)**
Development (D)	System managers and auditors	Application Developers; System Controller
Production Code (PC)	System managers and auditors	Ordinary Users; System Controller
Production Data (PD)	System managers and auditors	Ordinary Users; System Controller
System Development (SD)	System managers and auditors	System Programmers; System Controller
Software Tools (T)	System managers and auditors	Application Developers; System Programmers; System Controller

Lipner's Integrity Matrix

Objects and Classifications

- Objects are assigned to security levels/categories based on who should access them
- Objects that might be altered have two categories:
  - that of the data itself and that of the program that may alter it
- For example:
  - Ordinary user needs to execute (read) production code,
    - so this is labeled (SL, {PC})
    - This is based on simple security policy of the Bell-LaPadula Model
  - Ordinary users should be able to write production data,
    - so this is labeled (SL, {PC, PD})
    - This is based on *-property of the Bell-LaPadula Model

Objects	Security Level
Development code/test data	(SL, { D, T })
Production code	(SL, { PC })
Production data	(SL, { PC, PD })
Software tools	(SL, { T })
System programs	(SL, ∅)
System programs in modification	(SL, { SD, T })
System and application logs	(AM, { *appropriate* })

Bell LaPadula Model

innovate achieve lead

Access Modes

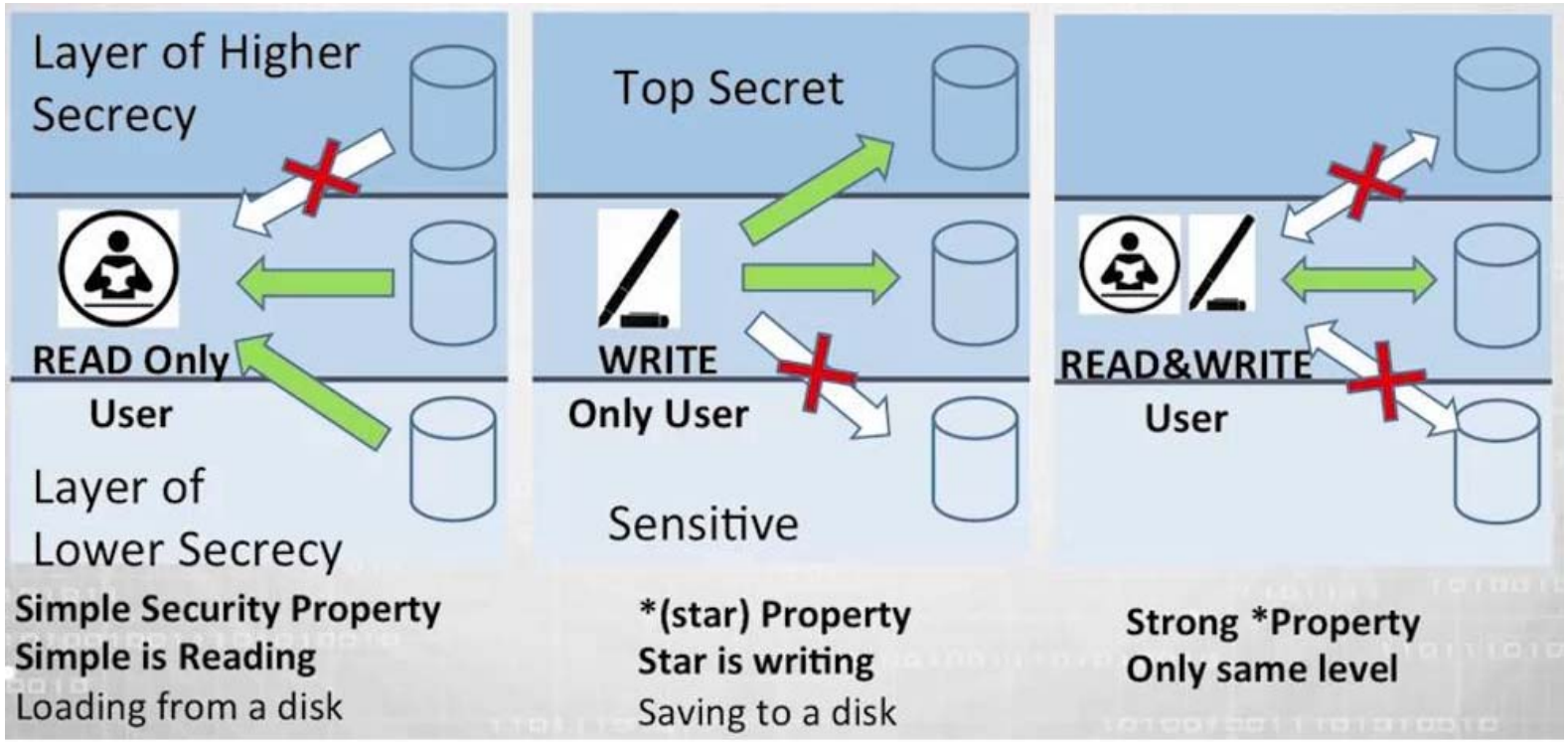


Image Source: Skillset.com

Lipner's Integrity Matrix

Subjects/Objects and Clearance/Classifications

Subjects	Clearance	Objects	Classification
Ordinary users	(SL, { PC, PD })	Development code/test data	(SL, { D, T })
Application developers	(SL, { D, T })	Production code	(SL, { PC })
System programmers	(SL, { SD, T })	Production data	(SL, { PC, PD })
System managers and auditors	(AM, { D, OC, OD, SD, T })	Software tools	(SL, { T })
System controllers	(SL, {D, PC, PD, SD, T}) and downgrade privilege	System programs	(SL, ∅)
		System programs in modification	(SL, { SD, T })
		System and application logs	(AM, { *appropriate* })

Here downgrade means the ability to move software (objects) from development to production

Lipner's Integrity Matrix

Check Requirements

Requirements	Check
Users will not write their own programs, but will use existing production programs and databases.	Users have no access to T, so cannot write their own programs
Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.	Applications programmers have no access to PD, so cannot access production data; if needed, it must be put into D, requiring the system controller to intervene
A special process must be followed to install a program from the development system onto the production system.	Installing a program requires downgrade procedure (from D to PC), so only system controllers can do it
The special process in requirement 3 must be controlled and audited.	Control: only system controllers can downgrade Audit: any such downgrading must be logged
The managers and auditors must have access to both the system state and the system logs that are generated.	System management and audit users are in AM and so have access to system state and logs

Lipner's Integrity Matrix

Problem

- The model is too inflexible in special-purpose software
  - For example, a program for repairing an inconsistent or erroneous production database cannot be application-level software
  - System managers cannot run programs for repairing inconsistent or erroneous production database
    - System managers at AM, production data at SL
- So to remedy these problems, Lipner integrates his model with Biba's model

Lipner's Integrity Matrix

Adding Biba

- Three integrity classifications (highest to lowest)
  - ISP(System Program): for system programs
  - IO (Operational): production programs, development software
  - ISL (System Low): users get this on log in
- Two integrity categories
  - ID (Development): development entities
  - IP (Production): production entities

ISP > IO > ISL

Lipner's Integrity Matrix

Simplify Bell-LaPadula (Confidentiality)

- In the original model, the security category T (tools) allowed:
  - application developers and system programmers to use the same programs without being able to alter those programs
- The revised model now distinguishes two integrity categories:
  - Development and Production
  - They serve the purpose of the security tools (T) category, which is eliminated from the model
- Production code and production data is collapsed into a single category (called SP)

Lipner's Integrity Matrix

Simplify Bell-LaPadula (Confidentiality)

- This gives rise to the following three confidentiality categories:
  - Production (SP):
    - Production code (PC) and data (PD)
  - Development (SD):
    - Same as previous category Development (D)
  - System Development (SSD):
    - Same as previous category System Development (SD)

Subjects	Original	New
Development	D	SD
Production Code (PC):	PC	SP
Production Data (PD):	PD	SP
System Development (SD):	SD	SSD
Software Tools (T):	T	Eliminated

Lipner's Integrity Matrix

Users and Levels

- The integrity classes are chosen to allow modification of data and programs as appropriate
- For Example:
  - Ordinary users should be able to modify production data, so users of that class must have write access to integrity category IP
  - App developers should be able to have write access to integrity category ID
- Table shows the integrity levels and security categories of users.

Subjects	Security Level	Integrity Level
Ordinary users	(SL, { SP })	(ISL, { IP })
Application developers	(SL, { SD })	(ISL, { ID })
System programmers	(SL, { SSD })	(ISL, { ID })
System managers and auditors	(AM, { SP, SD, SSD })	(ISL, { IP, ID})
System controllers	(SL, { SP, SD }) and downgrade privilege	(ISP, { IP, ID})
Repair	(SL, { SP })	(ISL, { IP })

ISP > IO > ISL

Lipner's Integrity Matrix

Comparison of Old and New Security Levels

	Original	New	New
Subjects	**Confidentiality Level**	**Confidentiality Level**	**Integrity Level**
Ordinary users	(SL, { PC, PD })	(SL, { SP })	(ISL, { IP })
Application developers	(SL, { D, T })	(SL, { SD })	(ISL, { ID })
System programmers	(SL, { SD, T })	(SL, { SSD })	(ISL, { ID })
System managers and auditors	(AM, { D, OC, OD, SD, T })	(AM, { SP, SD, SSD })	(ISL, { IP, ID})
System controllers	(SL, {D, PC, PD, SD, T}) and downgrade privilege	(SL, { SP, SD }) and downgrade privilege	(ISP, { IP, ID})
Repair	Not available	(SL, { SP })	(ISL, { IP })

Here downgrade means the ability to move software (objects) from development to production ISP > IO > ISL

Lipner's Integrity Matrix

Objects and Classifications

- The final step is to select integrity classes for objects
- Consider the objects Production Code and Production Data
- Ordinary users must be able to:
  - write production data, but not production code
- By placing:
  - Production Data in integrity class (ISL, {IP}) and
  - Production Code in integrity class (IO, {IP})

  an ordinary user cannot alter production code but can alter production data (IO > ISL)
- Similar analysis leads to the levels shown in the next table

Lipner's Integrity Matrix

Objects and Classifications

Objects	Security Level	Integrity Level
Development code/test data	(SL, { SD })	(ISL, { IP})
Production code	(SL, { SP })	(IO, { IP })
Production data	(SL, { SP })	(ISL, { IP })
Software tools	(SL, ∅)	(IO, { ID })
System programs	(SL, ∅)	(ISP, { IP, ID })
System programs in modification	(SL, { SSD })	(ISL, { ID })
System and application logs	(AM, { *appropriate* })	(ISL, ∅)
Repair	(SL, {SP})	(ISL, { IP })

ISP > IO > ISL

Lipner's Integrity Matrix

Subjects/Objects and Clearance/Classifications - Revised

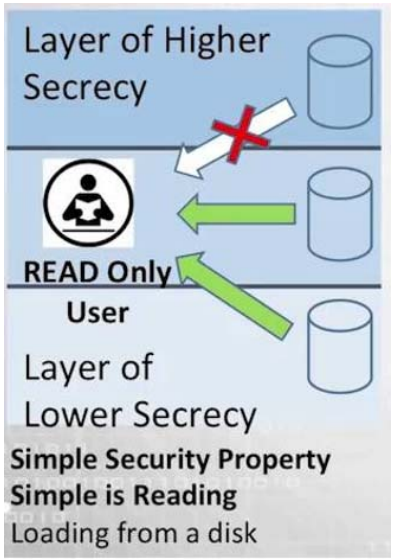
Subjects	Clearance	Integrity Level	Objects	Classification	Integrity Level
Ordinary users	(SL, { SP })	(ISL, { IP })	Development code/test data	(SL, { D, T })	(ISL, { IP})
Application developers	(SL, { SD })	(ISL, { ID })	Production code	(SL, { SP })	(IO, { IP })
System programmers	(SL, { SSD })	(ISL, { ID })	Production data	(SL, { SP })	(ISL, { IP })
System managers and auditors	(AM, { SP, SD, SSD })	(ISL, { IP, ID})	Software tools	(SL, {∅})	(IO, { ID })
System controllers	(SL, { SP, SD }) and downgrade privilege	(ISP, { IP, ID})	System programs	(SL, {∅})	(ISP, { IP, ID })
Repair	(SL, { SP })	(ISL, { IP })	System programs in modification	(SL, { SSD })	(ISL, { ID })
			System and application logs	(AM, { *appropriate* })	(ISL, {∅})
			Repair	(SL, {SP})	(ISL, { IP })

ISP > IO > ISL

Lipner's Integrity Matrix

Repair Class of Users

- Has the same integrity and security clearance as that of production data
  - so can read and write that data
- It can also
  - read production code
    - same security classification and (IO, {IP}) *dom* (ISL, {IP})
  - read system programs
    - (SL, {SP}) *dom* (SL, { ϕ }) and (ISP, { IP, ID }) *dom* (ISL, { IP })
  - repair objects
    - same security classes and same integrity classes



Lipner's Integrity Matrix

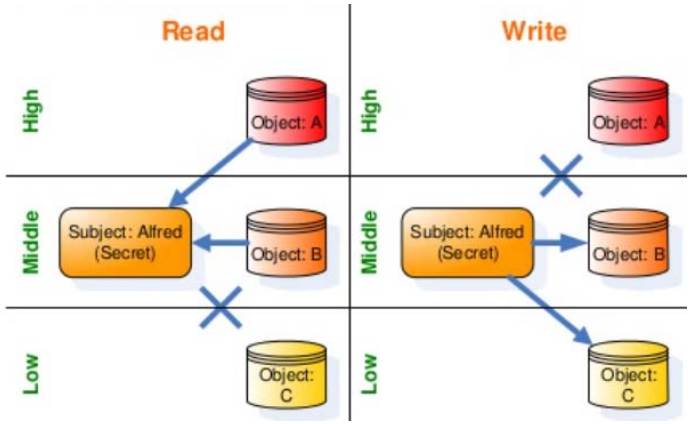
Repair Class of Users (Contd…)

- It can write, but not read
  - the system and application logs, because
    - (AM, { SP }) *dom* (SL, { SP }) and (ISL, { IP }) *dom* (ISL, { ϕ })
- It cannot access
  - development code/test data
    - since the security categories are disjoint
  - system programs in modification
    - since the integrity categories are disjoint
  - software tools
    - since the integrity categories are disjoint
- Thus, the repair function works as needed

Lipner's Integrity Matrix

What can an ordinary user do?

- Ordinary users can : (SL, { SP }) (ISL, { IP })
  - Read and write production data (same security integrity levels)
  - Read production code
    - same classification – Can Read
    - (IO, IP) *dom* (ISL, {IP}) – Cannot write
  - System program
    - (SL, {SP}) *dom* (SL, ∅) &
    - (ISP, {IP,ID}) *dom* {ISL, {IP})
  - Repair objects (same levels)
  - Write (not read) the system and application log
    - (AM, {SP}) *dom* (SL, {SP}) &
    - (ISL, {IP}) *dom* {ISL, ∅})



Biba model

Clark-Wilson Integrity Model

Clark-Wilson Integrity Model

Overview

- Clark and Wilson proposed a more elaborate and practical integrity model in 1987
- The Clark-Wilson integrity model (CWM) is specifically designed for commercial operations
- The CWM defines each data item and allows modifications through only a small set of programs
- The CWM does not use of a lattice structure used to define the levels of security that an object may have and that a subject may have access to
- Instead, it uses a three part relationship of subject/program (transaction)/object known as a triple or an access control triple

Clark-Wilson Integrity Model

Overview

- Integrity defined by a set of constraints
  - Data is said to be in a *consistent* state (or consistent) if it satisfies given properties
- Example: Bank
  - *D* today's deposits, *W* withdrawals, *YB* yesterday's balance, *TB* today's balance
  - Integrity constraint: $YB + D - W = TB$
- Before and after each action, the consistency conditions must hold.

Clark-Wilson Integrity Model

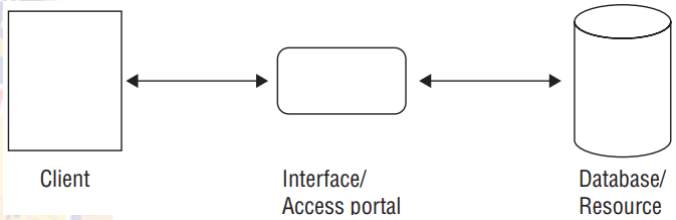
Four Basic Constraints

- Clark and Wilson claimed that the following are four fundamental constraints of any reasonable commercial integrity model:
- Authentication:
  - identity of all users must be properly authenticated.
- Audit:
  - modifications should be logged to record every program executed and by whom, in a way that cannot be subverted.
- Well-formed transactions:
  - Users manipulate data only in constrained ways. Only legitimate accesses are allowed.
  - Is a series of operations that transition the system from one consistent state to another consistent state
- Separation of duty:
  - Who examines and certifies that the transactions are performed correctly?
  - The system associates with each user a valid set of programs they can run and prevents unauthorized modifications, thus preserving integrity and consistency with the real world.

Clark-Wilson Integrity Model

Two Principles

- In CWM, subjects do not have direct access to objects
  - Objects can be accessed only through programs



- CWM provides an effective means of protecting integrity through the use of two principles:
  - Well-formed transactions:
    - A user should not manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of the data.
  - Separation of duty among users:
    - Any person permitted to create or certify a well-formed transaction may not be permitted to execute it (at least against production data)

Clark-Wilson Integrity Model

Entities

- The CWM defines data as:
  - Constrained Data Items (CDIs)
    - Is any data item whose integrity is protected by the security model
  - Unconstrained Data Items (UDIs)
    - Any data item whose integrity is not protected by the security model
    - Any data that is to be input and hasn't been validated, or any output. E.g., a simple text file
- The CWM also defines two sets of procedures:
  - Integrity verification procedures (IVPs)
    - Procedures that ensure CDIs conform to the integrity constraints at the time the IVPs are run
  - Transformation procedures (TPs)
    - Are the only procedures that are allowed to modify a CDI
    - Procedures that change the state of the data in the system from one valid state to another
    - TPs implement well-formed transactions

Clark-Wilson Integrity Model

Certification and Enforcement Rules

- The CWM enforces integrity by means of certification rules and enforcement rules on TPs
- Certification rules
  - are security policy restrictions on the behavior of Integrity verification procedure (IVPs) and Transformation procedures (TPs)
- Enforcement rules
  - are built-in system security mechanisms that achieve the objectives of the certification rules

Clark-Wilson Integrity Model

Certification and Enforcement Rules

- CR1: All IVPs must ensure that CDIs are in a valid state when the IVP is run
- CR2: All TPs must be certified as integrity-preserving
- CR3: Assignment of TPs to users must satisfy separation of duty
- CR4: The operation of TPs must be logged
- CR5: TPs executing on UDIs must result in valid CDIs
- ER1: Only certified TPs can manipulate CDIs
- ER2: Users must only access CDIs by means of TPs for which they are authorized
- ER3: The identity of each user attempting to execute a TP must be authenticated

Clark-Wilson Integrity Model

innovate achieve lead

Certification and Enforcement Rules

- Certification Rules 1 & 2
  - CR1:
    - All IVPs must properly ensure that all CDIs are in a valid state at the time the IVP is run.
    - When any IVP is run, it must ensure all CDIs are in a valid state
  - CR2:
    - All TPs must be certified to be valid and integrity-preserving
    - That is, they must take a CDI to a valid final state, given that it is in a valid state to begin with

Transformation Procedures (TPs)
Integrity verification procedures (IVPs)
Constrained Data Items (CDIs) = Data subject to integrity controls

Clark-Wilson Integrity Model

innovate achieve lead

Certification and Enforcement Rules

- Enforcement Rules 1 & 2
  - ER1
    - The system must maintain the list of certified relations specified in CR2 and must ensure that only TPs certified to run on a CDI manipulate that CDI.
  - ER2
    - Users must only access CDIs by means of TPs for which they are authorized
    - The system must associate a user with each TP and set of CDIs
    - The system must maintain a list of relations of the form (UserID, TPi, (CDIa, CDIb, CDIc, . . .)), which relates a user, a TP, and the data objects that TP may reference on behalf of that user
    - The TP may access those CDIs on behalf of the associated user
    - The TP cannot access that CDI on behalf of a user not associated with that TP and CDI

Clark-Wilson Integrity Model

innovate achieve lead

Certification and Enforcement Rules

- Users and Rules
  - CR3
    - The list of relations in ER2 must be certified to meet the separation of duty requirement.
  - ER3
    - The system must authenticate the identity of each user attempting to execute a TP.
      - Authentication not required before use of the system, but is required before manipulation of CDIs (requires using TPs)
- Logging
  - CR4
    - The operation of TPs must be logged
    - All TPs must be certified to write to an append-only CDI (the log)
    - All TPs must append enough information necessary reconstruct the operation
      - Auditor needs to be able to determine what happened during reviews of transactions

Clark-Wilson Integrity Model

innovate achieve lead

Certification and Enforcement Rules

- Handling Untrusted Input
  - CR5
    - Any TP that takes a UDI as an input value must be certified to perform only valid transformations, or else no transformations, for any possible value of the UDI
    - Typically, this is an edit program.
    - The transformation should take the input from a UDI to a CDI, or the UDI is rejected.
      - In bank, numbers entered at keyboard are UDIs, so cannot be input to TPs
      - TPs must validate numbers (to make them a CDI) before using them; if validation fails, TP rejects UDI

Clark-Wilson Integrity Model

innovate achieve lead

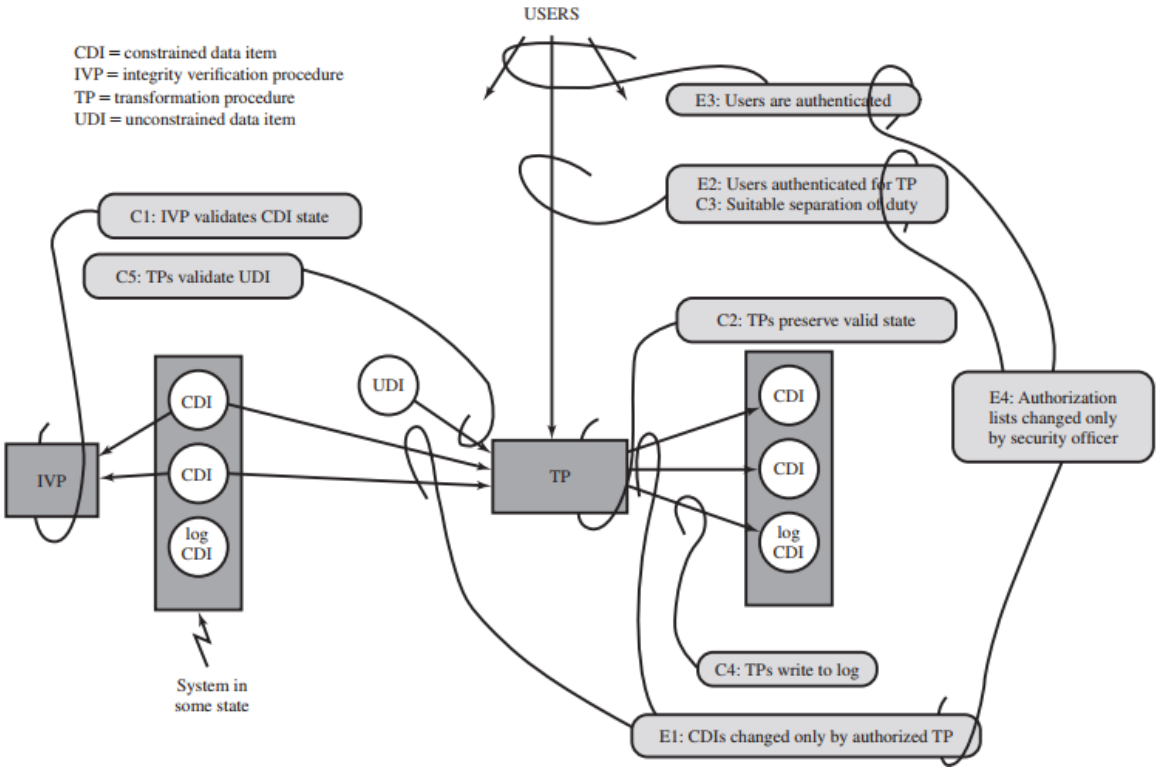
Certification and Enforcement Rules

- Separation of Duty Model
  - ER4
    - Only the agent permitted to certify entities may change the list of such entities associated with other entities:
      - Specifically, the list of TPs associated with a CDI and the list of users associated with a TP
    - An agent that can certify a TP or an entity associated with that TP may not have any execute rights with respect to that entity.
      - Enforces separation of duty with respect to certified and allowed relations

Clark-Wilson Integrity Model

innovate achieve lead

Certification and Enforcement Rules



Availability Policies

Availability Policies

Overview

- An availability policy ensures that a resource can be accessed in some way in a timely fashion
  - Availability is often expressed in terms of "quality of service."
- An availability policy defines the "type of access" and what a "timely fashion" means
  - "Timely fashion" depends on the nature of resource, the goals of subject using it

Availability Policies

innovate achieve lead

Overview

- Example_1:
  - A commercial website selling merchandise will need to display details of items for customer requests in a matter of seconds or, at worst, a minute
  - The goal of the customer is to see what the website is selling, and the goal of the site is to make information available to the customer
  - However, the site does not want customers to alter prices displayed on the website, so there is no availability for altering information
- Example_2:
  - A website enabling students to upload homework must allow some alterations (students must be able to upload their homework, possibly multiple times per assignment) quickly and no access for the students to read other students' assignments.

Availability Policies

Safety and Liveness

- When a resource or service is not available, a denial of service occurs
- This is related to two types problems: safety and liveness
- Safety problem
  - A denial of service resulting from the service giving incorrect responses
  - That is, the service is not performing the functions that the client is expecting
- Liveness problem
  - A denial of service that prevents users from accessing the service is a liveness problem
- But other problems can cause a denial of service, such as assignment of inadequate resources to a process

Availability Policies

Mechanisms to support availability

- Two requirements under which mechanisms are used to support availability:
  - a) in general
  - b) as a security requirement
- The difference between the two lies in the assumptions underlying the failures
  - That is, under what circumstances failures can occur

Availability Policies

Mechanisms to support availability

- Mechanisms to support availability in general
  - The failures occur naturally over time due to usage
  - Lack of accessibility is modeled using an average case, following a statistical model
  - For example:
    - The failure rates of disk drives depends upon many factors such as the age, the manufacturer, and environment and can be statistically modeled, although the precise model to be used is unclear
- Mechanisms used to support availability as a security requirement
  - Lack of availability assumes worst-case
  - Here, an adversary deliberately tries to make the resource or information unavailable
  - Because attackers induce this condition, models used in computer security describe failures that are nonrandom, and indeed may well be non-statistical

Deadlock

Overview

- A *deadlock* is a state in which some set of processes block each waiting for another process in the set to take some action.
- Deadlock can occur if four conditions hold simultaneously:
  - *Mutual exclusion:* At least one resource must be held in a non-sharable mode; If any other process requests this resource, then that process must wait for the resource to be released
  - *Hold and wait:* A process must be simultaneously holding at least one resource and waiting for at least one resource that is currently being held by some other process
  - *No preemption:* Once a process is holding a resource (i.e. once its request has been granted), then that resource cannot be taken away from that process until the process voluntarily releases it
  - *Circular wait:* A set of entities must be holding resources such that each entity is waiting for a resource held by another entity in the set
- Usually not due to an attack

Deadlock

innovate achieve lead

Methods of Handling Deadlocks

- *Prevention*: prevent 1 of the 4 conditions from holding
  - Do not allow the system to get into a deadlocked state.
  - Do not acquire resources until all needed ones are available
  - When needing a new resource, release all held
- *Avoidance*: ensure process stays in state where deadlock cannot occur
  - *Safe state*: deadlock can not occur
  - *Unsafe state*: may lead to state in which deadlock can occur
  - Abort a process or preempt some resources when deadlocks are detected
- *Detection*: allow deadlocks to occur, but detect and recover
  - If deadlocks only occur once a year or so, it may be better to simply let them happen and reboot as necessary than to incur the constant overhead and system performance penalties associated with deadlock prevention or detection
  - This is the approach that both Windows and UNIX take

Denial of Service

innovate achieve lead

Overview

- A denial of service occurs when a group of authorized users of a service makes that service unavailable to a (disjoint) group of authorized users for a period of time exceeding a defined maximum waiting time

Denial of Service

Overview

- What do we mean by "authorized user"?
- If a user is not authorized, then in theory access control mechanisms that protect the server will block the unauthorized users from accessing the server
- But in practice, the access control mechanisms may be ineffective
  - E.g., An intruder may compromise a user's account to gain access to a server
- The policy controlling access to a network server may be unworkable
- For example:
  - A policy states that only customers interested in the products sold may access the server—but the access control mechanisms could not tell whether a remote user accessing the server was interested in the products, or trying to block access by others
- Hence the first "group of authorized users" is simply the group of users with access to the service, whether the security policy grants them access or not.

Availability and Network Flooding

Example: SYN Flood Attack

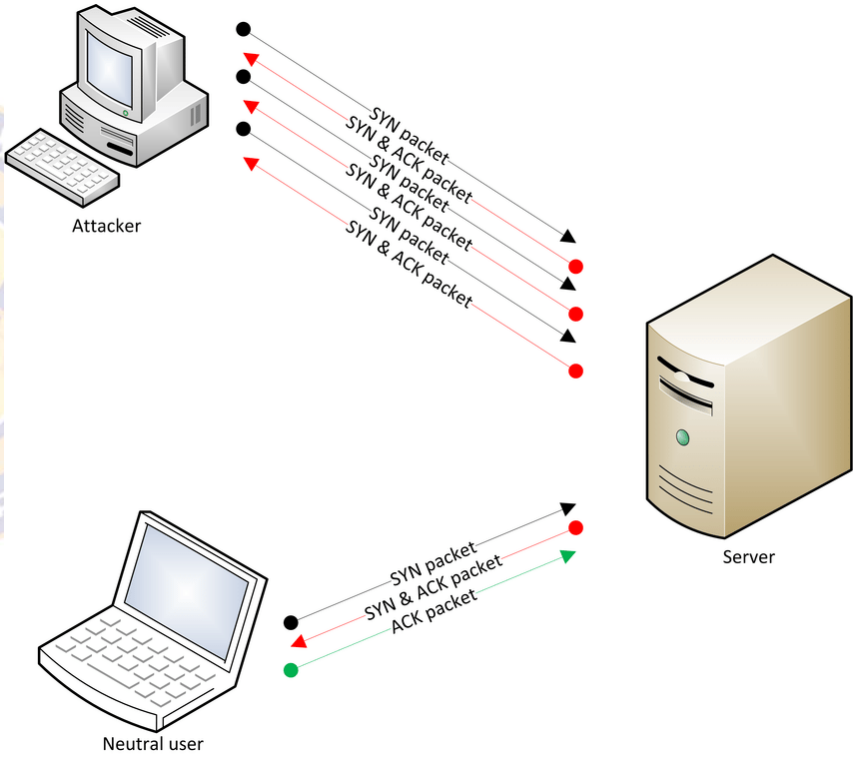
- Access over Internet must be unimpeded
- In flooding attacks attackers try to overwhelm system resources
- If many sources flood a target, it's called *distributed denial of service attack* (DDoS)
- The SYN flood is a type of most common type of flooding attack
  - SYN is short for "synchronize"
- It is based on the initiation of a connection using the TCP protocol
- A SYN flood sends a series of "SYN" messages to a computer (E.g., web server)

Availability and Network Flooding

innovate achieve lead

Example: SYN Flood Attack

- In a normal case, the user sends the SYN packet to the target
- When a server receives a SYN request, it responds with a SYN-ACK (synchronize acknowledge) message
- The source then responds with an ACK (acknowledge) message that establishes a connection between the two systems

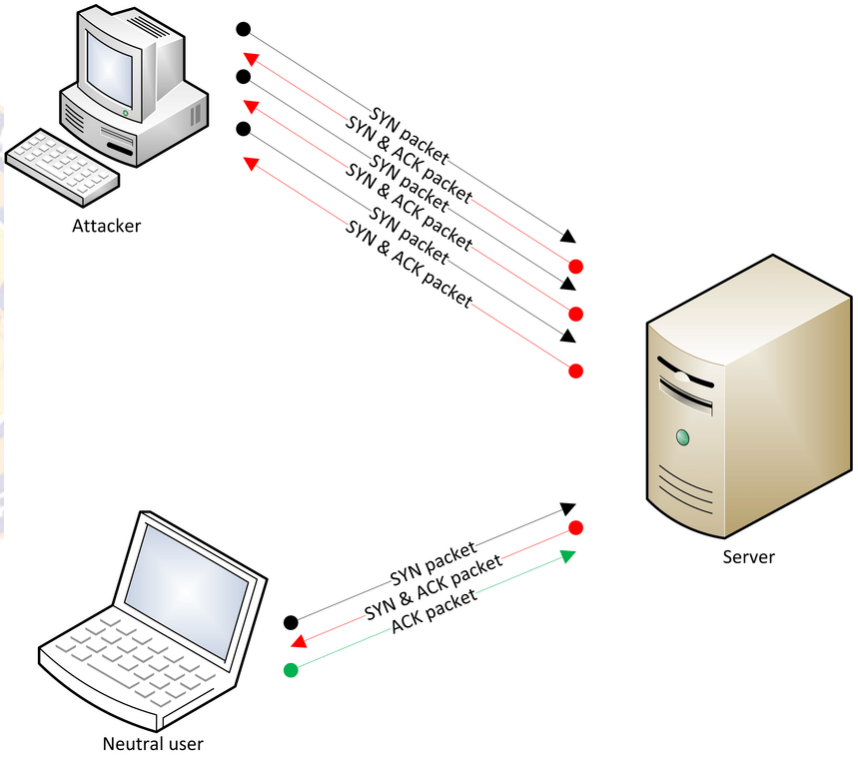


Availability and Network Flooding

innovate achieve lead

Example: SYN Flood Attack

- In a SYN flood attack, a computer sends a large number of SYN requests, but does not send back any ACK messages
- Therefore, the server ends up waiting for multiple responses, tying up system resources
- If the queue of response requests grows large enough, the server may not be able respond to legitimate requests
- This results in a slow or unresponsive server



Denial of Service

innovate achieve lead

Components of Denial of Service Models

- Denial of service models have two essential components
  - waiting time policy
  - user agreement
- Wait time policy
  - Controls the time between a request for a resource and the allocation of that resource to the requesting process
  - A denial of service occurs when the bound set by this policy is exceeded
  - The environment in which the request is made influences the policy
  - Example:
    - The acceptable waiting time for a pacemaker to take action affecting a patient's heart beating is considerably different than the acceptable waiting time for a purchase from an Internet website to be acknowledged.

Denial of Service

Components of Denial of Service Models

- User agreement
  - Establishes constraints a process ("user") must meet in order to ensure service
  - These are designed to ensure that a process will receive service within the waiting time
  - For example:
    - Consider parallel processes accessing a mutually exclusive resource
    - A user agreement for this situation would be that once a process acquires the resource, it must (eventually) release that resource
    - When released, there are enough unallocated resources to enable a process waiting for those resources to proceed

Denial of Service

Components of Denial of Service Models

- These two components (wait time policy & user agreement) in combination ensure that a process meets the conditions needed to receive the resources it needs and not create a denial of servive
- It will receive those resources after an acceptable waiting time
- Thus, the process can proceed and not itself be denied service
- Two types of models that formalize these notions are:
  - Constraint-based models
  - State-based models

Trust Models

Trust Models

innovate achieve lead

Overview

- Integrity Models
  - Integrity models deal with changes to entities
  - State conditions under which changes preserve those properties that define "integrity"
  - Do not deal with the confidence one can have in the initial values or settings of that entity
  - That is, integrity models deal with the preservation of trustworthiness, but not with the initial evaluation of whether the contents can be trusted
- Trust models
  - Provide information about the credibility of data and entities
  - Deal with confidence one can have in the initial values or settings
  - Are concerned with the *initial* evaluation of whether data can be trusted
  - Because trust is subjective, trust models typically express the trustworthiness of one entity in terms of another

Trust Models

Definition of Trust

A *trusts* B if

A believes, with a level of subjective probability, that B will perform a particular action, both before the action can be monitored (or independently of the capacity of being able to monitor it) and in a context in which it affects A's own action.

Trust Models

Definition of Trust

- The above definition involves actors, but it also can apply to the credibility of information
- If you ask whether the data is "trusted" is really asking if a reader of the data believes to some level of subjective probability that the entity providing the data
  - (i) obtained it accurately and without error, and is
  - (ii) providing it accurately and without error
- In the above definition, the reader is A, the provider is B, and the "particular action" is that of gathering and providing the data

Trust Models

innovate achieve lead

Definition of Trust

- This definition captures three important points about trust:
  - First
    - it includes the subjective nature of trust
  - Second
    - it captures the idea that trust comes from a belief in what we do not, or cannot, monitor
  - Third
    - the actions of those we trust affects our own actions
      - This also leads to the notion of transitivity of trust

Trust Models

innovate achieve lead

Transitivity of Trust

- *Transitivity of trust*:
  - if A trusts B and B trusts C, then A trusts C
- In practice, trust is not absolute, so whether trust is transitive depends on A's assessment of B's judgment
- This leads to the notion of *conditional transitivity of trust*, which says that A can trust C when:
  - B recommends C to A
  - A trusts B's recommendations
  - A can make judgments about B's recommendations; and
  - Based on B's recommendation, A may trust C less than B does.

Trust Models

Trust Propagation

- *Direct trust*:
  - A trusts C because of A's observations and interactions
- *Indirect trust*:
  - A trusts C because A accepts B's recommendation
- *Trust Propagation*:
  - Indirect trust may take a path involving many intermediate entities
  - This is called trust propagation because the trust propagates among many entities

Trust Models

innovate achieve lead

Types of Beliefs Underlying Trust

- Castelfranchi and Falcone argue that trust is a cognitive property,
  - so only agents with goals and beliefs can trust another agent
- This requires the trusting agent, A, to estimate risk and then decide, based on her willingness to accept (or not accept) the risk, whether to rely on the one to be trusted, B
- This estimation arises from social and technological sources, as well as A's observations and her taking into account recommendations
- They identify several belief types:

Trust Models

innovate achieve lead

Types of Beliefs Underlying Trust

- *Competence*: A believes B to be competent to aid A in reaching her goal
- *Disposition*: A believes the B will actually do what A needs to reach her goal
- *Dependence*: A believes she needs what B will do, depends on what B will do, or that it is better for A to rely on B than not to rely on him
- *Fulfillment*: A believes goal will be reached
- *Willingness*: A believes B has decided to do what A wants
- *Persistence*: A believes B will not change his mind before doing what A wants
- *Self-confidence*: A believes that B knows he can take the action A wants


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!

BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction to Networks and the Internet

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Agenda

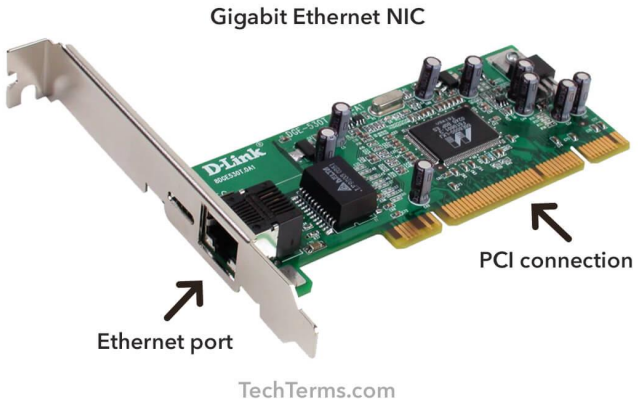
- Introduction
- Network Basics
- How the Internet Works
- History of the Internet
- Basic Network Utilities
- Other Network Devices
- Advanced Network Communications Topics:
  - Network communication types
  - Types of Networks
  - OSI Model
  - Network Protocols

Network Basics

Network Basics

Overview

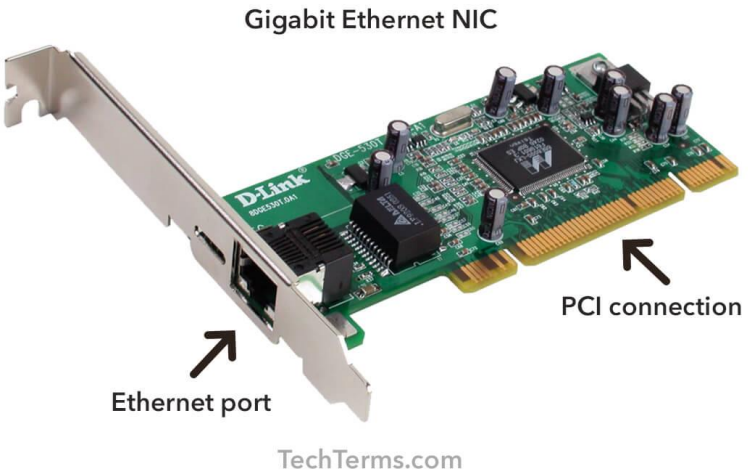
- Communication among computers
  - Requires connecting them physically through cables or wirelessly
  - Cables are plugged either directly to another computer or into a device
    - This device will, in turn, connects to several other computers
- Network Interface Card (NIC)
  - Wireless communication relies on a physical device for transmitting the data
    - This device is called *network interface card* (NIC)



Network Basics

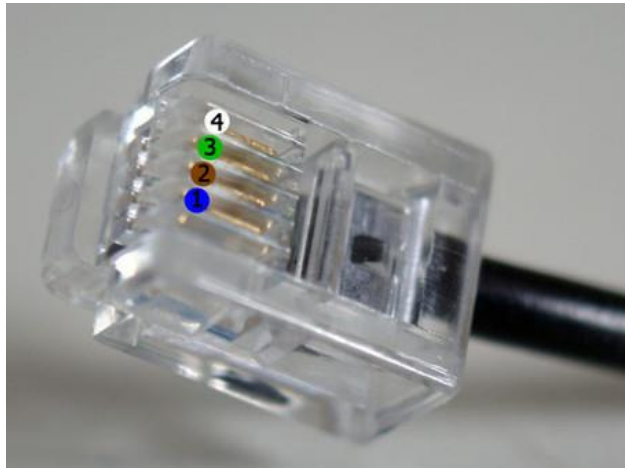
Overview

- Connection slot (Ethernet port)
  - If the connection is through a cable, the part of the NIC that is external to the computer has a connection slot that looks like a telephone jack, only slightly bigger
- Radio signals
  - Wireless networks also use a NIC
  - Rather than a slot for connecting a cable, NIC uses radio signals to transmit to a nearby wireless router or hub
- Antenna
  - Wireless routers, hubs, and NICs have an antenna to transmit and receive signals



The Physical Connection: Local Networks

- RJ-45
  - The cable connection used with wired NICs is called an RJ-45 connection
  - RJ = Registered Jack, an international industry standard
- RJ-11
  - In contrast to the computer's RJ-45 jacks, standard telephone lines use RJ-11 jacks
- RJ-45 Vs. RJ-11
  - The key difference between jacks is the number of wires in the connector (also called the terminator)
  - Phone lines (RJ-11) have four wires (some have six wires), RJ-45 connectors have eight wires
- This standard connector jack must be on the end of the cable



The Physical Connection: Local Networks

- Cat 5 or Cat 6 Cable
  - The cable used in most networks today is a Category 5 or 6 cable abbreviated as Cat 5 or Cat 6 cable
- Unshielded Twisted-Pair (UTP)
  - The cable used in connecting computers is referred to as *unshielded twisted-pair* (UTP) cable
  - The wires in the cable are in pairs, twisted together without additional shielding
- Shielded Twisted-Pair (STP)
  - There are other types of cable such as *shielded twisted-pair* (STP), but UTP is most commonly used

Cat5e VS Cat6		
Product Name	Cat5e UTP Cable	Cat6 UTP Cable
Speed	10BASE-T, 100BASE-TX(Fast Ethernet), 1000BASE-T (Gigabit Ethernet)	10BASE-T, 100BASE-TX(Fast Ethernet), 1000BASE-T (Gigabit Ethernet), 10G BASE-T (10-Gigabit Ethernet)
Frequency	100 MHz	250 MHz
Performance	Good	Better

The Physical Connection: Local Networks

- Table summarizes various categories of cable and their uses.

Cable Types and Uses

Category	Specifications	Uses
1	Low-speed analog (less than 1MHz)	Telephone, doorbell
2	Analog line (less than 10MHz)	Telephone
3	Up to 16MHz or 100Mbps (megabits per second)	Voice transmissions
4	Up to 20MHz/100Mbps	Data lines, Ethernet networks
5	100MHz/100Mbps	Most common a few years ago, still widely used
6	1000Mbps (some get 10Gbps)	Most common type of network cable
6a	10Gbps	High-speed networks
7	10Gbps	Very high-speed networks
8	40Gbps	Not yet commonly found

The Physical Connection: Local Networks

- Each subsequent category of cable is somewhat faster and more robust than the last
- Although Cat 4 can be used for networks, it almost never is used, as it is simply slower, less reliable, and an older technology
- We usually see Cat 5 cable and, increasingly, Cat 6
- We are focusing on UTP because that is what is found most often
- Other types of cable such as shielded twisted-pair (STP), but they are not nearly as common as UTP

The Physical Connection: Local Networks

- A key specification for cables is speed
  - measured in Mbps (megabits per second)
- Now a days, Gbps (gigabits per second) speeds are becoming more common
- Data specification for each cable indicated in the table is the maximum that the cable can handle
  - This is called *bandwidth* of a cable
  - E.g., a Cat 5 cable can transmit up to 100 mega (million) bits per second
- If multiple users simultaneously transmit data on a network, that traffic uses up bandwidth rather quickly
  - E.g., a scanned picture can easily take 2 megabytes (2 million bytes, or 16 million bits) or much larger
  - Streaming media, such as videos, are most demanding in terms of bandwidth

The Physical Connection: Local Networks

- Connecting two computers simply requires a cable to go directly from one computer to another
  - What about more than 2 computers or 100 computers?
- Three devices that can help accomplish this task:
  - The hub
  - The switch, and
  - The router
- These devices use Cat 5 or Cat 6 cable with RJ-45 connectors

Network Basics

The Hub

- A hub is a small electronic device into which network cables are plugged
- It can have 4 or more (commonly up to 24) RJ-45 jacks, each called a port
- A hub can connect as many computers as it has ports
  - E.g., an 8-port hub can connect eight computers
- Stacking
  - We can also connect one hub to another
  - This is referred to as "*stacking*" hubs

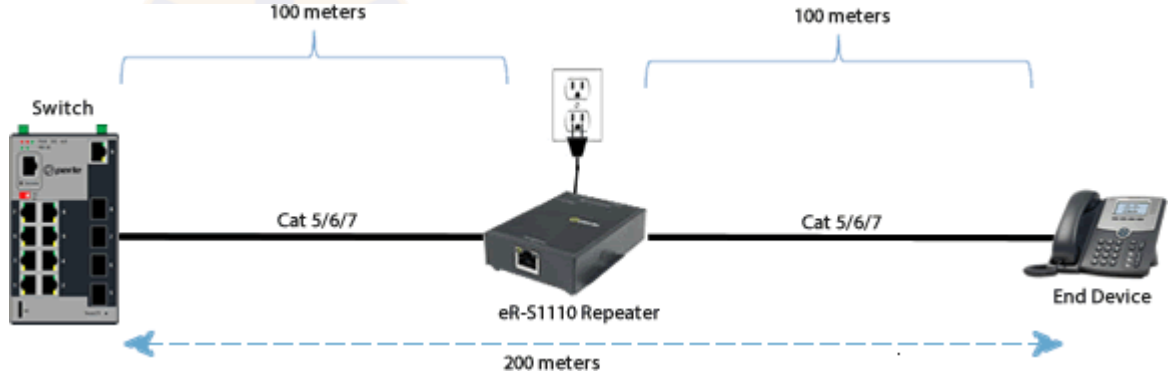
Downside of Hubs

- If a packet (a unit of data transmission) is sent from one computer to another
  - a copy of that packet is actually sent out from every port on the hub
- These copies leads to a lot of unnecessary network traffic
- This occurs because the hub, being a very simple device, has no way of knowing where a packet is supposed to go
- Therefore, it simply sends copies of the packet out all of its ports
- True hubs no longer exist, what we are really getting is a *switch*.

Network Basics

The Repeater

- Is a device used to boost signal
- Basically if the cable needs to go further than the maximum length (which is 100 meters for UTP), then we need a repeater
- There are two types of repeaters: amplifier and signal
- Amplifier repeaters simply boost the entire signal they receive, including any noise
- Signal repeaters regenerate the signal, and thus don't rebroadcast noise.



Network Basics

The Switch

- A switch is basically an intelligent hub
- It works and looks exactly like a hub
- When a switch receives a packet, it sends that packet only out the port for the computer to which it needs to go
- A switch is essentially a hub that is able to determine where a packet is being sent

Network Basics

The Router

- A router is used to connect two or more *networks*
- A router:
  - a) is similar in concept to a hub or switch, as it does relay packets;
  - b) is far more sophisticated
- Routers can be programmed and controlled how they relay packets
- Most routers have interfaces that allow us to configure them
- The specifics of router programming differs from vendor to vender
- Unlike using a hub or switch, the two networks connected by a router are still separate networks

Faster Connection Speeds

Internet Connection Types

Connection Type	Speed	Details
DS0	64Kbps	Standard phone line.
ISDN	128Kbps	Two DS0 lines working together to provide a high-speed data connection.
T1	1.54Mbps	Twenty-four DS0 lines working as one. Twenty-three carry data, and one carries information about the other lines. This type of connection has become common for schools and businesses.
T3	43.2Mbps	672 DS0 lines working together. This method is the equivalent of 28 T1 lines.
OC3	155Mbps	All OC lines are optical and do not use traditional phone lines. OC3 lines are quite fast and very expensive. They are often found at telecommunications companies.
OC12	622Mbps	The equivalent of 336 T1 lines, or 8,064 phone lines.
OC48	2.5Gbps	The equivalent of four OC12 lines.

Wireless

- The Institute of Electrical and Electronics Engineers (IEEE) standard 802.11 provides guidelines for wireless networking
- Various letter designations are used to denote different wireless speeds
- The various wireless speeds, starting from the oldest to the most recent, are listed here

Network Basics

Wireless

Designation	Description
802.11a	• This was the first widely used Wi-Fi; it operated at 5GHz and was relatively slow
802.11b	• This standard operated at 2.4GHZ and had an indoor range of 125 feet with a bandwidth of 11Mbps
802.11g	• There are still many of these wireless networks in operation • We can no longer purchase new Wi-Fi access points that use 802.11g. • This standard includes backward compatibility with 802.11b. • 802.11g has an indoor range of 125 feet and a bandwidth of 54Mbps
802.11n	• This standard was a tremendous improvement over preceding wireless networks • It provides a bandwidth of 100Mbps to 140Mbps and operates at frequencies of 2.4GHz or 5.0GHz over an indoor range of up to 230 feet
IEEE 802.11n-2009	• This technology provides a bandwidth of up to 600Mpbs with the use of four spatial streams at a channel width of 40MHz • It uses multiple-input multiple-output (MIMO), in which multiple antennas coherently resolve more information than is possible using a single antenna

Network Basics

Wireless

Designation	Description
IEEE 802.11ac	• This standard was approved in January 2014 • It has a throughput of up to 1Gbps and at least 500Mbps • It uses up to 8 multiple-input multiple-output (MIMO)
IEEE 802.11ad Wireless Gigabyte Alliance	• Supports data transmission rates up to 7Gbps • This is more than 10 times faster than the highest 802.11n rate
IEEE 802.11af	• Also referred to as "White-Fi" and "Super Wi-Fi," • This standard was approved in February 2014 • It allows WLAN operation in TV white space spectrum in the VHF and UHF bands between 54MHz and 790MHz.
IEEE 802.11aj	• It is a rebranding of 802.11ad • It is used in the 45GHz unlicensed spectrum available in some regions of the world (specifically China).

Securing Wi-Fi

- The methods for securing Wi-Fi have evolved over the years
  - First there was Wired Equivalent Privacy (WEP)
  - Next, Wi-Fi Protected Access (WPA)
  - Next, Wi-Fi Protected Access2 (WPA2)
  - Currently, Wi-Fi Protected Access3 (WPA3)

Securing Wi-Fi

- Wired Equivalent Privacy (WEP)
  - WEP uses the stream cipher RC4 algorithm to secure the data and a CRC-32 checksum for error checking
  - Standard WEP (known as WEP-40) uses a 40-bit key with a 24-bit initialization vector (IV) to effectively form 64-bit encryption
  - 128-bit WEP uses a 104-bit key with a 24-bit IV
  - Because RC4 is a stream cipher, the same traffic key must never be used twice
  - The purpose of an IV, which is transmitted as plain text, is to prevent any repetition
    - but a 24-bit IV is not long enough to ensure this on a busy network
  - The way its IV is used also opens WEP to a related key attack
  - For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets

Securing Wi-Fi

- Wi-Fi Protected Access (WPA)
  - WPA uses Temporal Key Integrity Protocol (TKIP)
  - TKIP is a 128-bit per-packet key
    - That is, it dynamically generates a new key for each packet
- Wi-Fi Protected Access (WPA2)
  - WPA2 is based on the IEEE 802.11i standard
  - Provides the Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)
    - This provides data confidentiality, data origin authentication, and data integrity for wireless frames

Securing Wi-Fi

- Wi-Fi Protected Access (WPA3)
  - WPA3 requires attackers to interact with your Wi-Fi for every password guess they make, making it much harder and time-consuming to crack
  - However, with WPA3’ s "Wi-Fi Easy Connect," you can connect a device by merely scanning a QR code on your phone
  - One of the important new security features is that with WPA3, even open networks will encrypt your individual traffic

Bluetooth

- The name comes from king Harald "Bluetooth" Gormsson, a tenth-century Danish king who united the tribes of Denmark.
  - There are different explanations for the king's nickname
    - One is that he had a bad tooth that was blue
    - Another is that he was often clothed in blue
- The idea behind the Bluetooth technology is that it unites communication protocols
- It is a short-distance radio using the 2.4GHz to 2.485GHz frequency
- The IEEE standardized Bluetooth as IEEE 802.15.1, but it no longer maintains the standard
  - This standard enables devices to discover other Bluetooth devices within range
- The speed and range of Bluetooth depends on the version

Version	Bandwidth	Range
3.0	25Mbps	10 meters (33 feet)
4.0	25Mbps	60 meters (200 feet)
5.0	50Mbps	240 meters (800 feet)

Other Wireless Protocols

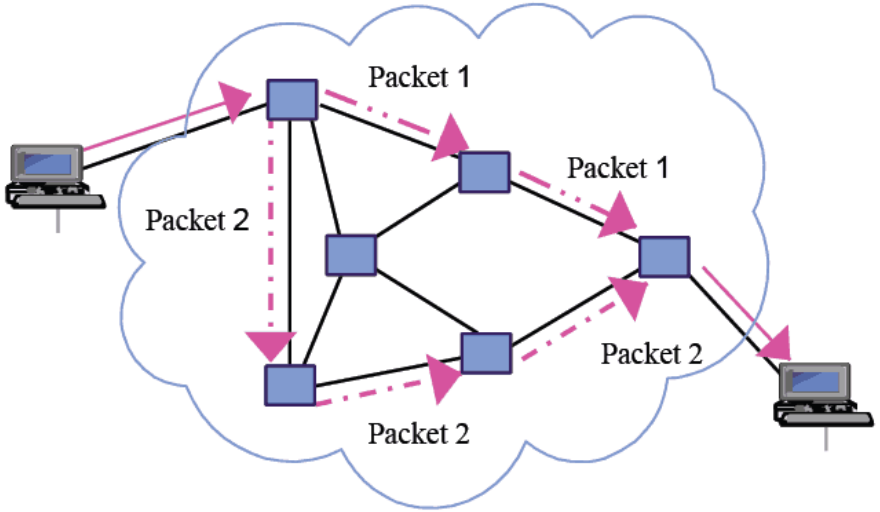
- ANT +:
  - This wireless protocol is often used with sensor data such as in bio sensors or exercise applications
- ZigBee:
  - This standard was developed by a consortium of electronics manufacturers for mainly residential applications of wireless devices related to appliances and security
  - It is based on the 802.15.4 standard
  - This standard is represented by the name "ZigBee" rather than a number
  - The term ZigBee is used similar to the way the term Wi-Fi is used
- Z-Wave:
  - This wireless communications protocol is used primarily for home automation
  - Uses a low-energy radio for appliance-to-appliance communication using a mesh network

Data Transmission

Data Transmission

Overview

- How is data actually transmitted in the networks?
- To transmit data, a packet is sent
- The basic purpose of a cable is to transmit packets from one machine to another

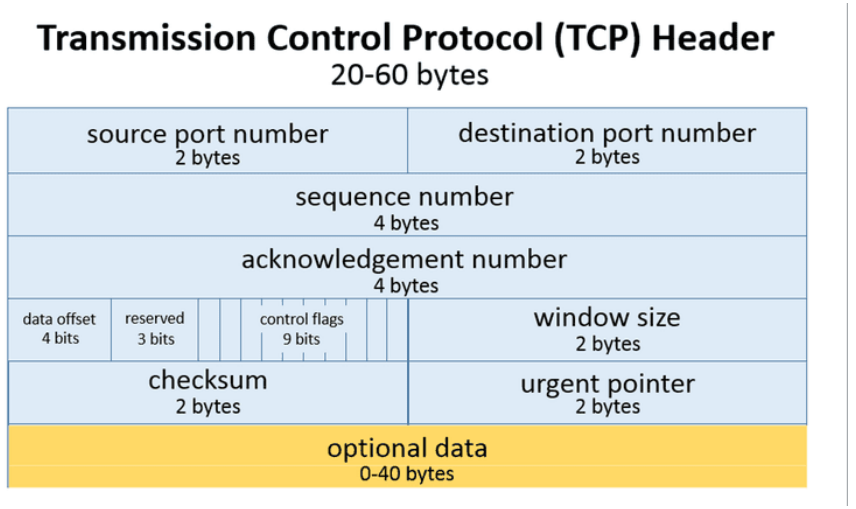


- It does not matter whether that packet is part of a document, a video, an image, or just some internal signal from the computer

Data Transmission

Overview

- Now, what exactly is a packet?
- A packet is a certain number of bytes divided into a header and a body
- The header is 20-60 bytes at the beginning of the packet that tells where the packet is coming from, where it is going, and more
- The body contains the actual data, in binary format
- The routers and switches read the header portion of the packets that come to them and determine where the packet should be sent



Data Transmission

Protocols

- There are different types of network communications for different purposes
- These network communications are called *protocols*
- A *protocol* is, essentially, an agreed-upon method of communication
- In fact, this definition is exactly how the word protocol is used in standard, non-computer usage, too
- Each protocol has a specific purpose and normally operates on a certain port

Data Transmission

Protocols

- Some of the most important, and most commonly used, protocols are listed in table below (see next slide)
- All of these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol)
- But no matter what protocol is used, all communication on networks takes place via packets
- These packets are transmitted according to certain protocols, depending on the type of communication that is occurring

Data Transmission

Protocols

Protocol	Purpose	Port(s)
FTP (File Transfer Protocol)	For transferring files between computers	20 & 21
TFTP (Trivial File Transfer Protocol)	A quicker but less reliable form of FTP	69
SSH (Secure Shell)	Used to securely connect to a remote system	22
Telnet	Used to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators	23
SMTP (Simple Mail Transfer Protocol)	Sends email	25
Whois	A query and response protocol that provides information about the registered Domain Names, an IP address block, Name Servers, etc.	43
DNS (Domain Name System)	Translates URLs into web addresses.	53
HTTP (Hypertext Transfer Protocol)	Displays web pages	80
POP3 (Post Office Protocol version 3)	Retrieves email	110

Data Transmission

Protocols

Protocol	Purpose	Port(s)
NNTP (Network News Transfer Protocol)	Used for network newsgroups (Usenet newsgroups). You can access these groups over the Web via www.google.com and selecting the Groups tab	119
NetBIOS	An older Microsoft protocol that is for naming systems on a local network	137, 138, or 139
IMAP (Internet Message Access Protocol)	More advanced protocol for receiving email. Widely replacing POP3	143
IRC (Internet Relay Chat)	Used for chat rooms	194
SMB (Server Message Block)	Used for Windows Active Directory	445
HTTPS	Encrypted HTTP; used for secure websites	443
SMTPS	Simple Mail Transfer Protocol Secure; Encrypted SMTP	465
POP3S	Post Office Protocol version 3 Secure; Encrypted POP3	995
IMAPS	Internet Message Access Protocol Secure; Encrypted IMAP	993

Data Transmission

Ports

- In a physical sense, ports are the connection locations on the back of our computer
  - E.g., serial ports, parallel ports, and RJ-45 and RJ-11 ports
- In networking terms, a port is a connection point
- It is a numeric designation for a particular pathway of communications
- It can be thought of as a channel number on our television
- We may have one cable coming into our TV, but you can tune to a variety of channels

Data Transmission

Ports

- Regardless of the type of computer or operating system, there are 65,535 network communications ports on our computer
- The combination of our computer's IP address and port number is referred to as a *socket*
- All network communication (regardless of the port used) comes into our computer via the connection on our NIC
- So, a network consists of computers connected to each other via cables, hubs, switches, or routers
- These networks transmit binary information in packets using certain protocols and ports

How Internet Works

How the Internet Works

Overview

- The Internet is essentially a large number of networks that are connected to each other
- These networks are connected into main transmission lines called *backbones*
- The points where the backbones connect to each other are called *network access points* (NAPs)
- The Internet works exactly the same way as a local network
- It sends the same sort of data packets, using the same protocols
- When we log on to the Internet, we typically use an *Internet service provider* (ISP)
- The ISP has a connection either to the Internet backbone or to yet another provider that has a backbone
- So, logging on to the Internet is a process of connecting the computer to ISP's network, which is, in turn, connected to one of the backbones on the Internet

How the Internet Works

IP Addresses

- When tens of thousands of networks and millions of individual computers communicate,
  - how to ensure that the data packets go to the correct computer?
- This task is accomplished in much the same way as traditional "snail" letter mail is delivered to the right person: via an address
- In network communications, this address is referred to as an "IP" address
- An IP address can be IP version 4 or version 6

How the Internet Works

IPv4

- An IP address is a series of four values, separated by periods
  - E.g., 107.22.98.198
- Each of the three-digit numbers must be between 0 and 255
  - For example, an address of 107.22.98.466 is not a valid one
- These addresses are actually four binary numbers; we just see them in decimal format
- Each of these numbers (being a decimal representation of 8 bits), are often referred to as octets
- A 8-bit binary number converted to decimal format will be between 0 and 255
- So there are four octets in an IPv4 address
- This rule gives a total of over 4.2 billion possible IP addresses
- There are methods already in place to extend the use of addresses

How the Internet Works

IPv4

- To extend the reach of the IPv4 address space, companies have turned to using private IPv4 addresses through a public-to-private address translation technique known as network address translation (NAT).
- The public IP addresses are for computers connected to the Internet
- Public IP addresses cannot be duplicate
- A private IP address, such as one on a private company network, only has to be unique in that network
- Often network administrators use private IP addresses that begin with a 10, such as 10.102.230.17.

How the Internet Works

IPv4

- An ISP typically buys a pool of public IP addresses and assign them to us when we log on
- An ISP might own 1,000 public IP address and have 10,000 customers
- The ISP simply assigns an IP address to a customer when he logs on, and the ISP un-assigns the IP address when the customer logs off
- The IP address of a computer tells us a lot about that computer
- The first byte (or the first decimal number) in an address tells you to what class of network that machine belongs

How the Internet Works

IPv4

- Table below summarizes the five network classes

Network Classes

Class	IP Range for the First Byte	Use
A	0–126	Extremely large networks. No Class A network IP addresses are left. All have been used.
B	128–191	Large corporate and government networks. All Class B IP addresses have been used.
C	192–223	The most common group of IP addresses. Your ISP probably has a Class C address.
D	224–247	These are reserved for multicasting (transmitting different data on the same channel).
E	248–255	Reserved for experimental use.

How the Internet Works

IPv4

- The IP range of 127 (not listed in the table) is reserved for testing
- The IP address of 127.0.0.1 designates the machine you are on, regardless of that machine's assigned IP address
- This address is often referred to as the *loopback address*
- That address is often used in testing our machine and our NIC
- In these network classes, one part of the address represents the network and the other part represents the node
- For example:
  - In Class A address, the first octet represents the network, and the remaining three represent the node
  - In Class B address, the first two octets represent the network, and the second two represent the node
  - In Class C address, the first three octets represent the network, and the last represents the node

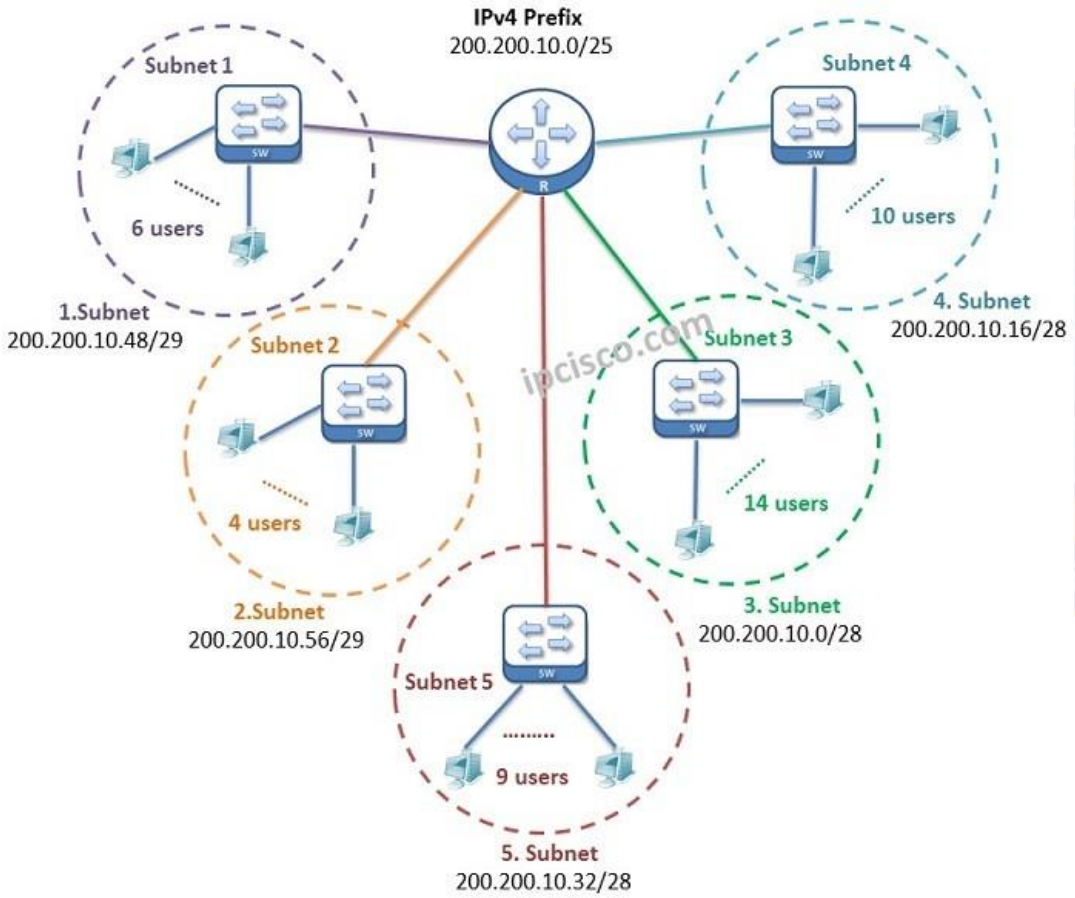
How the Internet Works

IPv4

- Special purpose IP addresses
  - IP 127.0.0.1, or the loopback address is used for referring to the network interface card of the machine we are on
  - Certain range of private IP addresses have been designated for use within networks
    - These cannot be used as public IP addresses but can be used for internal workstations and servers
      - 10.0.0.10 to 10.255.255.255
      - 172.16.0.0 to 172.31.255.255
      - 192.168.0.0 to 192.168.255.255
- The gateway router performs *network address translation* (NAT)
- NAT takes the private IP address on outgoing packets and replaces it with the public IP address of the gateway router
  - This allows the packet to be routed through the Internet

How the Internet Works

Subnetting

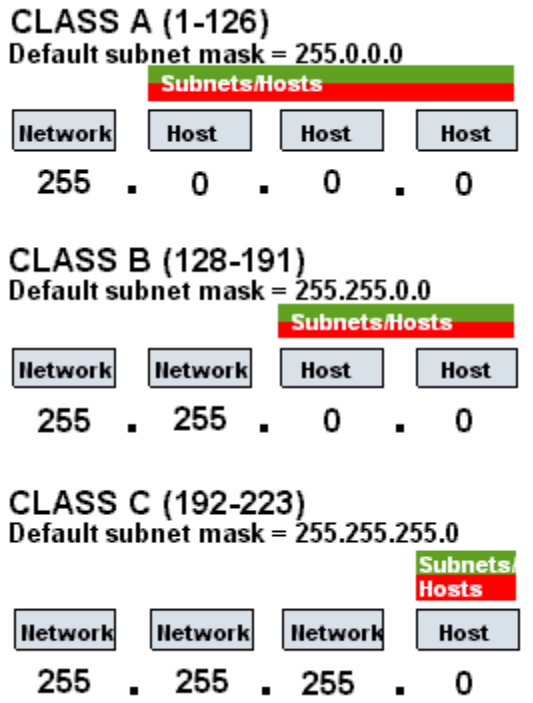


- Subnetting is simply slicing a network into smaller portions
- For example, consider a network using the IP address 192.168.1.X (x being whatever the address is for the specific computer), then we have allocated 255 possible IP addresses
- If we wish to divide this IP into two separate subnetworks, subnetting is the way to go
- More technically, the subnet mask is a 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions

How the Internet Works

Subnetting

- We already have a subnet mask even if you have not been subnetting
  - If we have a Class C IP address, then our network subnet mask is 255.255.255.0.
  - If we have a Class B IP address, then our subnet mask is 255.255.0.0.
  - If we have a Class A IP address, then our subnet mask is 255.0.0.0.
- The decimal value 255 converts to 11111111 in binary
- So we are literally "masking" the portion of the network address that is used to define the network, and the remaining portion is used to define individual nodes



How the Internet Works

Subnetting

- Now if we want fewer than 255 nodes in our subnet, then we need something like 255.255.255.240 for our subnet
- If we convert 240 to binary, it is 11110000
- That means the first three octets and the first 4 bits of the last octet define the network
- The last 4 bits of the last octet define the node
- That means we could have as many as 1111 (in binary) or 15 (in decimal) nodes on this subnetwork
- This is the basic essence of subnetting

How the Internet Works

CIDR

- Subnetting only allows a certain, limited subnets
- Another approach is *Classless InterDomain Routing* (CIDR)
- Rather than define a subnet mask, we have the IP address followed by a slash and a number
- That number can be any number between 0 and 32, which results in IP addresses like these:
  - 192.168.1.10/24 (basically a Class C IP address)
  - 192.168.1.10/31 (much like a Class C IP address with a subnet mask)
- When we use this, rather than having classes with subnets, we have *Variable-Length Subnet Masking* (VLSM) that provides classless IP address
- This is the most common way to define network IP addresses today

How the Internet Works

Subnetting

- Class A (CDIR Value = /8) = Classless Inter Domain Routing = Total number of network bits
- IP Address: 1-126
- Default Subnet Mask: 255.0.0.0
- 8 bits are reserved for network and the remaining 24 bits are reserved for the host

Network Bits								Host Bits																			
8								24																			
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
255								0								0											

How the Internet Works

Subnetting

- Class B (CDIR Value = /16) = Classless Inter Domain Routing = Total number of network bits
- IP Address: 128-191
- Default Subnet Mask: 255.255.0.0
- 16 bits are reserved for network and the remaining 16 bits are reserved for the host

Network Bits																Host Bits															
16																16															
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
255								255								0								0							

How the Internet Works

Subnetting

- Class C (CDIR Value = /24) = Classless Inter Domain Routing = Total number of network bits
- IP Address: 192-223
- Default Subnet Mask: 255.255.255.0
- 24 bits are reserved for network and the remaining 8 bits are reserved for the host

Network Bits																						Host Bits							
24																						8							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
255								255								255						0							

How the Internet Works

Subnetting – Example – Class C

- 192.168.1.0/24

255								255								255								0							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								0							
8 Bits								8 Bits								8 Bits								8 Bits							
Block 1								Block 2								Block 3								Block 4							

- Default subnet mask for class C = 255.255.255.0
- CDIR Value = 24 = Total number of network bits
- We can calculate the subnet mask only from the network bits not the host bits

How the Internet Works

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								2^7							
8 Bits								8 Bits								8 Bits								8 Bits							
Block 1								Block 2								Block 3								Block 4							

- Default subnet mask for class C = 255.255.255.0
- But, CDIR Value = 25. So, we need one extra bit. We borrow that from host
- The new subnet mask = 255.255.255.128

How the Internet Works

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

- Number of networks
  - 2^n (Where, n = number of bits borrowed from the host)
  - $2^1 = 2$ (We can create only two networks
- Number of IP addresses on each network
  - 2^b (Where, b = number of remaining host bits)
  - $2^7 = 128$ (On each network we can have 128 IP addresses)
- Number of hosts on each network (IPs that can be assigned to devices)
  - $2^b - 2$ (Where, b = number of remaining host bits)
  - $2^7 - 2 = 126$ (We can assign 126 IP addresses to devices)

Note:
In every network, the first IP address is reserved for the network ID and the last IP address is reserved for broadcast ID

How the Internet Works

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

Network 1	
192.168.10.0	Network ID
192.168.10.1	IP Addresses that can be assigned
…	
…	
192.168.10.126	
192.168.10.127	Broadcast ID

How the Internet Works

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

Network 1		Network 2	
192.168.10.0	Network ID	192.168.10.128	Network ID
192.168.10.1	IP Addresses that can be assigned	192.168.10.129	IP Addresses that can be assigned
…		…	
…		…	
192.168.10.126		192.168.10.254	
192.168.10.127	Broadcast ID	192.168.10.255	Broadcast ID

How the Internet Works

Subnetting – Example – Class C

- 192.168.1.0/26

255								255								255								192							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

- Number of networks
  - 2^n (Where, n = number of bits borrowed from the host)
  - $2^2 = 4$ (We can create only two networks
- Number of IP addresses on each network
  - 2^6 (Where, b = number of remaining host bits)
  - $2^6 = 64$ (On each network we can have 64 IP addresses)
- Number of hosts on each network (IPs that can be assigned to devices)
  - $2^6 - 2$ (Where, b = number of remaining host bits)
  - $2^6 - 2 = 62$ (We can assign 62 IP addresses to devices)

Note:
In every network, the first IP address is reserved for the network ID and the last IP address is reserved for broadcast ID

How the Internet Works

Subnetting – Example – Class C

- 192.168.1.0/26

255								255								255								128							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

Network No	Network ID	Number of IPs	Broadcast ID
1	192.168.10.0	192.168.10.1 - 192.168.10.62	192.168.10.63
2	192.168.10.64	192.168.10.65 - 192.168.10.126	192.168.10.127
3	192.168.10.128	192.168.10.129 - 192.168.10.190	192.168.10.191
4	192.168.10.192	192.168.10.193 - 192.168.10.254	192.168.10.255

How the Internet Works

Subnetting

- The first value of a subnet mask must be 255
- The remaining three values can be 255, 254, 252, 248, 240, or 224
- The computer will take our network IP address and the subnet mask and use a binary AND operation to combine them

How the Internet Works

IPv6

- IPv6 is an extension of IPv4
- IP version 4 is limited to 4.2 billion IP addresses
- Even with the use of private IP addresses, we will run out of available IP addresses
  - Consider all the computers, printers, routers, servers, smart phones, tablets, and so on connected to the Internet
- IP version 6 was designed to alleviate this problem
- IPv6 utilizes a 128-bit address (instead of 32), so there is no chance of running out of IP addresses in the foreseeable future
- IPv6 also utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5
- The hex address format will appear in the form of 3FFE:B00:800:2::C, for example.

How the Internet Works

IPv6

- IPv6 involves no subnetting, but it does use CIDR
- The network portion is indicated by a slash followed by the number of bits in the address that are assigned to the network portion
  - For example: /48 /64
- There is a loopback address for IPv6, and it can be written as ::/ 128
- Loopback address
  - An address that sends outgoing signals back to the same computer for testing
  - In a TCP/IP network, the loopback IP address is 127.0.0.1, and pinging this address will always return a reply unless the firewall prevents it
  - The loopback address allows a network administrator to treat the local machine as if it were a remote machine
  - The standard domain name for the address is localhost

How the Internet Works

IPv4 Vs. IPv6

- Link/machine-local address:
  - This is the IPv6 version of IPv4's APIPA (Automatic Private IP Addressing) address
  - If a machine is configured for dynamically assigned addresses and cannot communicate with a DHCP server, it assigns itself a generic IP address
  - DHCP, or Dynamic Host Configuration Protocol, is used to dynamically assign IP addresses within a network
  - IPv6 link/machine-local IP addresses all start with fe80::
  - So if your computer has this address, that means it could not get to a DHCP server and therefore made up of its own generic IP address.

How the Internet Works

IPv4 Vs. IPv6

- Site/ network-local address:
  - This is the IPv6 version of the IPv4 private address
  - Site/ network-local addresses are real IP addresses, but they only work on the local network and are not routable on the Internet
  - All site/ network-local IP addresses begin with FE and have C to F for the third hexadecimal digit: FEC, FED, FEE, or FEF
- The managed address configuration flag (M flag):
  - When the M flag is set to 1, the device should use DHCPv6 to obtain a stateful IPv6 address
- Other stateful configuration flag (O flag):
  - When the O flag is set to 1, the device should use DHCPv6 to obtain other TCP/ IP configuration settings
  - In other words, it should use the DHCP server to set things like the IP address of the gateway and DNS servers
- M flag:
  - This indicates that the machine should use DHCPv6 to retrieve an IP address.

How the Internet Works

Uniform Resource Locator (URL)

- When we visit websites, we type names rather than IP addresses in the browser's address bar
  - For example, www.yahoo.com
- This name (called a URL) needs to be translated into an IP address
- The DNS protocol handles this translation process
- If the address is found, the browser sends a packet (using HTTP) to port 80
- If that target computer has software that listens and responds to such requests, then the target computer will respond to our browser’s request, and communication will be established
  - The software is web server software such as Apache or Microsoft Internet Information Server

Uniform Resource Locator (URL)

- Error Messages
  - There are a series of error messages that the web server can send back to our web browser to indicate different situations
  - The browser handles many of these errors itself; we never see the error message
  - Error 400 series
    - All error messages in the 400 series are client errors
    - That is something is wrong on our side, not with the web server
    - E.g., Error 404
      - Refers to File Not Found
      - Indicates that our browser received back a packet (from the web server) with error code 404, denoting that requested page could not be found

Uniform Resource Locator (URL)

- Error Messages
  - Error 500 series
    - These are server errors, meaning, there is a problem on the web server
  - Error 100 series
    - These are simply informational
  - Error 200 series
    - These indicate success
    - We usually do not see these, the browser simply processes them
  - Error 300 series
    - These are re-directional, meaning the page you are seeking has moved, and your browser is then directed to the new location

How the Internet Works

Uniform Resource Locator (URL)

- Emails
  - Using email works the same way as visiting websites
  - Our email client will seek out the address of your email server
  - Then our email client will use either Post Office Protocol version 3 (POP3) to retrieve the incoming email or Simple Mail Transfer Protocol (SMTP) to send the outgoing email
  - The email server (probably at our ISP or our company) will then try to resolve the address we are sending to
  - If we send something to joe@yahoo.com, the email server will translate that email address into an IP address for the email server at yahoo.com
    - Then our server will send our email there
  - There is another protocol called Internet Message Access Protocol (IMAP) for retrieving emails from remote server, but POP3 is still the most commonly used

How the Internet Works

Uniform Resource Locator (URL)

- Chat Rooms
  - A chat room (like the other communication methods), works with packets
  - We first find the address of a chat room, and then connect
  - The difference here is that our computer's chat software is constantly sending packets back and forth
  - Whereas email only sends and receives when we tell it to
    - or on a predetermined time interval
  - The packet header section contains our IP address and the destination IP address (as well as other information)

How the Internet Works

What is a Packet?

- Network traffic is really a lot of 1s and 0s that are transmitted as
  - voltages (over *unshielded twisted-pair* (UTP))
  - light wave (over optic cable) or
  - radio frequencies (over Wi-Fi)
- The data is divided into small chunks called packets
- A packet is divided into three sections:
  - The header, the data, and the footer
- The header contains information about how to address the packet, what kind of packet it is, and related data
- The data portion is the information we want to send
- The footer serves both to show where the packet ends and to provide error detection

How the Internet Works

What is a Packet?

- Header
  - There are usually at least three headers
    - Ethernet header, TCP header, and IP header
  - Each contains different information, in combination they have several pieces of information that will be interesting for forensic investigations
- TCP header
  - Contains information related to the transport layer of the OSI model
  - Contains the source and destination port for communications
  - It also has the packet number, such as packet 10 of 21

How the Internet Works

What is a Packet?

- IP header
  - Contains the source IP address, the destination IP address, and the protocol
  - The IP header also has a version number (4.0 or 6.0) for the IP packet
  - The size variable describes how large the data segment is
- Ethernet header
  - Contains information regarding the source MAC address and destination MAC address
  - When a packet gets to the last network segment in its journey, MAC address is used to find the NIC that the packet is being sent to

How the Internet Works

Basic Communications

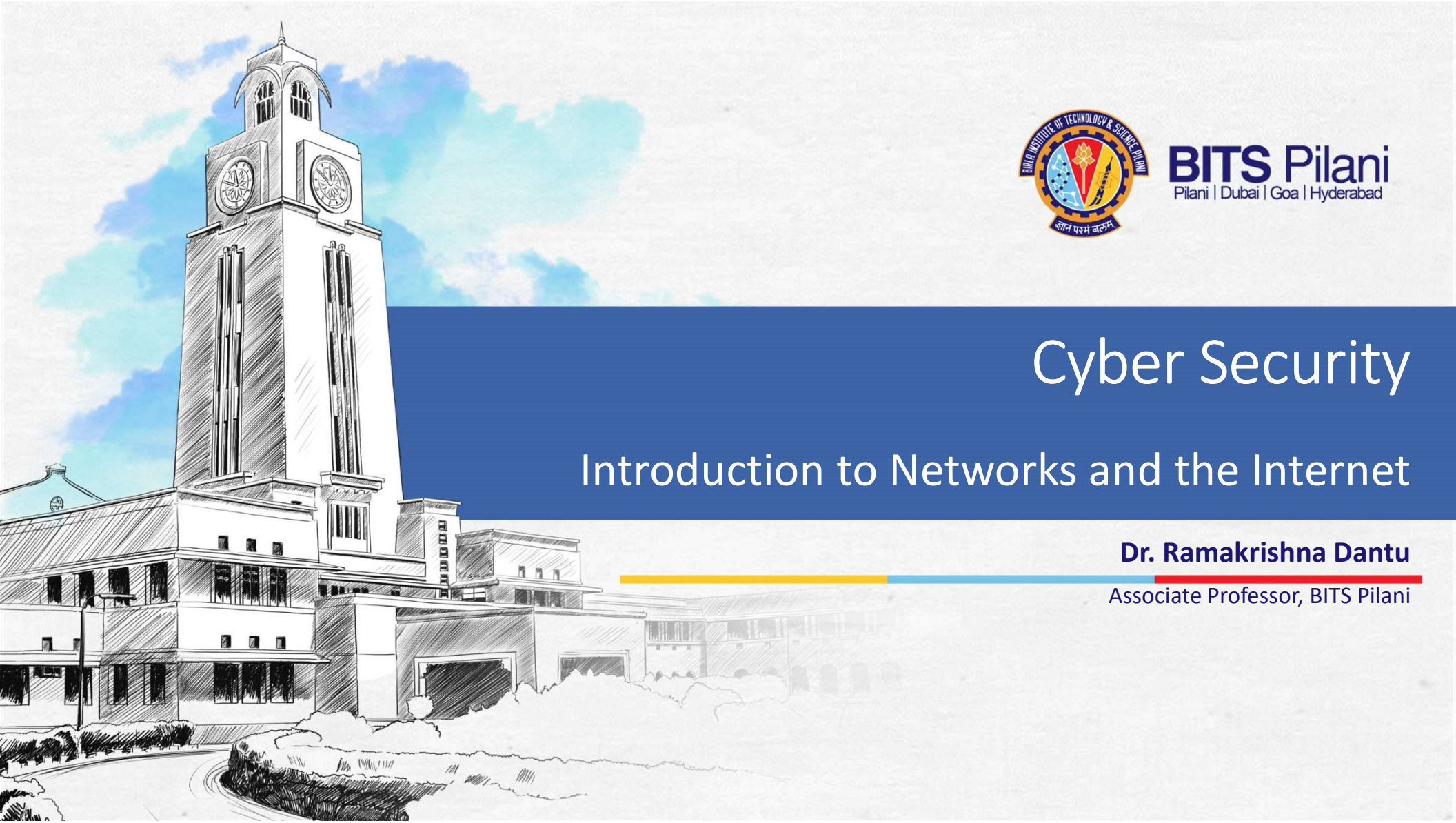
- The packet headers also contain some signal bits
- These are single bit flags that are turned on to indicate some type of communication
- A normal network conversation starts with one side sending a packet with the SYN (synchronize) bit turned on
- The target responds with both SYN and ACK (acknowledge) bits turned on
- Then the sender responds with just the ACK bit turned on, and communication commences
- To end the communication, the original sender terminates the communication by sending a packet with the FIN (finish) bit turned on

How the Internet Works

Reference

- Easttom, Chuck. Computer Security Fundamentals (Pearson IT Cybersecurity Curriculum (ITCC)) – 4th Edition

Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction to Networks and the Internet

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

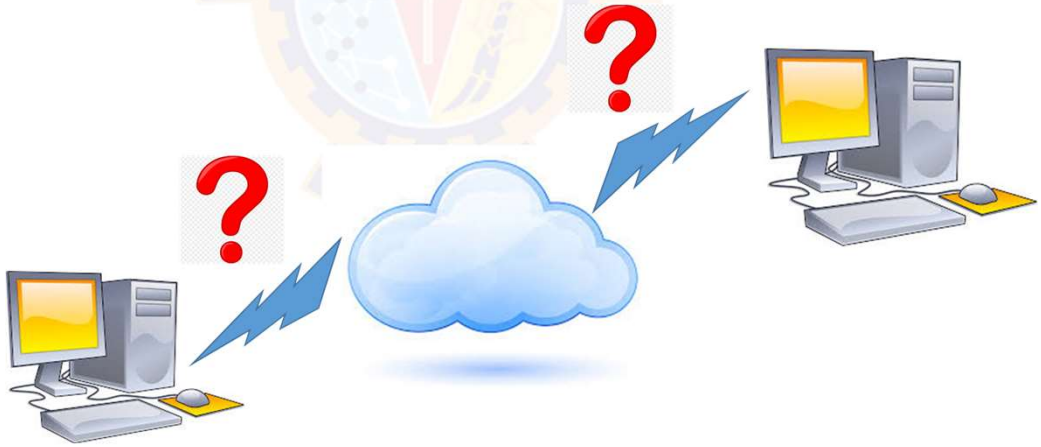
The OSI Model

The OSI Model

innovate achieve lead

Overview

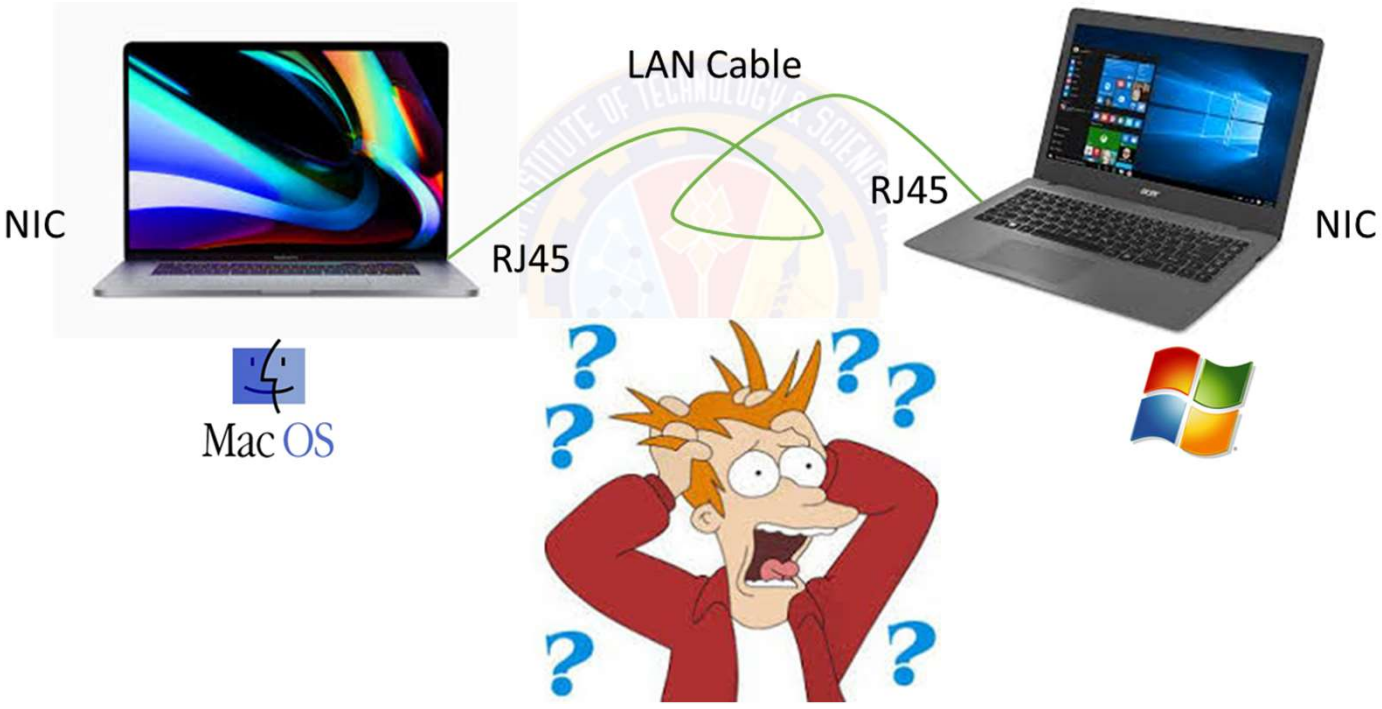
- Open Systems Interconnection (OSI) model describes how computers communicate with each other on a network
- It outlines the various protocols and activities, and tells how the protocols and activities relate to each other



The OSI Model

innovate achieve lead

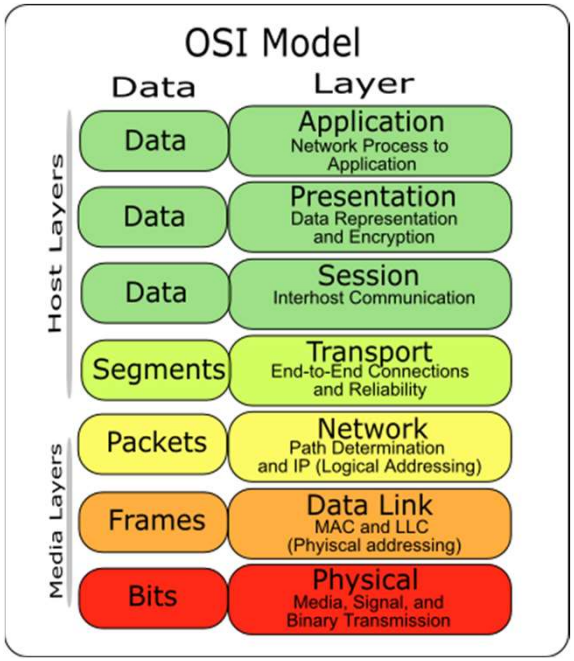
Overview



The OSI Model

Overview

- This model was originally developed by the International Organization for Standardization in 1984
- The model is divided into seven distinct and separate layers
- Each layer is a package of protocols
- Each layer possesses a trait known as 'successive dependence.'
  - This means that the successively higher layers in the model depend on the services and characteristics of the preceding lower layers



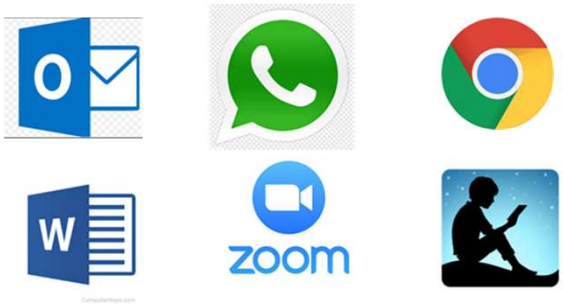
Open Systems Interconnection (OSI) Model

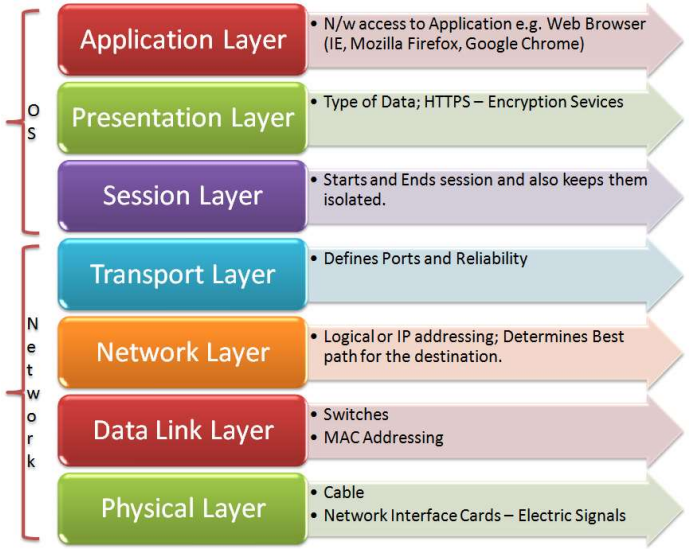
The OSI Model

innovate achieve lead

Layer 7: Application Layer

- This doesn't mean applications such as chrome, email client, word processor, etc.,.
- The application layer is the end user's access to the network
- This layer includes protocols to make these applications work correctly
- These are applications that rely on the Internet to work
- For Example:
  - Chrome, Skype, Outlook, etc.,.

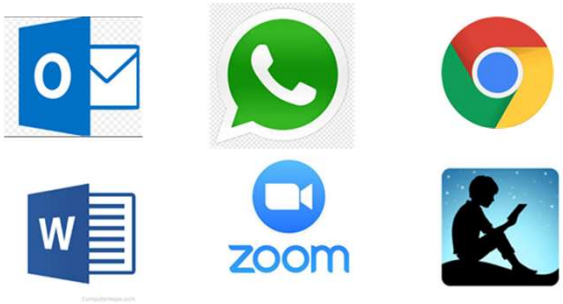


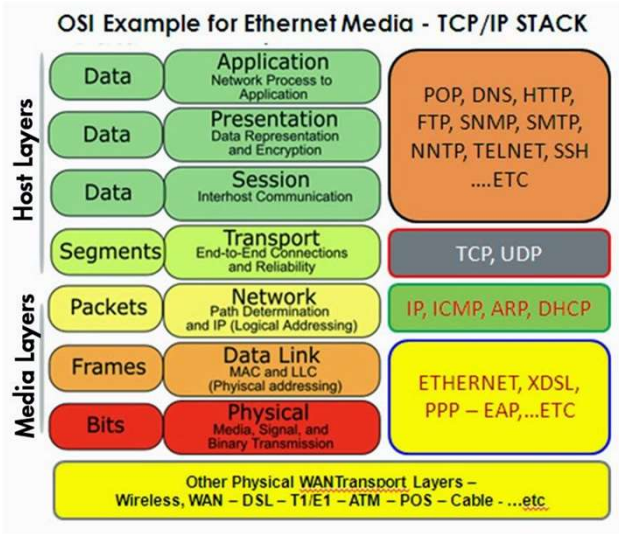


The OSI Model

Layer 7: Application Layer

- These protocols form the basis for various network services such as
  - File transfer, Web surfing, Emails, Virtual terminals, etc.,.
- For example:
  - File transfer relies on FTP
  - Web surfing relies on HTTP/HTTPS
  - Emails use SMTP
  - Virtual terminals use Telnet

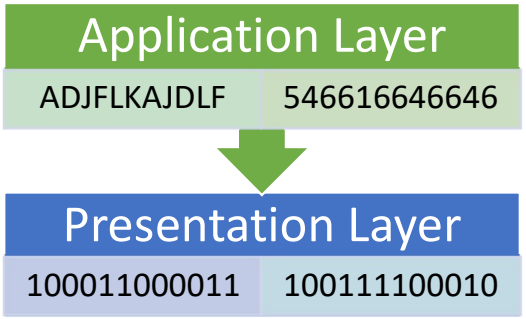




The OSI Model

Layer 6: Presentation Layer

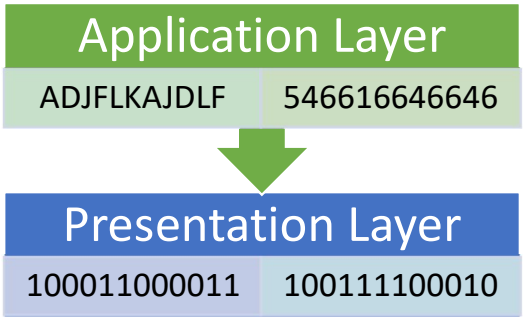
- This layer receives data from the Application Layer
- This data is in the form of characters and numbers
- The presentation layer formats the data converts this data into machine understandable binary format (0's and 1's)
  - E.g., conversion of ASCII to EBCDIC
    - Extended Binary Coded Decimal Interchange Code
  - This process is called translation
- Before the data is transmitted, the presentation layer reduces the number of bits used to represent the original data
  - 100011000011 → 10010011
  - This reduction of data is called data compression
- Data compression can be lossy or lossless



The OSI Model

Layer 6: Presentation Layer

- Data compression reduces the amount of space required to store the original file
  - E.g., 5MB → 3MB
- As the file size is reduced, data transmission can happen faster
- Data compression is useful in real-time audio and video streaming
- Data is encrypted before transmission to maintain the integrity/security of the data
- At the receiver side, data is decrypted, before presenting
- Secure Socket Layer (SSL) protocol is used in the presentation layer for encryption and decryption
- Essentially, presentation layer performs three functions:
  - Translation, Compression, & Encryption/Decryption



The OSI Model

innovate achieve lead

Layer 5: Session Layer

- Suppose we decide to have a party at our home

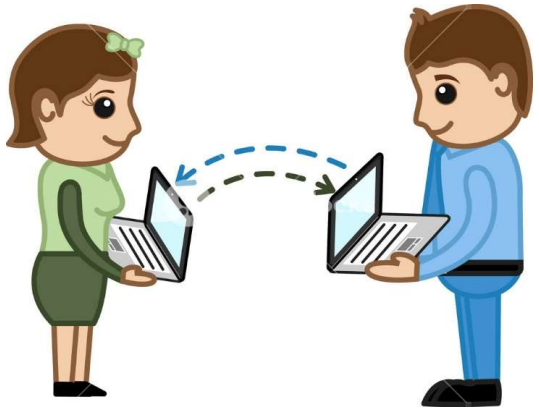
- We hire an event management team to help us organize the party
- Helpers will help us with setting up, assisting, cleaning, and closing the party

- The Session Layer performs a similar function

The OSI Model

Layer 5: Session Layer

- The session layer is responsible for setting up and managing all connections or sessions
- It enables sending and receiving of data, followed by the termination of connections or sessions
- Similar to the way we had helpers in organizing the party, session layer also has its own helpers
- These helpers are called APIs or Application Programming Interfaces
  - E.g., NETBIOS – Network Basic Input/Output System allows applications on different computers to communicate with each other

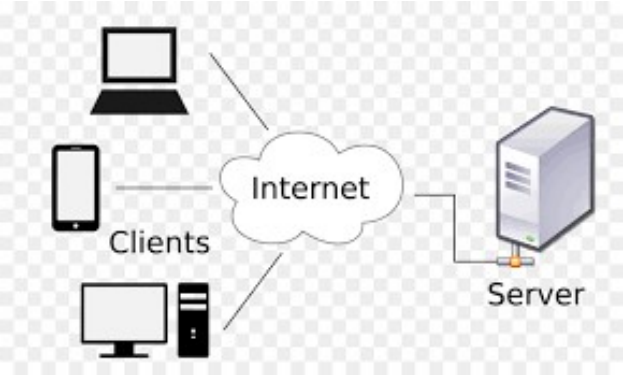


The OSI Model

innovate achieve lead

Layer 5: Session Layer

- Session Layer performs two functions – Authentication & Authorization
- Before establishing a session or connection, the server performs a function called authentication
- Authentication process verifies the identity of the client where the user name and password are matched
- Once authenticated, a session or connection is established between the computer and the server
- After authenticating the user, authorization is checked
- Authorization is the process where the server checks if the user has permission to access a file or any resource
  - If not, users gets a message saying "Access Denied"

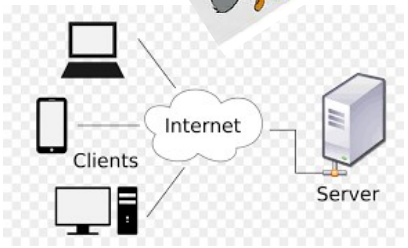


The OSI Model

innovate achieve lead

Layer 5: Session Layer

- Thus session layer also performs session management
- Session layer keeps track of files that are being downloaded
- For e.g., a web page contains images, text, etc.



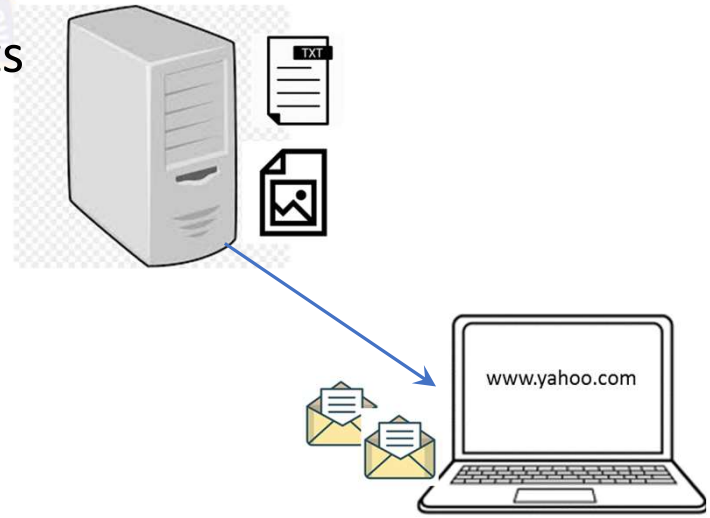
- These images and text are stored as separate files on the web server

The OSI Model

innovate achieve lead

Layer 5: Session Layer

- When we request a web page, web browser opens a separate connection or session with the server
- This session enables us to download each of these text and image files separately
- These files are received in the form of data packets
- Session layer keeps track of which data packet belongs to which file
- It also tracks where the received packet should go (the destination)
  - in this case, it goes to web browser
- Thus session layer helps in session management



The OSI Model

Layer 5: Session Layer

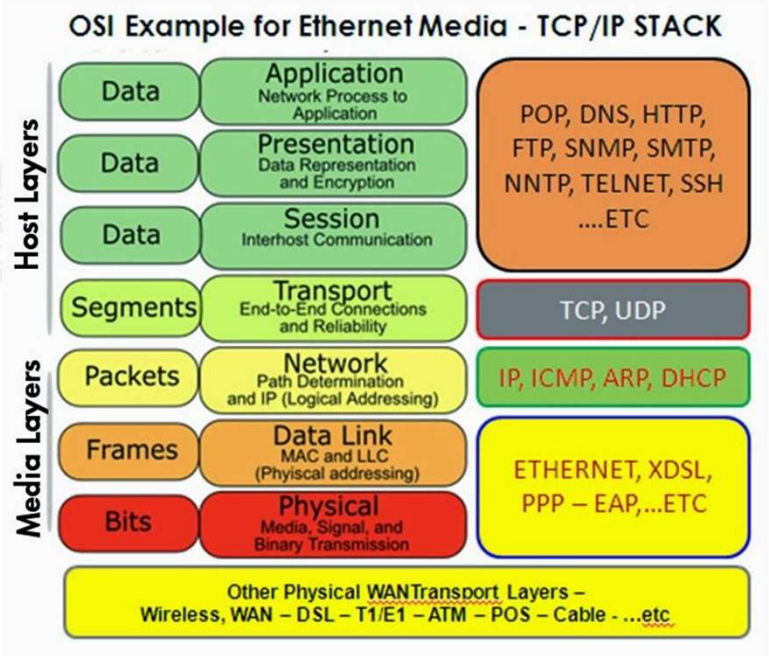
- Thus, the session layer performs three key functions
  - Authentication
  - Authorization
  - Session Management
- Our web browser performs all these functions of:
  - Session layer
  - Presentation layer, and
  - Application layer

The OSI Model

innovate achieve lead

Layer 4: Transport Layer

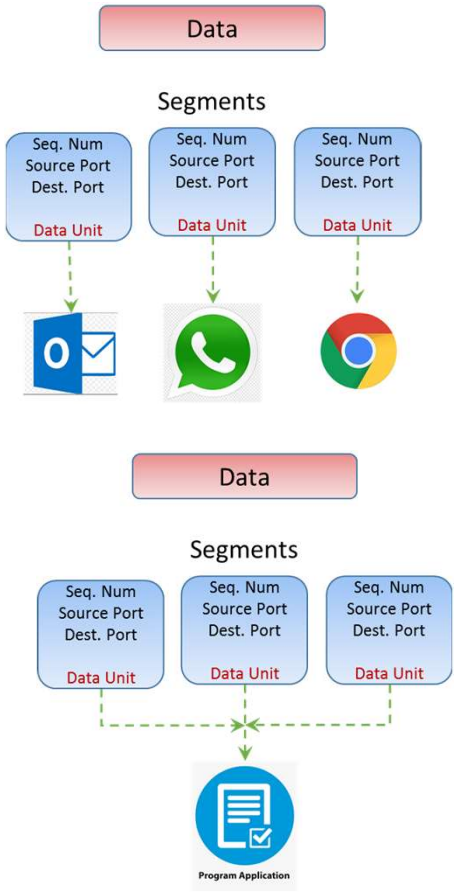
- The transport layer deals with end-to-end issues, such as procedures for entering and departing from the network
- Transport layer controls the reliability of communication through
  - Segmentation
  - Flow Control
  - Error Control
- It is responsible for:
  - breaking a large data into smaller packets (if needed),
  - ensuring that all the packets have been received,
  - eliminating duplicate packets, and
  - performing flow control to ensure that no computer is overwhelmed by the number of messages it receives



The OSI Model

Layer 4: Transport Layer

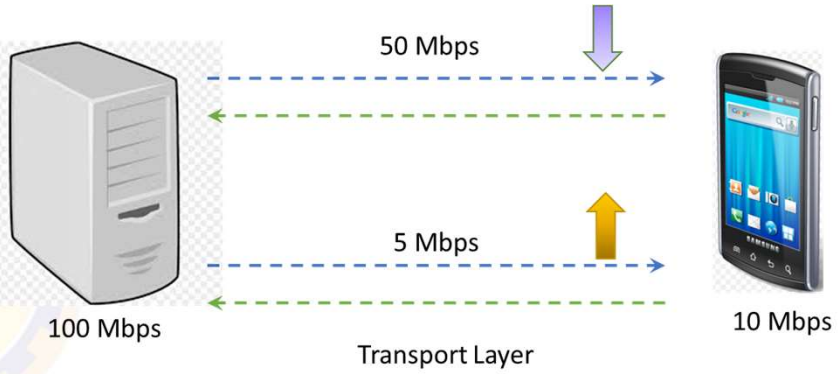
- Segmentation
  - Data is divided into smaller units called segments
  - Each segment contains:
    - port number of source and destination, and
    - sequence number
  - Port number helps direct each segment to the correct application
  - Sequence number helps to reassemble the segments in correct order to form correct message at the receiver
    - so that it can be delivered to the correct application in that order



The OSI Model

Layer 4: Transport Layer

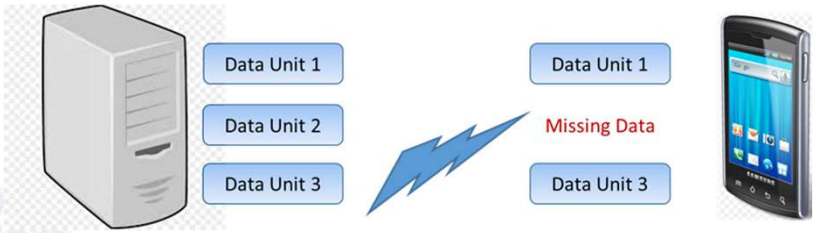
- Flow Control
  - Here, transport layer controls the amount of data being transmitted
  - Consider that the
    - server can transmit data at a maximum of 100 Mbps
    - mobile phone can process data at a maximum of 10 Mbps
  - Server sends data at 50 Mbps
    - This is more than the processing capacity of mobile phone
    - Mobile phone with the help of transport layer can tell the server to slow down data transmission rate to 10 Mbps so there is no data loss
  - Server sends data at 5 Mbps
    - Mobile phone tells the server to increase the speed to 10 Mbps to maintain system performance



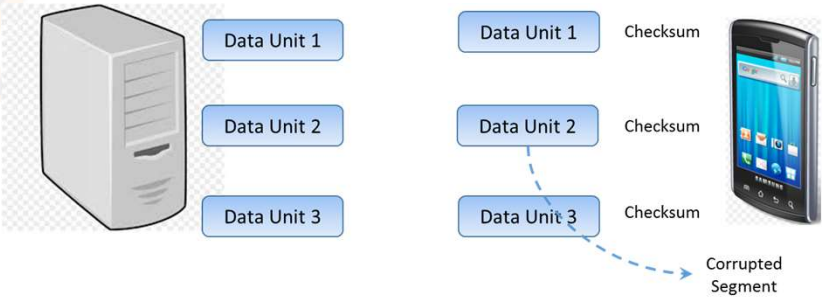
The OSI Model

innovate achieve lead

Layer 4: Transport Layer



- Error control
  - Transport layer also performs error control
  - If a data packet doesn't arrive at the destination, transport layer uses Automatic Repeat Request scheme to retransmit the lost or corrupted data
  - A group of bits called checksum is added to each segment by the transport layer to find out received corrupted segment



The OSI Model

Layer 4: Transport Layer

- Transport layer protocols are
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
- Transport layer performs two types of transmission services
  - Connection-oriented Transmission
    - Done using TCP
  - Connectionless Transmission
    - Done using UDP

The OSI Model

Layer 4: Transport Layer

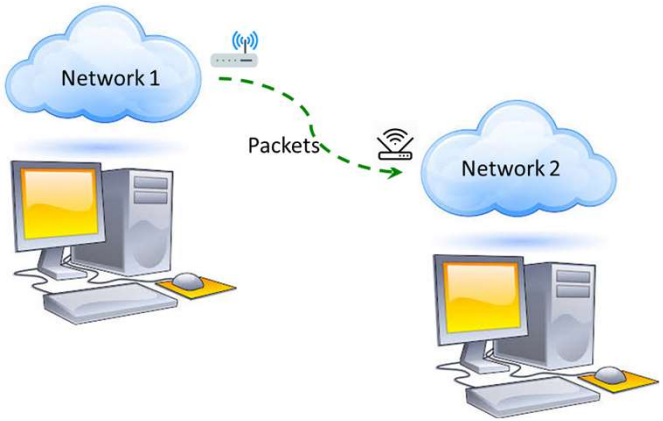
- UDP Vs. TCP
  - UDP is faster than TCP, because
    - UDP does not provide any feedback
    - TCP provides feedback so that lost data can be retransmitted
  - UDP is used where it doesn't matter if we received all data
    - E.g., Online video streaming, Songs, Games, VOIP
  - TCP is used where full data delivery is must
    - E.g., WWW, Email, FTP, etc.,

TCP	UDP
Connected	Connectionless
State Memory	Stateless
Byte Stream	Packet/Datagram
Ordered Data Delivery	No Sequence Guarantee
Reliable	Lossy
Error Free	Error Packets Discarded
Handshake	No Handshake
Flow Control	No Flow Control
Relatively Slow	Relatively Fast
Point to Point	Supports Multicast
Security: SSL/TLS	Security: DTLS

The OSI Model

Layer 3: Network Layer

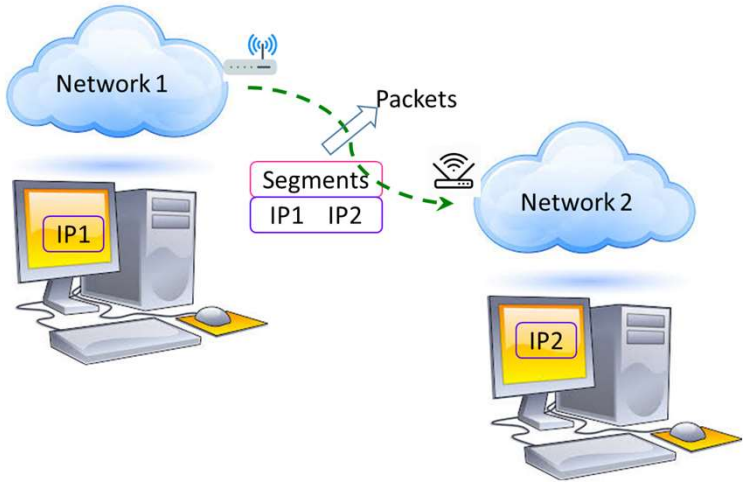
- Transport layer passes data segments to Network Layer
- Network layer works for the transmission of the received data segments from one computer to another located in different networks
- Data units in the network layer are called packets
- It is the layer where routers reside
- Key functions of network layer are
  - Logical addressing
  - Routing
  - Path determination



The OSI Model

Layer 3: Network Layer

- Logical addressing
  - IP addressing (IPv4 & IPv6) done in network layer is called Logical Addressing
  - Every computer in a network has a unique IP address
  - Network layer assigns sender's and receiver's IP address to each segment to form an IP packet
  - IP addresses are assigned to ensure that each data packet reaches the correct destination

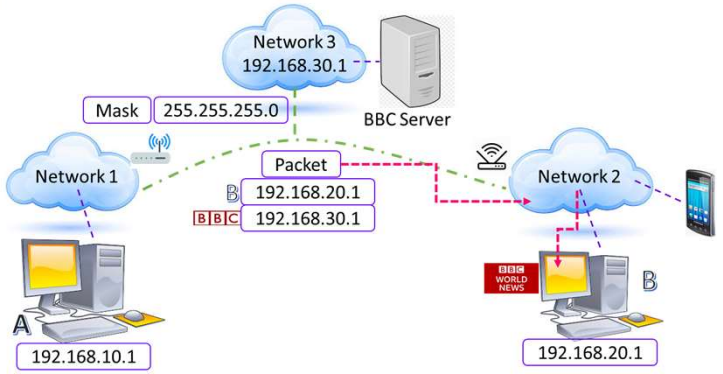


The OSI Model

innovate achieve lead

Layer 3: Network Layer

- Routing
  - Routing is a method of moving data packets from source to destination
  - Based on IP address and mask, routing decisions are made in a computer network
  - It is based on the logical address format of IPv4 or IPv6 and subnet mask
  - Suppose computers A & B are connected to networks 1 & 2 respectively
  - From computer B we requested to access BBC NEWS website
  - There is a reply from BBC server to computer B in the form of a packet
  - This packet must be delivered to computer B only

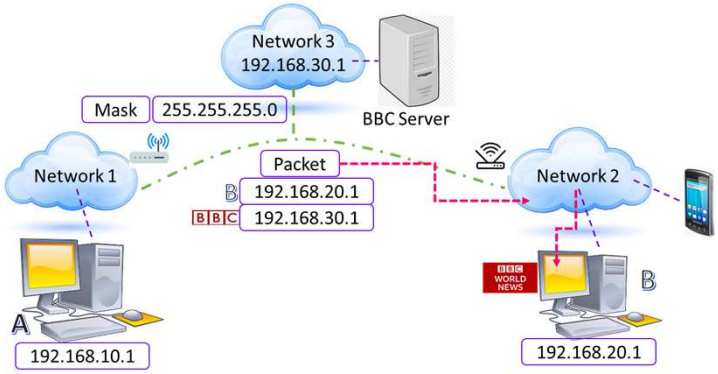


The OSI Model

innovate achieve lead

Layer 3: Network Layer

- Routing
  - As we know, both computers A & B have their unique IP addresses
  - Network layer of the BBC server adds sender and receiver's IP address in the packet



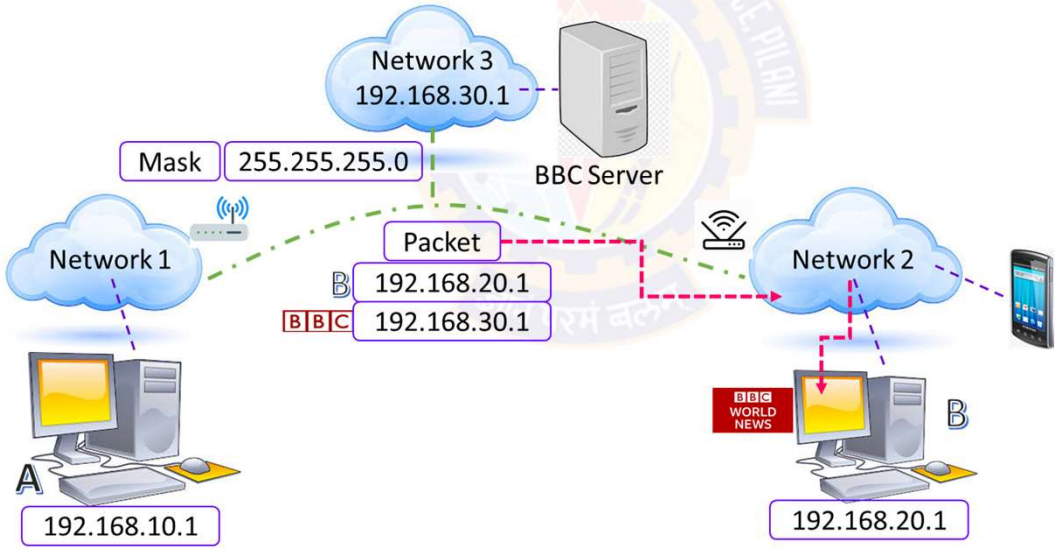
  - The mask 255.255.255.0 tells that the first three octets (192.168.20.1) of the IP address represent network, while the last octet represents host or computer B
  - Based on the IP address format, the received data packet will first move to network2 and then to computer B
  - Based on IP address and mask, routing decisions are made in a computer network

The OSI Model

innovate achieve lead

Layer 3: Network Layer

- Routing
  - Based on IP address and mask, routing decisions are made in a computer network



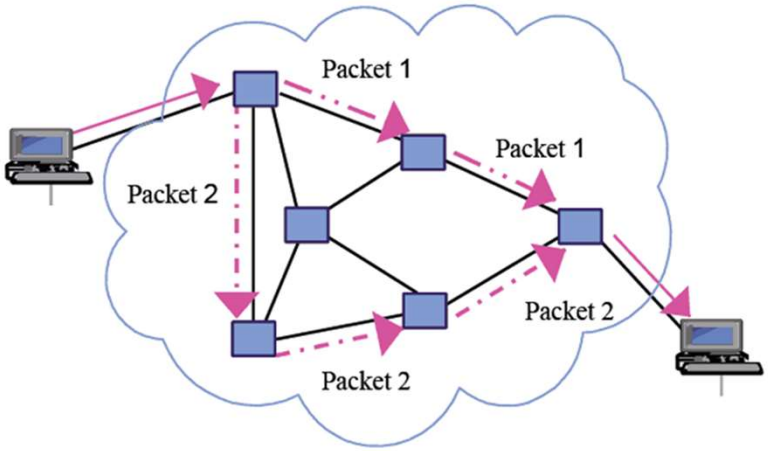
The OSI Model

innovate achieve lead

Layer 3: Network Layer

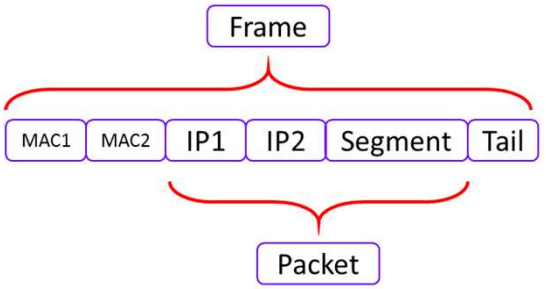
- Path Determination
  - A computer can be connected to an Internet server in a number of ways
  - Choosing the best possible path for data delivery from source to destination is called path determination
  - Layer 3 devices use protocols such as:
    - OSPF - Open Shortest Path First
    - BGP – Border Gateway Protocol
    - IS-IS - Intermediate System to Intermediate System

  To determine the best possible path for data delivery



The OSI Model

Layer 2: Data Link Layer



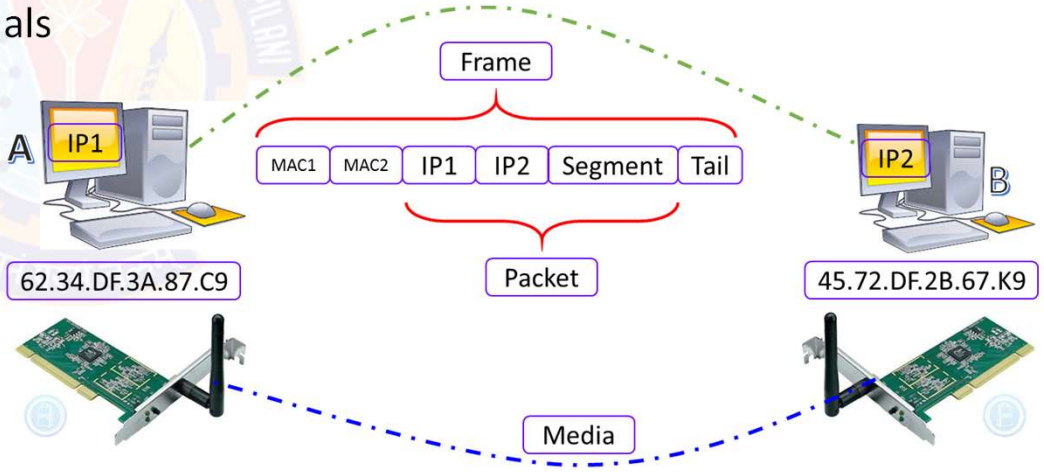
- Data Link Layer receives data packets from the Network Layer
- Data unit in the data link layer is called a frame
- Data packets contain IP addresses of the sender and the receiver
- There are two kinds of addressing
  - Logical addressing
    - Done in the network layer where sender's and receiver's IP address are assigned to each segment to form a data packet
  - Physical addressing
    - Done in the data link layer, where MAC address of sender and receiver are assigned to each data packet to form a frame
    - MAC address is a 12 digit alpha-numeric number embedded in the NIC of a computer

The OSI Model

innovate achieve lead

Layer 2: Data Link Layer

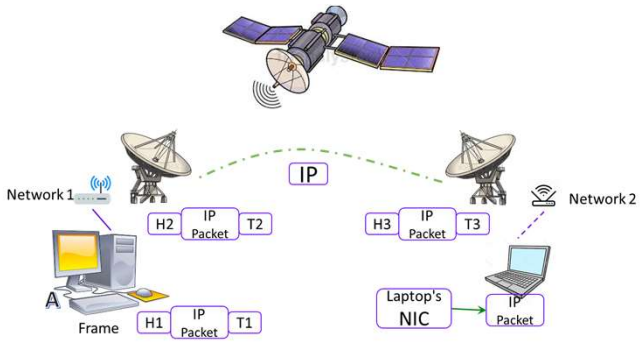
- Data Link Layer is embedded as software in the NIC of the computer
- It provides a means for transferring data from one computer to another via a local media
- Local media includes:
  - copper wire, fiber optics, or air for radio signals
- Data Link Layer performs two basic functions:
  - it allows the upper layers of OSI model to access media
  - controls how data is placed and received from the media using such as
    - Media Access Control (MAC)
    - Error Detection



The OSI Model

Layer 2: Data Link Layer

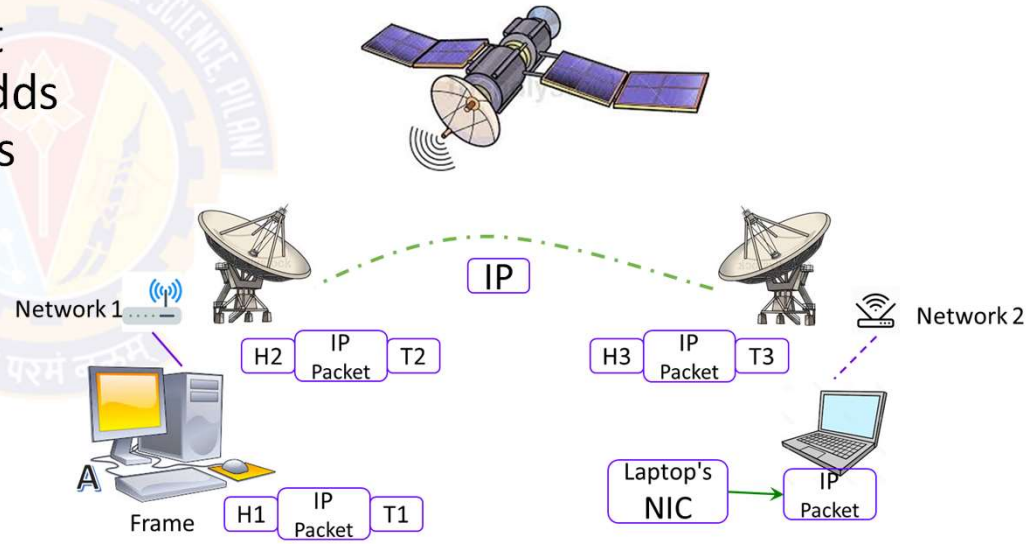
- Consider two distant hosts:
  - A desktop and a Laptop communicating with each other
- As laptop and desktop are connect to two different networks
  - they will be using network layer protocols (E.g., IP) to communicate with each other
- Desktop is connected to router R1 via an Ethernet cable
- Laptop is connected to router R2 via a wireless link
- Router R1 and R2 are connected via a satellite link



The OSI Model

Layer 2: Data Link Layer

- Desktop wants to send some data to laptop
  - Based on the medium used to connect desktop to router R1, data link layer adds some data in the head and tail sections of the IP packet and converts it to a frame (E.g., Ethernet frame)

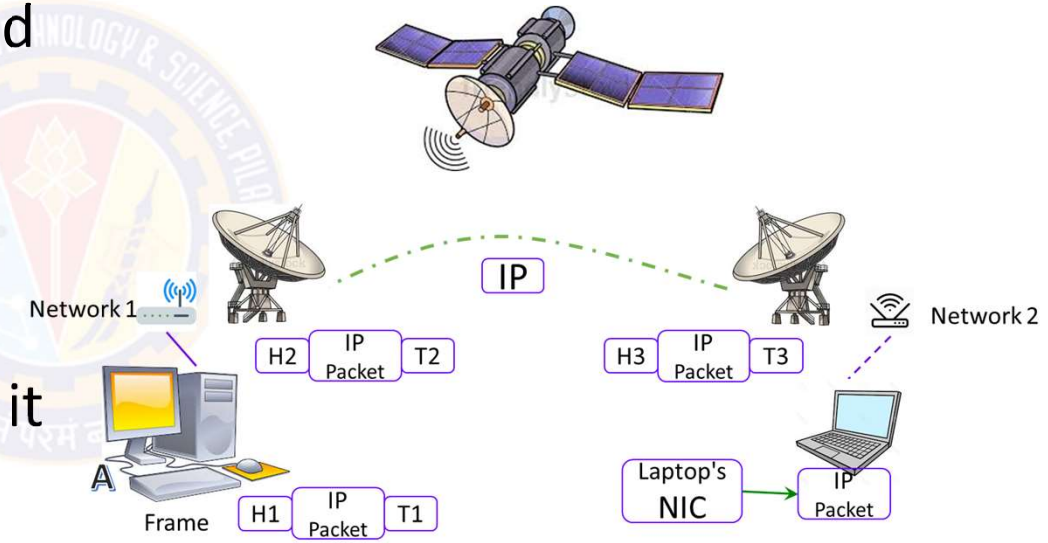


The OSI Model

innovate achieve lead

Layer 2: Data Link Layer

- Router R1 receives this frame, decapsulates it to an IP Packet and then encapsulates it again to a frame so that it can cross the satellite link to reach router R2
- Router R2 again decapsulates the received frame and encapsulates it again to form a wireless data link frame

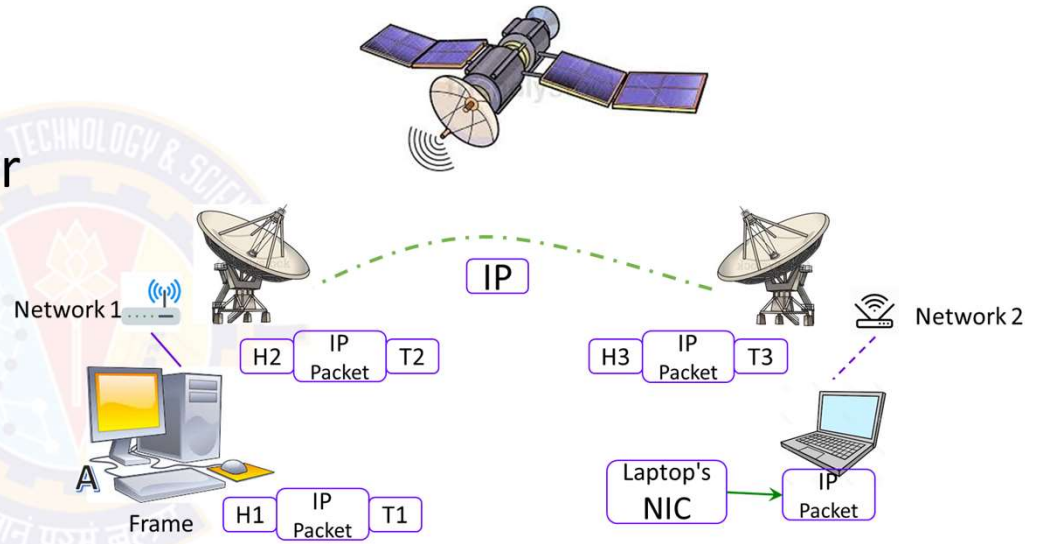


The OSI Model

innovate achieve lead

Layer 2: Data Link Layer

- Laptop receives this wireless data link frame, decapsulates it, and forwards IP packet to network layer
- Finally data arrives at the application layer
- Application layer protocols make the received data visible on computer screen
- Higher level layers are able to transfer data over the media with the help of data link layer



The OSI Model

Layer 2: Data Link Layer

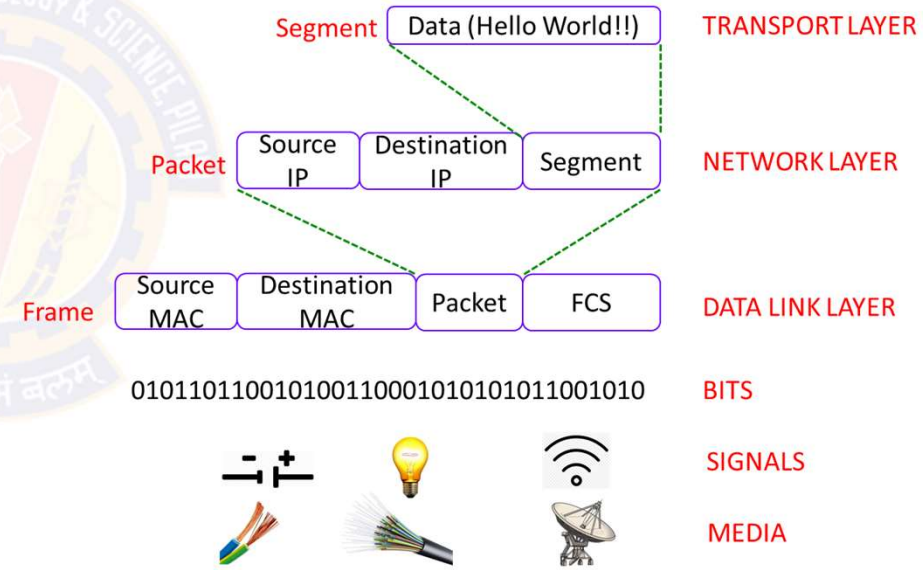
- Media Access Control
  - Data link layer also controls how the data is placed and received from the media
  - The technique used to get the frame on and off the media is called Media Access Control
  - There may be a number of devices connected to a common media
  - If two or more devices connected to same media send data simultaneously, there may be collisions of data packets resulting in loss of data
  - To avoid this situation, data link layer keeps an eye on when the shared media is free so that devices can transmit data for the receiver
  - This is called Carrier Sense Multiple Access (CSMA)
- Error Control
  - Tail of each frame contains bits which are used to check for errors in the received frame
  - Errors occur due to certain limitations of the media used for transmitting data

The OSI Model

innovate achieve lead

Layer 1: Physical Layer

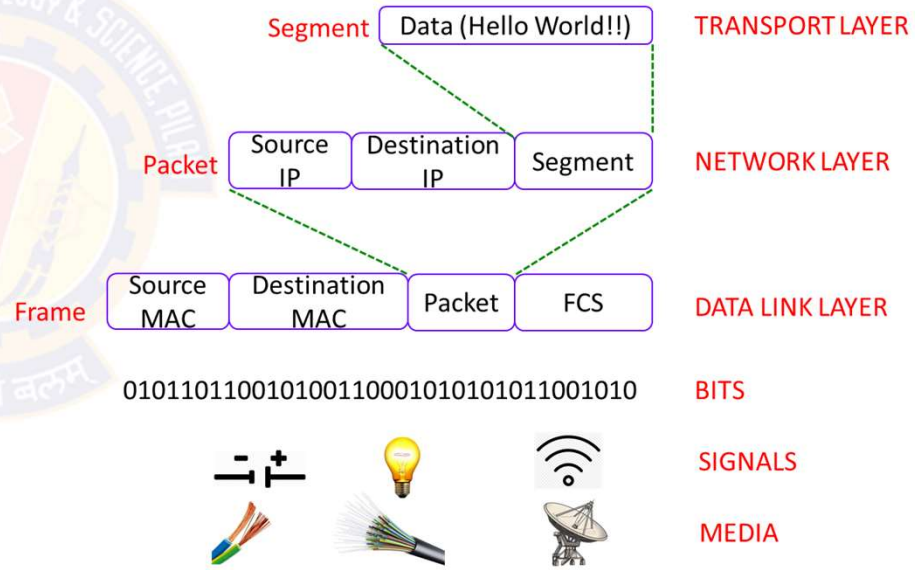
- Till now, data from application layer has been
  - segmented by transport layer,
  - placed into packets by network layer, and
  - framed by data link layer
- This is a sequence of binary 0's and 1's



The OSI Model

Layer 1: Physical Layer

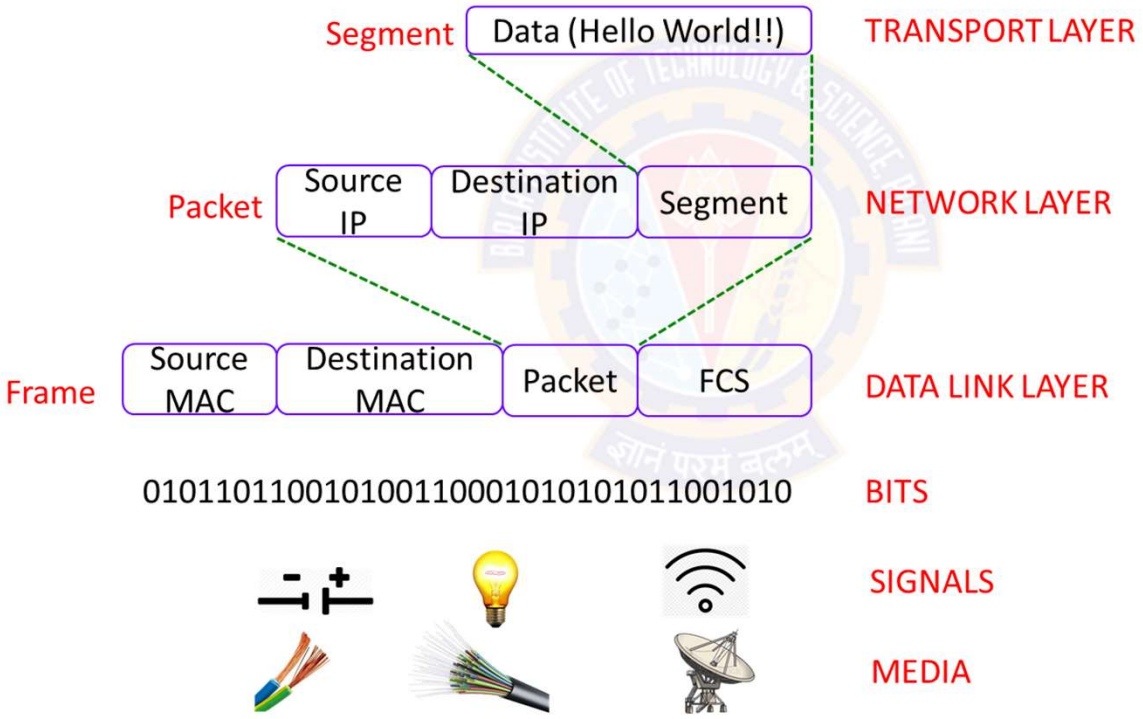
- Physical layer converts this binary sequence into signals and transmits over the local media
- It can be an electrical signal (for copper cable), light signal (optical fiber), and radio signal (in case of air)
- Signal generated by physical layer depends on the type of media used to connect two devices



The OSI Model

innovate achieve lead

Layer 1: Physical Layer



The OSI Model

Seven Layers of the OSI Networking Model

Layer	Description	Protocols
Application Layer	This layer controls and mediates the interaction of the network with the Operating System and the applications installed on this OS It basically defines how the applications handle the communications in which the system becomes involved when connected to a network	POP, SMTP, DNS, FTP, and so on
Presentation Layer	Performs data compression/ decompression and encryption/decryption	
Session Layer	Defines the connection between two computers as either a client-server connection or a peer-to-peer connection The term 'session' is used to describe this virtual network connection between computers	NetBIOS
Transport Layer	Mediates the movement of data between all the other layers	TCP, UDP

The OSI Model

Seven Layers of the OSI Networking Model

Layer	Description	Protocols
Network Layer	Defines the route through which the data packets will travel from node to node For this purpose, the transport layer masks the characteristics of lower layers from the upper layers in the OSI model	IP, Internet Control Message Protocol
Data Link Layer	Bridges the connection between the third layer (network layer) and the first layer (physical layer) by defining and implementing a protocol through which the network layer transmits its data to the physical layer	Address Resolution Protocol, Serial Line Internet Protocol, Point-to-Point Protocol
Physical Layer	Specifies the network cable, the router, the DSU/CSU box, and the other physical mediums involved.	None

Thank You!

BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Threat Landscape and Common Cyber Attacks

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Threat Landscape and Common Cyber Attacks

innovate achieve lead

Agenda

- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
  - Stages and Patterns
  - Targeted and Non-targeted Attacks
  - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
  - Boundary firewalls and Internet gateways
  - Secure configuration
  - Whitelisting and execution control
  - User access control
  - Password policy
  - Content checking

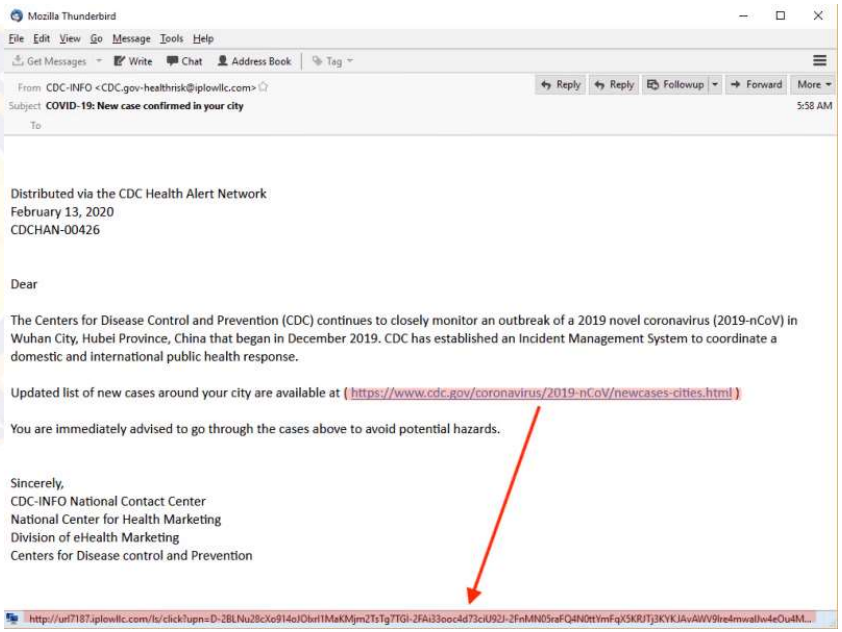
The Threat Landscape

The Threat Landscape

innovate achieve lead

Scenario

- Before we take a look at the cyber security threat landscape, let's look at this scenario
- Cybercrime Up 600% Due To COVID-19 Pandemic
- There is a rise in sophisticated phishing emails due to COVID-19
- Malicious actors are posing as the CDC or WHO representatives
- These emails are designed to deceive and trick recipients into taking an action:
  - clicking a malicious link, or opening an attachment with a virus



CDC = Center for Disease Control and Prevention
WHO = World Health Organization

https://purplesec.us/resources/cyber-security-statistics/

The Threat Landscape

innovate achieve lead

Key Industry Trends

- The cyber threat landscape is complex and constantly changing
- Cybersecurity has never been more important than before
- COVID-19 has forced companies to create remote workforces and operate off cloud-based platforms
- The rollout of 5G has made connected devices more connected than ever
- Some industry trends to watch for in 2021 and beyond
  - Remote workers will continue to be a target for cybercriminals
  - As a side effect of remote workforces, cloud breaches will increase
  - The cybersecurity skills gap will remain an issue
  - As a result of 5G increasing the bandwidth of connected devices, IoT devices will become more vulnerable to cyber attacks

https://www.varonis.com/blog/cybersecurity-statistics/

The Threat Landscape

innovate achieve lead

Some Facts

Fact	Source
95% of cybersecurity breaches are caused by human error	Cybint
The worldwide information security market is forecast to reach $170.4 billion in 2022	Gartner
88% of organizations worldwide experienced spear phishing attempts in 2019	Proofpoint
68% of business leaders feel their cybersecurity risks are increasing	Accenture
On average, only 5% of companies' folders are properly protected	Varonis
Data breaches exposed 36 billion records in the first half of 2020	RiskBased
86% of breaches were financially motivated and 10% were motivated by espionage	Verizon
45% of breaches featured hacking, 17% involved malware and 22% involved phishing	Verizon
Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches	ID Theft Resource Center
The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%	Symantec
An estimated 300 billion passwords are used by humans and machines worldwide	Cybersecurity Media

https://www.varonis.com/blog/cybersecurity-statistics/

The Threat Landscape

innovate achieve lead

Some Facts

Fact
There is a hacker attack every 39 seconds
43% of cyber attacks target small business
The global average cost of a data breach is $3.9 million across SMBs
9.7 Million Records healthcare records were compromised in September 2020 alone
Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021
Connected IoT devices will reach 75 billion by 2025
Unfilled cybersecurity jobs worldwide is already over 4 million
More than 77% of organizations do not have a Cyber Security Incident Response plan
Most companies take nearly 6 months to detect a data breach, even major ones
Share prices fall 7.27% on average after a breach
Total cost for cybercrime committed globally will reach $6 trillion by 2021

https://www.cybintsolutions.com/cyber-security-facts-stats/

The Threat Landscape

innovate achieve lead

Some Perspectives of Security

- Let's understand some perspectives of security
  - Technology is the cause of attack
  - Risk-Reward Ratio and Ease of stealing
  - Cyber crime Vs. Physical crime
  - Information is an asset to both criminals and organizations
  - Personal Computing Assets (Remote Working due to COVID-19)
  - The Digital Divide
  - The Growing Internet of Things
  - Increasing use of Social Media

The Threat Landscape

innovate achieve lead

Technology is the cause of attack

- In today's world the growth and prominence of technologies and data are showing no signs of slowing down
- The technology changes in unimaginable ways
  - We can be attacked both physically and virtually
- For today's organizations that rely heavily on technology (particularly the Internet) for doing their business
  - Virtual attacks are far more threatening
- For every vulnerability fixed, another pops up, ripe for exploitation
- When a vulnerability is identified, a tool that can exploit it is often developed and used within hours
  - This is faster than the time it normally takes for the vendor to release a patch, and certainly quicker than the time many organizations take to install that patch
- The adoption of new innovations creates an environment where threat landscapes can change quickly

The Threat Landscape

innovate achieve lead

Risk-Reward Ratio & Ease of Stealing

- The technology gives attackers a huge advantage over the defenders
  - They attack anyone, anywhere, from the comfort of their home
  - They often have automated tools to identify their victims – and their vulnerabilities
- From an attacker's perspective, there is often a very good risk-to-reward ratio:
  - For the victim, it can be hard enough to detect that the attack happened at all, never mind trace who was behind it
- It is the very nature of the digital information that we are trying to protect that is easy to copy
- In fact, stealing the information does not require removing it from its original location at all
  - meaning that the owner of that information may never realize that the theft happened

The Threat Landscape

innovate achieve lead

Cyber crime Vs. Physical crime

- Committing crimes over the Internet can also be very lucrative
- Physical pickpocketing compared with digitally targeting someone
  - Stealing cash and credit cards can only be beneficial for short term
  - Stealing a person's identity can get credit cards issued in the victim's name
- Upscale that to targeting businesses
  - A criminal might get access to thousands or even millions of credit card details and personal information
  - They can use the information for themselves or sell it on the dark web
    - where you can buy virtually anything, from drugs and organs to hacking software and stolen credentials
- The profits are certainly far greater compared to a physical crime conducted in the same timescale and with the same manpower

The Threat Landscape

innovate achieve lead

Information is asset to both criminals and organizations

- Information 'assets' – by definition, someone else wants to get hold of them
- Individuals normally go through the proper channels – but not everyone will take the legal route
- Everyone is a target because virtually every organization (even a small business) holds valuable information (often in huge quantities)
- Being the most important asset, organizations cannot do business if they lose access to that information
- The fact that criminals can extract significant value from this information means that it is an asset to them too

The Threat Landscape

innovate achieve lead

Personal Computing Assets (Remote Working)

- Threat landscapes commonly prioritize corporate and governmental networks assets as high priorities
  - Personal networks and resources are treated as lower-level threats
- Covid-19 pandemic resulted in over 40% of people working from home
  - This requires a reassessment of prioritization levels
- This change enabled bad actors with more opportunities to prey on remote workers
  - This forces reassessment of the risk level of home networks
- Today's threat landscape must also include personal computing assets as high-risk and high-value targets
  - This is because often-sensitive data being accessed outside of the protected corporate networks

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

The Digital Divide

- The changing threat landscape has made a large segment of society to use technology securely
- People who may lack skills needed to protect themselves from security attacks now use their computers for education, work, and play
- In many situations, multiple family members utilize the same electronic device, greatly increasing the chance for exposure to malware
- Educational institutions are now required to quickly transition to online learning without implementing necessary training and cybersecurity protocols
  - These training and protocols are part of traditional online models
- Educators who may have not previously utilized technology are now sharing files as part of their daily online classroom interactions
  - This could introduce malware onto their devices

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Growing Internet of Things

- Connected appliances
- Smart home security systems
- Autonomous farming equipment
- Wearable health monitors
- Smart factory equipment
- Wireless inventory trackers
- Ultra-high speed wireless internet
- Biometric cybersecurity scanners
- Shipping container and logistics tracking

- Connected Cars
- Connected Homes
- Connected Agriculture
- Connected Retail
- Connected Hospitality
- Connected Health
- Connected Manufacturing
- Connected Citites

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Growing Internet of Things

- A growing Internet of Things (IoT) has exposed devices to cyberattacks
  - A few years ago these would never have been included in most threat landscape models
- More healthcare and fitness apps for people to manage their health
  - This increases scope for attack surfaces
  - An attack on such apps, exposes large amounts of personal data and puts personal lives at risk
- Large number of payment apps such as GooglePay & PayTM
  - Such apps expose the possibility of stealing credit card and bank account information
- Modern agriculture equipment incorporates large amounts of technology
  - including data centers, networks, satellites and even artificial intelligence (AI)
  - a successful large-scale attack by either a lone individual or an organized group could potentially damage our food supply

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Increasing use of Social Media

- Greater numbers of individuals use social media as a news source
  - More than half of Americans receive their news by social media (Forbes)
- The manipulation of video using techniques such as deepfake make it increasingly difficult to recognize altered videos in social media
  - https://youtu.be/EfREntgxmDs
  - https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/
- Conspiracy theories are often shared online as facts, introducing yet more confusion in actual messaging to users looking for current news
- The risk of wireless technology remains constant
  - In addition, widespread use of 5G has introduces additional vulnerabilities

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Wireless Technology

- Previous mobile network topology provided for fewer pieces of hardware at which point traffic could be monitored
- The decentralized nature of 5G requires implementation of monitoring and security solutions at an exponentially greater number of devices
- The increased bandwidth and ability to add large numbers of IoT devices will require security solutions that are scalable and able to respond rapidly in order to provide a secure computing environment
- Understanding today's threat landscape is critical to developing strategies and solutions to establish a strong cybersecurity framework
- It is critical for both organizations and individuals to not become complacent and remain vigilant, regularly defending their threat landscape

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

References

- The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks by Alan Calder *Published by IT Governance Publishing, 2020*
- UK Department for Digital, Culture, Media & Sport, "Cyber Security Breaches Survey 2020", March 2020, https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

Understanding Vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Overview

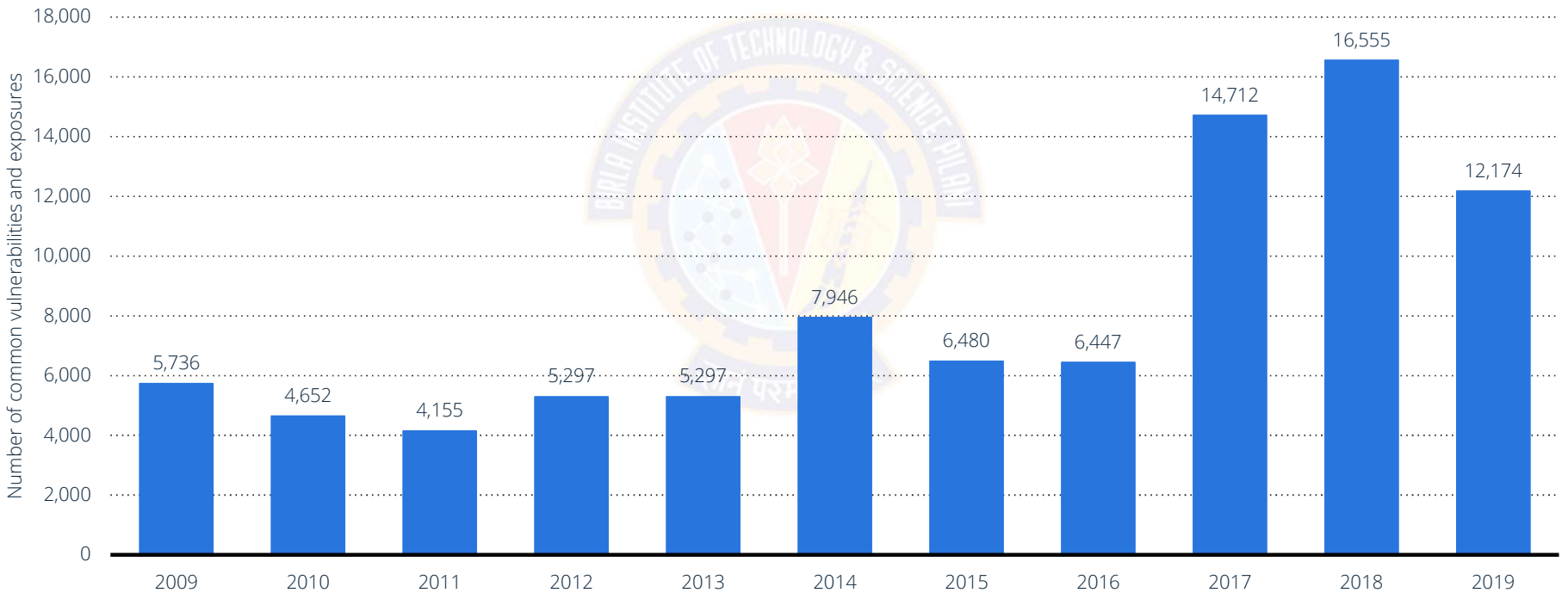
- A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack
- Attackers will look to exploit any of them, often combining one or more, to achieve their end goal
- To exploit an existing vulnerability, an attacker needs to have at least one tool that connects to a system weakness:
  - The vulnerability then becomes what is known as the "attack surface".

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Common IT vulnerabilities and exposures worldwide 2009-2019



Note(s): Worldwide; 2009 to 2019
Source(s): Website (cvedetails.com); ID 500755

statista

Understanding Vulnerabilities

innovate achieve lead

Vulnerability Categories

- Virtually, there can be 1000s of vulnerabilities
- However, they can be broadly grouped into following categories
  - Server and Host Vulnerabilities
  - Network Vulnerabilities
  - Virtualization Vulnerabilities
  - Web Application Vulnerabilities
  - Internet of Things Vulnerabilities
  - Database Vulnerabilities

Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

About MITRE

- The MITRE Corporation is an American not-for-profit organization based in Bedford, Massachusetts, and McLean, Virginia
- It manages federally funded R&D centers (FFRDCs) supporting several U.S. government agencies
- MITRE maintains the Common Vulnerabilities and Exposures (CVE) system and the Common Weakness Enumeration (CWE) project
- Since 1999, the MITRE Corporation has been functioning as editor and primary numbering authority of the CVEs
- CVE is now the industry standard for vulnerability and exposure names
- It provides reference points for data exchange so that information security products and services can interoperate with each other

Source: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Understanding Vulnerabilities

innovate achieve lead

Common Computer Security Vulnerabilities - 2020

- The Common Weakness Enumeration (CWE) identified the Top 25 Most Dangerous Software Errors
- The CWE Top 25 provides insight into the most severe and current security weaknesses
- This is a demonstrative list of the most common and impactful issues experienced over the previous two calendar years
- While the list remains comprehensive, there are many other threats that leave software vulnerable to attack
- These weaknesses are dangerous because they are often easy to find, exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities

Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82	Exposure of Sensitive Information to an Unauthorized Actor	19.16
Out-of-bounds Write	46.17	Use After Free	18.87
Improper Input Validation	33.47	Cross-Site Request Forgery (CSRF)	17.29
Out-of-bounds Read	26.50	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73	Integer Overflow or Wraparound	15.81
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13.67

2020 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities

Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
NULL Pointer Dereference	8.35	Use of Hard-coded Credentials	5.19
Improper Authentication	8.17	Deserialization of Untrusted Data	4.93
Unrestricted Upload of File with Dangerous Type	7.38	Improper Privilege Management	4.87
Incorrect Permission Assignment for Critical Resource	6.95	Uncontrolled Resource Consumption	4.14
Improper Control of Generation of Code ('Code Injection')	6.53	Missing Authentication for Critical Function	3.85
Insufficiently Protected Credentials	5.49	Missing Authorization	3.77
Improper Restriction of XML External Entity Reference	5.33		

2020 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- They can occur through:
  - Flaws
  - Features
  - User error
  - Zero-day vulnerabilities

Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Flaws
  - A flaw is an unintended functionality
  - This may either be a result of poor design or through mistakes made during implementation (coding)
  - Flaws may go undetected for a significant period of time
  - The majority of common attacks we see today exploit these types of vulnerabilities
  - Between 2014 and 2015, nearly 8,000 unique and verified software vulnerabilities were disclosed in the US National Vulnerability Database (NVD)
  - Vulnerabilities are actively pursued and exploited by the full range of attackers
  - Consequently, a market has grown in software flaws, with 'zero-day' vulnerabilities fetching hundreds of thousands of dollars

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Features
  - A feature is intended functionality which can be misused by an attacker to breach a system
  - Features may improve the user's experience, help diagnose problems or improve management, but they can also be exploited by an attacker
  - Example:
    - Microsoft introduced macros into their Office suite in the late 1990s. They soon became the vulnerability of choice
      - E.g., Melissa virus in March, 1999
      - It was a mass-mailing macro virus. It targeted Microsoft Word and Outlook-based systems, and created considerable network traffic
      - The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username
      - Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each
      - It would then mass mail itself to the first 50 people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

Causes of Vulnerabilities

- Features
  - Macros are still exploited today
    - The Dridex banking Trojan that was spreading in late 2014 relies on spam to deliver Microsoft Word documents containing malicious macro code, which then downloads Dridex onto the affected system.
  - JavaScript, widely used in dynamic web content, continues to be used by attackers
    - E.g., Diverting the user's browser to a malicious website and silently downloading malware, and hiding malicious code to pass through basic web filtering.

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- User Error
  - Users can be a significant source of vulnerabilities
  - They make mistakes, such as choosing a common or easily guessed password, or leaving their laptop or mobile phone unattended
  - Even the most cyber aware users can be fooled into giving away their password, installing malware, or divulging confidential information
  - These details would allow an attacker to target and time an attack appropriately
  - A carefully designed and implemented computer system can minimize vulnerabilities
  - Such efforts can be easily undone
    - E.g., an inexperienced system administrator who enables vulnerable features, fails to fix a known flaw, or leaves default passwords unchanged

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Zero-day vulnerabilities
  - The term "zero-day" refers to a newly discovered software vulnerability
  - Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released
  - So, "zero-day" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers
  - Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users.
  - But the software vendor may fail to release a patch before hackers manage to exploit the security hole
  - That's known as a zero-day attack.

Source: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Vulnerabilities are not just software-based
- Vulnerabilities can be found on software, hardware, network, even the users — impacting all assets across an organization
- Vulnerabilities can come from many sources, complexity, misconfiguration, connectivity, software bugs, etc.
- The most common source of vulnerabilities is the human user
  - Which poses a significant risk for organizations and their security posture.

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Common Vulnerability Scoring System (CVSS)

- While software bugs aren't inherently harmful (except for potential performance issues), many can be taken advantage of by "bad" actors
  - These are known as vulnerabilities.
- Vulnerabilities can be leveraged to force software to act in ways it's not intended to
  - E.g., gleaning information about the current security defenses in place.
- Once a bug is determined to be a vulnerability, it is registered by MITRE as a CVE, or common vulnerability or exposure
- The vulnerability is assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to the organization
- This central listing of CVEs serves as a reference point for vulnerability scanners

Source: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Understanding Vulnerabilities

Scanning Vulnerabilities

- A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses
- They are used to identify and detect vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc.,
- A vulnerability scanner scans and compares an organization's environment against a vulnerability database, or a list of known vulnerabilities
- Once the vulnerabilities are detected, developers can use penetration testing as a means to see where the weaknesses are
- These problems can be fixed and future mistakes can be avoided
- Frequent and consistent scanning will enable us to see common threads between vulnerabilities and a better understanding of the system

Source: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- Before we discuss identifying vulnerabilities, we need to understand threat and risk
- Threat
  - A potential for an attacker to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner
- Risk
  - The potential for loss computed as the combination of the *likelihood* that an attacker exploits some vulnerability to an asset, and the *magnitude* of harmful consequence that results to the asset's owner

Source: Computer and Security – Principles & Practice by William Stallings

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- Not all vulnerabilities are a security risk
- For example:
  - The risk of a vulnerability can depend on the potential impact that it could have on the business, in relation to which asset it impacts
- If the vulnerability is on a low-risk asset then it is much less likely of posing a significant risk
- The risk also depends on the time a vulnerability has existed
- A vulnerability which has been identified and quickly addressed poses much less risk than one that goes undetected for days, weeks, or even months

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- Identifying potentially significant risks to the assets requires answering the following questions for each asset:
  - Who or what could cause it harm?
    - This involves identifying potential threats to assets
  - How could this occur?
    - This involves identifying flaws or weaknesses in the organization's IT systems or processes that could be exploited by a threat source
- Mere existence of some vulnerability does not mean harm will be caused to an asset
  - There must also be a threat source for some threat that can exploit the vulnerability
- The combination of a *threat* and a *vulnerability* creates a risk to an asset

Source: Computer and Security – Principles & Practice by William Stallings

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- If you have a threat without a vulnerability, it isn't a risk
  - Threat
    - Hackers are using zero-day exploit against Windows XP systems
  - Vulnerability
    - We don't use Windows XP system in our organization
  - Risk
    - None

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- If you have a vulnerability without a threat, it isn't a risk
  - Threat
    - Hackers haven't found any exploitable coding errors
  - Vulnerability
    - Unpatched operating system software
  - Risk
    - None

Sources of Vulnerability Information

innovate achieve lead

Security Mailing Lists

- The following mailing lists contain interesting and useful discussion relating to current security vulnerabilities and issues
  - BugTraq (http://www.securityfocus.com/archive/1)
  - Full Disclosure (http://seclists.org/fulldisclosure/)
  - Pen-Test (http://www.securityfocus.com/archive/101)
  - Web Application Security (http://www.securityfocus.com/archive/107)
  - Honeypots (http://www.securityfocus.com/archive/119)
  - CVE Announce (http://archives.neohapsis.com/archives/cve/)
  - Nessus development (http://list.nessus.org)
  - Nmap-hackers (http://seclists.org/nmap-hackers/)
  - VulnWatch (http://www.vulnwatch.org)

Source: Network Security Assessment, 2nd Edition, by Chris McNab

Sources of Vulnerability Information

innovate achieve lead

Vulnerability Databases

- The following vulnerability databases and lists can be searched to enumerate vulnerabilities in specific technologies and products:
  - MITRE CVE (http://cve.mitre.org)
  - NIST NVD (http://nvd.nist.gov)
  - ISS X-Force (http://xforce.iss.net)
  - OSVDB (http://www.osvdb.org)
  - BugTraq (http://www.securityfocus.com/bid)
  - CERT vulnerability notes (http://www.kb.cert.org/vuls)
  - FrSIRT (http://www.frsirt.com)

Source: Network Security Assessment, 2nd Edition, by Chris McNab

Sources of Vulnerability Information

Underground Web Sites

- The following underground web sites contain useful exploit scripts and tools that can be used during penetration tests:

- Milw0m (http://www.milw0rm.com)
- Raptor's labs (http://www.0xdeadbeef.info)
- H D Moore's pages (http://www.metasploit.com/users/hdm/)
- The Hacker's Choice (http://www.thc.org)
- Packet Storm (http://www.packetstormsecurity.org)
- Insecure.org (http://www.insecure.org)
- Top 100 Network Security Tools (http://sectools.org)
- IndianZ (http://www.indianz.ch)
- Zone-H (http://www.zone-h.org)
- Phenoelit (http://www.phenoelit.de)
- Uninformed (http://uninformed.org)
- Astalavista (http://astalavista.com)
- cqure.net (http://www.cqure.net)
- TESO (http://www.team-teso.net)
- ADM (http://adm.freelsd.net/adm/)
- Hack in the box (http://www.hackinthebox.org)
- cnhonker (http://www.cnhonker.com)
- Soft Project (http://www.s0ftpj.org)
- Phrack (http://www.phrack.org)
- LSD-PLaNET (http://www.lsd-pl.net)
- w00w00 (http://www.w00w00.org)
- Digital Offense (http://www.digitaloffense.net)

Source: Network Security Assessment, 2nd Edition, by Chris McNab

Sources of Vulnerability Information

innovate achieve lead

Vulnerability Databases

- https://cve.mitre.org/
  - Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cybersecurity vulnerabilities
- https://nvd.nist.gov/
  - The National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP)
  - This data enables automation of vulnerability management, security measurement, and compliance
  - The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.

Thank You!