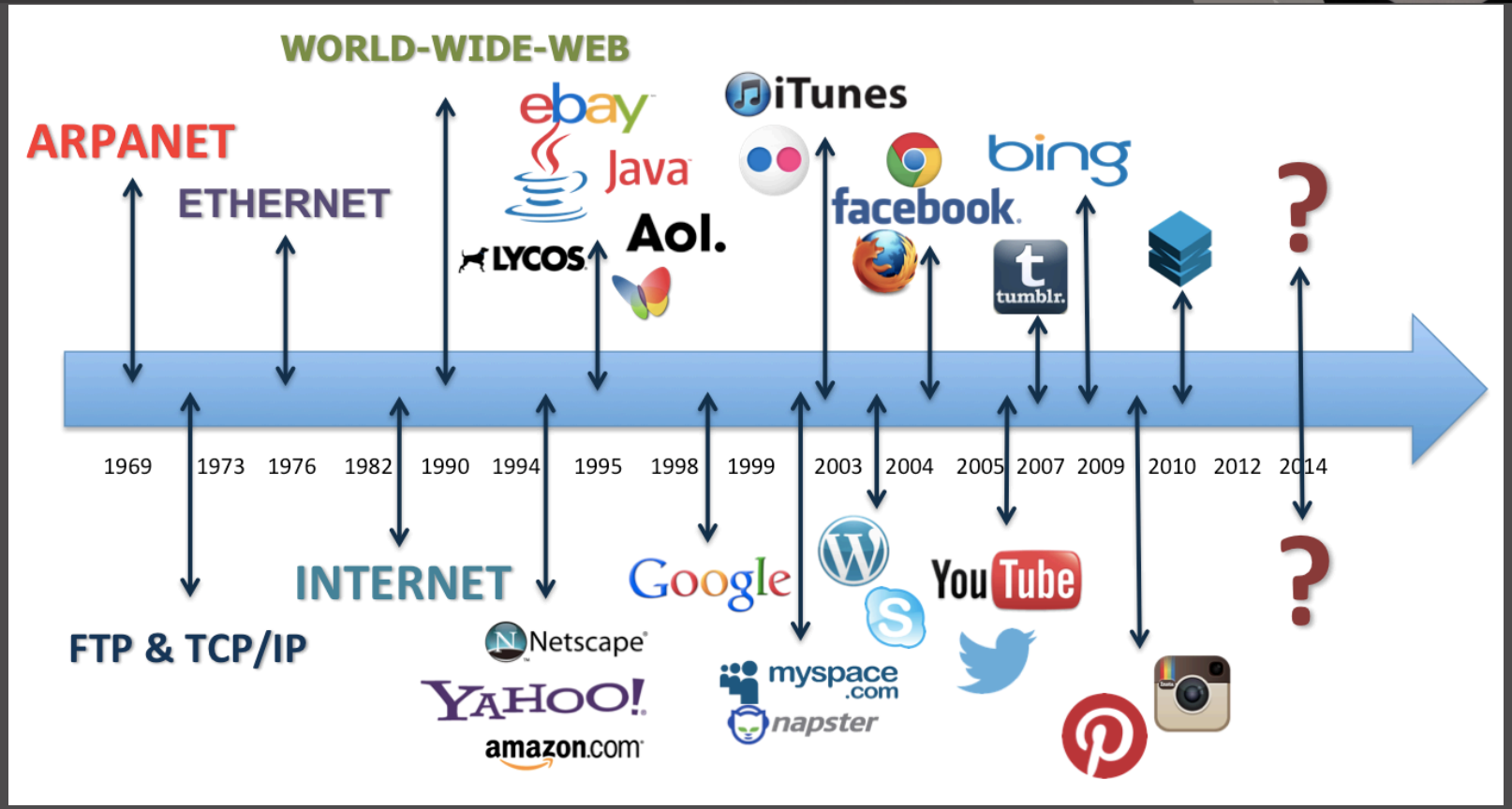
Security Essentials

Khandakar Rashedul Arefin

Presentation Outlines

- Internet and Information
- Information Security Goals
- Information Security-Holes
- Area of Attack and Security
- DDoS Attack and Traffic Types
- Information Security Control

Internet and Information



Information Security Goals

Confidentiality: Set of rules that limits access to information and Protect it from unauthorized access and misuse

Integrity: Protect information from unauthorized alteration and assurance that the information is trustworthy and accurate

Availability: Protect timely, reliable and uninterrupted access to the system by authorized user

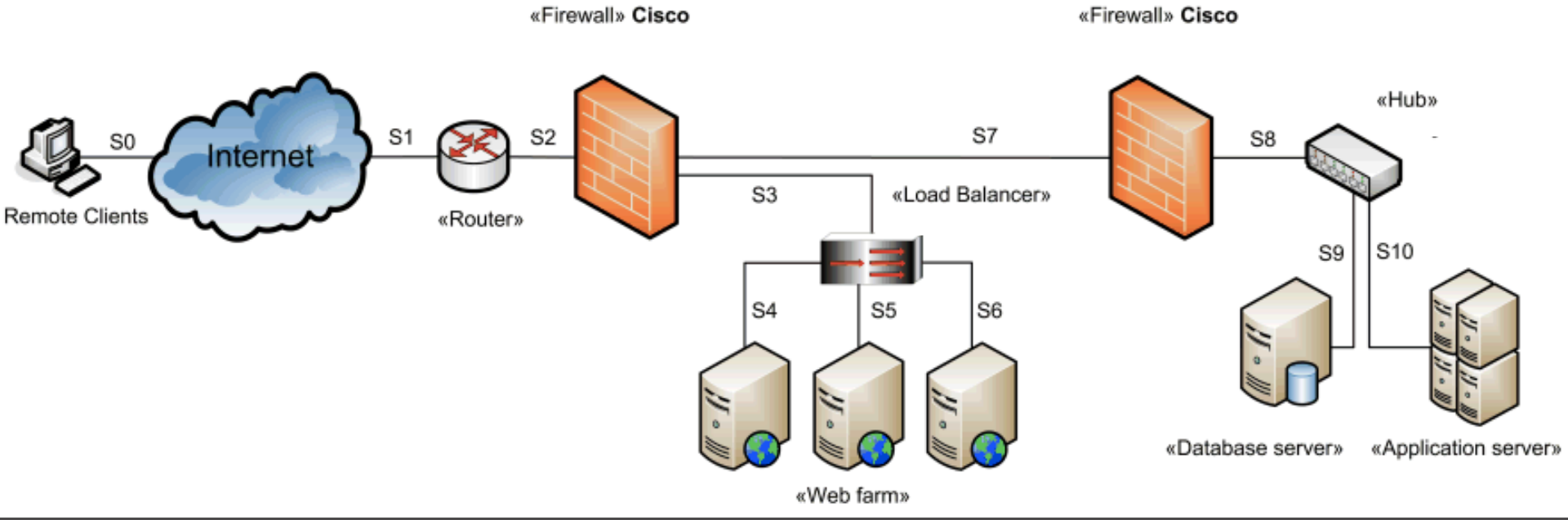
Information Security-Holes

Threat: A threat is what we're trying to protect against.

Vulnerability: A vulnerability is a weakness or gap in our protection efforts.

Risk: Risk is the intersection of assets, threats, and vulnerabilities.

Area of Attack and Security



Physical / Perimeter

Logical (TCP/IP Host Communication)

Data at Rest

Area of Attack and Security

Assets

- ✓ Storage Devices
- ✓ Hard Drives
- ✓ Computers
- ✓ Organization's Machine
- ✓ Laptops
- ✓ Servers

Threats and Crime

- ✓ Unauthorized Access
- ✓ Natural Disaster like fire and flood
- ✓ Human-Made Disaster like theft

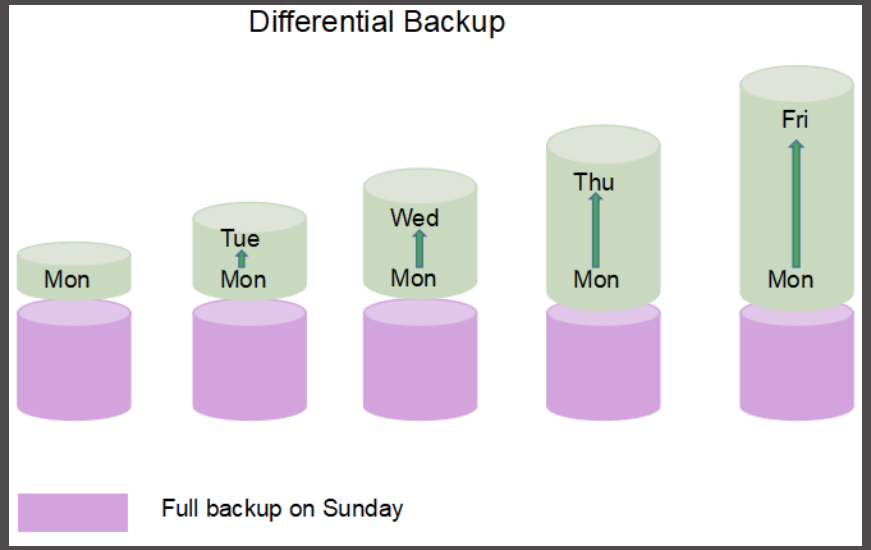
Physical Control

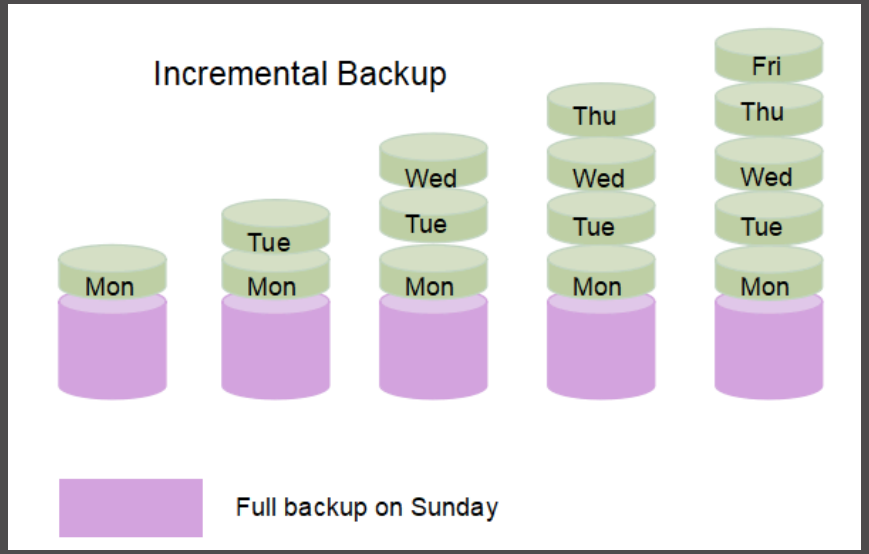
- ✓ Locks
- ✓ Protective Barriers
- ✓ In-penetrable walls and doors
- ✓ Backup Power (UPS)
- ✓ Security personnel for protecting sensitive data stored at Server

Area of Attack and Security

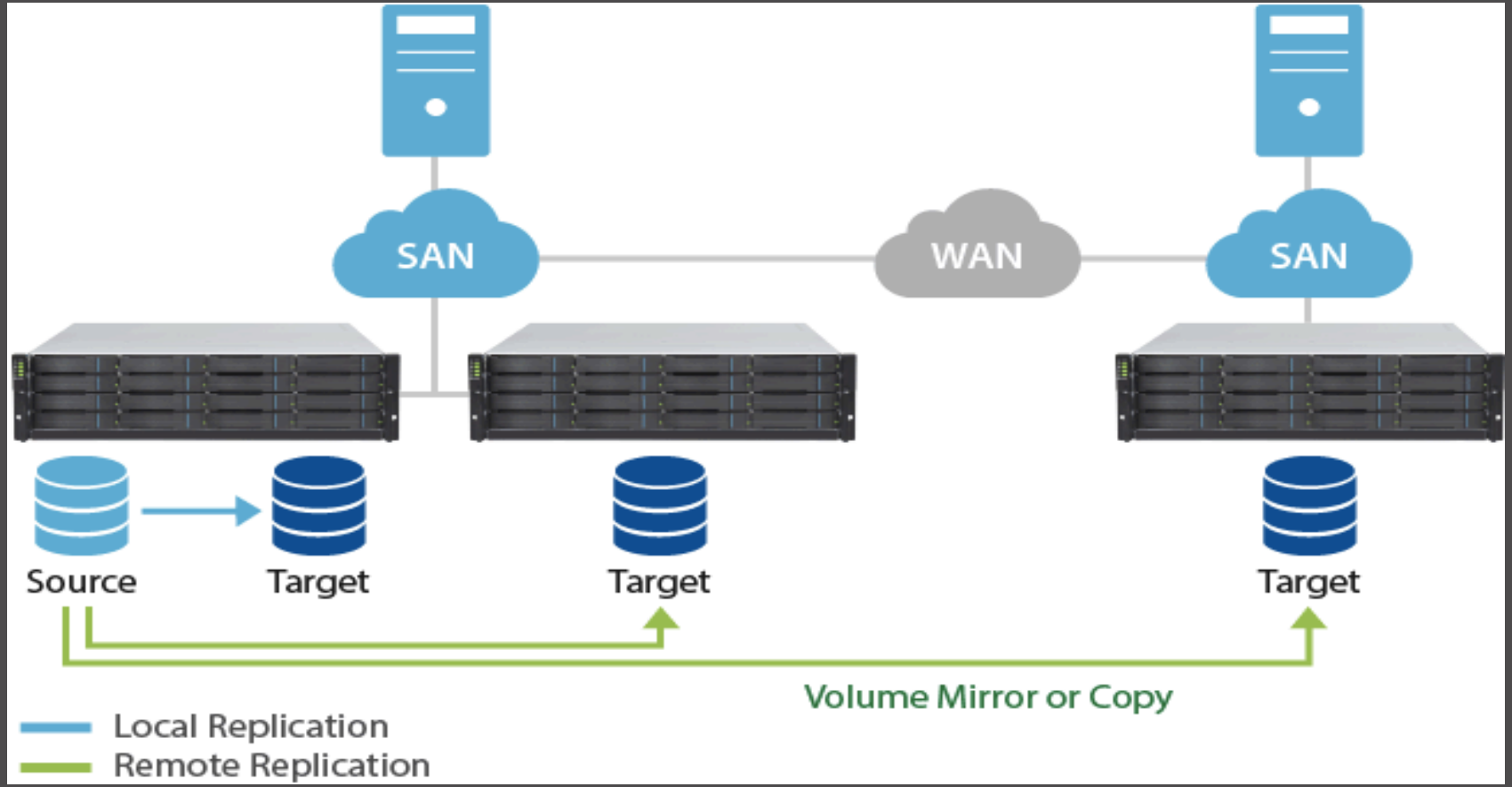
Application design & Program logic flaws	Application Layer	Testing and Review of App code & Functionality
System crash via Poor handling of input	Presentation Layer	Careful specification & checking of received input
Session Spoofing and Hijacking	Session Layer	Session ID information via random cryptography
TCP SYN and UDP Flooding	Transport Layer	Stateful Inspection at Firewall Layer
IP Address Spoofing	Network Layer	Anti-Spoofing Policy with Firewalls
MAC Address Spoofing	Data Link Layer	MAC Address Filtering
Disconnection of Physical Links	Physical Layer	Active Monitoring

Area of Attack and Security

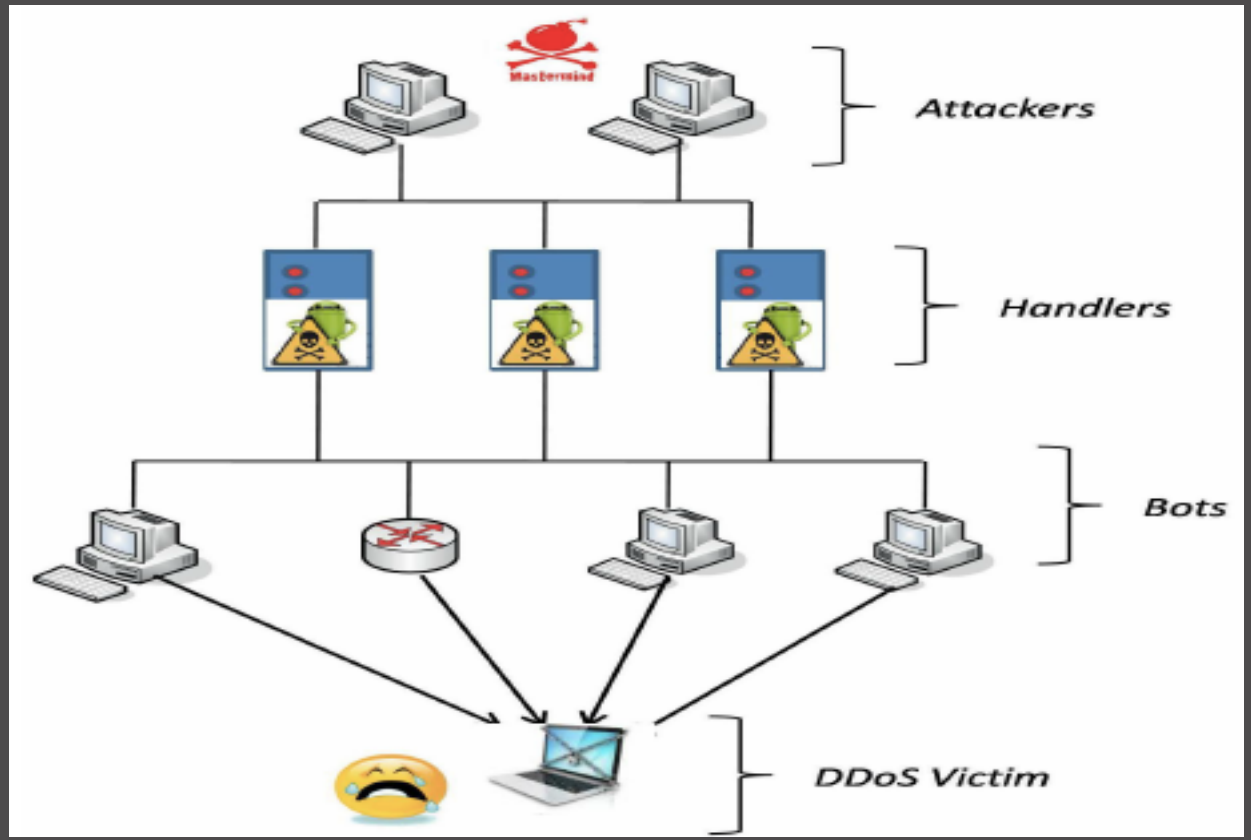




Area of Attack and Security



DDoS Attack and Traffic Types



- HTTP POST Flood
- HTTP POST Request
- HTTPS POST Flood
- HTTPS POST Request
- HTTP GET Flood
- HTTP GET Request
- HTTPS GET Flood
- HTTPS GET Request
- SYN Flood (TCP/SYN)
- UDP Flood
- ICMP Flood
- MAC Flood

Information Security Control

Category	Example of Controls
Policy and Procedure	Cyber Security Policy, Incident Handling Procedure
Technical	Firewall, Intrusion Detection System (IDS), Anti Virus Software
Physical	CCTV, Locks, Secure Working Space

- ✓ Controlling Data Access
- ✓ Controlling Network Access
- ✓ Protecting Information in Transit
- ✓ Ensuring Network Availability
- ✓ Preventing Intrusions
- ✓ Responding to Incidences

Information Security Control

Authentication: Identification of a user

Authorization: Who is allowed to use a Service

Accountability: What did a user do

Information Security Control

Layer 8:

- ✓ The user, the most vulnerable and threat to the system.
- ✓ It's High Risk

Enforcing Policy:

- ✓ Force to Change Password at first login
- ✓ Change password with predefined length and complexity
- ✓ Force to change password after specific timeline
- ✓ Password reset policy

System Access Policy:

- ✓ Disable root login
- ✓ SSH instead of Telnet
- ✓ Password less Login


Home
End
Delete
Enter
Shift