Computer Intrusion Detection

Lecture 2

Contributors to Computer Security;
Risk Analysis; TCP/IP Network

Xiangyang Li

Outline

Contributors to Computer Security

Risk Analysis

Introduction to TCP/IP Networking

Contributing Factors to Security

Risk assessment identifies three contributing factors to any risks

- Assets
- Vulnerabilities
- Threats

Risks of intrusions into computer and network systems

Threats explore vulnerabilities of a computer and network system to attack assets on the system

Assets

- Three kinds of services to users and three kinds of assets providing these services
  - Information processing
  - Information storage
  - Information communication
- Basic elements of a computer and network system
  - Host machines: a computer or a router
  - Communication links: networks

Asset Value

- Asset value measures the relative importance of an asset, and is related to the relative importance of services an asset provides to users
- Assets are what we protect, and asset value explains why we protect them
- Example: data of a new product is more important to an organization than data of a discontinued product

Assets

- The higher the value of an asset, the higher risk of intrusions the asset faces, and the higher level of security measures is required
- Asset assessment: rank assets or attributes (e.g., the CIA triad) of assets by asset value, and, intuitively, take security measures in proportion to the value of each asset
- But there is more to this

Vulnerability

- Describe the security strength of an asset. An asset is vulnerable if there is an opportunity of damage or loss of asset value.
- Example: a system administrator account without a password
- Example: the limited bandwidth of a communication link
- An asset may have more than one vulnerability.

Vulnerability Value

- Vulnerability value: indicates the severity of asset damage or loss due to the vulnerability
  - Example: a system administrator account without a password can lead to more severe problems than a regular user account without a password
- Weaknesses as causes of vulnerabilities
  - Weaknesses in computer and network technology to build a computer and network system, e.g., the limited bandwidth of a communication channel, a weak encryption algorithm, flaws in program code such as an operation system
  - Weaknesses in operation practice to configure a computer and network system and manage its operation, e.g., a user account without a password or with a weak password

Vulnerability Analysis

Formal Verification

Determine preconditions, postconditions

Validate that a system ensures postconditions given preconditions

Penetration testing

Start with system/environment characteristics, and state

Try to find vulnerabilities

Vulnerability Taxonomies

- RISOS (Research Into Secure Operating System) study in the mid-1970s
  - Incomplete parameter validation: parameters passed to a function call should be checked for the number, order, data types, values, ranges, access rights, and consistency of these parameters, e.g., the SENDMAIL program in UNIX allows an attacker to put special characters along with a shell command.
  - Inconsistent parameter validation: e.g., one function accepts a file name containing blanks, whereas another function does not allow blanks in a file name
  - Implicit sharing of privileged/confidential data: e.g., covert channels

Vulnerability Taxonomies

- RISOS (Research Into Secure Operating System) study in the mid-1970s (continued)
  - Inadequate identification/authentication/authorization: authorization grants access rights based on identification and authentication, e.g., a file is not uniquely identified (a file of Trojan program), a user is not authenticated, or an authorization is completely omitted
  - Violable prohibition/limit: e.g., buffer overflow problems
  - Exploitable logic errors: include error handling, timing condition and side effect problems, e.g., ping-of-death
  - Backdoors or trapdoors: those are intentionally created by programmers for program testing or system maintenance to gain access without going through authorization, e.g., default accounts shipped with system software

Threat

- Threats are potential attacks, and are what we protect from. We can better protect assets if we know what and where threats come from.
- Threat value: likelihood of the threat
- Types of threats
  - Environmental
  - Man-made
    - Intent: hostile versus non-hostile
    - Complexity: sophisticated versus unsophisticated
    - Source: internal versus external
    - Goal: denying service, gaining access, gathering or stealing information, modifying or deleting data, and so on

Example: Finger Daemon

- finger sends name to fingerd
  - fingerd allocates 512 byte buffer on stack
  - Places name in buffer
  - Retrieves information (local finger) and returns
- Problem: If name > 512 bytes, overwrites return address
- Exploit: Put code in “name”, pointer to code in bytes 513+
  - Overwrites return address

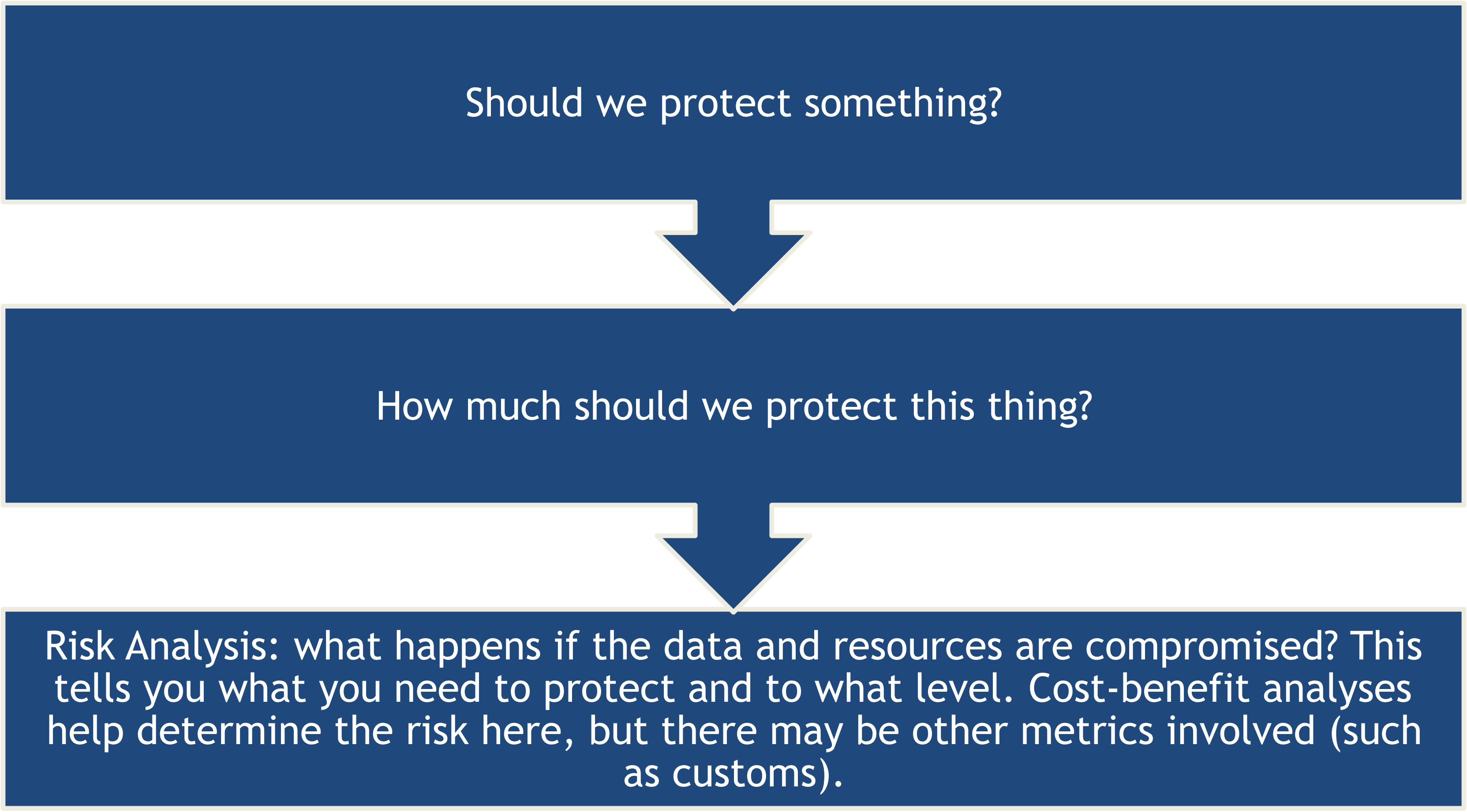
Threat Classificatio n

- Common Vulnerabilities and Exposures (CVE) - http://cve.mitre.org/cve/
- Common Weakness Enumeration (CWE) - https://cwe.mitre.org/

Outline

- Contributors to Computer Security
- Risk Analysis
- Introduction to TCP/IP Networking

Risk Assessment



Should we protect something?

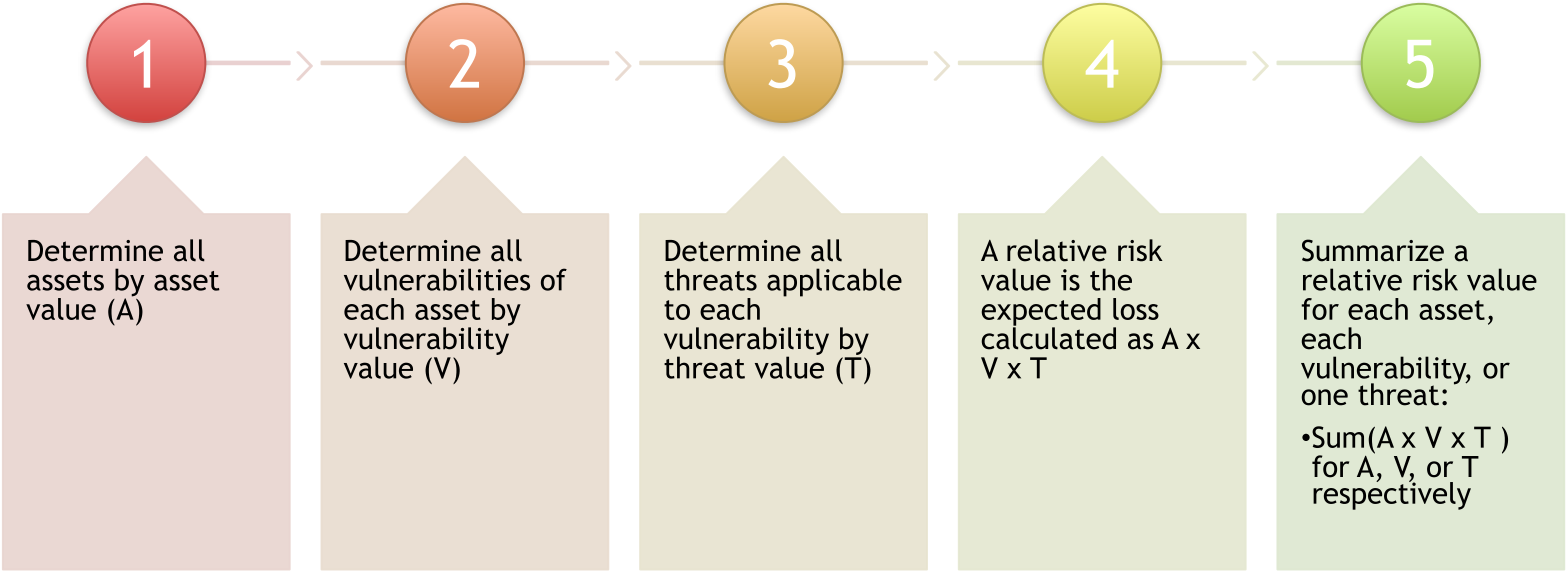
How much should we protect this thing?

Risk Analysis: what happens if the data and resources are compromised? This tells you what you need to protect and to what level. Cost-benefit analyses help determine the risk here, but there may be other metrics involved (such as customs).

Risk Assessment Example

- Assets are defined here as functions provided by a target information system. Let’s consider a military information system. We try to consider three assets: confidentiality, integrity, and availability of this information system.
- Vulnerabilities: violable prohibition/limit in user authentication program, and violable prohibition/limit in email system
- Threats: buffer overflow attack.

Probabilistic Risk Assessment in Information Assurance



1

Determine all assets by asset value (A)

2

Determine all vulnerabilities of each asset by vulnerability value (V)

3

Determine all threats applicable to each vulnerability by threat value (T)

4

A relative risk value is the expected loss calculated as A x V x T

5

Summarize a relative risk value for each asset, each vulnerability, or one threat:

- Sum(A x V x T) for A, V, or T respectively

Two Ways to Estimate Values

Historic Data

Real

Any problem?

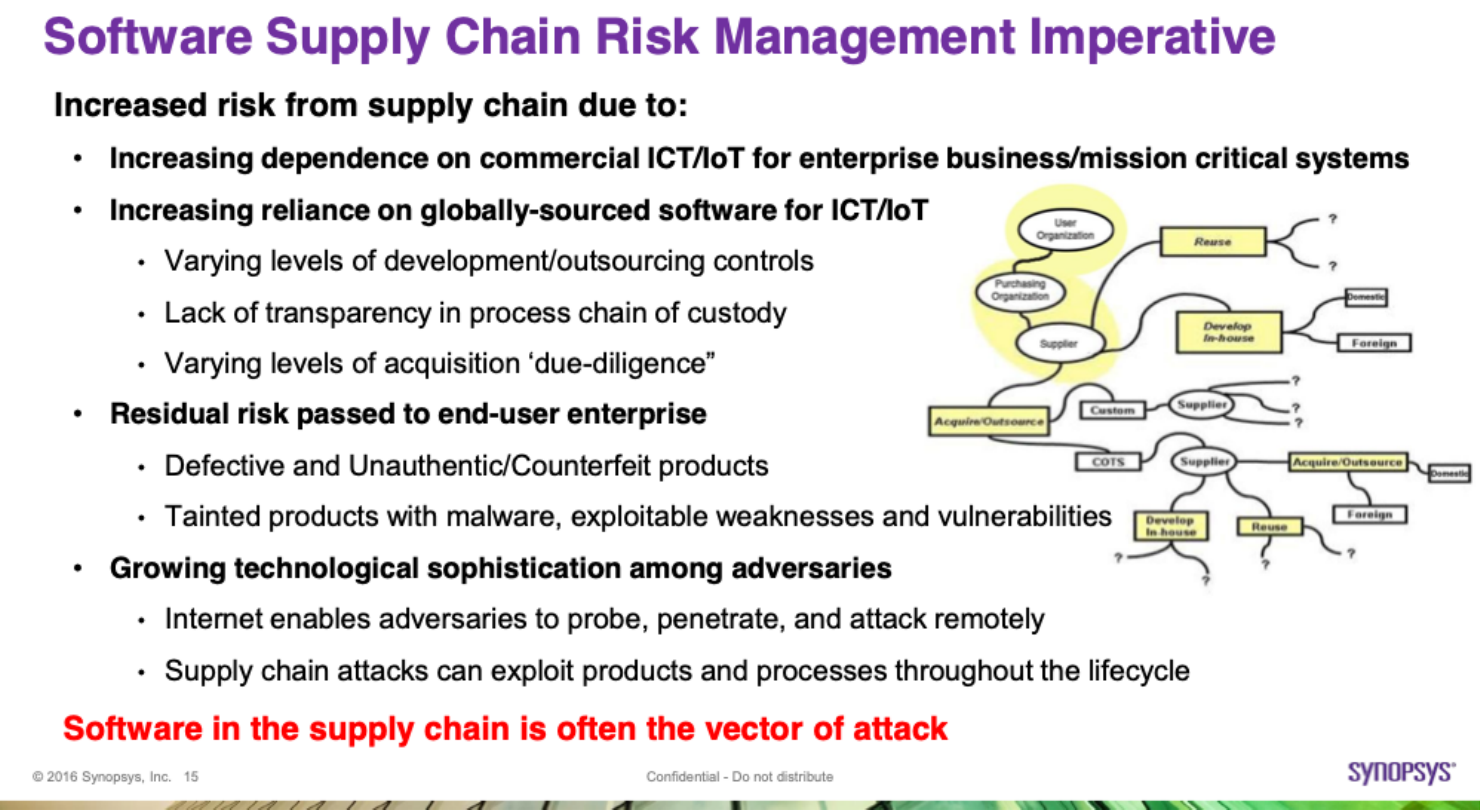
Expert Input

Subjective

Maybe the only information available!

Complexity of Risk Assessment

- An asset may have multiple vulnerabilities, and each vulnerability may face multiple applicable threats
- Relative risks must be examined at various scales of assets, because
  - Components of a computer and network system interact in complicated ways
  - A threat to a vulnerability of an asset may produce cascading effects of damage in the system
  - A threat may take a series of related actions that exploit vulnerabilities on multiple assets



Software Supply Chain Risk Management Imperative

Increased risk from supply chain due to:

- **Increasing dependence on commercial ICT/IoT for enterprise business/mission critical systems**
- **Increasing reliance on globally-sourced software for ICT/IoT**
  - Varying levels of development/outsourcing controls
  - Lack of transparency in process chain of custody
  - Varying levels of acquisition 'due-diligence"
- **Residual risk passed to end-user enterprise**
  - Defective and Unauthentic/Counterfeit products
  - Tainted products with malware, exploitable weaknesses and vulnerabilities
- **Growing technological sophistication among adversaries**
  - Internet enables adversaries to probe, penetrate, and attack remotely
  - Supply chain attacks can exploit products and processes throughout the lifecycle

Software in the supply chain is often the vector of attack

Confidential - Do not distribute

SYNOPSYS

Joe Jarzombek, *Software Supply Chain Management*, Presentation

Outline

Contributors to Computer Security

Risk Analysis

Introduction to TCP/IP Networking

Networking Process

EACH PACKET HAS AN ADDRESS AND DATA.

THE ADDRESS IS IN THE HEADER OF THE PACKET.

ROUTERS NEED ONLY LOOK AT THE HEADER FOR ROUTING INFO.

AT EACH STAGE THE ROUTER ONLY NEEDS TO KNOW THE NEXT LEG OF THE ROUTE.

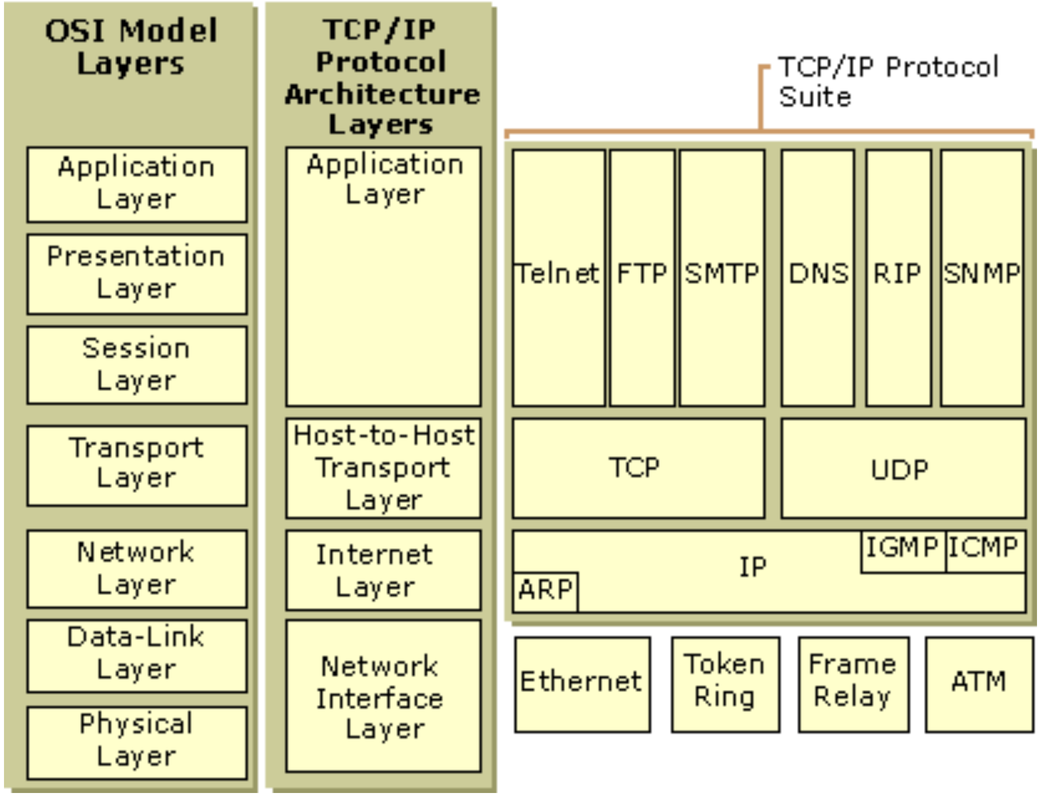
ROUTES CAN CHANGE DYNAMICALLY BUT ARE RELATIVELY STABLE SHORT-TIME.

AFTER A FINITE TIME LOST PACKETS ARE DROPPED.

LOST PACKETS MAY GENERATE AN ERROR, OR THEY MAY SIMPLY DISAPPEAR.

Networking Layers and Protocols

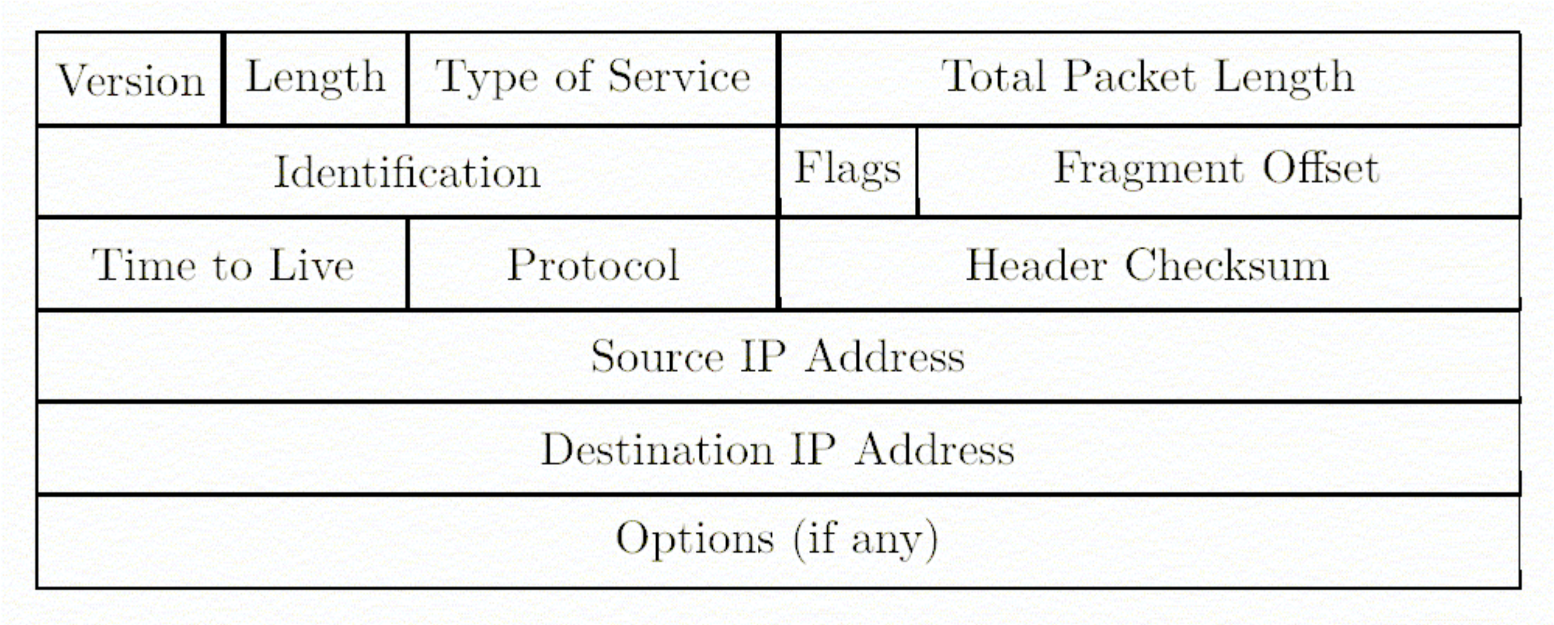
EN.650.654 Computer Intrusion Detection



TCP/IP Networking Layers

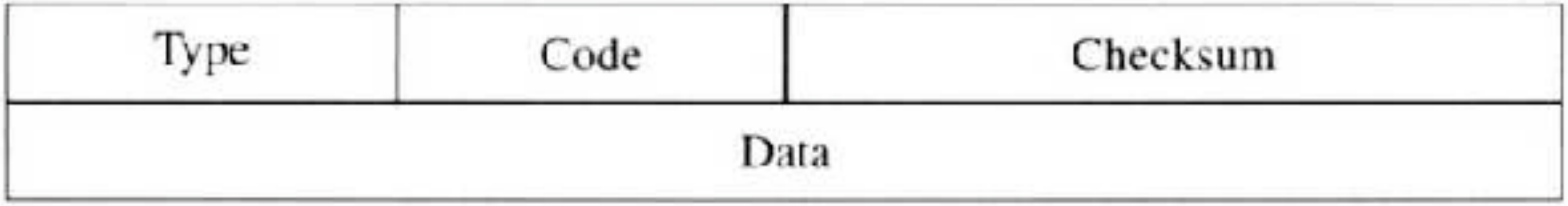
- Hardware Layer
- IP Layer
- Protocol Layer
- Application Layer

IP Header



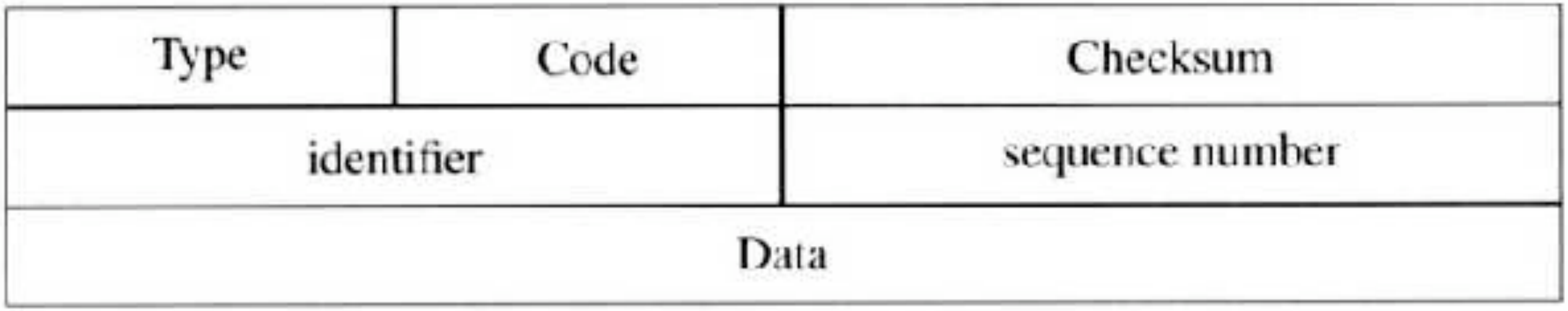
<table>
<tr><td>Version</td><td>Length</td><td>Type of Service</td><td colspan="2">Total Packet Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Options (if any)</td></tr>
</table>

ICMP Header



<table>
<tr><td>Type</td><td>Code</td><td>Checksum</td></tr>
<tr><td colspan="3">Data</td></tr>
</table>

ICMP Header

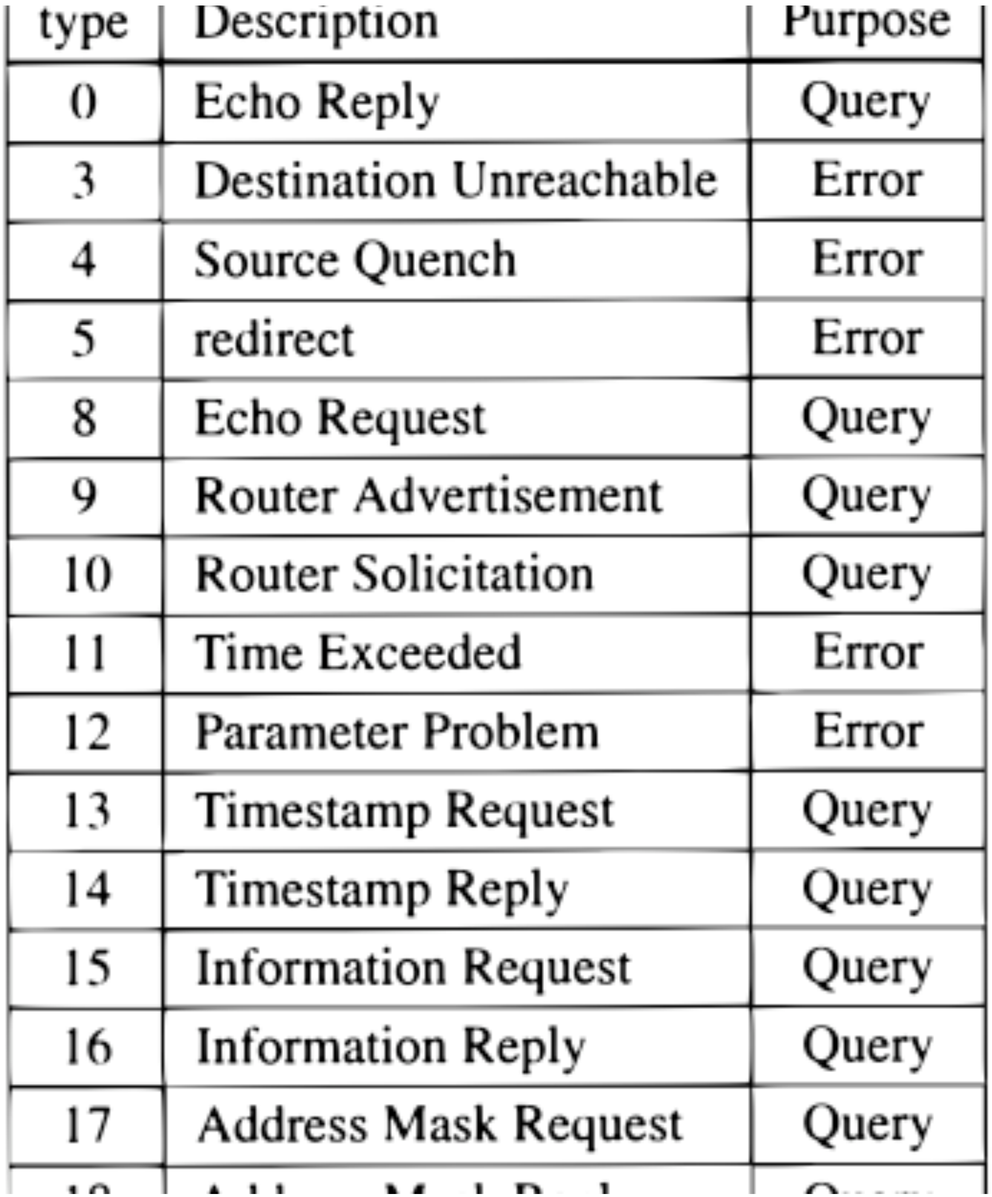


<table>
<tr><td>Type</td><td>Code</td><td>Checksum</td></tr>
<tr><td colspan="2">identifier</td><td>sequence number</td></tr>
<tr><td colspan="3">Data</td></tr>
</table>

Echo Request/Reply Header

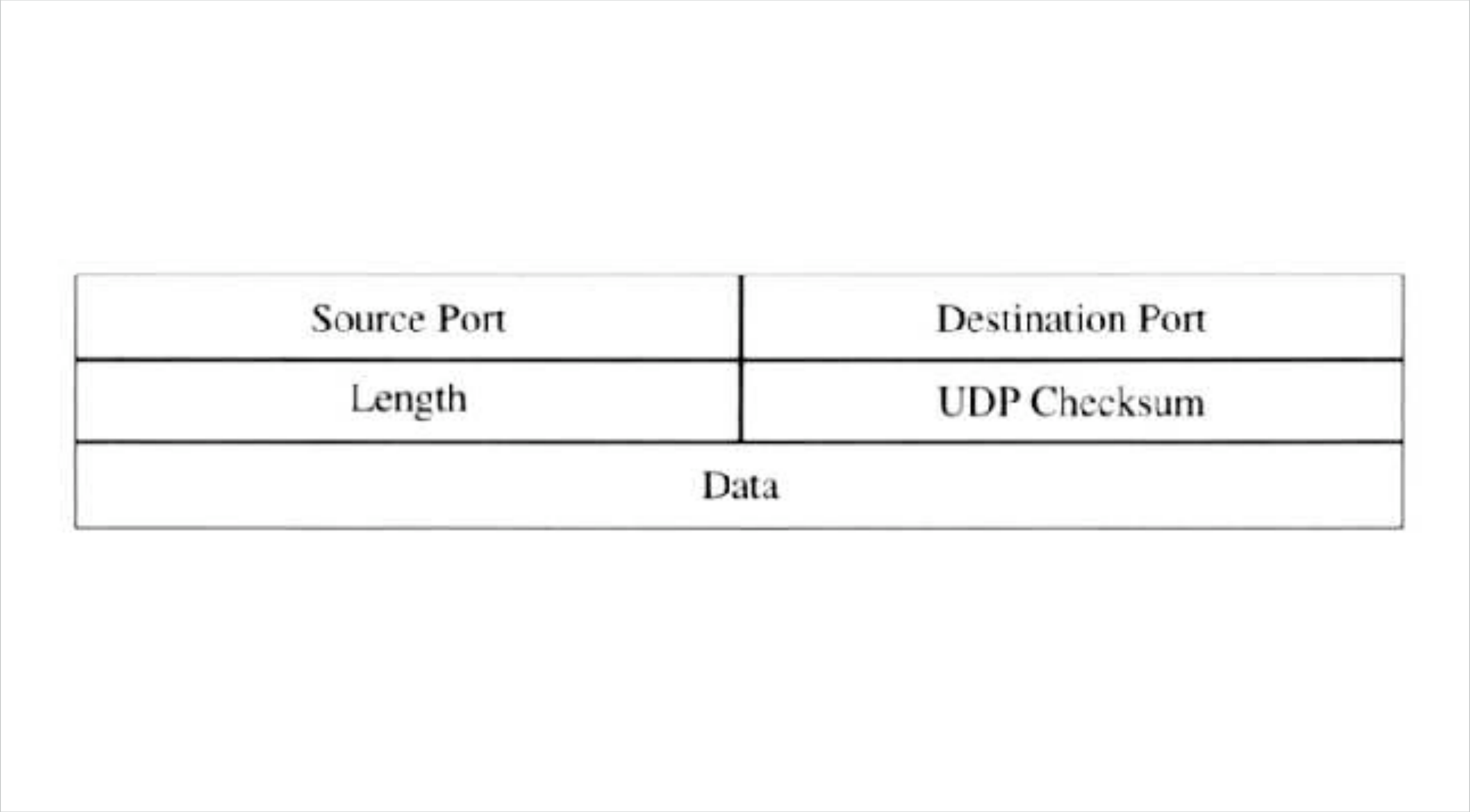
ICMP Types

EN.650.654 Computer Intrusion Detection



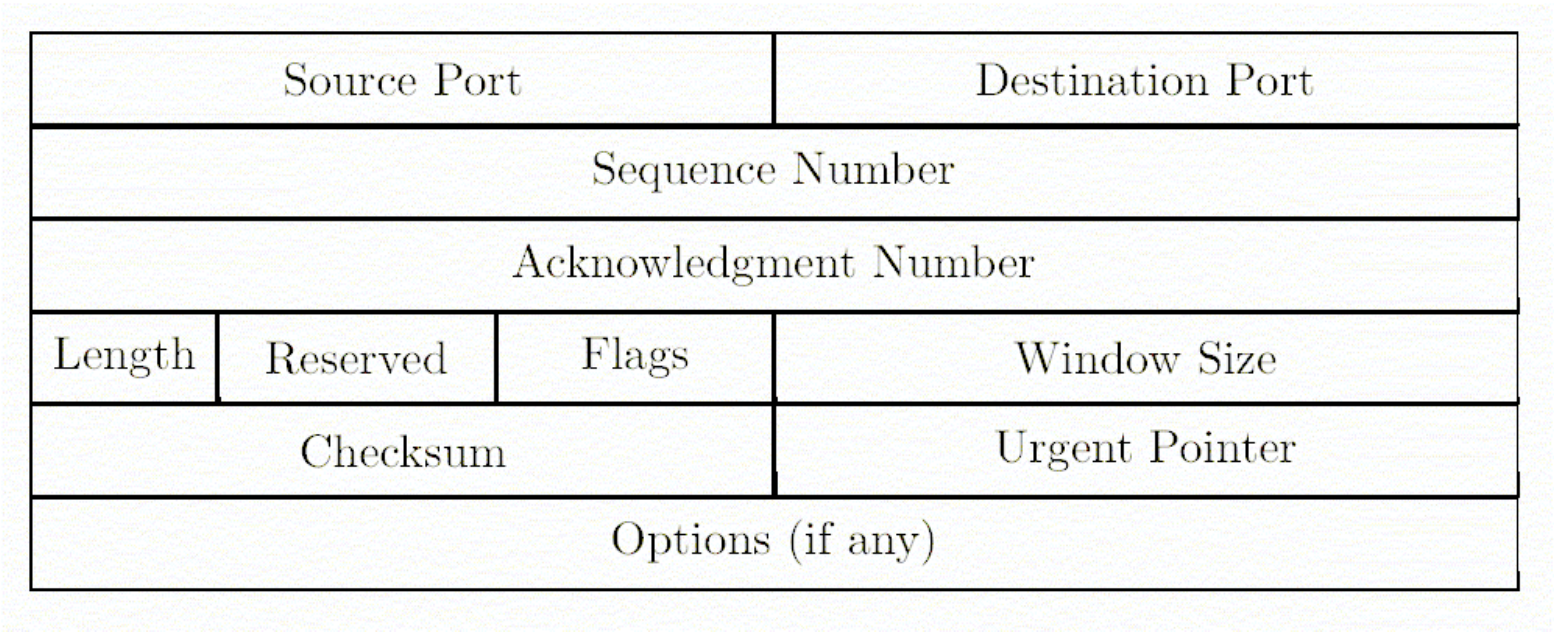
type	Description	Purpose
0	Echo Reply	Query
3	Destination Unreachable	Error
4	Source Quench	Error
5	redirect	Error
8	Echo Request	Query
9	Router Advertisement	Query
10	Router Solicitation	Query
11	Time Exceeded	Error
12	Parameter Problem	Error
13	Timestamp Request	Query
14	Timestamp Reply	Query
15	Information Request	Query
16	Information Reply	Query
17	Address Mask Request	Query
18	Address Mask Reply	Query

UDP Header



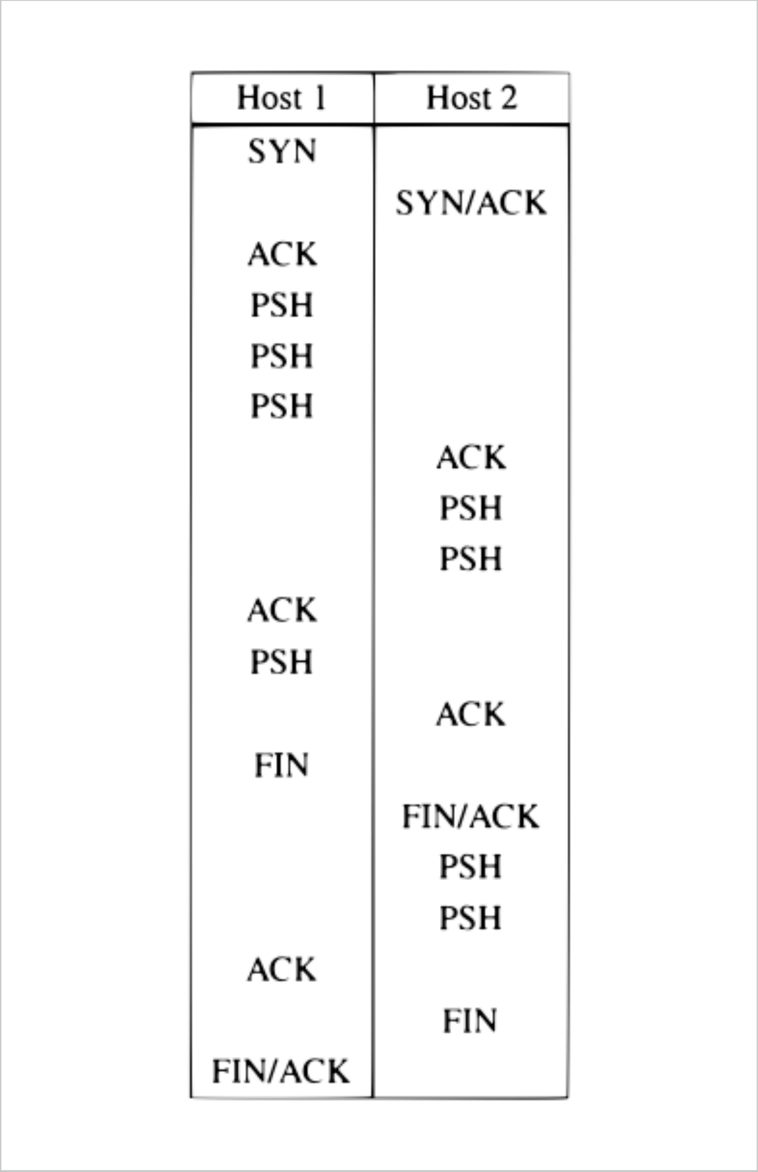
Source Port	Destination Port
Length	UDP Checksum
Data	

TCP Header



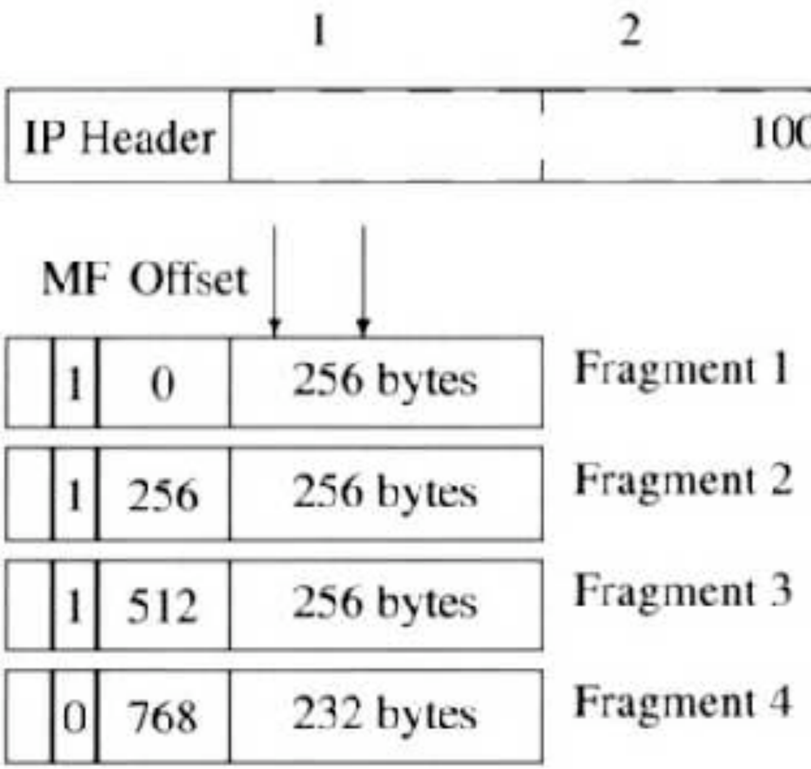
<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgment Number</td></tr>
<tr><td>Length</td><td>Reserved</td><td>Flags</td><td>Window Size</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="4">Options (if any)</td></tr>
</table>

A Possible TCP Session



Host 1	Host 2
SYN	
	SYN/ACK
ACK	
PSH	
PSH	
PSH	
	ACK
	PSH
	PSH
ACK	
PSH	
	ACK
FIN	
	FIN/ACK
	PSH
	PSH
ACK	
	FIN
FIN/ACK	

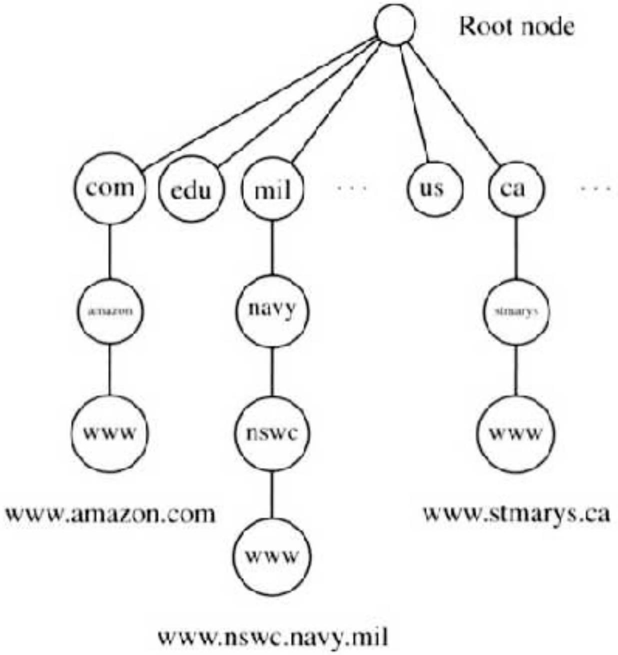
IP Fragmentation



1 2 3 4

IP Header | 1000 bytes

MF	Offset		
1	0	256 bytes	Fragment 1
1	256	256 bytes	Fragment 2
1	512	256 bytes	Fragment 3
0	768	232 bytes	Fragment 4



Routing and DNS

Useful Utilities

- tcpdump
- ping and traceroute
- nslookup and whois
- ifconfig, netstat and pppstats
- lsof

tcpdump

- A packet sniffer with filtering capability.
- You must be root to run it. You must get permission of the owner of the network.
- It allows you to look at the data sent on the network.
- Examples
  - Get all incoming email packets:
    - tcpdump -n “tcp and dst port 25”
  - Get incoming packets to network 10.10.xxx.xxx:
    - tcpdump -n “ip and dst net 10.10.”