गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायिक विज्ञान विश्वविद्यालय
National Forensic Sciences University

Network Security & Forensics



Dr. Lokesh Chouhan

Associate Professor

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)
National Forensic Sciences University
(An Institution of National Importance under Ministry of Home Affairs, Government of India)

E-Mail: Lokeshchouhan@gmail.com, Lokesh.chouhan_goa@nfsu.ac.in

Mob: +91-898924399, 9827235155

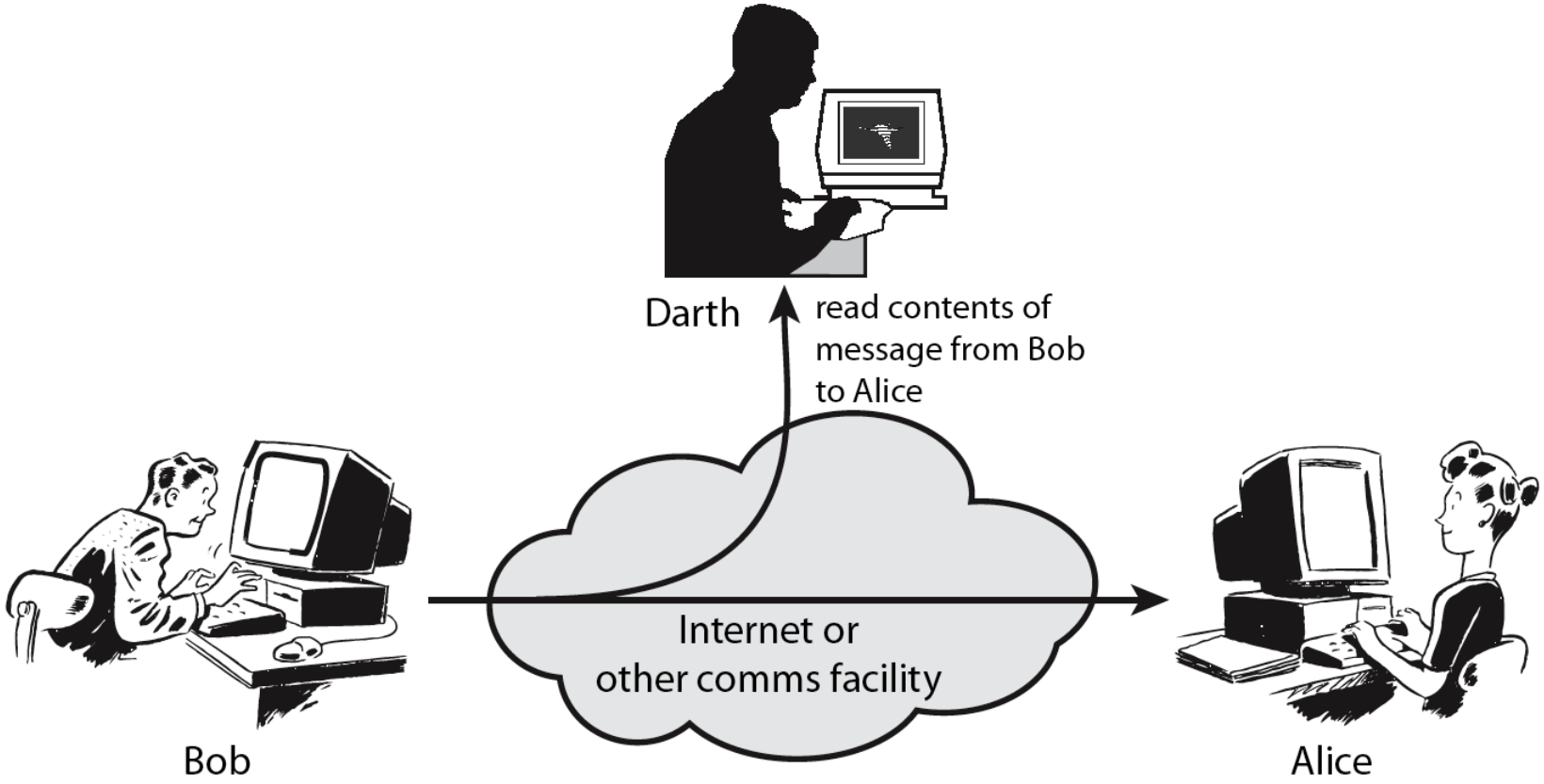
Services, Mechanisms, Attacks

- need systematic way to define requirements
- consider three aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- consider in reverse order

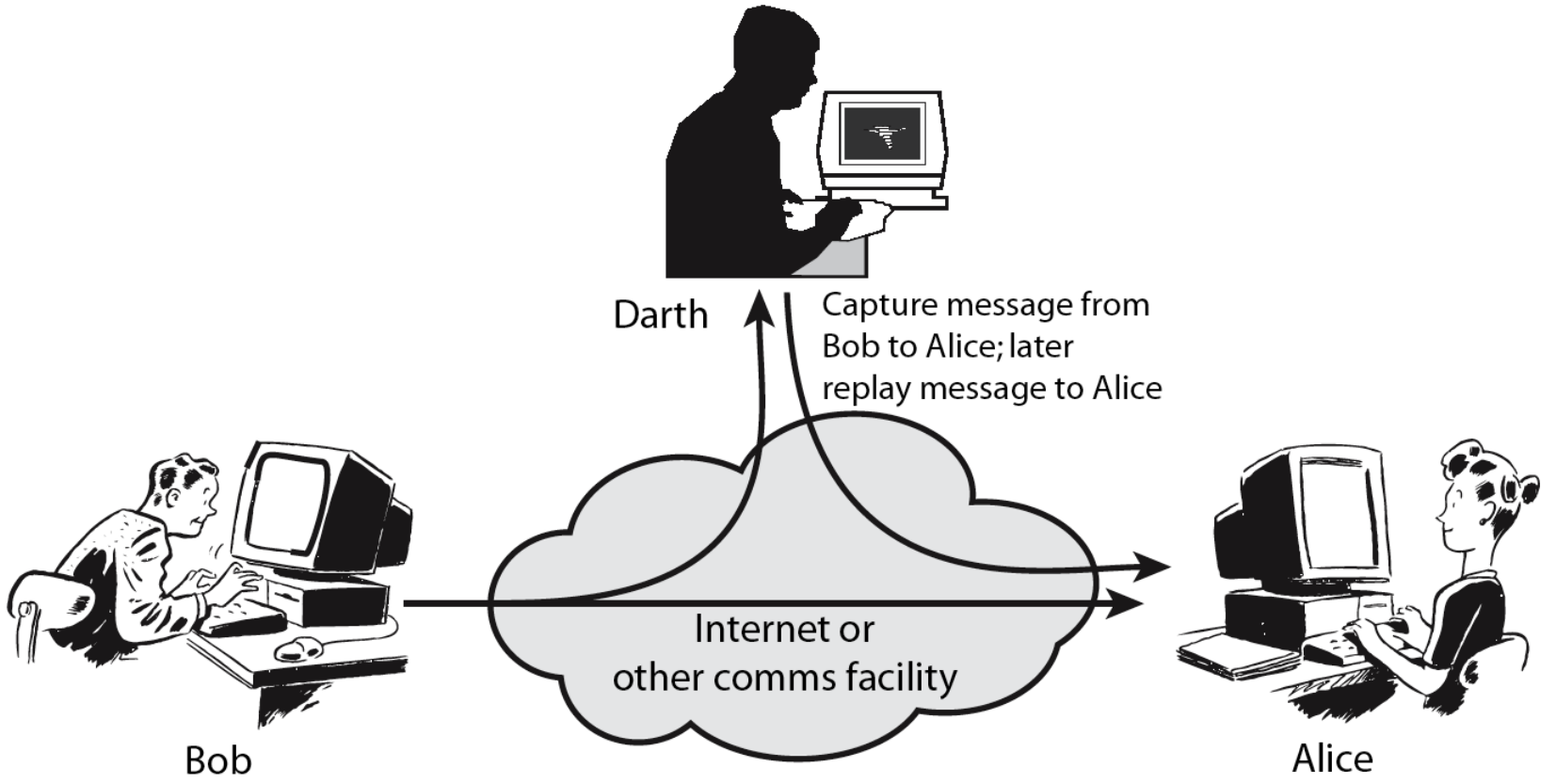
Attacks

- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

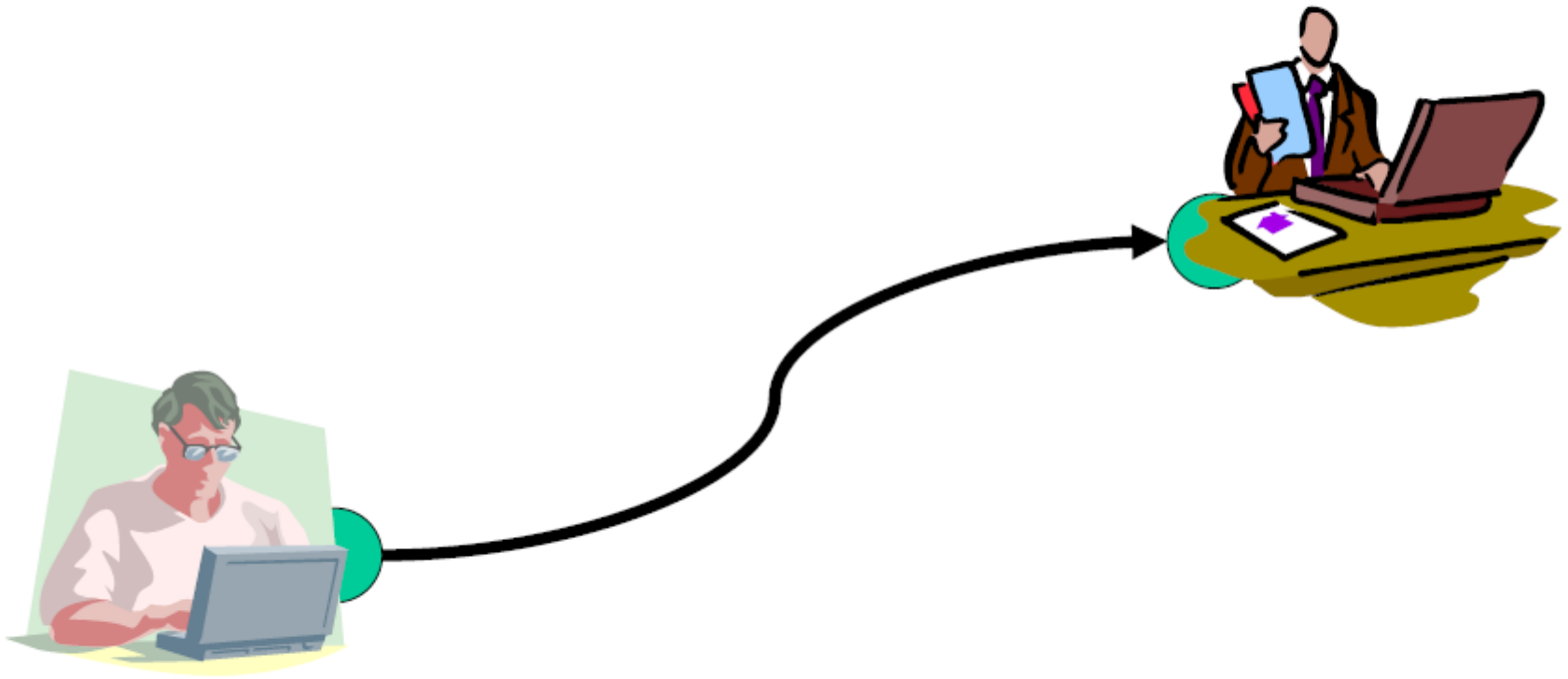
Passive Attacks



Active Attacks



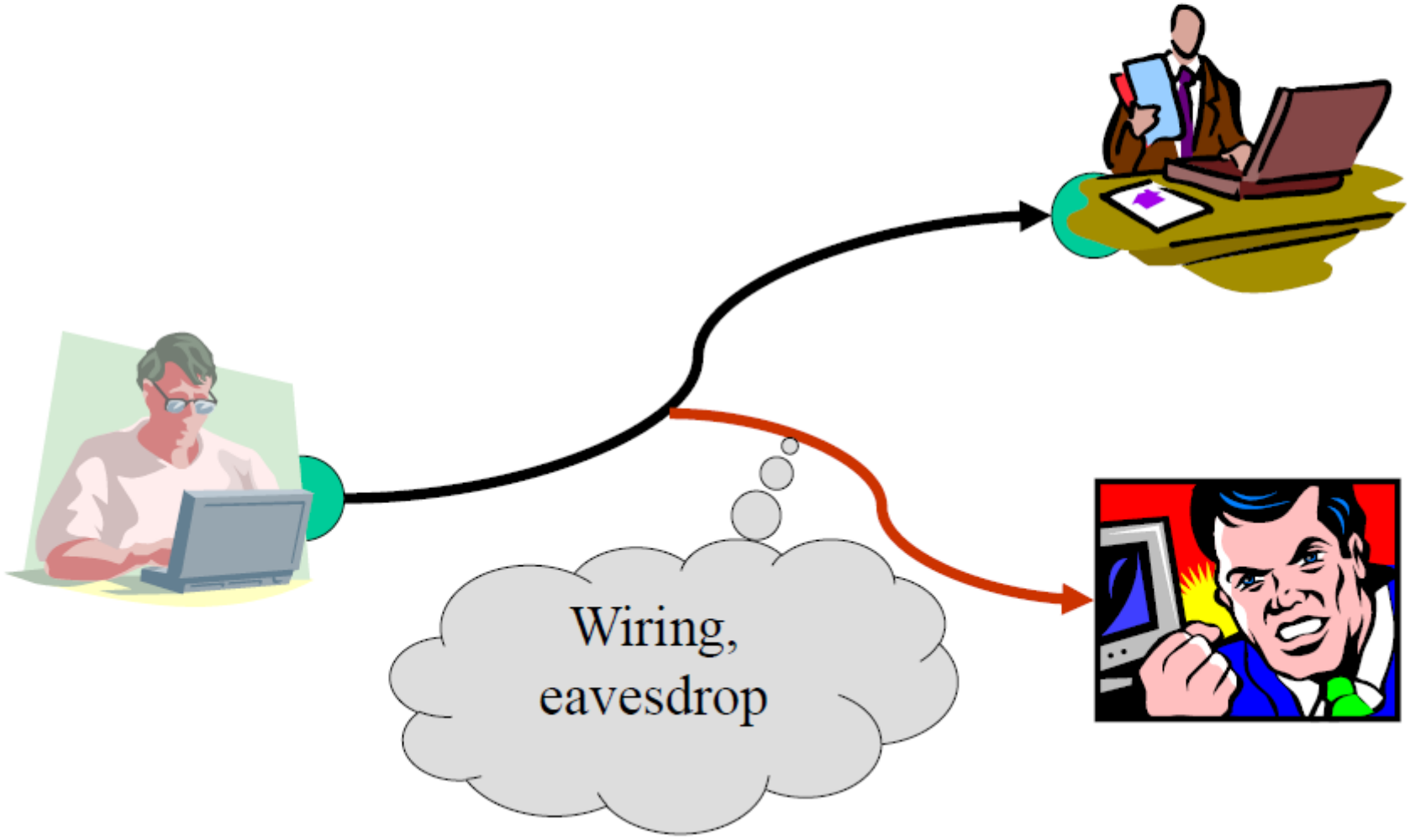
Information Transferring



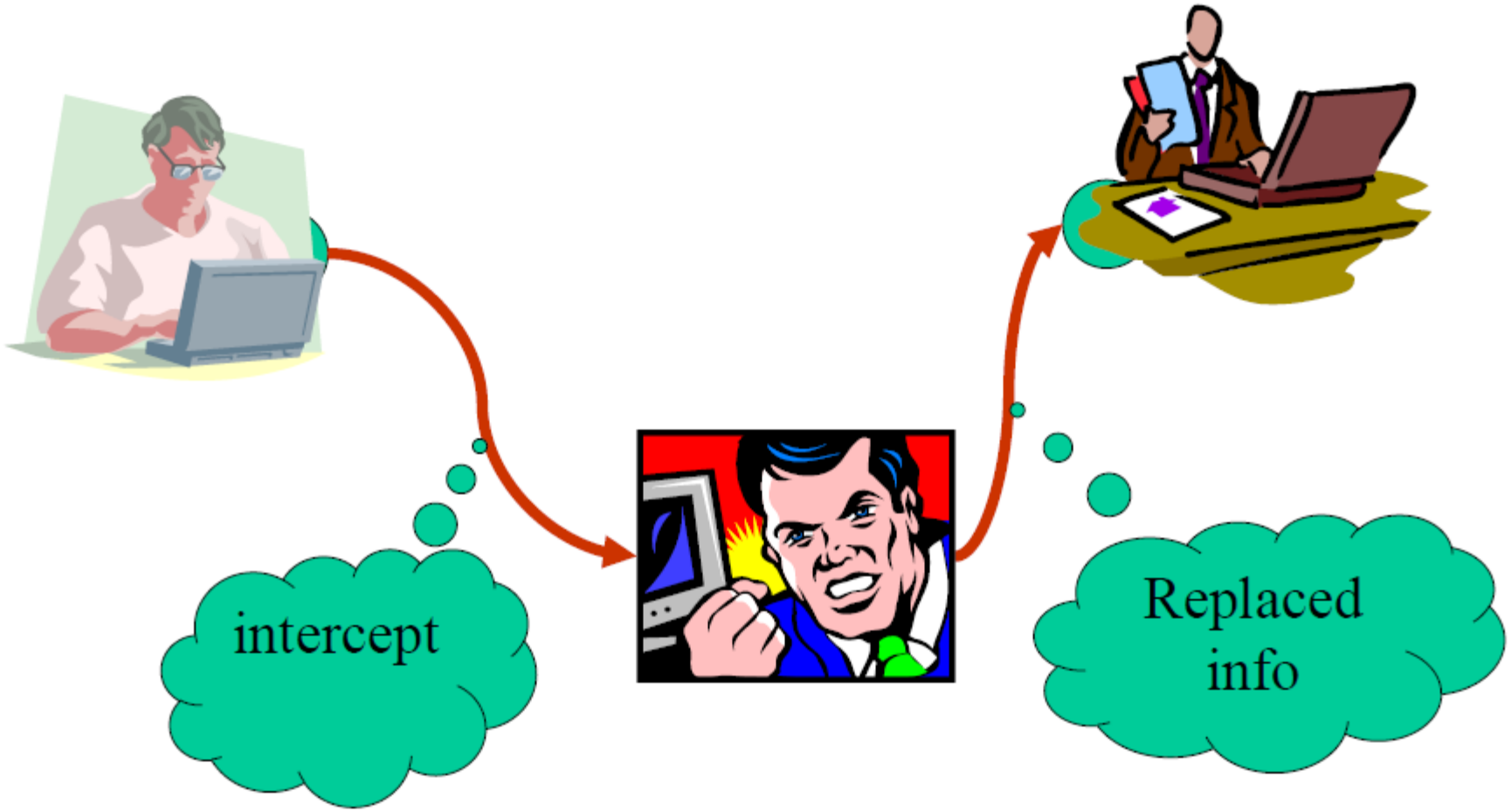
Attack: Interruption

Cut wire lines,
Jam wireless
signals,
Drop packets,

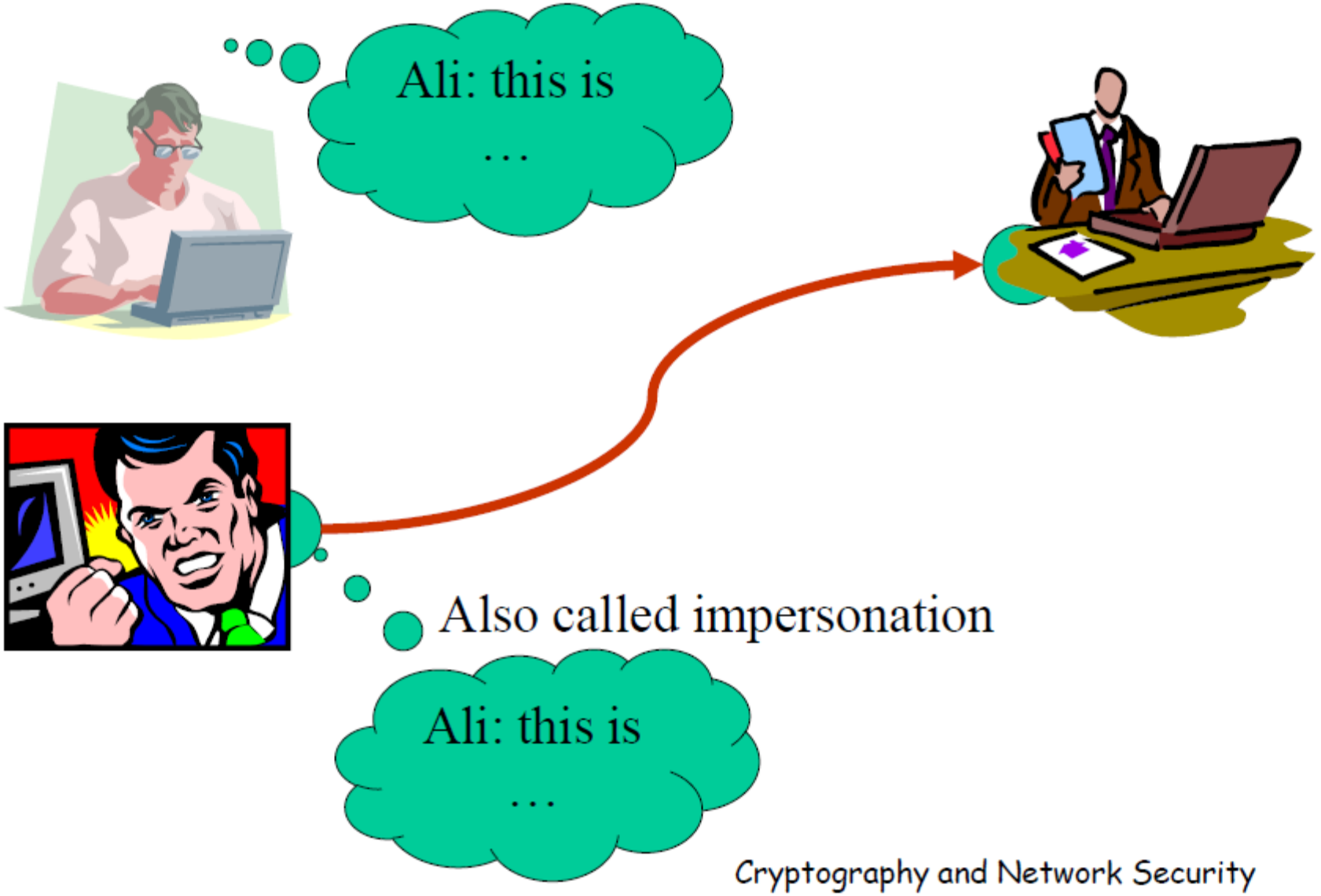
Attack: Interception



Attack: Modification



Attack: Fabrication



Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents
  - eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**
- hence our focus on this area

Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat* & *attack* mean same

OSI Security Architecture

- ITU-T X.800 Security Architecture for OSI
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Security Services

- X.800 defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- RFC 2828 defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources
- X.800 defines it in 5 major categories

Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Classify Security Attacks as

- **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

Attack Surface

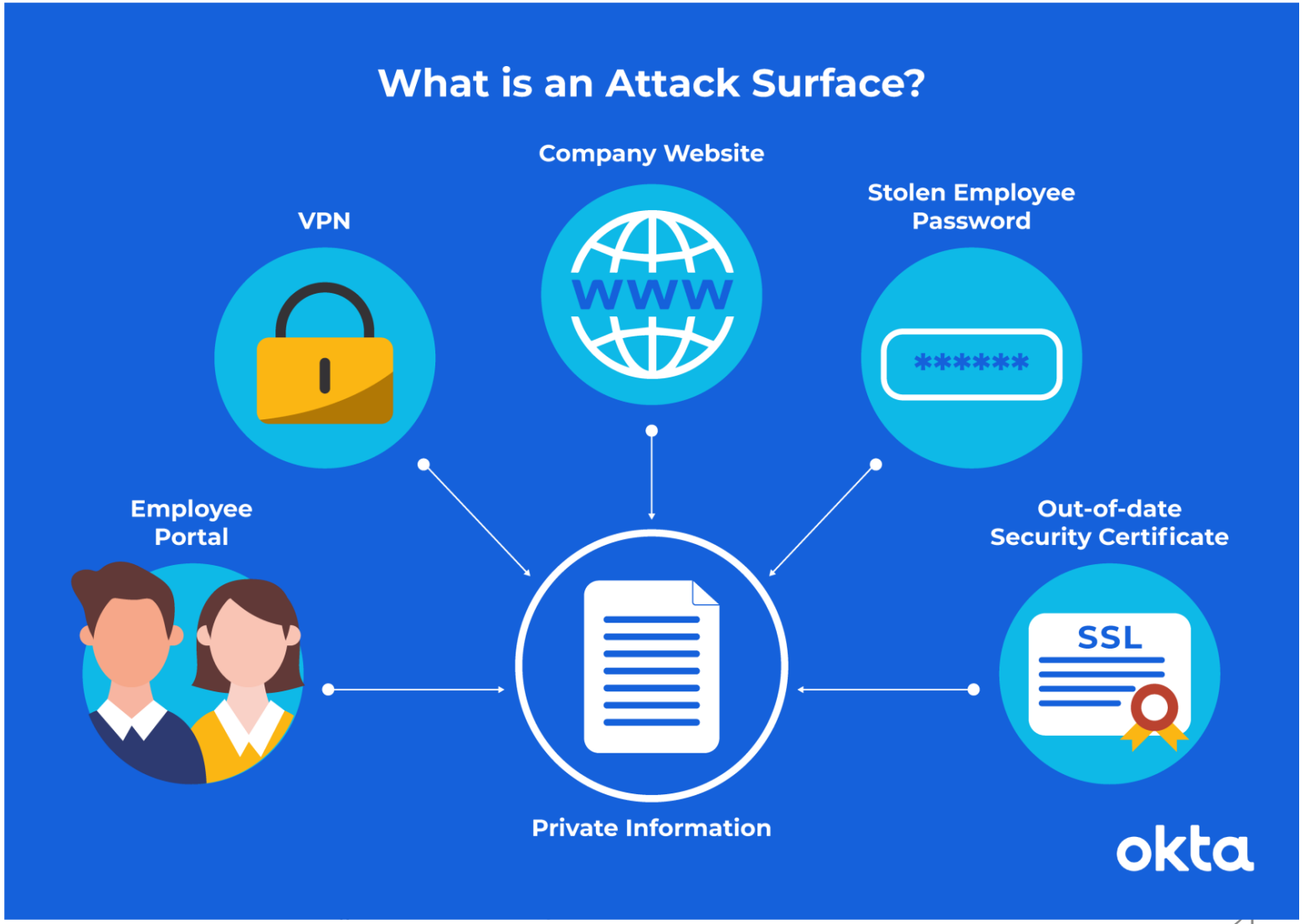
- An attack surface is the entire area of an organization or system that is susceptible to hacking.
- It's made up of all the points of access that an unauthorized person could use to enter the system.
- Once inside your network, that user could cause damage by manipulating or downloading data.

Attack Surface

- The smaller your attack surface, the easier it is to protect your organization.
- Conducting a surface analysis is a good first step to reducing or protecting your attack surface.
- Follow it with a strategic protection plan to reduce your risk of an expensive software attack or cyber extortion effort.

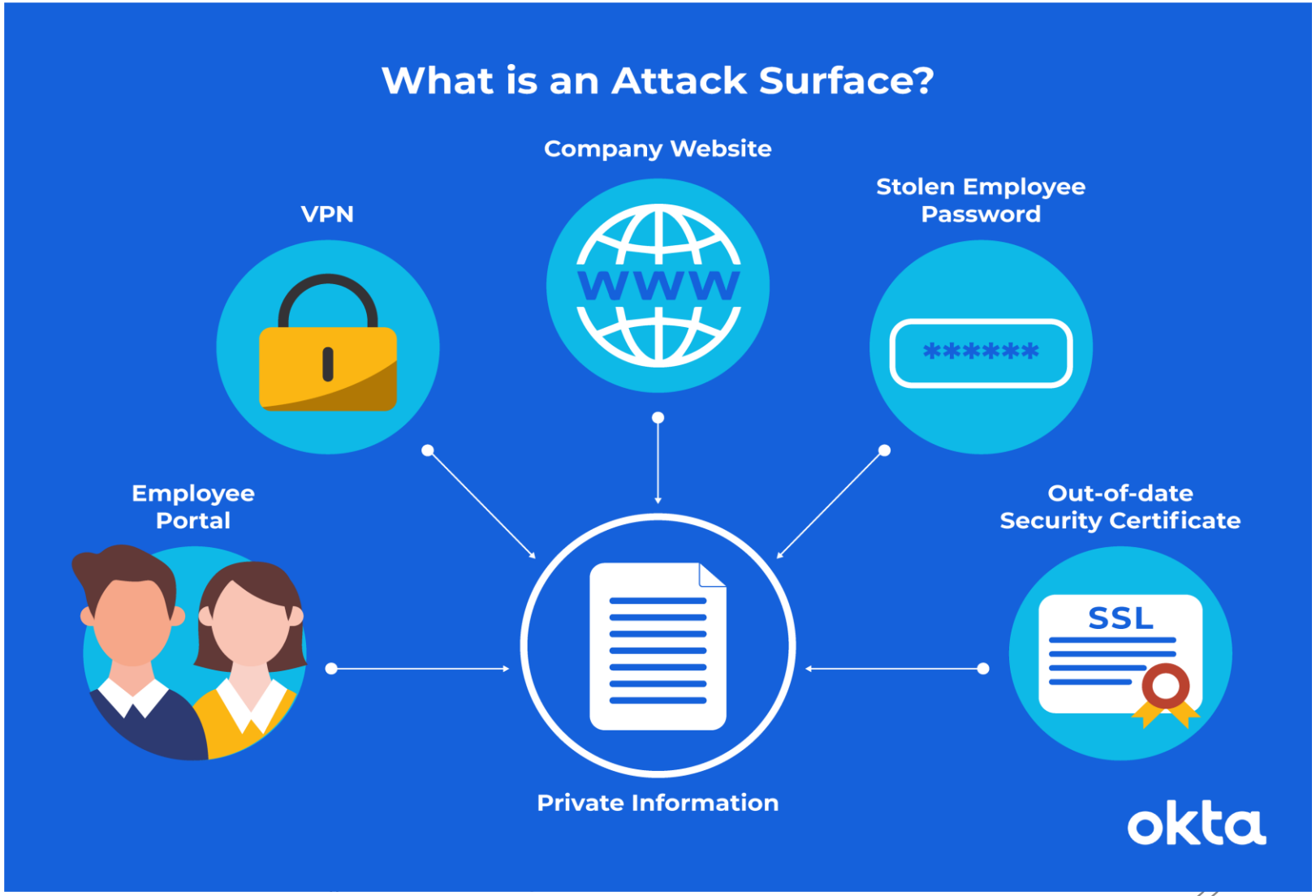
Attack Surface and Attack Vector

- An attack surface is essentially the entire external-facing area of your system.
- The model contains all of the attack vectors (or vulnerabilities) a hacker could use to gain access to your system.



Attack Surface and Attack Vector

- Vulnerabilities are everywhere, and often, they're exploited.
- For example, in 2014, reporters said nearly half of all Fortune 500 companies had employee email addresses and passwords exposed in hacker forums within the year.



Attack Vector

- In cybersecurity, an attack vector is a method of achieving unauthorized network access to launch a cyber attack.
- Attack vectors allow cybercriminals to exploit system vulnerabilities to gain access to sensitive data, personally identifiable information (PII), and other valuable information accessible after a data breach.
- Attack vectors are the landmarks on an attack surface. Each one represents vulnerabilities, such as access points, protocols, and services.

Attack Vector

Attack Vector	Issue	Solution
APIs	APIs can supercharge business growth, but they also put your company at risk if they are not properly secured.	Secure all APIs by using tokens, encryption, signatures, and other means to keep your organization protected.
Distributed denial of service (DDoS)	A DDoS attack floods a targeted server or network with traffic in an attempt to disrupt and overwhelm a service rendering inoperable.	Protect your business by reducing the surface area that can be attacked. This is done by restricting direct access to infrastructure like database servers. Control who has access to what using an identity and access management system.
Encryption	If your protocols are weak or missing, information passes back and forth unprotected, which makes theft easy.	Confirm all protocols are robust and secure.
Insiders	A disgruntled employee is a security nightmare. That worker could share some or part of your network with outsiders. That person could also hand over passwords or other forms of access for independent snooping.	Work with HR to put protocols in place, so you're ready if this situation occurs.
Malware	This is a nasty type of software designed to cause errors, slow your computer down, or spread viruses. Spyware is a type of malware, but with the added insidious purpose of collecting personal information.	Keeping abreast of modern security practices is the best way to defend against malware attacks. Consider a centralized security provider to eliminate holes in your security strategy.
Passwords	Weak passwords (such as 123456!) or stolen sets allow a creative hacker to gain easy access. Once they're in, they may go undetected for a long time and do a lot of damage.	Set up requirements to ensure all passwords are strong, or use multi-factor, or even passwordless authentication.
Phishing	A seemingly simple request for email confirmation or password data could give a hacker the ability to move right into your network. Many phishing attempts are so well done that people give up valuable info immediately.	Your IT team can identify the latest phishing attempts and keep employees apprised of what to watch out for.
Ransomware	Hackers move into your network, lock it down, and ask for money to release it. In 2019, more than 205,000 organizations faced a demand just like this.	Identify where your most important data is in your system, and create an effective backup strategy. Added security measures will better protect your system from being accessed.

Attack Vector Vs Attack Surface Vs Threat Vector?

- An **attack vector** is a method of gaining unauthorized access to a network or computer system.
- An **attack surface** is the total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.
- **Threat vector** can be used interchangeably with attack vector and generally describes the potential ways a hacker can gain access to data or other confidential information.

Types of Attacks

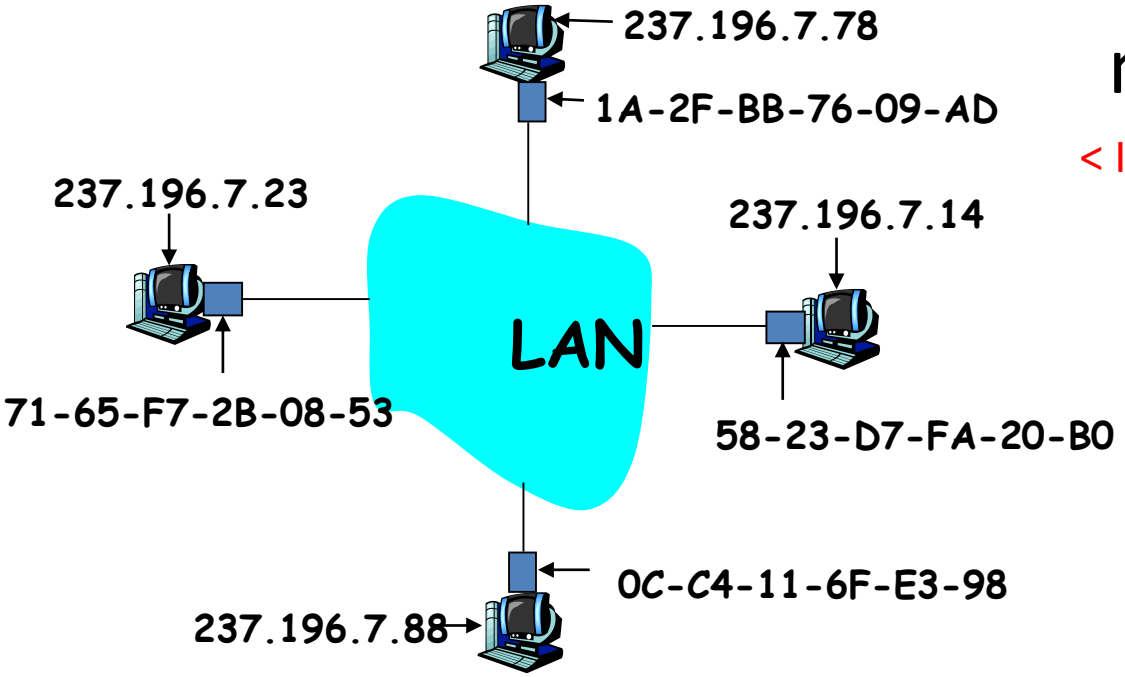
- ARP poising,
- Phishing attack,
- MAC flooding,
- DoS and
- DDoS.

MAC Addresses and ARP

- 32-bit IP address:
  - *network-layer* address
  - used to get datagram to destination IP subnet
- MAC (or LAN or physical or Ethernet) address:
  - Data link layer address
  - used to get datagram from one interface to another physically-connected interface (same network)
  - 48 bit MAC address (for most LANs) burned in the adapter ROM
  - Some Network interface cards (NICs) can change their MAC

ARP: Address Resolution Protocol

Question: how to determine MAC address of host B when knowing B's IP address?



- Each IP node (Host, Router) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes

  < IP address; MAC address; TTL>

  - TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

ARP

- ARP works by broadcasting requests and caching responses for future use
- The protocol begins with a computer broadcasting a message of the form

  who has <IP address1> tell <IP address2>

- When the machine with <IP address1> or an ARP server receives this message, its broadcasts the response

  <IP address1> is <MAC address>

- The requestor's IP address <IP address2> is contained in the link header
- The Linux and Windows command arp - a displays the ARP table

```
  Internet Address      Physical Address      Type
  128.148.31.1          00-00-0c-07-ac-00     dynamic
  128.148.31.15         00-0c-76-b2-d7-1d     dynamic
  128.148.31.71         00-0c-76-b2-d0-d2     dynamic
  128.148.31.75         00-0c-76-b2-d7-1d     dynamic
  128.148.31.102        00-22-0c-a3-e4-00     dynamic
  128.148.31.137        00-1d-92-b6-f1-a9     dynamic
```

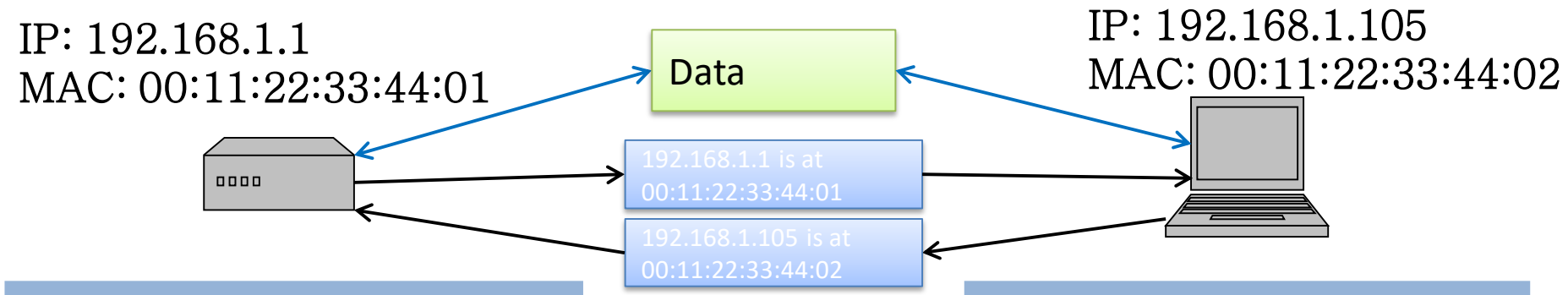
ARP Spoofing

- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated
- Machines trust each other
- A rogue machine can spoof other machines

ARP Poisoning (ARP Spoofing)

- According to the standard, almost all ARP implementations are stateless
- An arp cache updates every time that it receives an arp reply… even if it did not send any arp request!
- It is possible to “poison” an arp cache by sending gratuitous arp replies

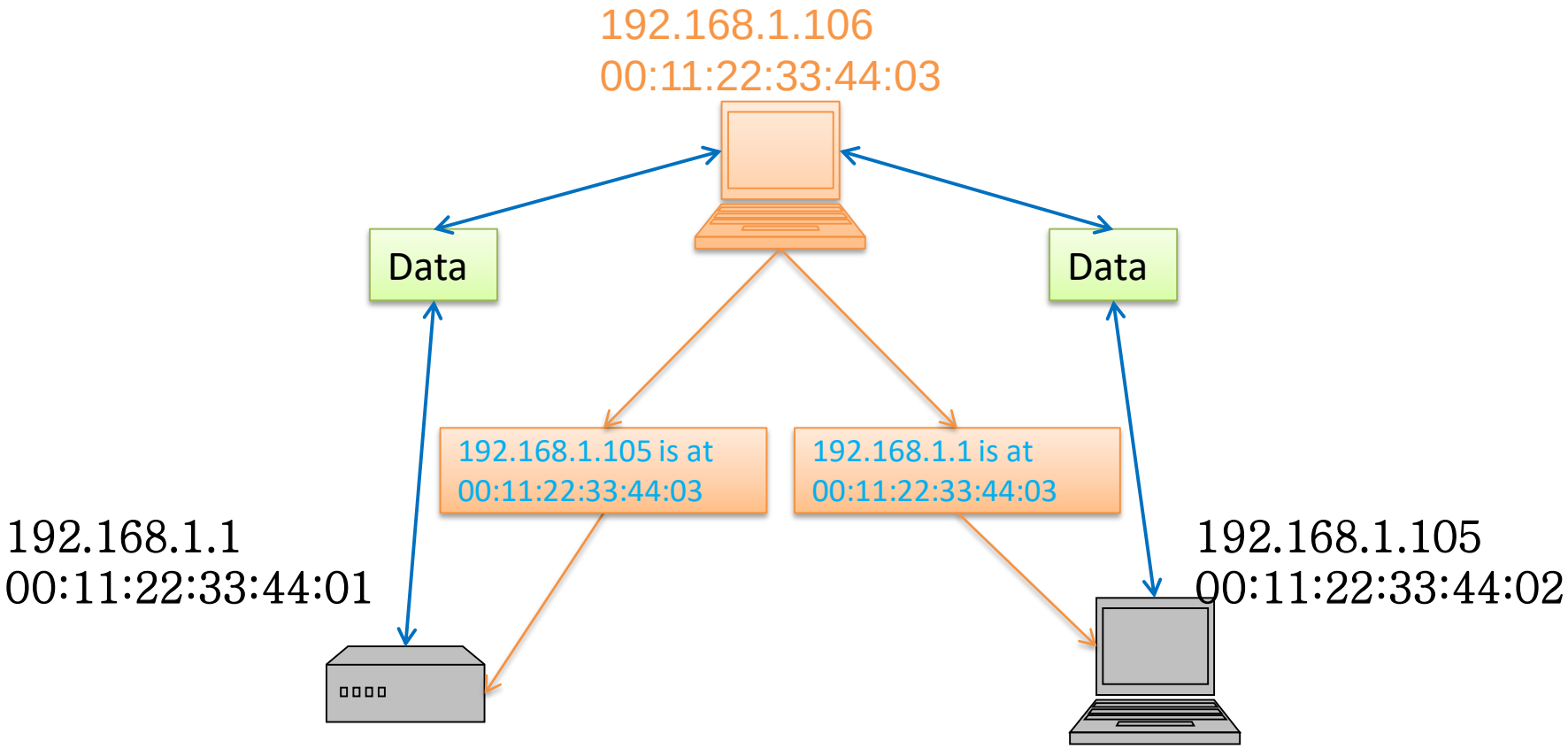
ARP Caches



ARP Cache	
192.168.1.**105**	00:11:22:33:44:**02**

ARP Cache	
192.168.1.**1**	00:11:22:33:44:**01**

Poisoned ARP Caches (man-in-the-middle attack)



Poisoned ARP Cache	
192.168.1.**105**	00:11:22:33:44:**03**

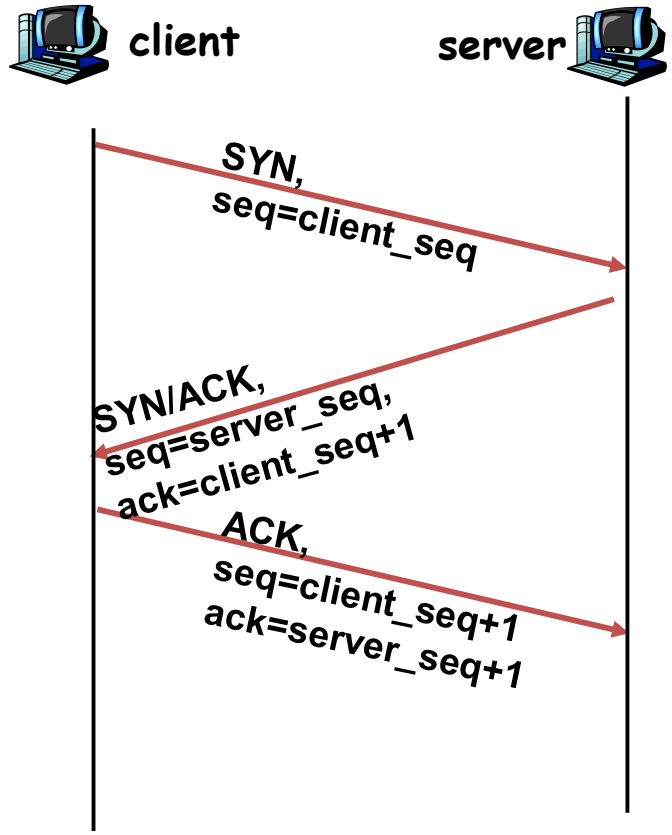
Poisoned ARP Cache	
192.168.1.**1**	00:11:22:33:44:**03**

ARP Spoofing

- Using static entries solves the problem but it is almost impossible to manage!
- Check multiple occurrence of the same MAC
  - i.e., One MAC mapping to multiple IP addresses (see previous slide's example)
- Software detection solutions
  - Anti-arpspoof, Xarp, Arpwatch

TCP Session Hijacking

- TCP connection has both sequence number and acknowledge number in each packet.
- The two ends negotiate what seq. and ack. Numbers to be used in TCP set up stage.
- seq and ack number size: 2^{32}
  - Makes seq/ack guessing very hard to achieve
  - Very hard to hijack an already setup TCP connection!



TCP Session Hijacking

- Possible when an attacker is on the same network segment as the target machine.
  - Attacker can sniff all back/forth tcp packets and know the seq/ack numbers.
  - Attacker can inject a packet with the correct seq/ack numbers with the spoofed IP address.
    - IP spoofing needs low-level packet programming, OS-based socket programming cannot be used!

TCP Session Hijacking

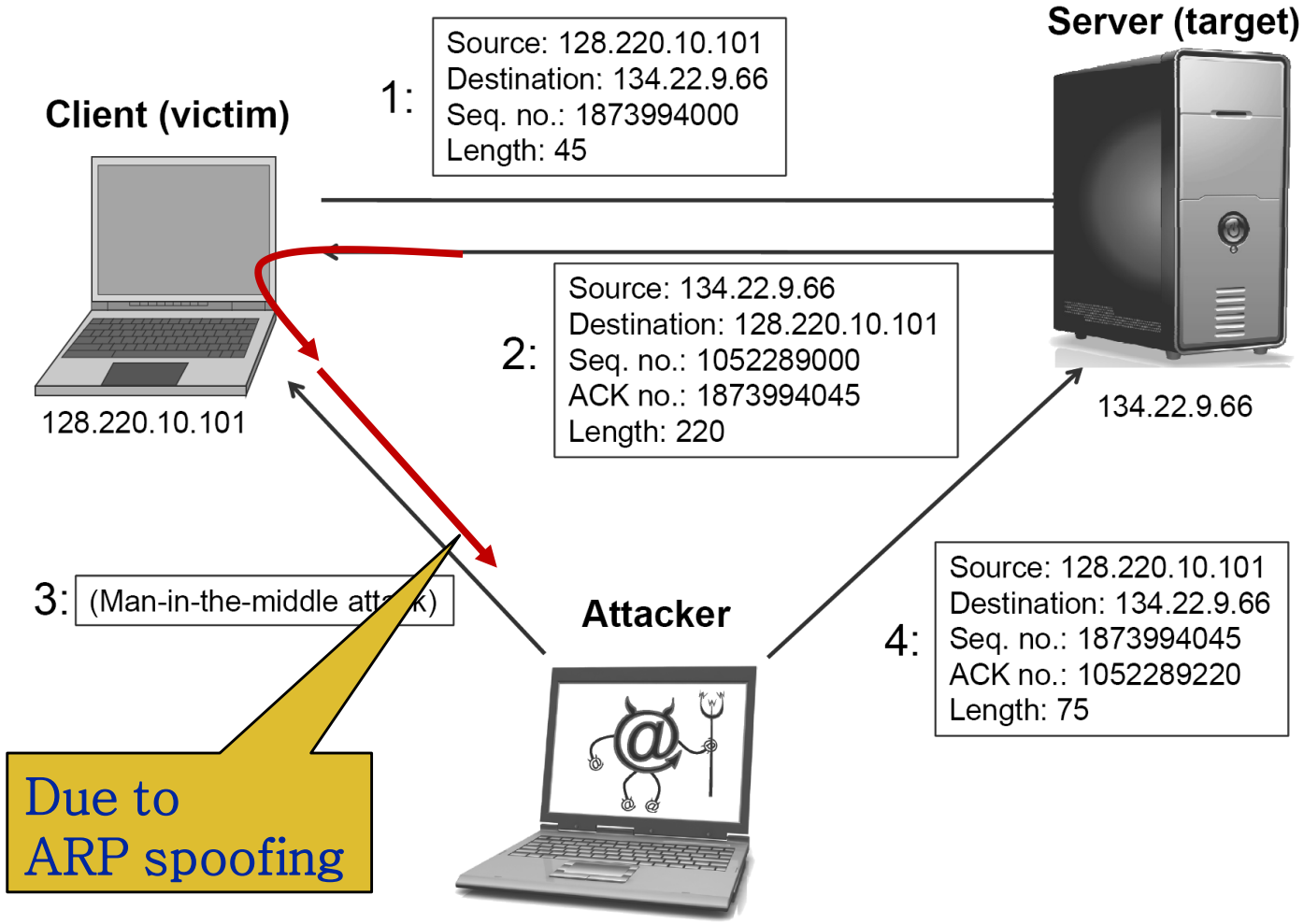
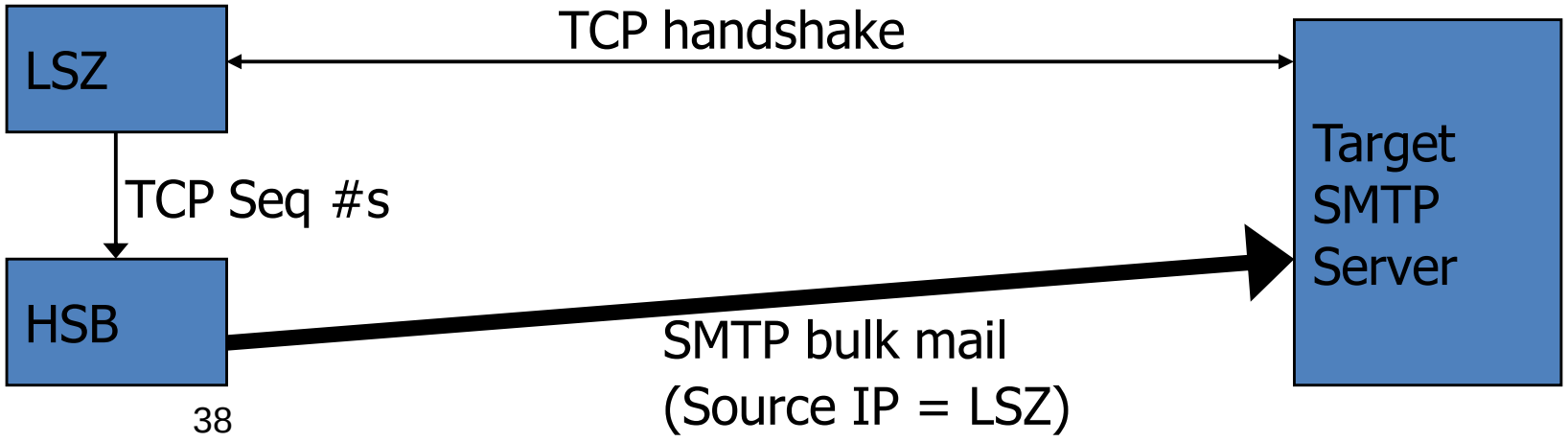


Figure 5.18: A TCP session hijacking attack.

TCP Session Hijacking

- Another way is “coordinated IP spoofing” by using two computers, such as the “Thin pipe / Thick pipe method” introduced in spam lecture:
  - High Speed Broadband connection (HSB)
  - Controls a Low Speed Zombie (LSZ)
  - Assumes no egress filtering at HSB’s ISP
  - Hides IP address of HSB. LSZ is blacklisted.



Denial-of-Service (DoS) Attack

- An attempt to make a computer or network resource unavailable to its intended users
  - DoS to the network bandwidth of targeted server
  - DoS to the computing resource of targeted server
    - Memory, CPU
  - DoS to the vulnerability in targeted server
    - Causing server OS crash (buffer overflow bug, logic bug, etc)
    - Causing server program crash (e.g., Apache, Sendmail, SQL)
- Distributed Denial-of-Service (DDoS) attack
  - Sending attack packets from multiple computers
  - Botnet is the root cause for DDoS attacks

Denial-of-Service (DoS) Attack

- Format:
  - Real IP-based attack using botnets
    - Attacker does not worry about exposing bots' IP addresses.
    - TCP flooding, UDP flooding, icmp flooding
  - Spoofed IP-based attack
    - SYN flooding with spoofed IPs.
  - Source address hiding attack
    - Smurf attack

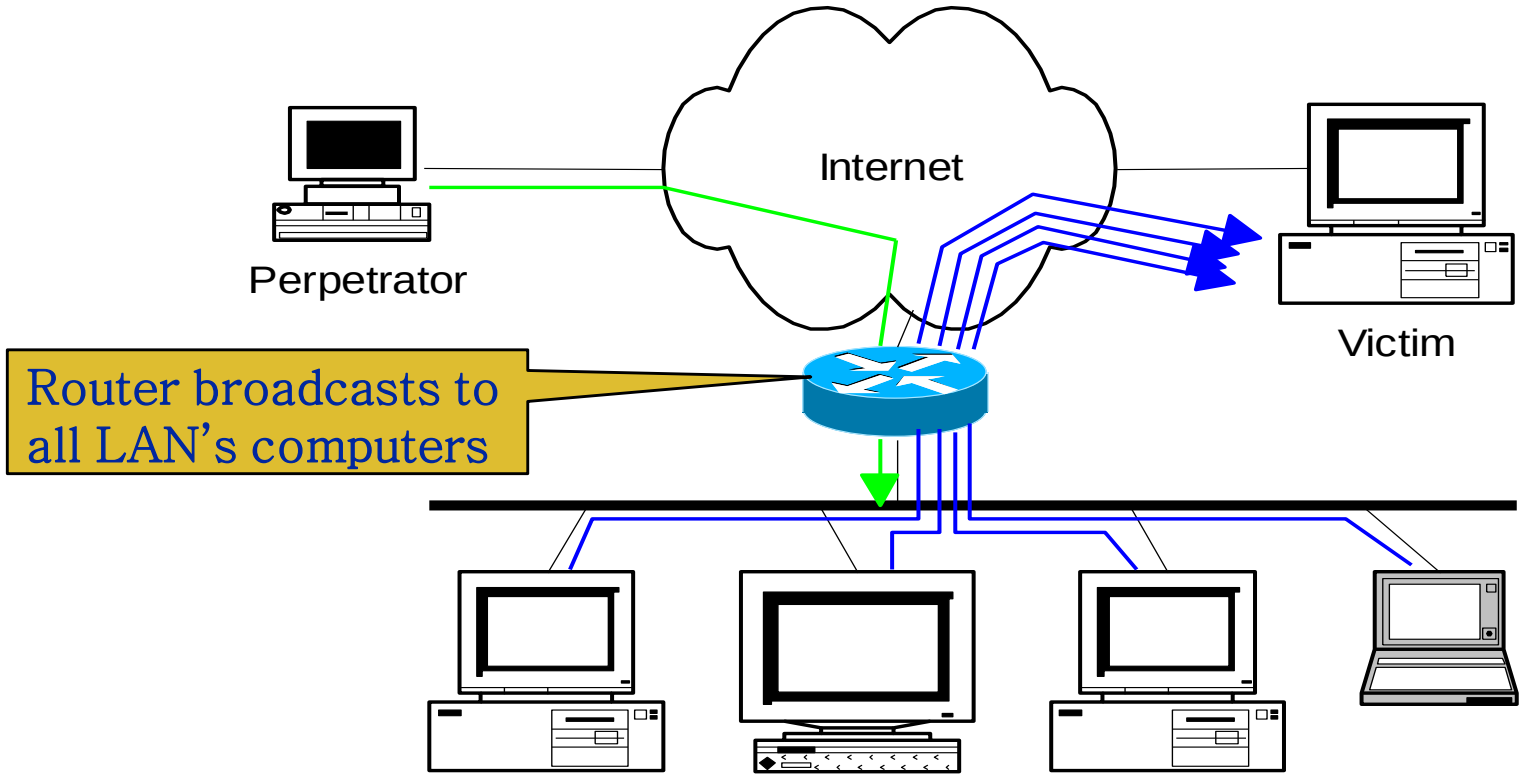
Smurf Attack

- Some contents from this link:
- *www.pentics.net/denial-of-service/.../ms**ppt**/19971027_**smurf.ppt***
- Uses ICMP echo/reply packets with broadcast networks to multiply traffic
- Requires the ability to send spoofed packets
- Abuses “bounce-sites” to attack victims
  - Traffic multiplied by a factor of 50 to 200

Description of Smurfing Attack

ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

ICMP echo reply

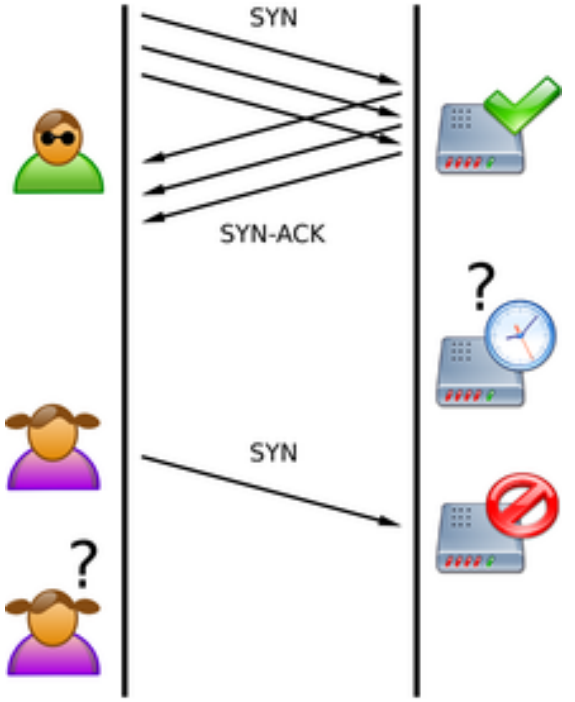


How to prevent being a “bounce site”

- Turn off directed broadcasts to subnets with 5 hosts or more
  - Cisco router: Interface command “no ip directed-broadcast”
- Use access control lists (if necessary) to prevent ICMP echo requests from entering your network
  - Probably not an elegant solution; makes troubleshooting difficult
  - But many networks are doing this now
- Encourage vendors to turn off replies for ICMP echos to broadcast addresses
  - Host Requirements RFC-1122 Section 3.2.2.6 states “An ICMP Echo Request destined to an IP broadcast or IP multicast address MAY be silently discarded.”
  - Patches are available for free UNIX-ish operating systems.

SYN Flooding Attack

- An attacker sends a large number of SYN requests to a target's system
  - Target uses too much memory and CPU resources to process these fake connection requests
  - Target's bandwidth is overwhelmed
- Usually SYN flood packets use spoofed source IPs
  - No TCP connection is set up (not like the TCP hijacking!)
  - Hide attacking source
  - Make the target very hard to decide which TCP SYN is attack and which TCP SYN is from legitimate users!

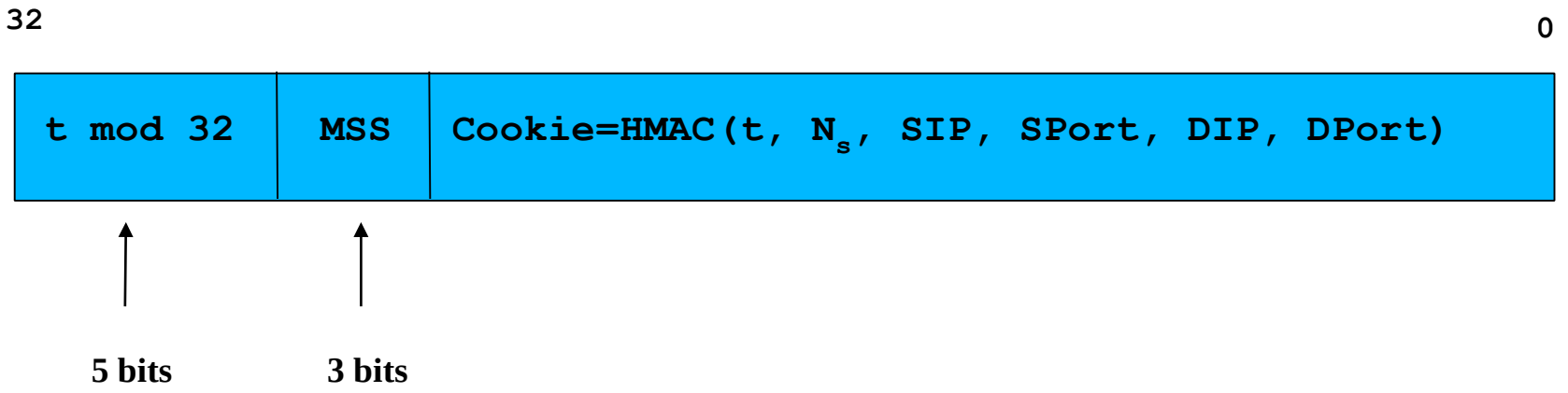


SYN Flood Defense: SYN Cookie

- Some contents from:
- http://www.cc.gatech.edu/classes/AY2007/cs7260_spring/lectures/L18.ppt
- General idea
  - Client sends SYN to server (client_seq number only)
  - Server responds to Client with SYN-ACK cookie
    - Server_sqn = f(src addr, src port, dest addr, dest port, rand)
    - Ack number is normal value: client_seq +1
    - Server does not save state
  - Honest client responds with ACK(client_ack = server_sqn+1)
  - Server checks response
  - If matches SYN-ACK, establishes connection

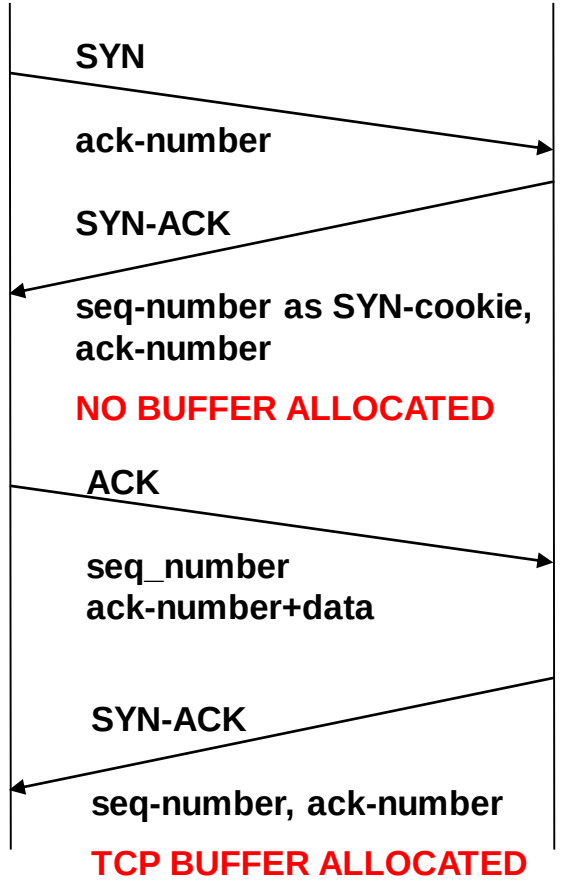
TCP SYN cookie

- TCP SYN/ACK server_seq encodes a cookie
  - 32-bit sequence number
    - **time mod 32:** counter to ensure sequence numbers increase every 64 seconds
    - **MSS:** encoding of server MSS (can only have 8 settings)
    - **Cookie:** easy to create and validate, hard to forge
      - Includes timestamp, nonce, 4-tuple



SYN Cookies

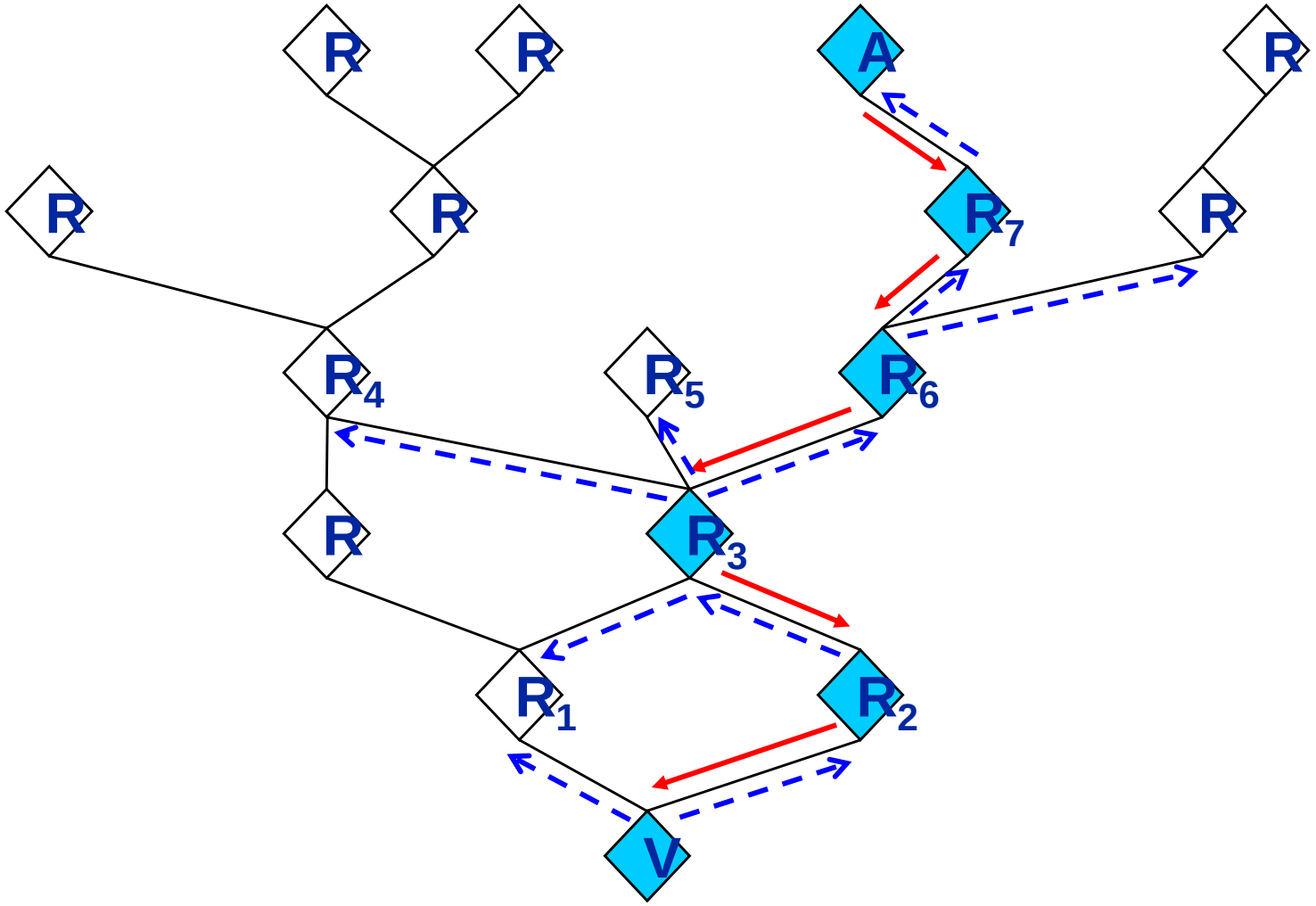
- **client**
  - sends SYN packet and ACK number to server
  - waits for SYN-ACK from server w/ matching ACK number
- **server**
  - responds w/ SYN-ACK packet w/ initial SYN-cookie sequence number
  - Sequence number is cryptographically generated value based on client address, port, and time.
- **client**
  - sends ACK to server w/ matching sequence number
- **server**
  - If ACK is to an unopened socket, server validates returned sequence number as SYN-cookie
  - If value is reasonable, a buffer is allocated and socket is opened



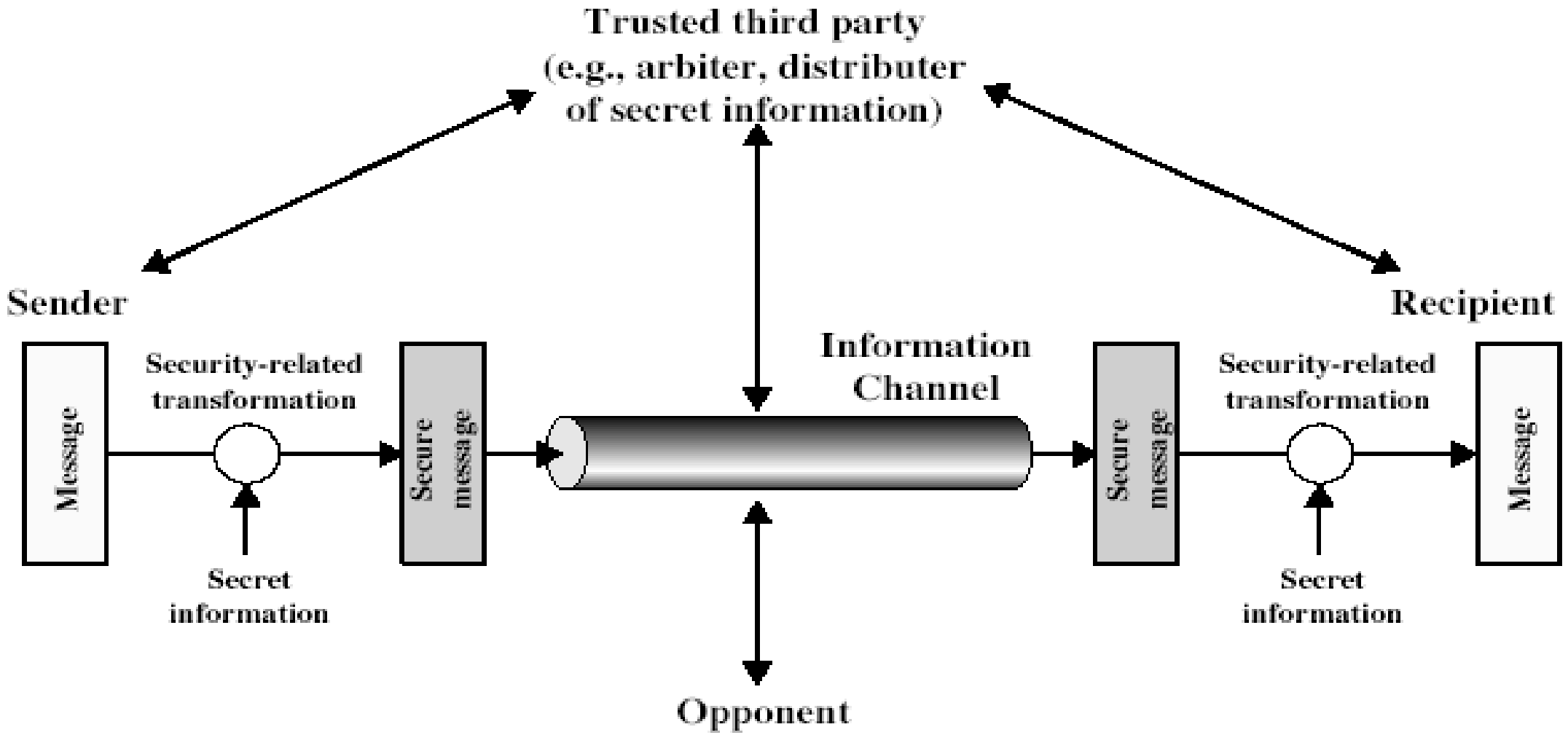
SYN Cookies Limitation

- Windows has not adopted SYN cookies
- Some Linux distributions have used it
- Maximum segment size can only be 8 possible values
- Do not allow the use of TCP option field
  - Many TCP option fields have been used by many programs

IP Traceback



Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Dr. Lokesh Chouhan
NFSU Goa
Lokesh.chouhan_goa@nfsu.ac.in