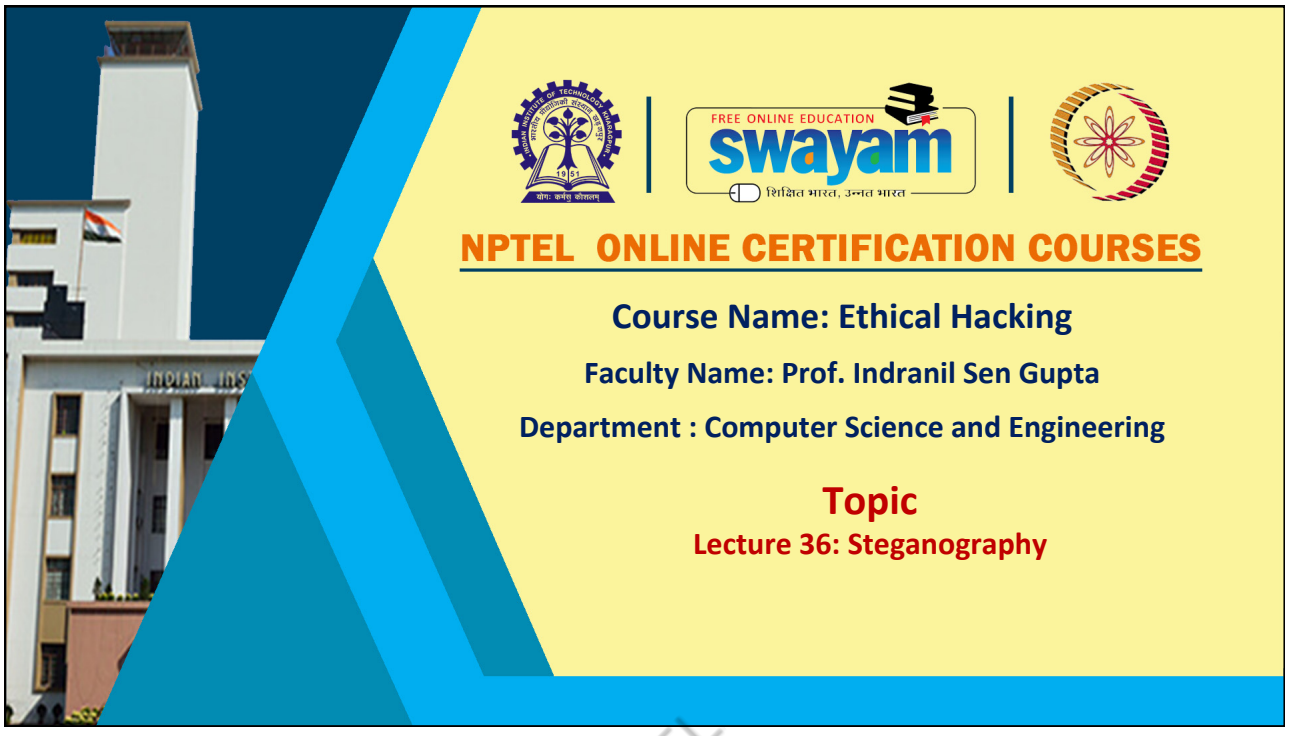


NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 36: Steganography

CONCEPTS COVERED

- Steganography and digital watermarking
- Steganography in image files
- Examples

Steganography

- Literally means "*covered writing*" (Greek).
- Hiding messages in innocent media.
- May be used in conjunction with cryptography, i.e., the message may be encrypted before hiding.
- An encrypted message arouses suspicion during transmission.
  - A hidden message is invisible and is not expected to arouse suspicion.


3

Digital Watermarking

- Digital watermarking embeds copyright, ownership, license and similar information in a medium.
- It is different from steganography only in the intent of hiding. They share same operational and functional behaviours.


4

Steganography : History

- Shave the messenger's head, tattoo the secret message, allow hair to grow and then send the messenger. When the messenger reaches the destination, his head can be shaved once again in order to see the hidden message.
- German spy sent this message during World War II:

  Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

  - Extracting second letters from the words gives:

    Pershing sails from NY June I.


5

Terminologies

- Basic concept:

  Cover-medium + Embedded-message + Stego-key = Stego-medium

- Multimedia files are good covers for hiding messages:
  - Images
  - Sound files
  - Movies
  - Binary files
  - Text files


6

Steganography in Image Files

- Size of an image is determined by *pixels. A pixel is an instance of color.*
  - A color can be specified by the primary components: Red, Green and Blue.
  - Each component is represented by a byte (an 8-bit value between 0 and 255).
  - Example: 00 00 00 is black, FF 00 00 is red, FF FF 00 is yellow, and FF FF FF is white.
- Each pixel is represented by an 8-bit value (GIF) or a 24-bit value (JPEG, BMP).
- The image data is usually compressed.
  - **Lossless compression***: The exact pixel values are stored.*
  - **Lossy compression***: Approximate pixel values are stored.*


7

- A GIF (Graphic Interchange Format) image is an 8-bit image file.
  - Supports at most 256 colors per image.
- Color-map table: An index of 256 (or less) colors occurring in the image.
  - Each pixel represented by an 8-bit value which refers to the index in color-map table.
- A JPEG (Joint Photography Experts Group) image is a 24-bit image file that uses lossy compression based on the discrete cosine transform (DCT).
- Both GIF and JPEG formats use adaptations of the Lempel-Ziv (LZ) compression algorithm.


8

Steganography: Methods

- **Least significant bit (LSB) insertion**: Modify the LSB of a pixel value based on the message to hide. Small changes in the pixel values cannot be noticed by human observers.
- **Properties**:
  - Simple to implement.
  - Compatible with lossless compression.
  - Better adapted to 24-bit images.
  - Often works well with gray-scale images.
  - Extremely vulnerable to image manipulations.


9

Other Methods

- **Masking and filtering:**
  - Mark the image in a non-detectable manner.
  - For example, by increasing the intensity subtly at certain locations of the image.
  - Typically noisy and busy areas of an image are chosen to hide the message.


10

- **Algorithms and transformation:**
  - These are the most sophisticated hiding mechanism that use special algorithms to hide a message in an image.
  - For example, the DCT algorithm may be exploited in order to hide a message in a JPEG file.
    - ❖ DCT uses floating-point calculations with rounding-off errors and so the compression is lossy.
    - ❖ Suitably modifying the floating point arithmetic may hide a message.

Example: LSB Steganography

- Suppose we want to hide the letter 'C' in a GIF image. The ASCII value of 'C' is 67, i.e., 01000011.
- Suppose that the first eight pixels of the GIF image are:

  00110101 01001000 00101000 00110101

  00101111 00011100 01001000 01001000
- Modifying the LSBs corresponding to 'C' gives:

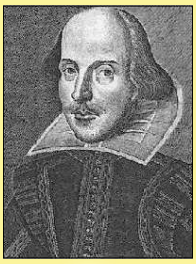
  00110100 01001001 00101000 00110100

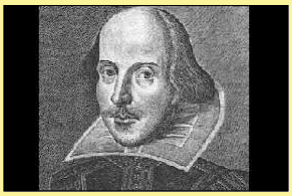
  00101110 00011100 01001001 01001001
- Changes in the index values (in the color-map table) may lead to easily detectable patterns in the image (for example, a red spot in the blue sky).

Examples

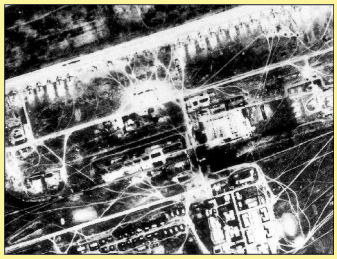
- **Text message to hide**
  - Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present.

Cover Image

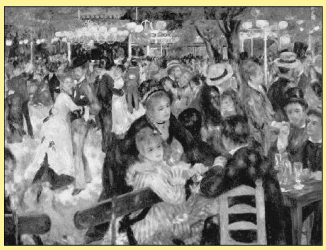




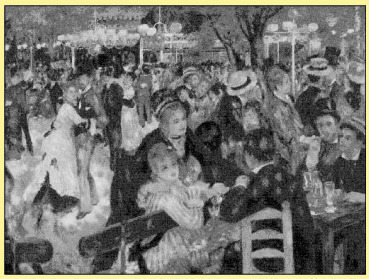
Stego Image



A major strategic Soviet bomber base



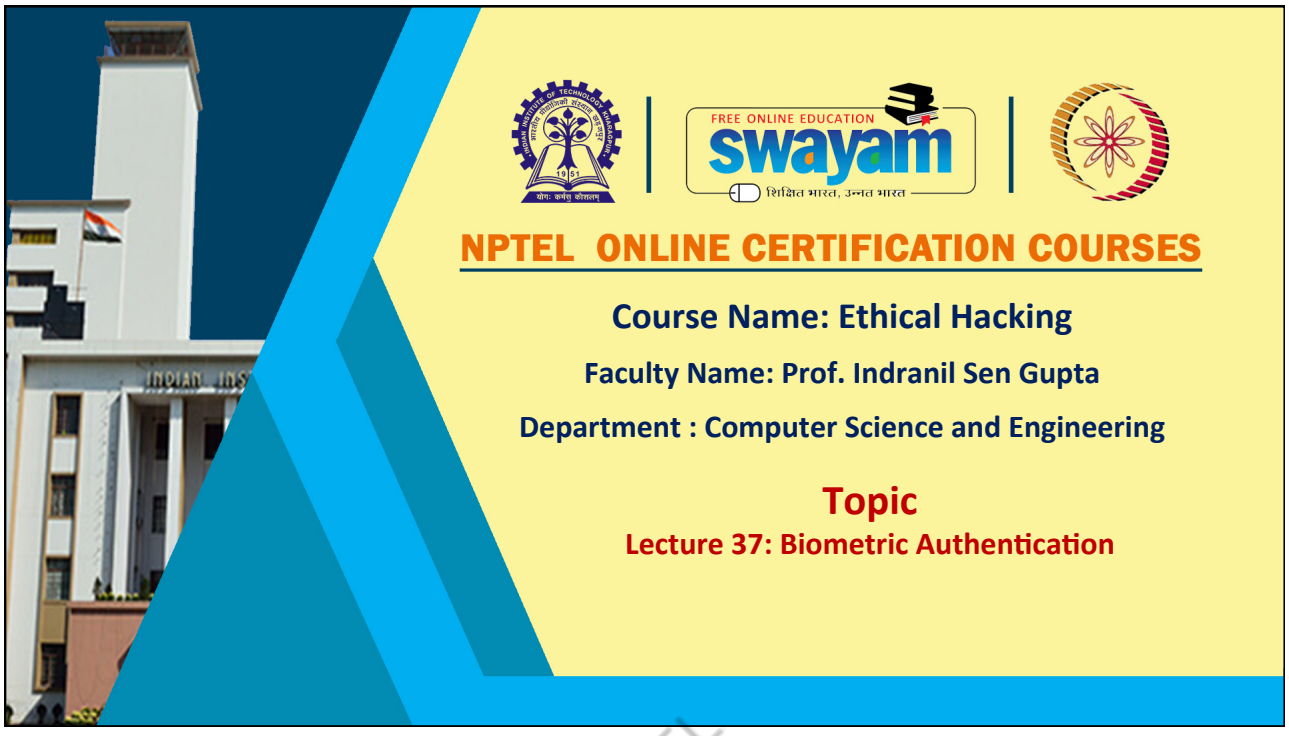
Cover Image



Stego Image

15

16



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 37: Biometric Authentication

CONCEPTS COVERED

- What is biometrics?
- Various biometrics used in practice
- Applications

What is Biometrics?

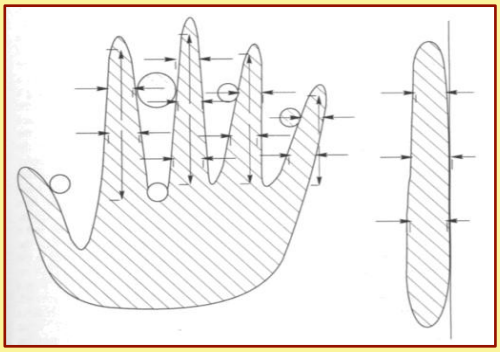
- Automated method for recognizing individuals based on measurable *biological* and *behavioral* characteristics.
- Types of biometrics:
  - Fingerprint, Face, Hand geometry, Iris scan, Retina scan
  - Signature, Keystroke dynamics, Gait, DNA
  - Several others

Fingerprint Recognition

- Minutiae
- Pattern matching
- Problems:
  - Not robust
  - Sometimes unusable

Hand Geometry

- Captured using a CCD camera, or LED
- More accurate than fingerprints
- Require larger scanner

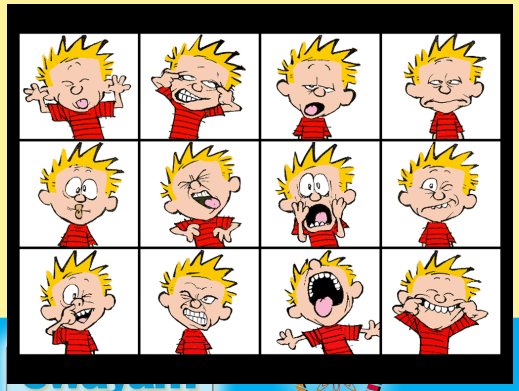


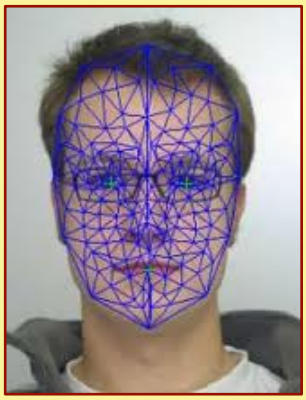
Iris Recognition

- Uses infrared light
- Converts images to vectors
- Not very accurate yet

Facial Recognition

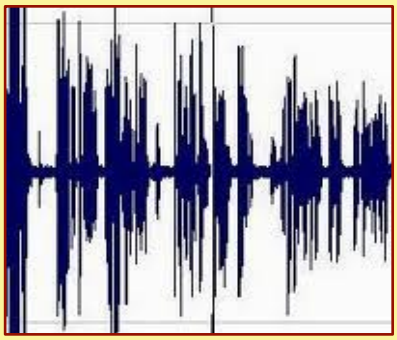
- Location and position of facial features.
- Dependent on background and lighting conditions.





Voice Verification

- Features:
  - Pitch, intensity, quality and duration.
  - Requires proper handling of background noise.



Retina Recognition

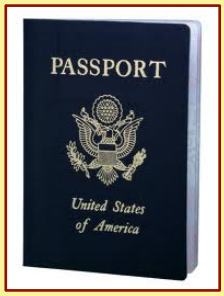
- One of the most secure means of biometrics.
- Unique to each person.
- Unique to each eye.
- Problem:
  - Requires effort on the part of the subject.
  - Often stressful to the subject.

Commercial Applications of Biometrics

- Server login
- Electronic payment
- Access control to regions
- Record protection

Government Applications of Biometrics

- Passport control
- Border control
- Access control to facilities
- Adhaar UID



11

Forensic Applications of Biometrics

- Missing persons
- Corpse identification
- Criminal investigations

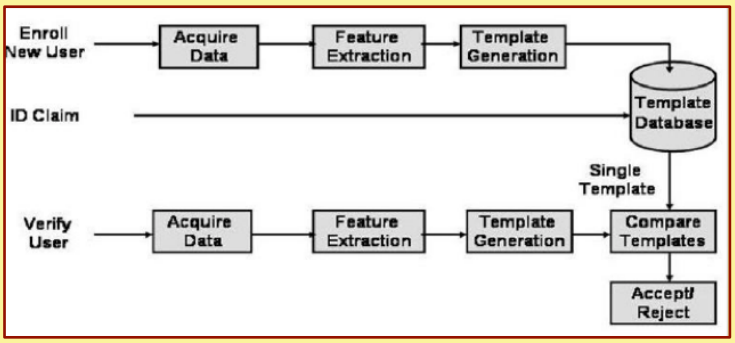
12

Practical Systems

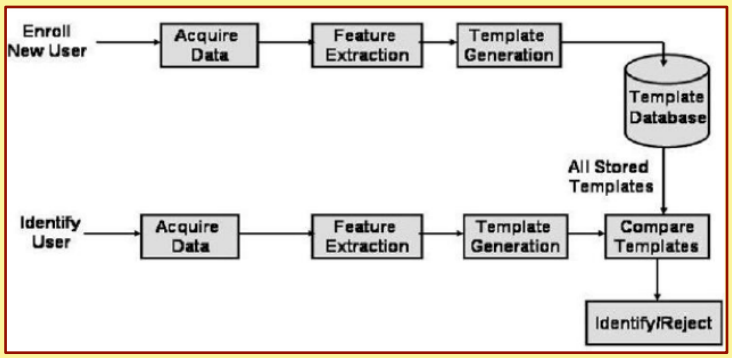
- No single biometric feature may not be accurate enough.
- Multimodal biometrics is a feasible option.
  - Voice + Face
  - Fingerprint + Hand Geometry + Face
  - Face + Voice

Usage of Biometrics

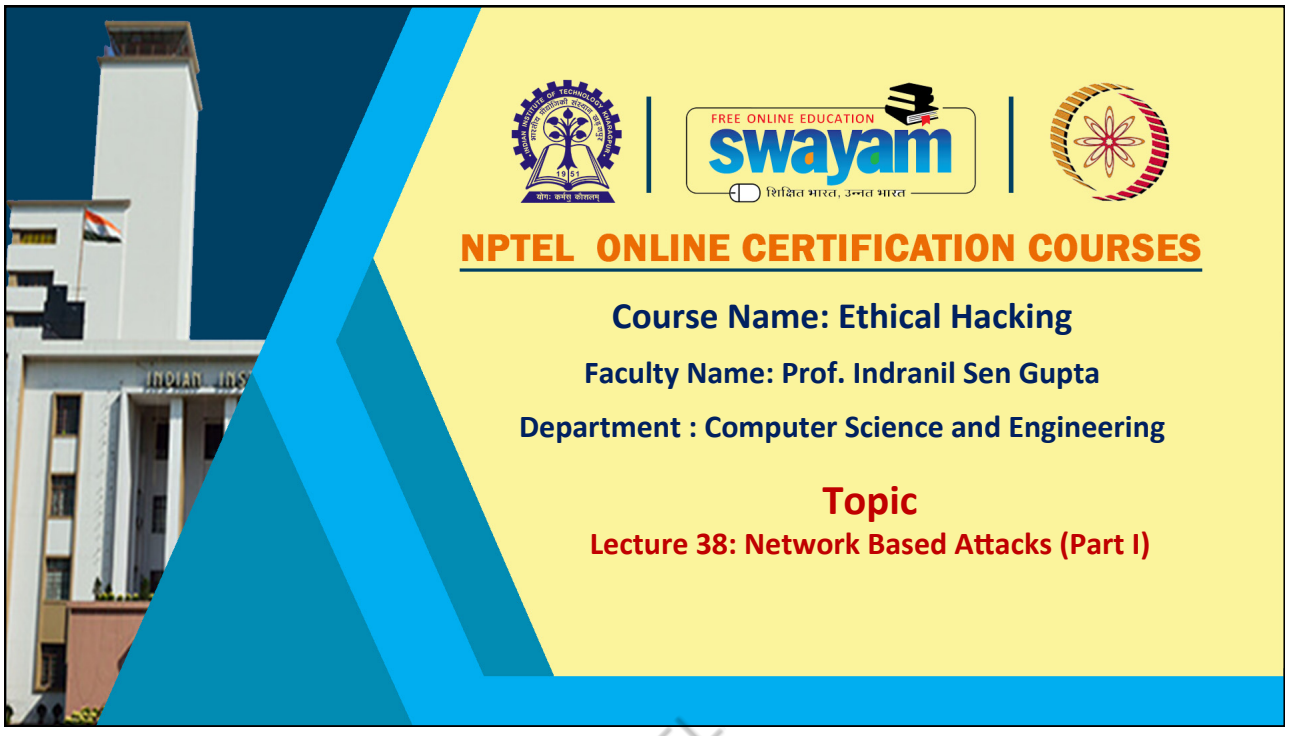
- Authentication (1:1)



- Verification (1:N)



15



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

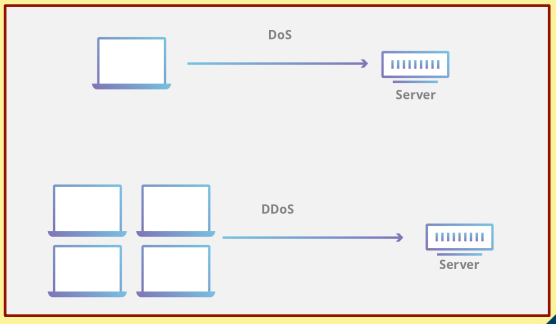
Lecture 38: Network Based Attacks (Part I)

CONCEPTS COVERED

- Denial of Service attacks
- Smurf DoS attack
- Ping of death attack
- SYN flooding attack

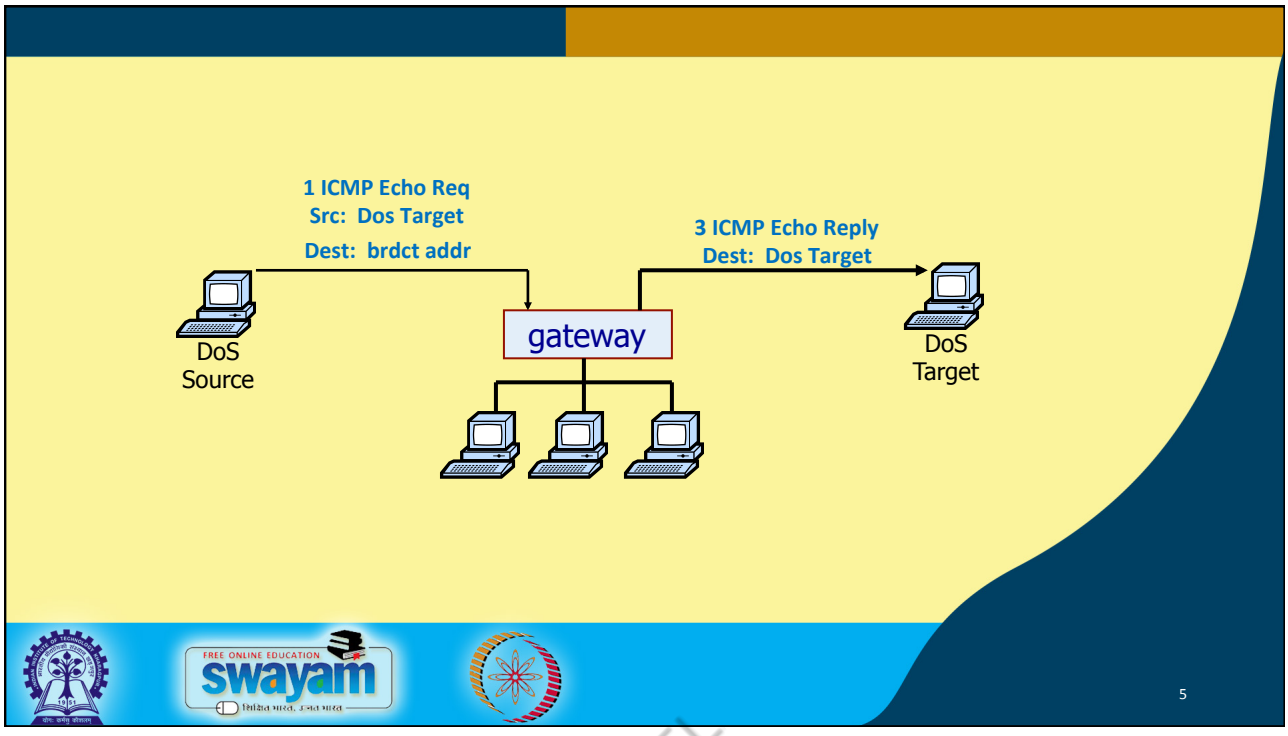
Denial-of-Service (DoS) Attack

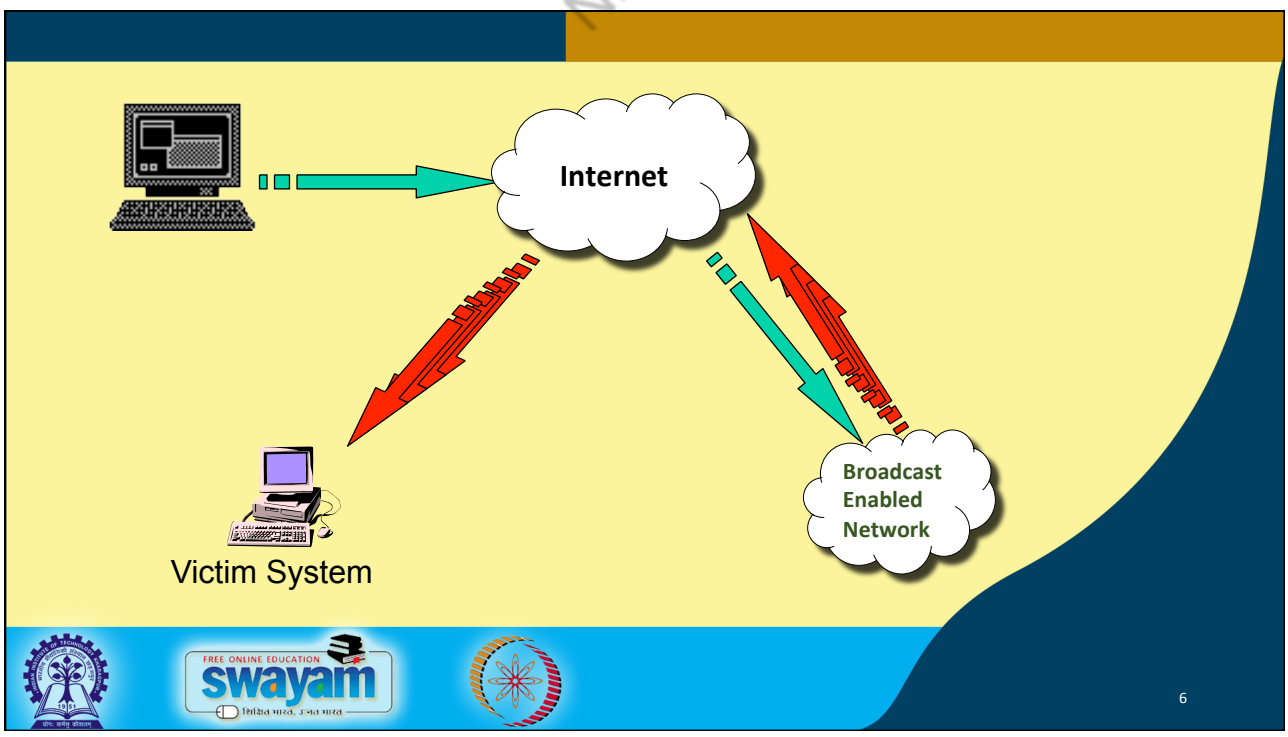
- An explicit attempt by attackers to prevent legitimate users of a service from using that service.
- Such attacks have increased in frequency, severity and sophistication with time.



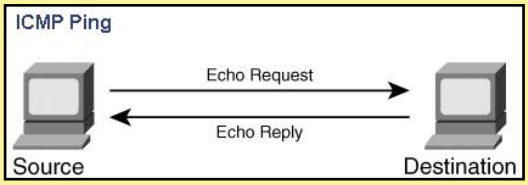
(a) Smurf DoS Attack

- Send "*ping request*" to broadcast address (*ICMP Echo Request*).
- A large number of response packets:
  - Every host on target network generates a "*ping reply*" (*ICMP Echo Reply*) to victim.
  - Ping reply stream can overload victim.
- Prevention?
  - Configure edge router to reject external packets to broadcast address.


1 ICMP Echo Req
Src: Dos Target
Dest: brdct addr
3 ICMP Echo Reply
Dest: Dos Target
gateway
DoS
Source
DoS
Target
5

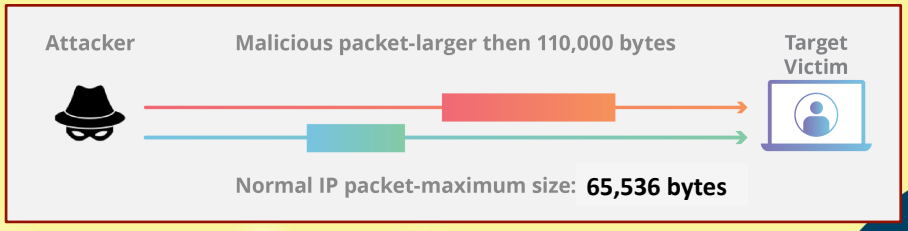

Internet
Broadcast
Enabled
Network
Victim System
6

(b) Ping-of-Death Attack



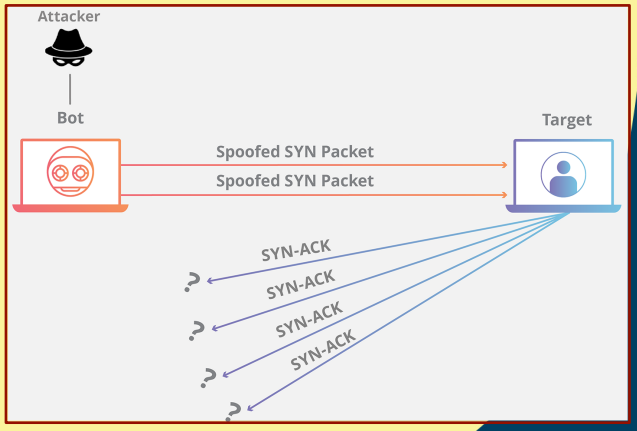
- This attack uses ICMP ping messages.
  - A normal ping has two messages:
- The attack …
  - An echo packet is sent that is larger than the maximum allowed size of 65,536 bytes.
  - The packet is broken down into smaller segments, but when it is reassembled, it is discovered to be too large for the receiving buffer.
  - Systems that are unable to handle such abnormalities either crash or reboot.

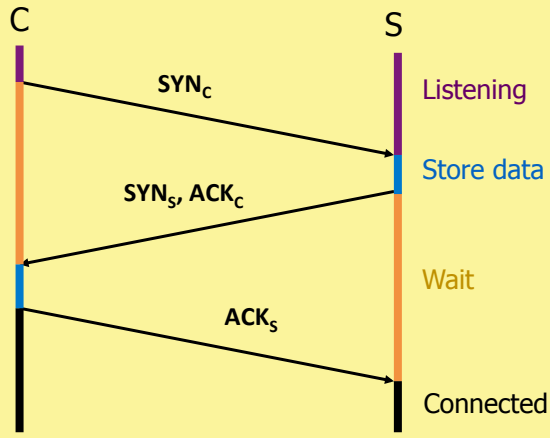
- Mounting the attack …
  - We can mount the Ping of Death attack from within Linux by typing ***ping –f –s 65537***.
  - The -f switch causes the packets to be sent as quickly as possible.
  - Often the cause of a DoS attack is not just the size or amount of traffic, but the rapid rate at which packets are being sent to a target.



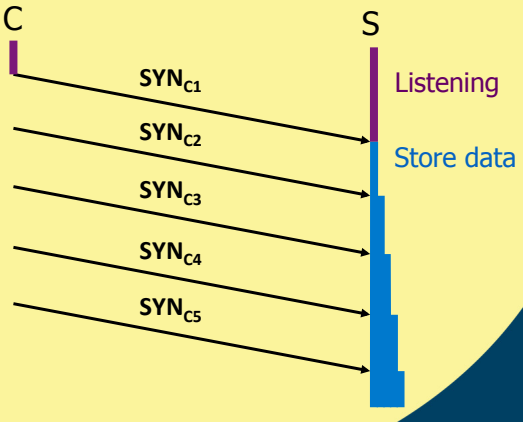
(c) SYN Flooding Attack

- **Basic idea:**
  - The attacker exploits the 3-way handshake protocol for TCP connection establishment.
  - Server accumulate "half-open" connections.
  - The half-open connections build up until the queue becomes full, and all additional requests are blocked.





TCP 3-way handshake

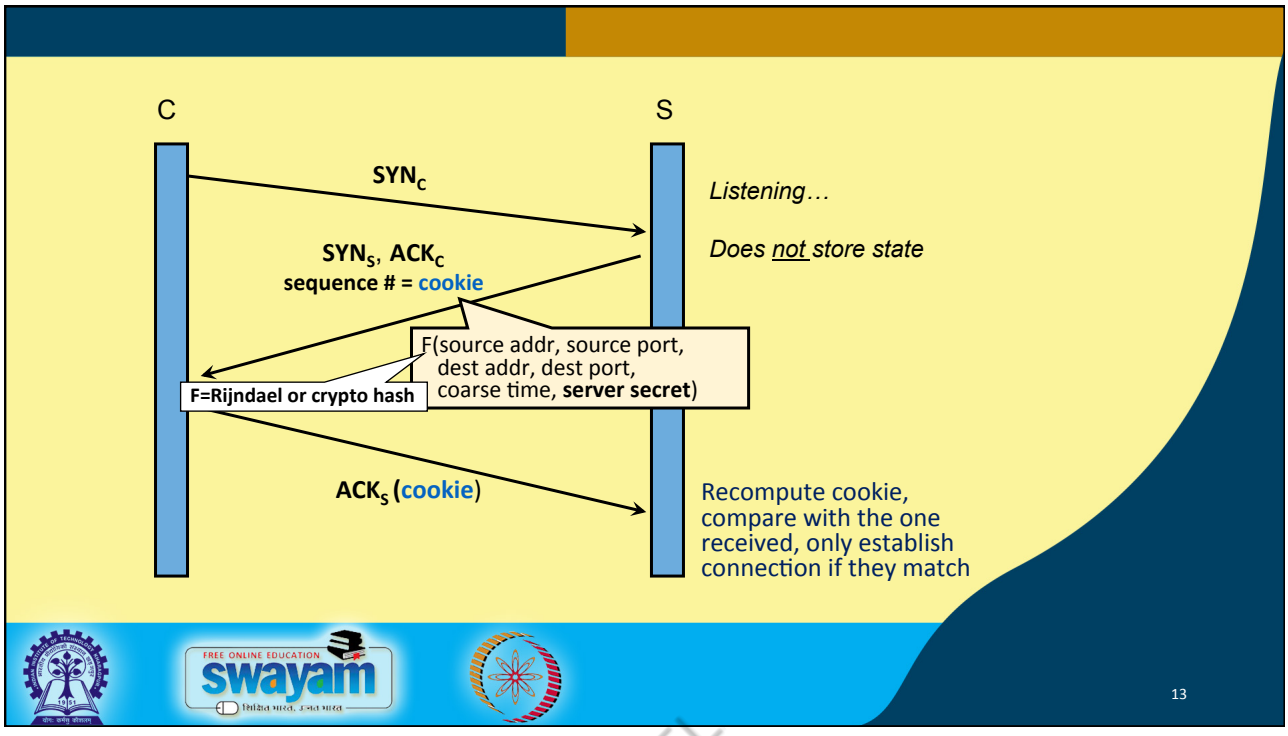


SYN Flooding

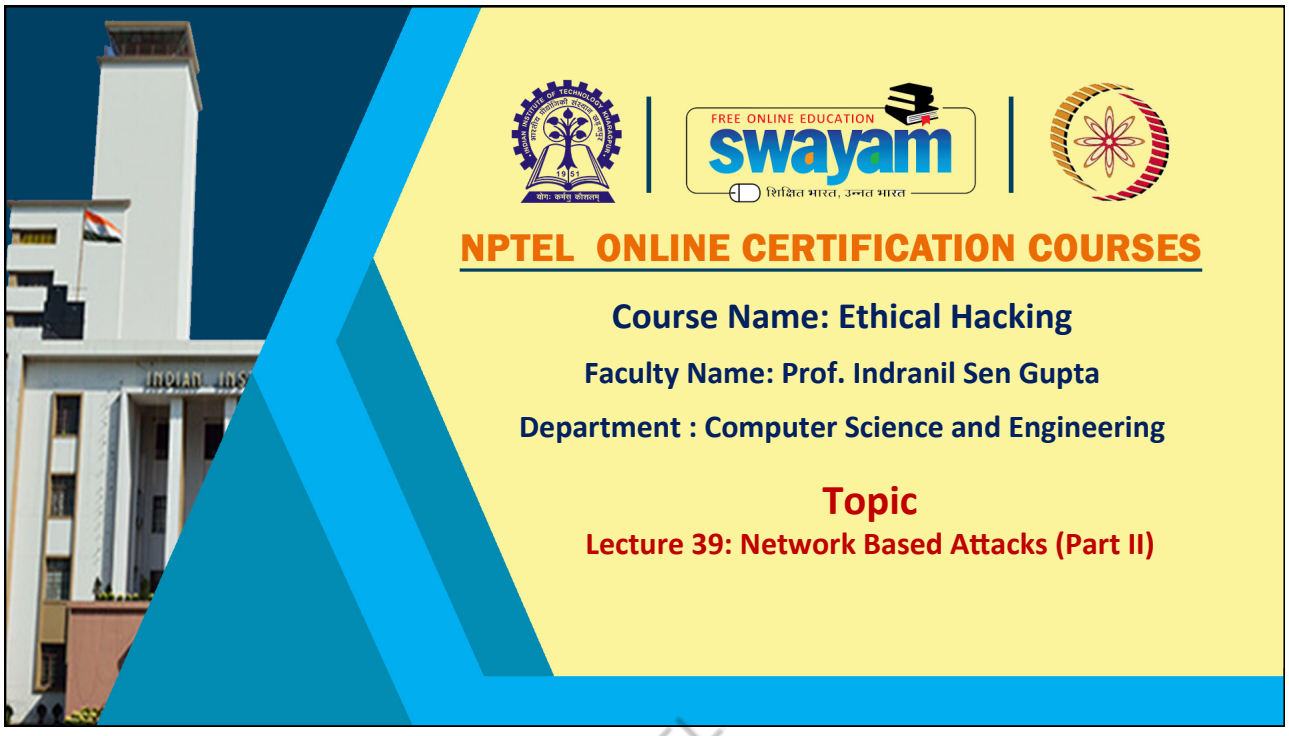
- What happens actually?
  - Attacker sends many connection requests with spoofed source addresses.
  - Victim allocates resources for each request.
    - ❖ New thread, connection state maintained until timeout.
    - ❖ Fixed bound on half-open connections.
  - Once resources are exhausted, requests from legitimate clients are denied.
- Point to note:
  - It costs nothing to TCP initiator to send a connection request.
  - But TCP responder must spawn a thread for each request.


Preventing Denial of Service Attack

- DoS is caused by asymmetric state allocation.
  - If responder opens new state for each connection attempt, attacker can initiate thousands of connections from bogus or forged IP addresses.
- Cookies ensure that the responder is stateless until initiator produced at least two messages.
  - Responder's state (IP addresses and ports of the connection) is stored in a cookie and sent to initiator.
  - After initiator responds, cookie is regenerated and compared with the cookie returned by the initiator.



C
S
SYN$_C$
Listening…
Does not store state
SYN$_S$, ACK$_C$
sequence # = cookie
F(source addr, source port,
dest addr, dest port,
coarse time, server secret)
F=Rijndael or crypto hash
ACK$_S$ (cookie)
Recompute cookie,
compare with the one
received, only establish
connection if they match
13


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
14

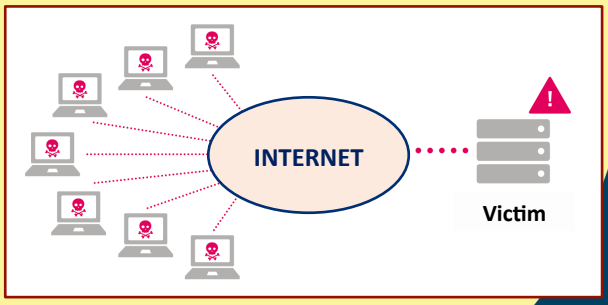


CONCEPTS COVERED

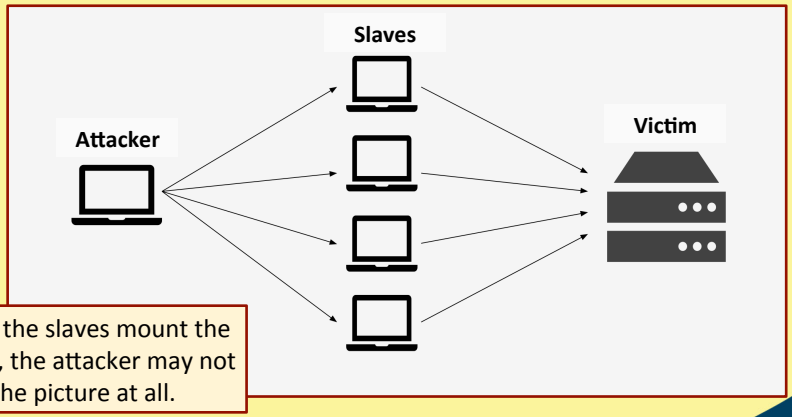
- Distributed Denial of Service (DDoS) attacks
- How DDoS attack works?
- HTTP Flood Attack
- General Defense against DoS/DDoS attacks

Distributed DoS (DDoS) Attack

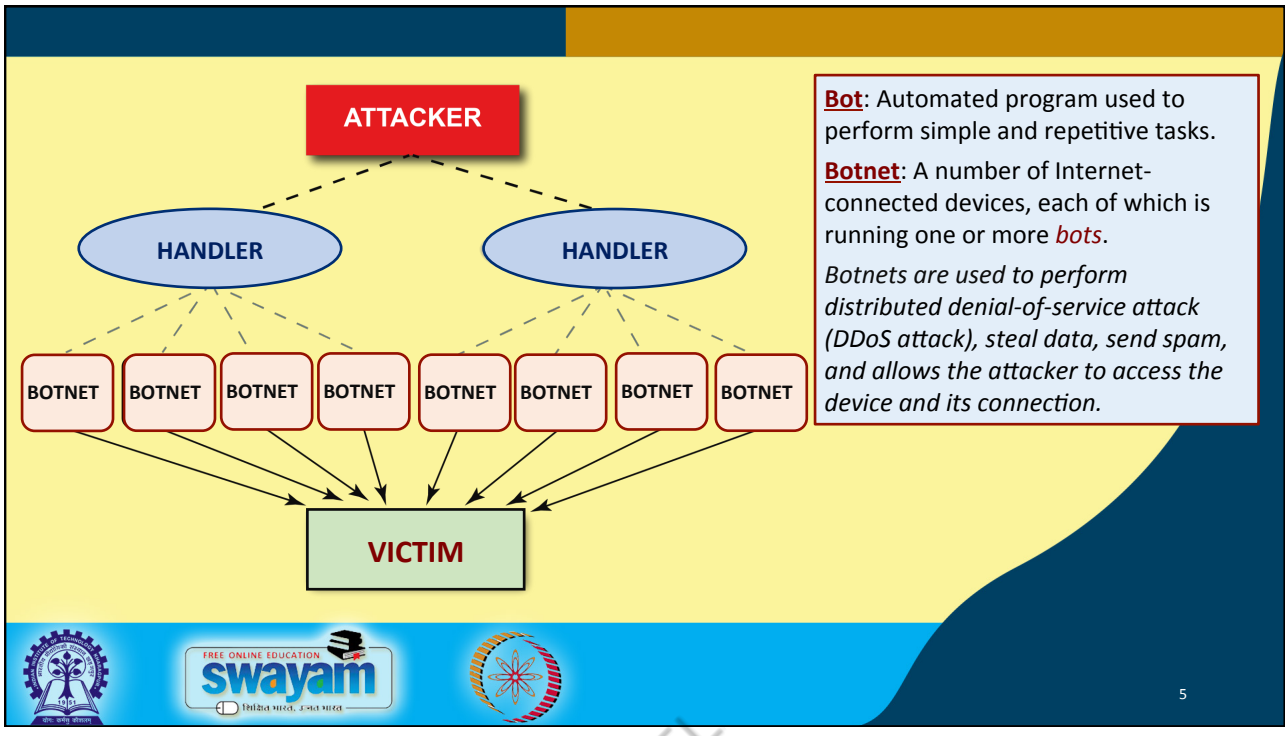
- Multiple compromised systems are used to attack a single target.
- Since a DDoS attack is launched from multiple sources, it is often more difficult to detect and block than a DoS attack.

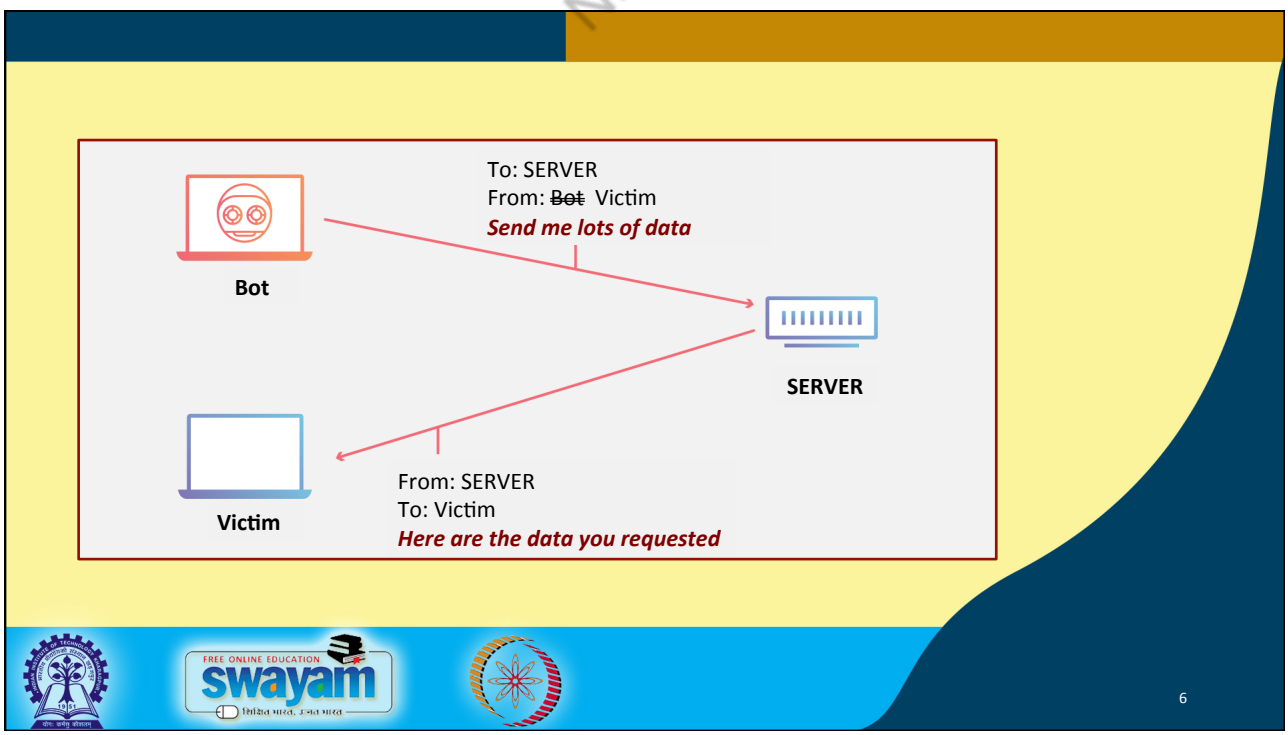


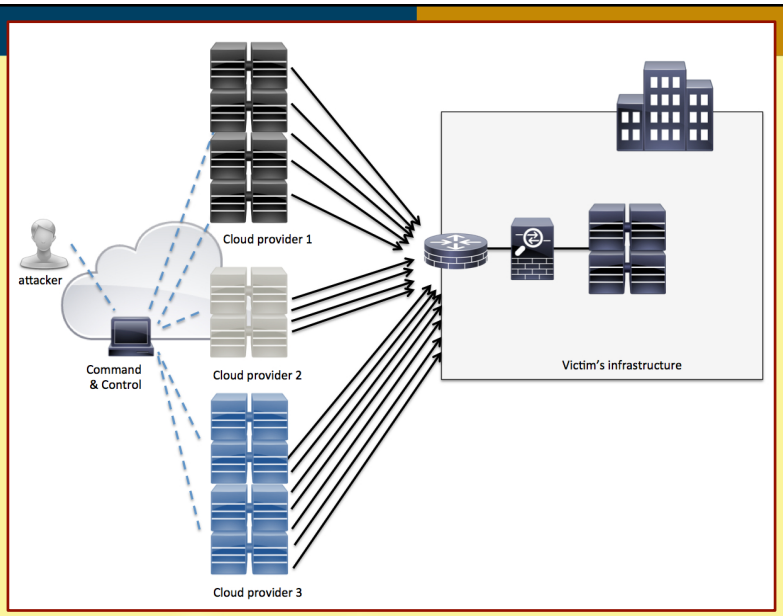
DDoS: Basic Idea



When the slaves mount the attack, the attacker may not be in the picture at all.


ATTACKER
HANDLER
HANDLER
BOTNET
BOTNET
BOTNET
BOTNET
BOTNET
BOTNET
BOTNET
BOTNET
VICTIM
Bot: Automated program used to perform simple and repetitive tasks.
Botnet: A number of Internet-connected devices, each of which is running one or more bots.
Botnets are used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection.
5


To: SERVER
From: Bot Victim
Send me lots of data
Bot
SERVER
Victim
From: SERVER
To: Victim
Here are the data you requested
6



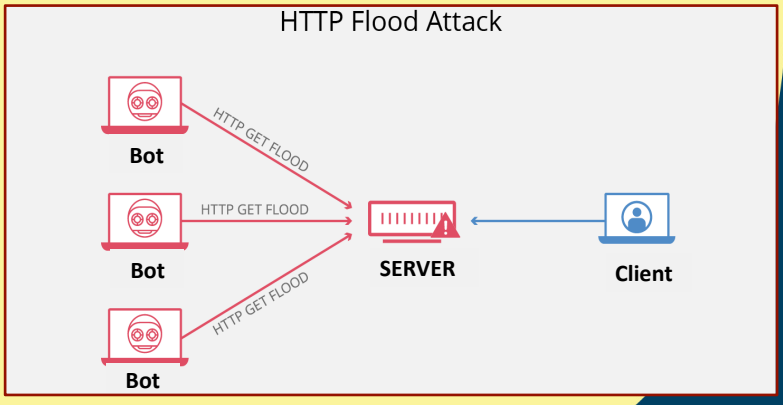
7

- Difficult to locate the source of the attack.
  - Hard to find the attacker.
    - ❖ Originator of attack compromised the Handlers.
    - ❖ Originator may not be active when DDoS attack occurs.
  - Can try to find the Agents / Botnets.
    - ❖ Source IP address in packets is not reliable (may be spoofed).
    - ❖ Need to examine traffic at many points, modify traffic, or modify routers.

8

HTTP Flood Attack

- It is a type of DDoS attack designed to overwhelm a targeted server with HTTP requests.
- Once the target has been saturated with requests and is unable to respond to normal traffic, denial-of-service will occur for additional requests from legitimate users.



Types of HTTP Flood Attacks

a) HTTP GET attack

- Multiple computers or other devices coordinate to send multiple requests for images, files, or some other asset from a targeted server.
- When the target is flooded with incoming requests and responses, denial-of-service will occur to additional requests from legitimate traffic sources.

b) HTTP POST attack

- When a form is submitted on a website, the server must handle the incoming request and push the data into a persistence layer, most often a database.
- The process of handling the form data and running the necessary database commands is relatively intensive compared to the amount of processing power and bandwidth required to send the POST request.
- This attack utilizes the disparity in relative resource consumption, by sending many post requests directly to a targeted server until it's capacity is saturated and denial-of-service occurs.


- **Mitigating HTTP flood attack:**
  - One method is to implement a challenge to the requesting machine in order to test whether or not it is a bot.
    - ❖ Similar to a captcha test commonly found when creating an account online.
    - ❖ Or a JavaScript computational challenge.
  - Other avenues for stopping HTTP floods include the use of a *web application firewall*, managing an IP reputation database in order to track and selectively block malicious traffic.


General Defense Against DoS and DDoS Attacks

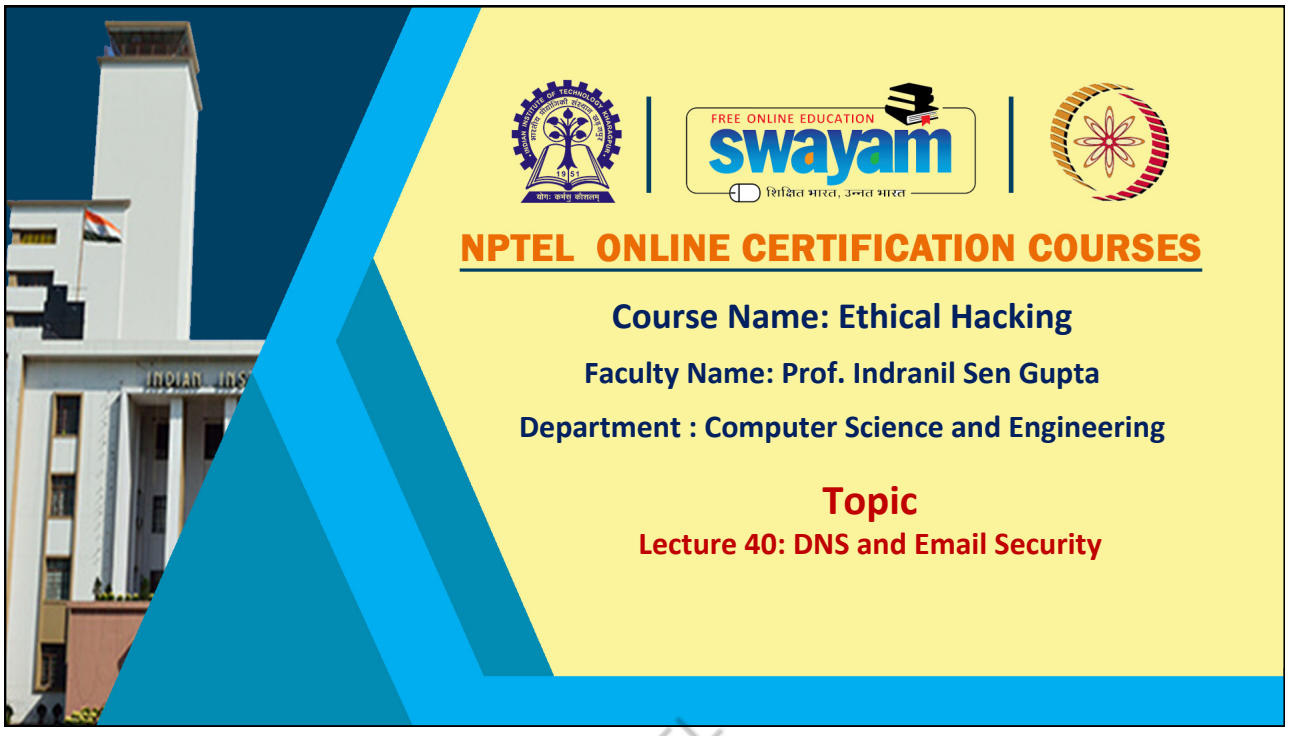
- **By the Internet Service Providers (ISPs)**
  - Deploy source address anti-spoof filters (*very important!*).
  - Turn off directed broadcasts.
  - Develop security relationships with neighbor ISPs.
  - Set up mechanism for handling customer security complaints.
  - Develop traffic volume monitoring techniques.


- **In the Highly Loaded Machines**
  - Look for too much traffic to a particular destination.
  - Look for traffic to that destination at the border routers.
  - Can we automate the tools – too many queue drops on an access router will trigger source detection?
  - Disable and filter out all unused UDP services.


- **General precautions**
  - Routers, machines, and all other Internet accessible equipment should be periodically checked to verify that all security patches have been installed.
  - System should be checked periodically for presence of malicious software (Trojan horses, viruses, worms, back doors, etc.).

15

16



CONCEPTS COVERED

- Domain Name System (DNS)
- DNS poisoning attacks
- Securing electronic mails

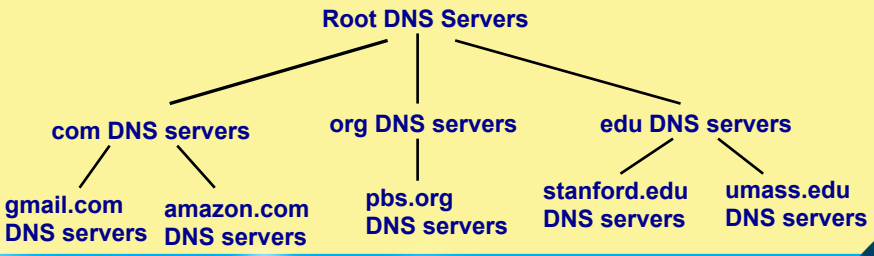
Domain Name System (DNS)

- Maintains the correspondence between host name and IP address.
- Stored in a database, in a hierarchical fashion.
  - Centralized database can lead to single point of failure, and high traffic volume.
- Typical DNS services:
  a) Host name to IP address translation
  b) Host aliasing – many names for a single host.
  c) Load distribution – set of IP addresses for one canonical name.


3

Distributed DNS Servers

- Example: Client wants IP for www.gmail.com
  - Client queries a root server to find "*com*" DNS server.
  - Client queries "*com*" DNS server to get "*gmail.com*" DNS server.
  - Client queries "*gmail.com*" DNS server to get IP address for "*www.gmail.com*".




4

Query Resolution Alternatives

a) Iterative Name Resolution

- Contacted server responds with name of the next server to contact.

b) Recursive Name Resolution

- DNS client requires the DNS server to respond with either the requested resource record, or an error message stating that the domain name does not exist.
- Each DNS server can recursively get information from the next server.


5

DNS Caching

- Once a DNS server learns about a (name, IP address) mapping, it caches it.
  - Cache entries timeout (disappear) after some time.
  - Top-level DNS servers typically cached in local DNS servers.
  - Avoids frequent visit to root DNS servers.


6

DNS Vulnerability

- Most DNS queries and responses are in plaintext.
- No authentication is done for DNS response.
  - Difficult to tell whether the response is trustable or not.
- DNS mostly relies on UDP packets.
  - IP address spoofing is rather easy for UDP packets.
  - No sequence or acknowledgement numbers.


7

DNS Cache Poisoning

- Basic idea:
  - Give DNS servers false records and get them cached.
  - Cache may be *poisoned* when a DNS server disregards the 16-bit request identifiers to pair queries to answers, or accepts unsolicited DNS records.
- Various ways to do DNS cache poisoning:
  - Redirect the nameserver of the attacker's domain to the nameserver of the target domain, and then assign a fake IP address to this target nameserver.
  - Redirect the nameserver of another, unrelated domain to a fake nameserver.
  - Racing the real nameserver to give an answer.


8

A DNS Cache Poisoning Procedure

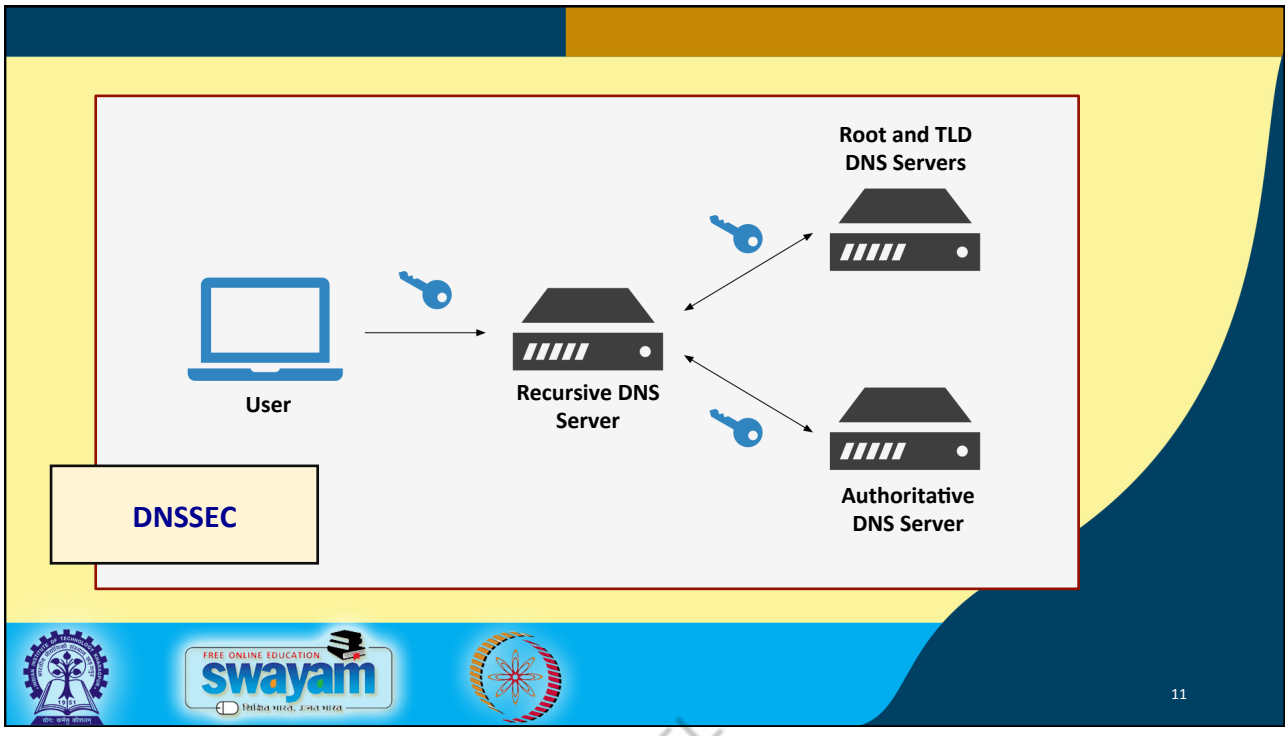
- **Scenario**: Attacker X wants to poison attack an ISP's DNS server.
- **Procedure**:
  - X transmits a DNS query to this server, which in turn queries an authoritative DNS on behalf of X.
  - X simultaneously sends a DNS response to the server, spoofing with the authoritative server's IP address.
  - The ISP's DNS server accepts the forged response and caches a wrong DNS entry.
    - ❖ All downstream users of this ISP will be directed to the wrong website.

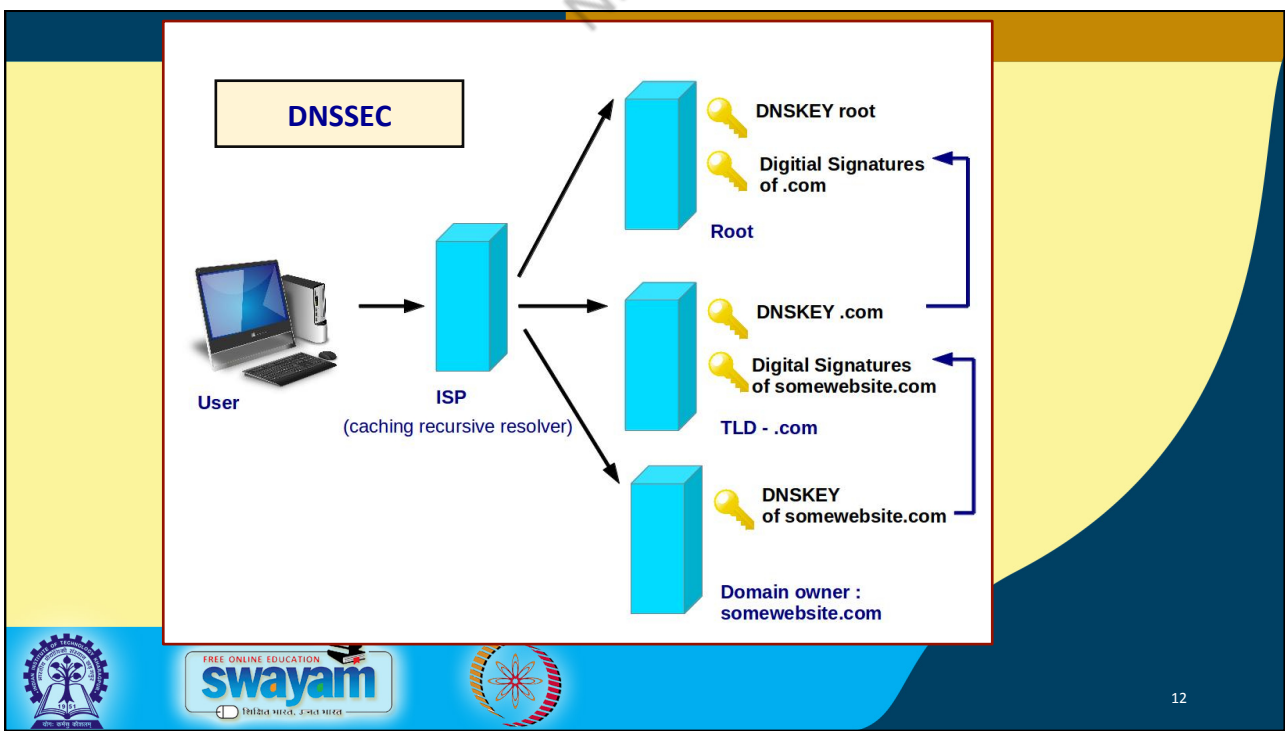

9

DNSSEC: A Secure DNS Server

- DNSSEC guarantees:
  - Authenticity of DNS response origin.
  - Integrity of DNS query response.
  - Authenticity of denial of existence.
- Accomplished by digitally signing DNS responses at every step.
  - Uses public-key cryptography to sign responses.
  - May add considerable load to DNS servers with packet sizes becoming larger.


10


Root and TLD
DNS Servers
User
Recursive DNS
Server
Authoritative
DNS Server
DNSSEC
11


DNSSEC
DNSKEY root
Digitial Signatures
of .com
Root
User
ISP
(caching recursive resolver)
DNSKEY .com
Digital Signatures
of somewebsite.com
TLD - .com
DNSKEY
of somewebsite.com
Domain owner :
somewebsite.com
12

EMAIL Security (A Case Study)

Pretty Good Privacy (PGP)

- Provides confidentiality and authentication service that can be used for electronic mail and file storage applications.
- Why popular?
  - It is availiable free on a variety of platforms.
  - Based on well known algorithms.
  - Wide range of applicability.
  - Not developed or controlled by governmental or standards organizations.

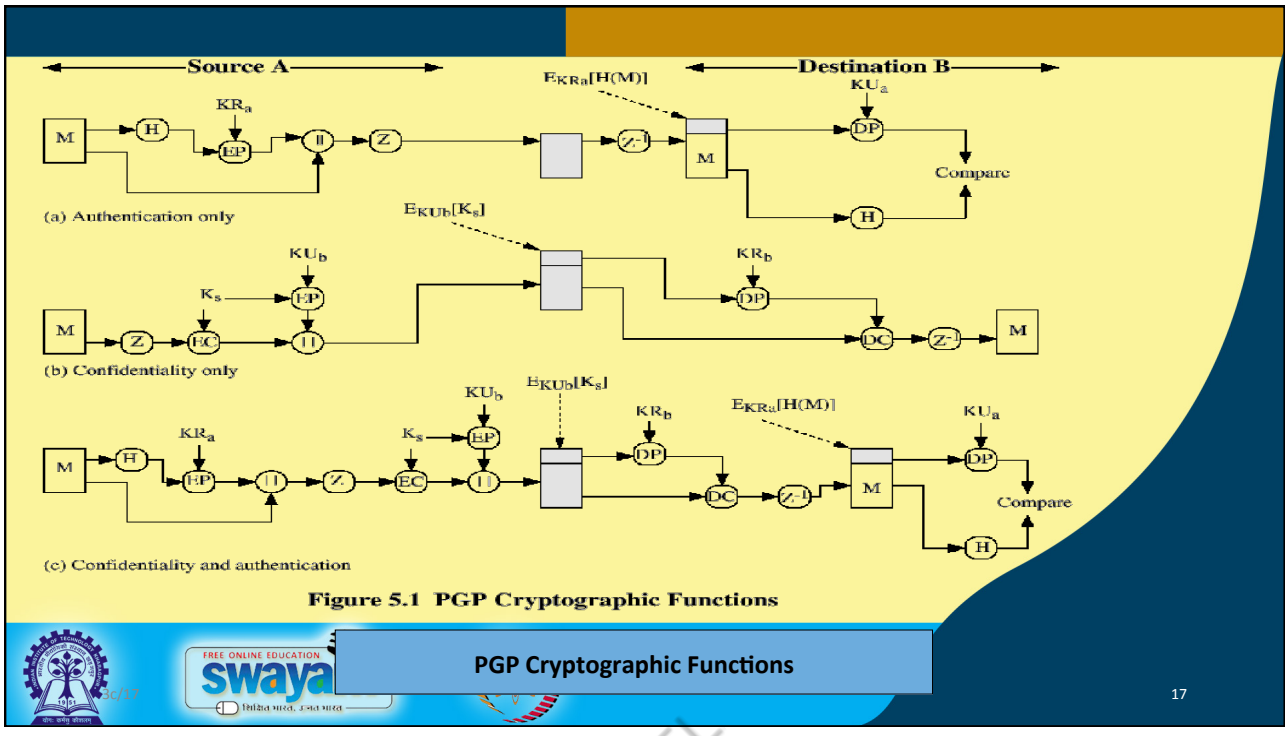
Services in PGP

- Consists of five services:
  a) Authentication
  b) Confidentiality
  c) Compression (compresses message using ZIP after applying signature)
  d) E-mail compatibility (uses base-64 encoding)
  e) Segmentation (maximum segment length of 50 KB; breaks into multiple as required)


15

Authentication and Confidentiality


16


Source A
Destination B
(a) Authentication only
(b) Confidentiality only
(c) Confidentiality and authentication
Compare
Figure 5.1 PGP Cryptographic Functions
PGP Cryptographic Functions
17


FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
18