홍익대학교
HONGIK UNIVERSITY

Network Security

<CH 8>

Youn Kyu Lee
Hongik University

Internet Protocols and Service Denial

- DoS/DDoS attacks
  - attacker can steal your IP address space, or domains to send spam -> you may find it's been blacklisted!
  - attacker can send you huge floods of traffic from a botnet of many compromised machines (via TCP SYN, …)

- BGP(Border Gateway Protocol) security
  - Internet is an interconnected network of networks, consisting of AS(autonomous system)es w.r.t routing

Internet Protocols and Service Denial

- BGP(Border Gateway Protocol) security
  - (by mistake or by malware) lots of routers advertise large number of false routes, … clogging the routing tables …

    : 2008, YouTube down for a few hours because Pakistan gov't announced *false* routes to it, which propagated globally

    : 2010, China Telecom advertised over 100,000 *invalid* routes -> accident?? Or testing a 'cyber-nuke'?

    : 2016(Feb.~July), traffic from Canada to Korean government websites routed via China -> 'hijacking'??
  - BGP security mechanism at present is *Resource Public Key Infrastructure(RPKI)* : enables registries to certify "AS *X* announces IP address range *Y* "

    -> will not prevent attackers from announcing a malicious route having the right AS at the end of route following the attacker's in the middle

Internet Protocols and Service Denial

- DNS security
  - DNS: a massively distributed system with a lot of very fast machines on very high-capacity networks -> service denial attacks on it are rare
  - Hijacking

    : (for censorship) intercept and redirect DNS queries

    : (for other purpose) to hack a DNS server at an ISP to drive clients to a wicked website (called *pharming*)

    : lure you to a web page containing Javascript that changes your home router's DNS server to one under the attacker's control
    (eg. emulated 'www.citibank.com')

Internet Protocols and Service Denial

- DNS security
  - DNSSEC for preventing DNS hijacking
    : adds digital signatures to DNS name records
    : verify signature to ensure the record came from the authoritative server and was not altered en route
  - DNSSEC gets abused in denial-of-service attack
    : eg. Alice attacks Bob by sending Charlie a message "can you tell me the very large answer to this question? Bob"
    → signed DNS records(responses to the query) are a lot larger
    → Alice can send packets that purport to come from Bob's IP address to many DNS servers, which then bombards the target with replies

Internet Protocols and Service Denial

- DNS security
  - DNS-over-https(DoH)

    : (Google-Chrome, Mozilla-Firefox) propose that (rather than sending DNS traffic in the clear) it will go *encrypted* over https to a DoH resolver -> good for privacy!

    : many enterprise security products monitor DNS to detect abuse or under attack

    eg.)

    → spot a machine tries to access to a certain domains, which are inappropriate for work

    → if malware compromises a machine in your organization, you may spot it when it tries to contact a command-and-control server

Internet Protocols and Service Denial

- Packet Amplification

  - TCP 3-way handshake

    A → B: SYN; my number is *X*

    A ← B: ACK; now *X*+1

    SYN; my number is *Y*

    A → B: ACK; now *Y*+1

    (start talking)

  - SYN flooding: sends a lot of SYN packets and never acks any of the replies
  - (countermeasure) SYN cookie: B simply sends out as *Y* an encrypted version of *X* (do not keep a copy of incoming SYN)

  - SYN reflection: A sends a lot of packets that purport from Charlie(the target victim); B replies to Charlie, not to A!

Internet Protocols and Service Denial

- Other denial-of-service attack

  - arrange a lot of infected machines to send packets to the target

  - botnet: a lot of infected machines controlled by attacker

    : machines are in many cases IoT devices(such as CCTV cameras), connected to home WiFi networks with reasonable bandwidth, but which tend to have known default passwords and often incapable of being patched eg. Mirai botnet

Malware

- worm, virus, Trojan, rootkit, …

  - worm: a malicious program that replicates itself on other systems
  - virus: a malicious program that hooks itself into the code of other programs (eg. macros in MS Word documents)
  - Trojan: a program doing something malicious when run by unsuspecting user

    cf. RAT(remote access Trojan): a program that may or may not run as root but that enables a remote party to access the device it runs on
  - rootkit: a program installed as root on a device and that stealthily enables a third party to control it
  - ransomware: a program to lock up(encrypt) victim’s files to demand ransom

    …

Malware

- Botnet: a “network” of infected machines
- Infected machines are “bots”
  - victim is unaware of infection (stealthy)
- Botmaster controls botnet via
  - P2P network
  - IRC
- Botnets used for Spam, DoS attacks, …
- Botnet Examples
  - Mirai, 3ve, Emotet, Srizbi, Methbot, …

Malware

- How malware works?

  - malware structure: replication mechanism(dropper)+payload

    : replication mechanism

    a worm makes a copy of itself somewhere else when it's run(by breaking into another system by password guessing or using a remote code execution vulnerability)

    : payload

    i) exfiltrate your confidential data

    ii) encrypt your data and demand ransom money

    iii) installed software in it to do surveillance of traffic passing through or to attack others

    iv) install a rootkit to enable its controller to do something

    v) perform something undesirable, such as mining Bitcoins

    …

Malware

- Countermeasures

  - antivirus software: arms race between virus and antivirus developers

    : how to detect suspicious code?

    1) scanners

       - search for indicator of compromise, typically a string of bytes from a specific virus (‘a kind of *pattern matching* ’)
       - fast and efficient to find ‘known’ malware
       - do not detect ‘unknown’ malware

Encrypted Malware

- Malware writers know scanners used
- So, how to evade scanners-based detection?
- Encrypting the virus is a good approach
    - Ciphertext looks like random bits
    - Different key, then different “random” bits
    - So, different copies have no common “signature”
- Encryption often used in viruses today

Encrypted Malware

- How to detect encrypted malware?
- Scan for the decryptor code
  - more-or-less standard scanners-based detection
- Why not encrypt the decryptor code?
  - then encrypt the decryptor of the decryptor (and so on…)
- but, cannot repeat this encrypt-decrytor game endlessly

Polymorphic Malware - Polymorphism

- Idea
  - Body of malware is encrypted
  - Decryptor code is “morphed”
  - Trying to hide decryptor signature (goal) to change malware each time it replicates

    malware = decryptor + encrypted body

    → malware re-encrypts body with a different key on each replication

    → tweaks decryptor by substituting equivalent sequences of instructions

Metamorphic Malware

- A metamorphic malware mutates before infecting a new system
- in principle, can evade scanners-based detection
- Mutated malware must function the same
  - and be “different enough” to avoid detection
- One approach to metamorphic replication
  - the malware is disassembled
  - random variations inserted into code (permute the code, insert dead code, etc.)
  - assemble the resulting code
- Result is a malware with same functionality as original, but with a different signature

Malware

- Countermeasures

  2) checksummers

  - a kind of "change" detection
  - keeps a whitelist of all authorized executables on the system with checksums(typically, a hash function) of the original versions
  - malware watches out for system calls used by checksummers and avoids being detected whenever a check is done (restore infected files back to originals ..)

Malware: Change Detection

- Malware must live somewhere and modify some files on the system in most cases
- If you detect a file has changed, it might have been infected
- How to detect changes?
  - hash files and (securely) store hash values
  - periodically re-compute hashes and compare
  - if hash changes, file might be infected
- Advantages
  - virtually no false negatives
  - can even detect previously unknown malware
- Disadvantages
  - many not-infected files change - and often
  - many false alarms (false positives)

Malware

- Countermeasures

3) anomaly detection

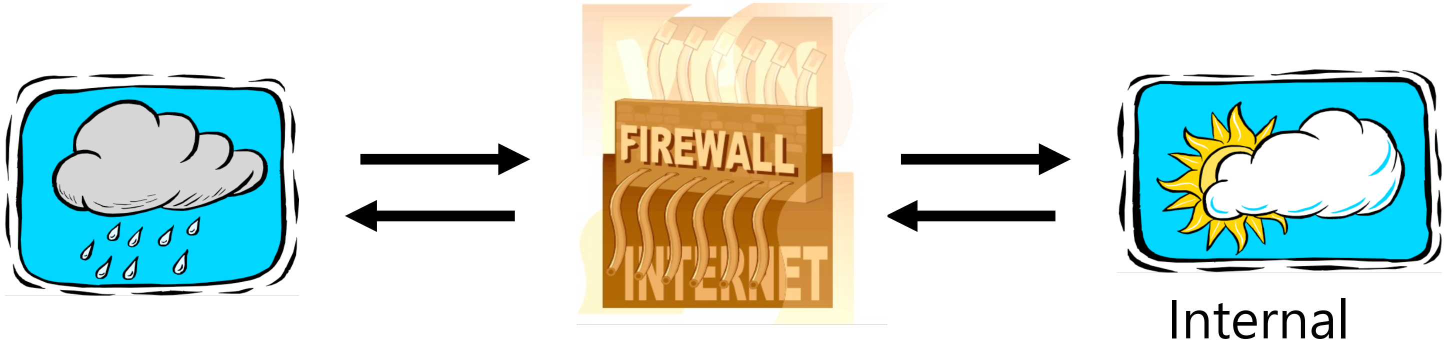
- Monitor system for anything “unusual” or “malware-like” or “potentially malicious” or …
- Examples of “unusual”
  - files change in some unexpected way
  - system misbehaves in some way
  - unexpected network activity
  - unexpected file access, etc.
- But, we must first define “normal”
  - normal can (and will) change over time

Malware: Anomaly Detection

- Advantage
  - chance of detecting unknown malware
- Disadvantages
  - needs a lot to be done to prove its effectiveness
  - adversary can make abnormal look normal
  - not used alone and should be combined with another method (eg. scanners-based detection)
- Not an easy problem at all, but
  - ML techniques actively adopted in this area of research

Networking Tools for Monitoring

- Firewall



Internet

Firewall

Internal network

- firewall decides what to let into internal network and what to let out
- access control feature(to stop known malware and network exploits)

vs. intrusion detection : to monitor your networks and/or machines for indicators of compromise so you can catch the stuff that got through

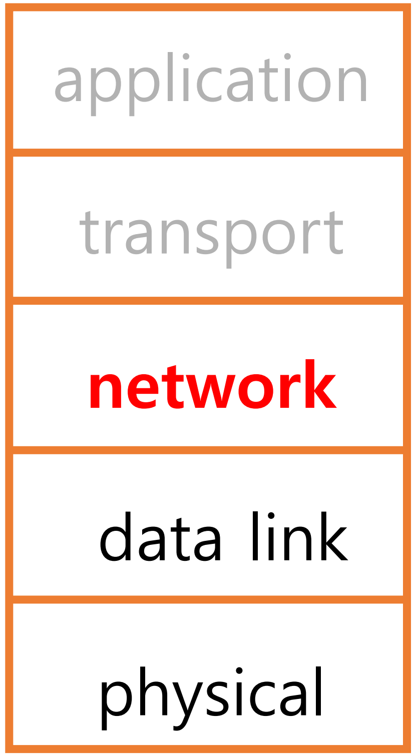
Firewall Classification

- No standard firewall terminology
- Depending on where they operate on
  - Packet filter: works at network layer (IP)
  - Circuit Gateway: at transport layer (TCP)
  - Application proxy: at application layer
- Other terms often used
  - eg, “deep packet inspection” firewall …
    - -> do not put too much trust on it before you fully understand the very details of the product

1) Packet Filter

- Operates at network layer
- Inspects
  - Source IP address
  - Source Port #
  - Destination IP address
  - Destination Port #
  - Flag bits (SYN, ACK, etc.)
  - Egress or ingress
- Ensuring
  - only 'local' packets leave a network
  - only 'foreign' packets enter a network
  - block traffic to/from 'known' bad IP addresses
  - block all traffic except that arriving on specific ports

…



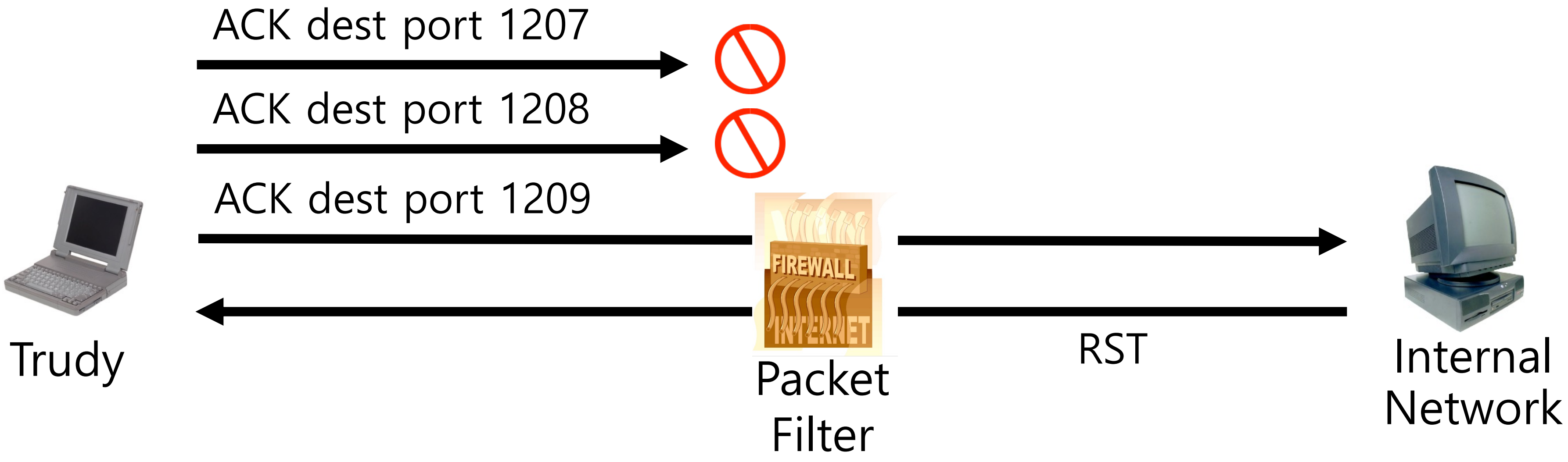
1) Packet Filter

- Advantages
  - Speed
- Disadvantages
  - IP addresses can be spoofed
  - Port numbers are often used to distinguish different machines under a NAT device
  - blind to TCP connections or application data
  - maintaining a blacklist is difficult since IP addresses can change (eg. by switching ISPs, …)

TCP ACK Scan against Packet Filter

- Attacker scans for open ports thru firewall
  - Port scanning is *first step* in many attacks
- Attacker sends packet with ACK bit set, without prior 3-way handshake
  - violates TCP/IP protocol
  - ACK packet pass through packet filter firewall
  - appears to be part of an ongoing connection
  - RST sent by recipient of such packet

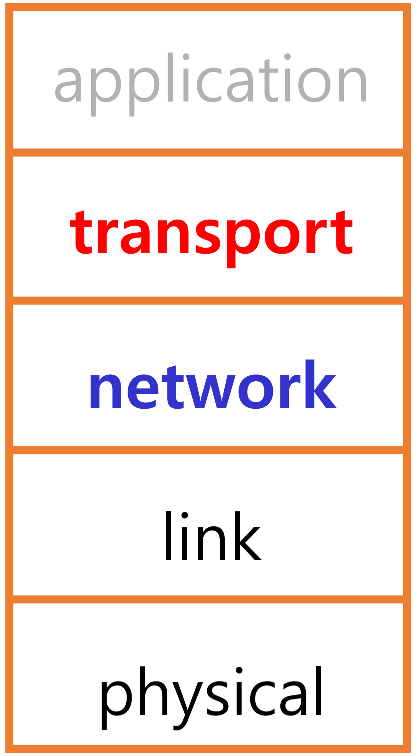
TCP ACK Scan against Packet Filter



- Attacker knows port 1209 open thru firewall
- A “stateful” firewall can prevent this

2) Circuit Gateway

- Adds state to packet filter
- Operates at TCP
  - reassembles and examines all the packets in each TCP session
  - remembers TCP connections, flag bits, etc.
- Advantages
  - can do everything a packet filter can do plus…
  - keep track of ongoing connections(so can prevent TCP ACK scan)
- Disadvantages
  - cannot see application data
  - slower than packet filtering



application

transport

network

link

physical

3) Application Proxy

- A proxy is something that acts on your behalf
- Application proxy looks at incoming application data

  eg. mail filters that try to block spam or macros from attached Word file, or web proxies that block or remove undesirable content
- Verifies that data is safe before letting it in
- Eg. Great Firewall of China – tried to block mail and

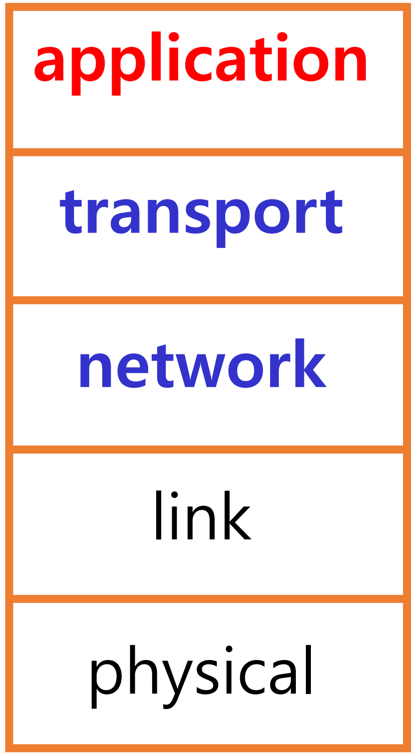
  web content that refers to banned subjects

  (through the 2000s ~)
- Advantages

  - full view of connections and applications data

  - filter bad data at application layer (worms, …)
- Disadvantages

  - very slow (could be a source of big performance degradation)



application

transport

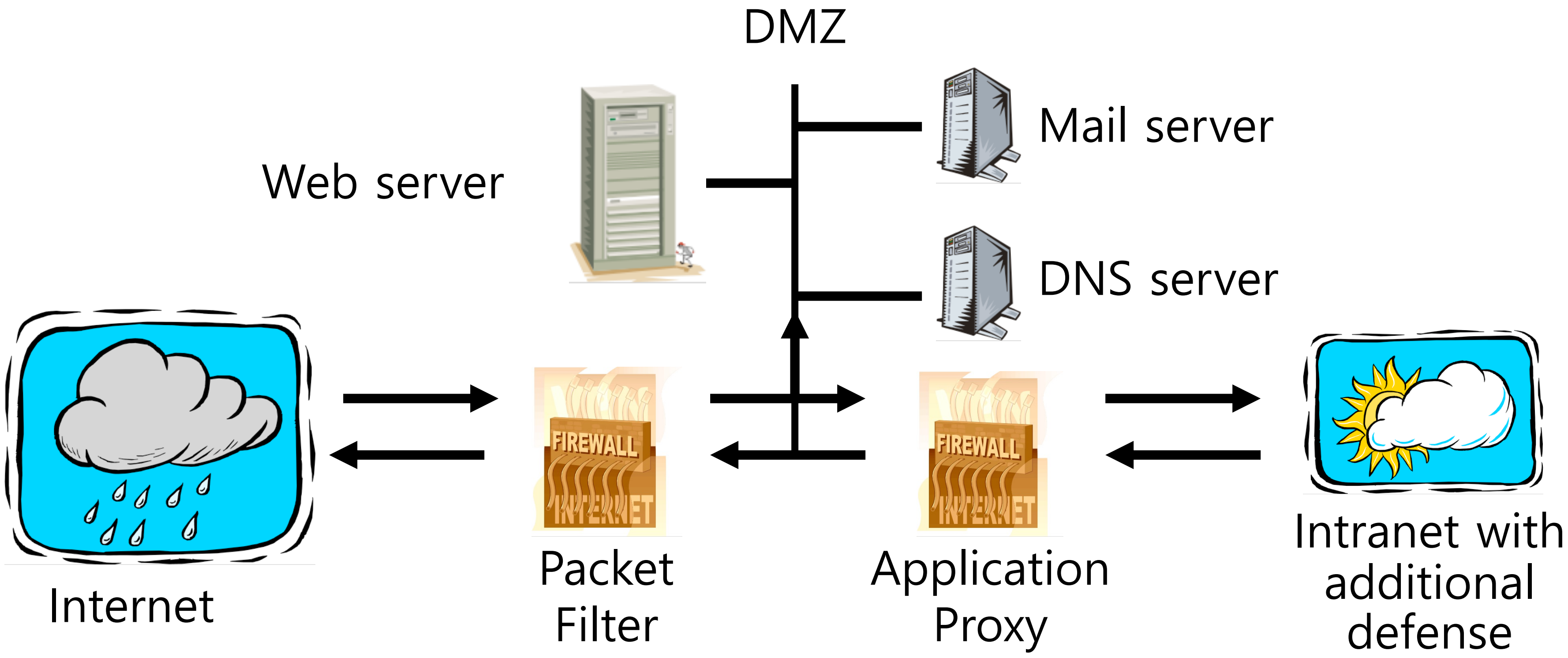
network

link

physical

Firewalls and Defense in Depth

Example. A Typical network security architecture



Two Basic Questions on Intrusion Detection

- Who is likely intruder?
  - may be outsider who got through firewall
  - may be evil insider
- What do intruders do?
  - launch well-known attacks
  - launch variations on well-known attacks
  - launch new/little-known attacks
  - “borrow” system resources
  - use compromised system to attack others. etc.

Networking Tools for Monitoring

- Intrusion Detection Systems (IDS)

  - a networking device sits on your network and look for signs of an attack in progress or a compromised machine

    eg. Signs of an attack

    i) machine trying to contact an IRC channel used to control a botnet, or a known bad IP address, or trying to resolve a known bad DNS name

    ii) packets with forged source addresses such as packets claiming to be from outside but that actually originate from inside

    iii) spam coming from a machine in your network

  - tells the sysadmin to look at a particular machine or a particular subnet

Networking Tools for Monitoring

- Intrusion Detection Systems (IDS)
  - how to detect intrusions?

    i) **misuse detection**

    · models the likely behavior of an intruder

    eg. banking system alarms if someone draws max. amount from a cash machine on 3 successive days

    eg. Unix alarms if a naïve user suddenly starts to use sophisticated tools like debuggers, dumps, …

    · looks for a 'signature' – a known characteristic of a specific attack – which can be either explicit in data

    (eg. a substring of an executable) or in behavior (eg. machine contacting a known bad IP address of a botnet)

    · can take a number of signatures as signals and train a ML classifier to make the decisions

    · reminds of scanners-based malware detection

Networking Tools for Monitoring

- Intrusion Detection Systems (IDS)

  - how to detect intrusions?

  ii) **anomaly detection**

  - looks for anomalous behavior in the absence of a clear model of the attacker's line of actions
  - detects attacks that have not been previously reported
  - it is very hard to define 'normal', if at all possible, and normal-ness can and will change over time
  - attacker may convince IDS that an attack is 'normal' by keep training it very slowly so as not to cause an alarm
  - ML techniques take a role here as well

Networking Tools for Monitoring

- Intrusion Detection Systems (IDS)
  - how to detect intrusions?

    ii) **anomaly detection**

    · advantages

    - chance of detecting unknown attacks

    · disadvantages

    - cannot use anomaly detection alone(well, not yet) and should be used with 'misuse' detection altogether
    - IDS itself can be subject to attack
    - no sufficient proven record showing its effectiveness
    - indicates "something unusual", but lacks specific info on possible attack(characteristics of the attack)

Q & A

aiclasshongik@gmail.com