

# Network Security

# Instructor and AI

- **Instructor: Professor Yeonjoon Lee**
  - Office: 제 3 공학관, 504호
  - Email: yeonjoonlee@hanyang.ac.kr
  - Office hour: Right after class or by appointment
- **Class meeting time and location:**
  - 수업: Monday 15:00 PM – 17:00 PM (제 1공학관, 305 강의실)
  - 실습: Tuesday 15:00 PM – 17:00 PM (제 4공학관, PC1 실)
- **Als:**
  - 이석원 (sevenshards00@gmail.com)
  - Office hour: Will be announced later
- Slides: <https://github.com/luc2yj/HY-CSE4047>

# Tell me what you want from the class

- Your name
- Your cognate, program
- What do you expect from the class?
  - Credits only?
  - Know something about security
  - Some hands-on experiences
    - To which extent?
- What's your capability?
  - Programming (especially C)?
  - Operating systems?
  - Networking?

# Course Objectives

- Introduction to information security
  - Give you a general survey of security and privacy technologies
  - Help you understand the basic concepts, ideas
  - Prepare you for taking more advanced security courses
- Try to offer some “experience” of security technologies
  - Get some hands-on experience on threats and defense
  - Capture the trend of some security threats
  - Learn how to do security-related research

# Prerequisites

- You will be able to fully enjoy the fun of the course if you have the following skills:
  - Programming, especially C
  - Operating systems
  - Networking

# Why should I take this course?

- For job interview
- Learn the basics about protection of your computers
- For taking more advanced security courses

# Textbook

- *Computer Security: Principles and Practice (3rd or 4th Edition)*, by William Stallings and Lawrie Brown
  - There is [online version](#) for 3<sup>rd</sup> Edition
- [\*The Security Development Lifecycle\*](#), Michael Howard and Steve Lipner
- Additional materials on slides
- Articles from the web (your reading project)

# Grading

- Class attendance (10%)
- Weekly lab assignments (25%)
- Reading projects (25%)
  - Project proposal (20%)
  - Project report (80%)
  - Presentation (TBD)
- Final (40%)



# Policies for Class Attendance

- Points that are subtracted from the total points for the semester associated for non-attendance will commence ONLY after 2 unexplained absences.
- Besides these two classes, you can ask for medical leave if you can provide proper evidence (see the course website).
- Otherwise, you will lose 3 points whenever you miss one class.

# Policies for Class Participation

- You are expected to actively engage in class
- Lectures are intended to be interactive, involving discussion
- Ask questions, participate in discussion, don't look at your laptop

# Reading projects

- Review and analyze existing security technologies
  - One or Two students (with different expectations, see course website)
  - Bonus could be given to the project involving implementation and evaluation
- Suggested topics will be posted on the web, but you are encouraged to come up with your own topics

# Ethics and Cheating

- Ethics

DO NOT TRY HACKING EXPERIMENTS ON PUBLIC NETWORKS!!!

- Cheating Policy

학교 규정에 따라 처리

# Caution!!!

- Lesson: DO NOT TRY HACKING EXPERIMENTS ON PUBLIC NETWORKS!!!

# Tentative Arrangement

- Basic concepts: 2 weeks
- Authentication and access control: 2 weeks
- Database and Web security: 2.5 weeks
- Malware: 1 week
- Buffer overflow and defense: 2.5 weeks
- Security development lifecycle: 1.5 weeks
- Final talk: To be discussed

# Tentative Arrangement (cont'd)

- Quizzes and labs start from Week 2
- Reading assignments will be posted online
- Reading Project
  - Proposal: 2019/10/7
  - Final report: Will announce later (2019/11/17)
  - Final presentations: To be discussed

# Reading Project Topic Examples

- Android Security
  - Detection approaches
  - Vulnerabilities
  - Type of malware
- IoT Security
  - Study on platforms (e.g., smartthings)
  - Study on the type of threats
- Cloud Security
- Threats on Autonomous Vehicles
- Cybercrime (e.g., Dark web, Crowdturfing)



# If you want to build something..

- Let me know!
- NLP related things
- GUI automation
- Reverse Engineering
- Static or Dynamic analysis

# Questions?

# Basic concepts

# What is security?

- Protect information assets from intentional human misuses
- Information assets: valuable computing resources
  - Hardware: CPU, disk, network adapter card, etc.
  - Software: Operating System, utilities, applications, etc.
  - Data: files, database, password, etc.
  - Communication facilities and networks: link, bridge, router, etc.

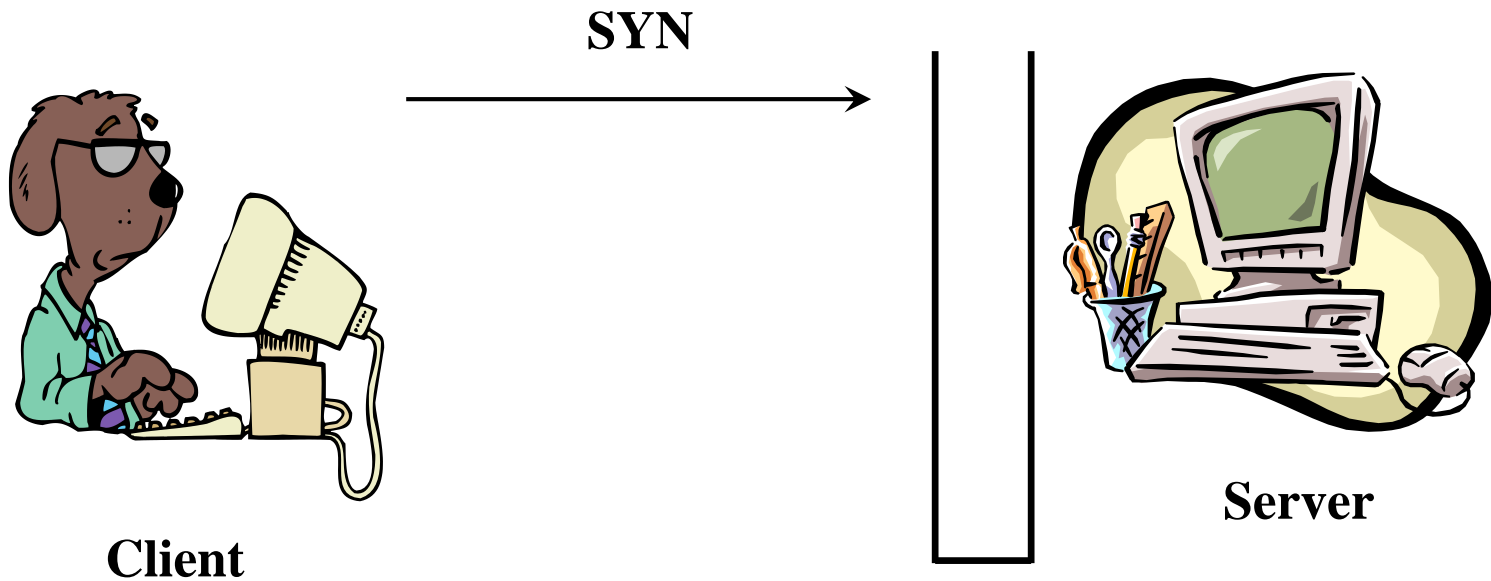
# Security concerns

- Information assets could be easily abused
  - Break into your systems to steal confidential data
  - Destroy your valuable files
  - Spy your communication
  - Squander your resources ...
  
- Principle of easiest penetration (Magenot **Line**):
  - An intruder must be expected to use any available means of penetration, not necessarily from the most obvious one or the one against the most solid defense

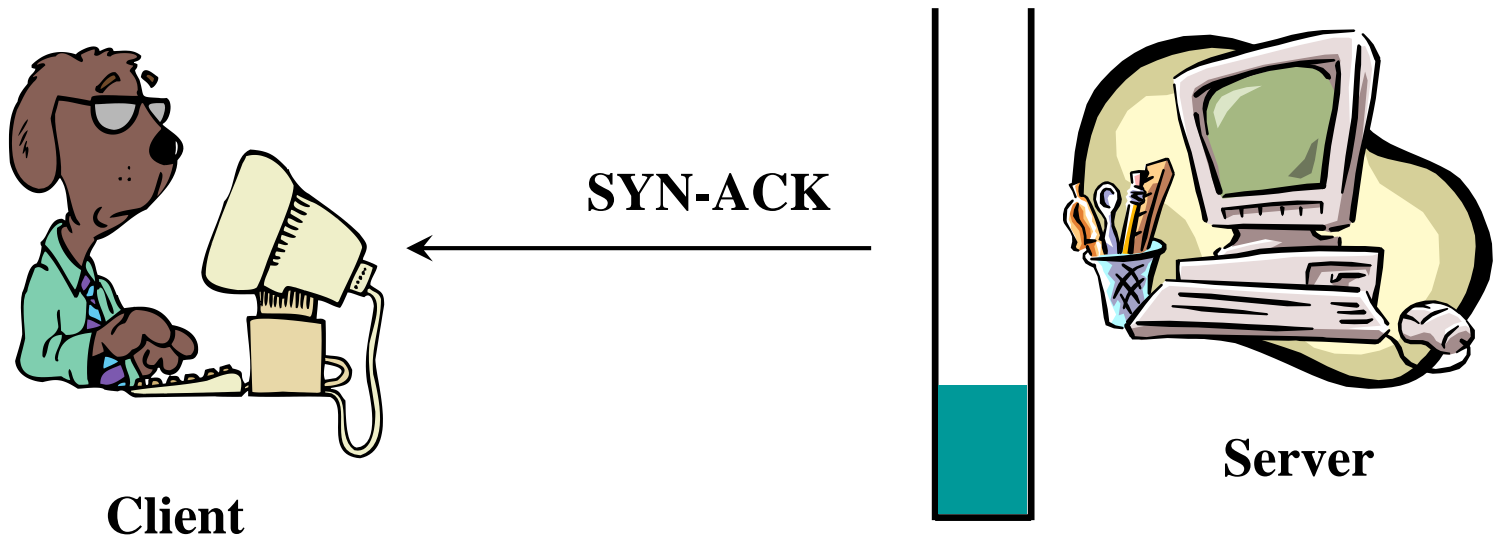
# Vulnerability, Threat, Risk and Attack (RFC4949)

- Vulnerability: weakness in the security system
  - Corruption, leakage and unavailability
  - e.g., software bugs, defense holes...
- Threat: a set of circumstances that has the potential to cause exploit of vulnerabilities and damages to information assets
- Risk: Loss as the probability that threat causes harm
- Attack: an assault (evading protection, violation of policy) on system that derives from a threat

# Example: TCP three-way handshaking

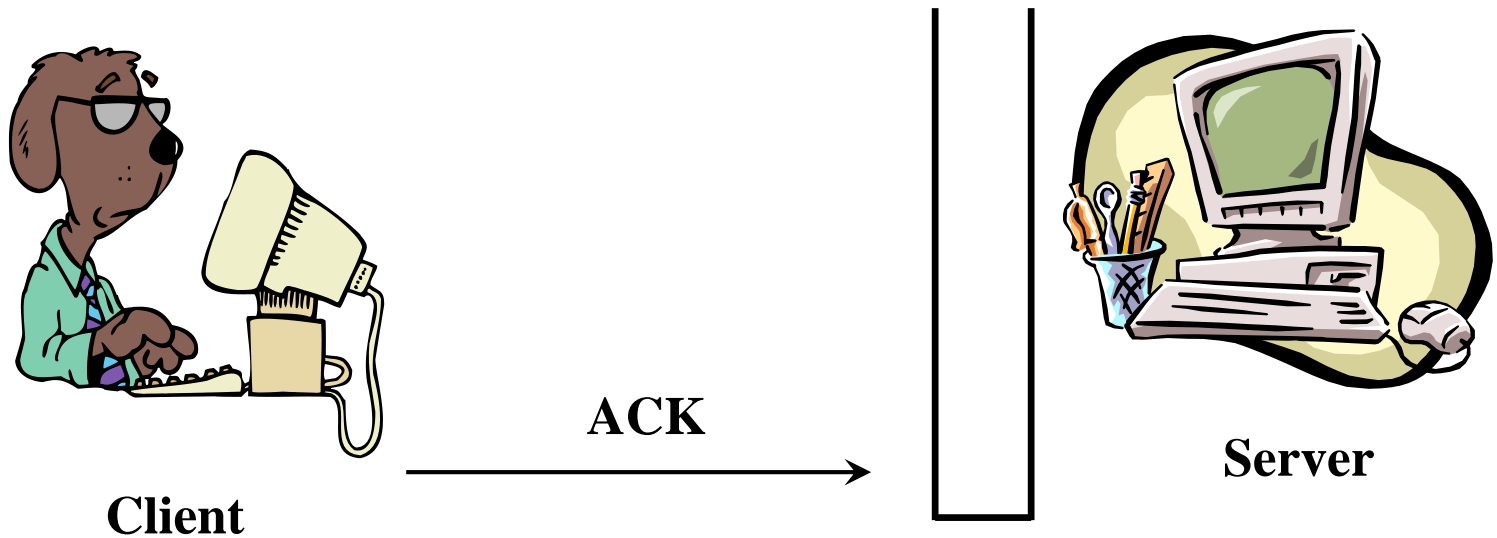


# Example: TCP three-way handshaking

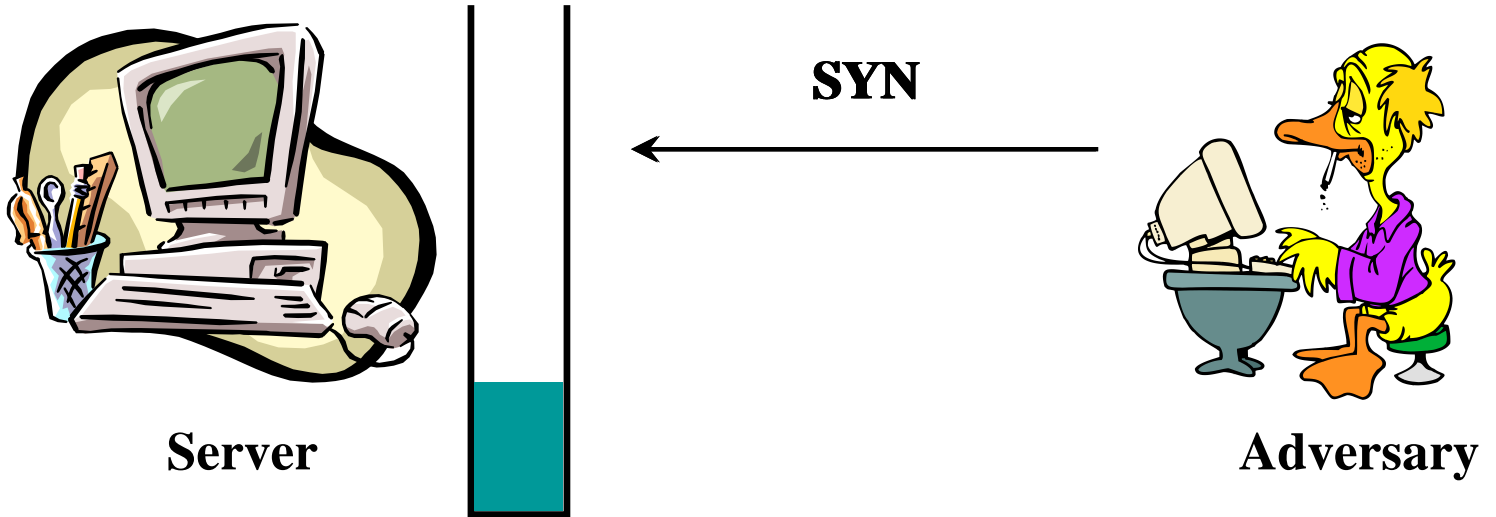




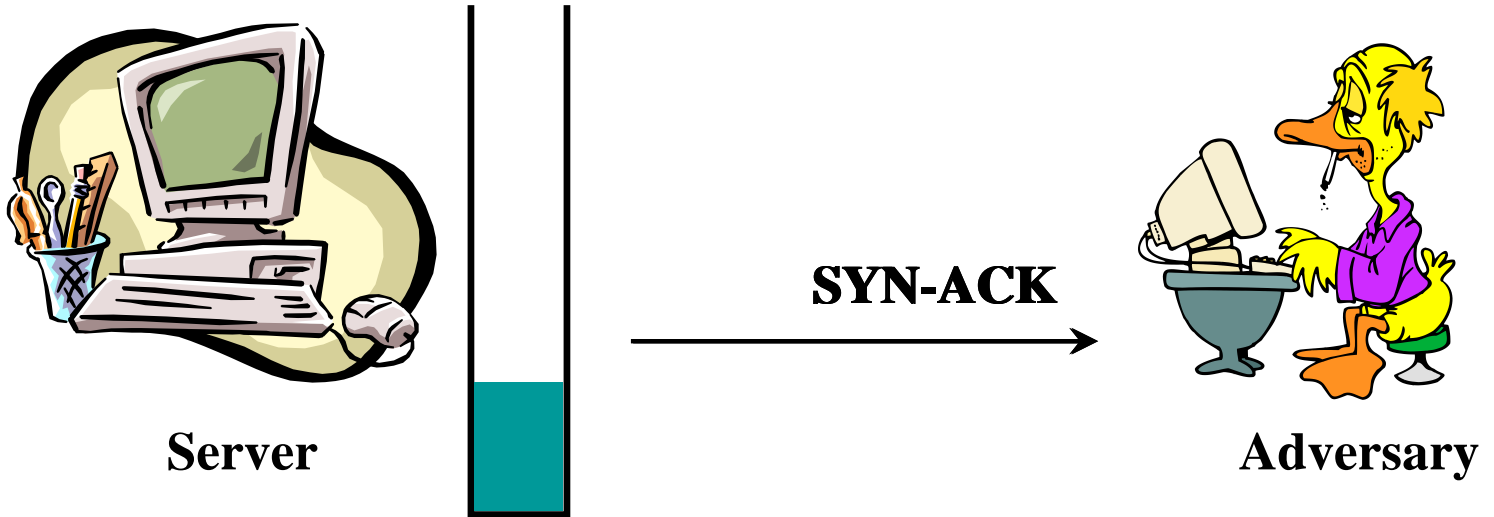
# Example: TCP three-way handshake



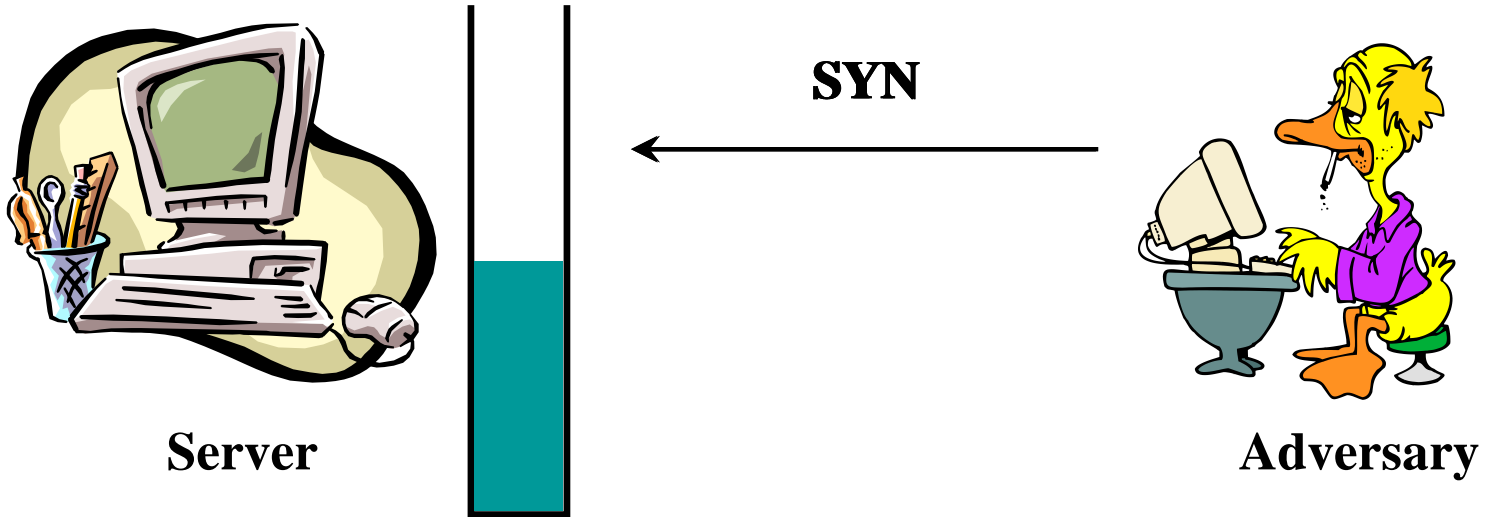
# Syn-flooding!



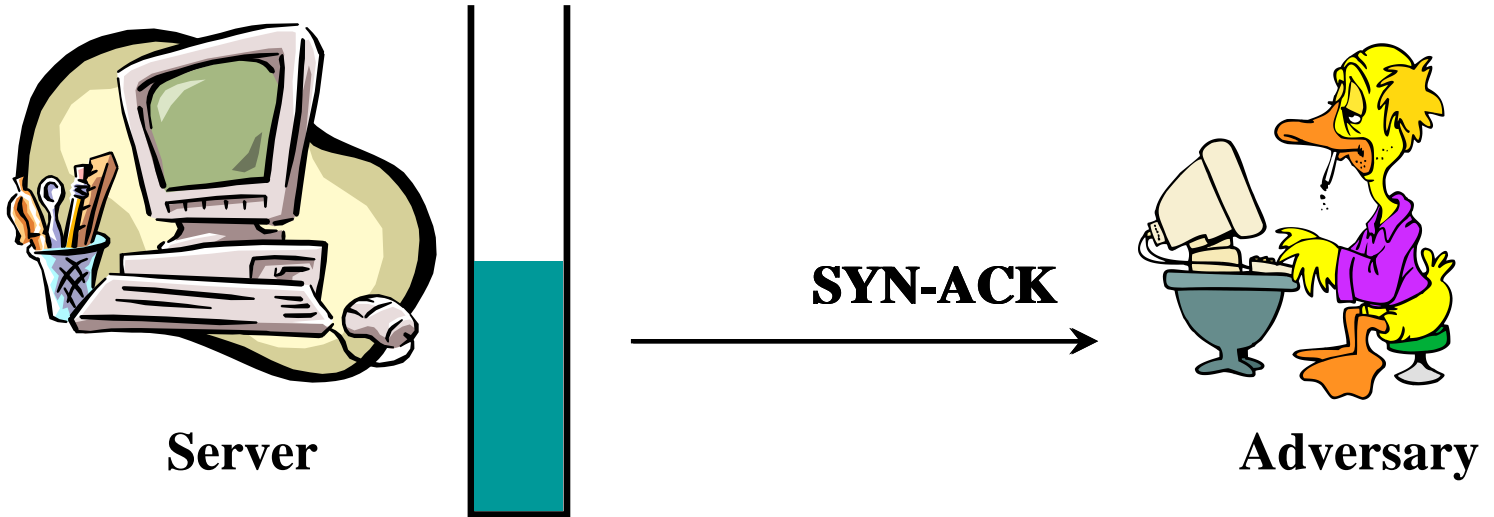
# Syn-flooding!



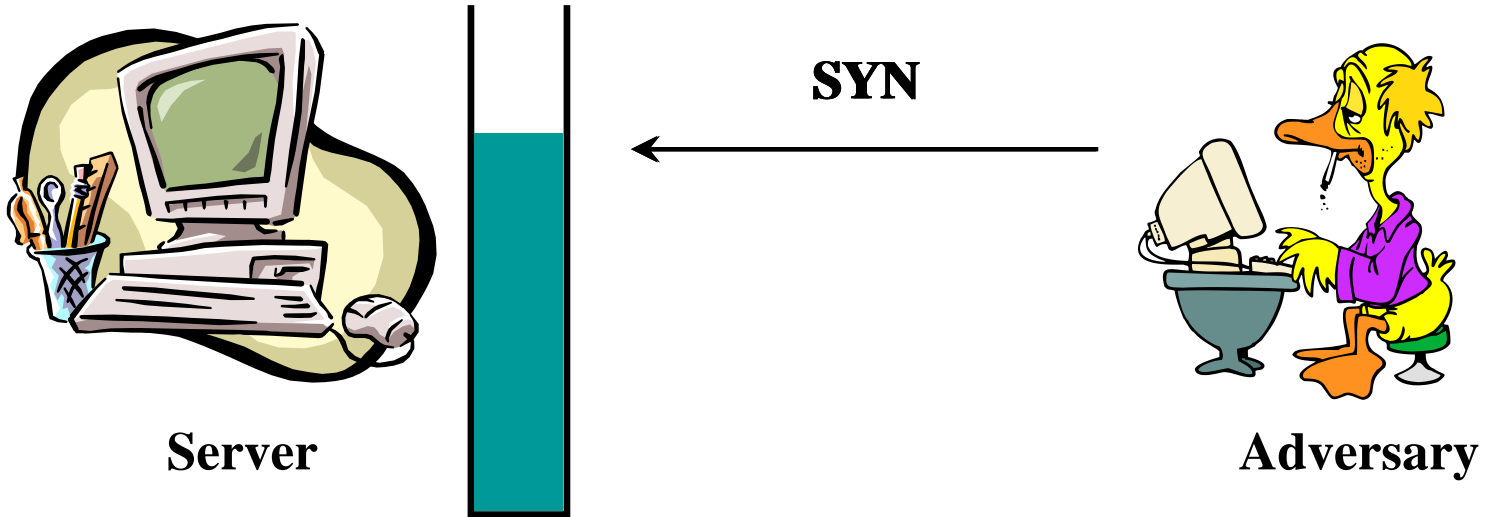
# Syn-flooding!



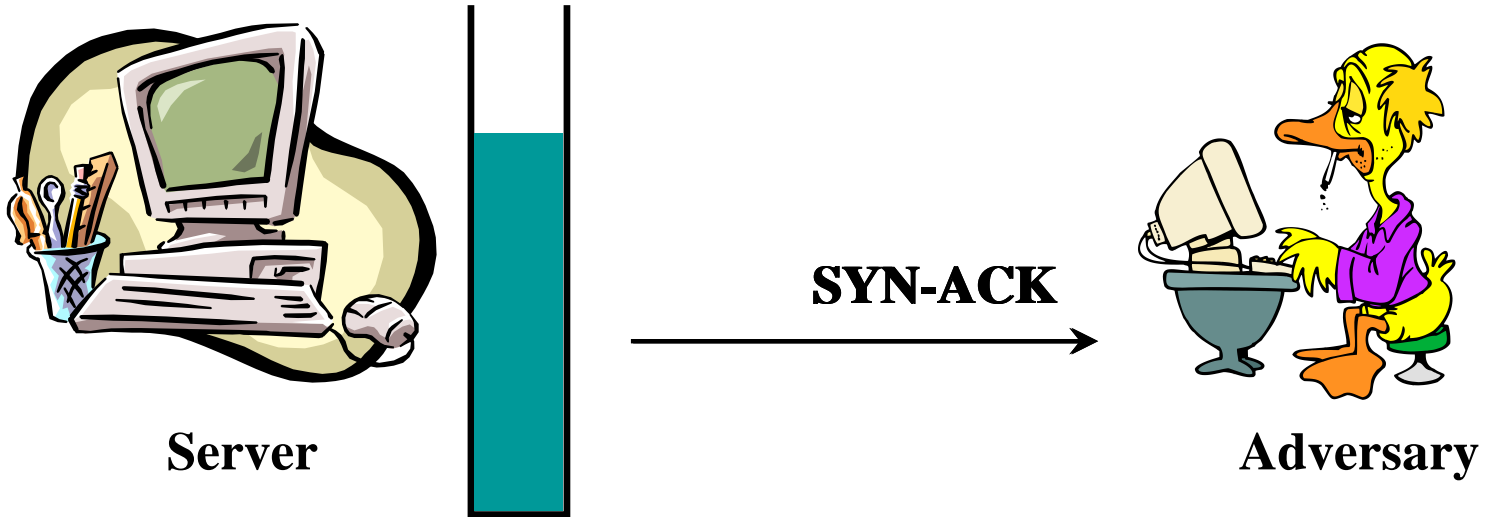
# Syn-flooding!



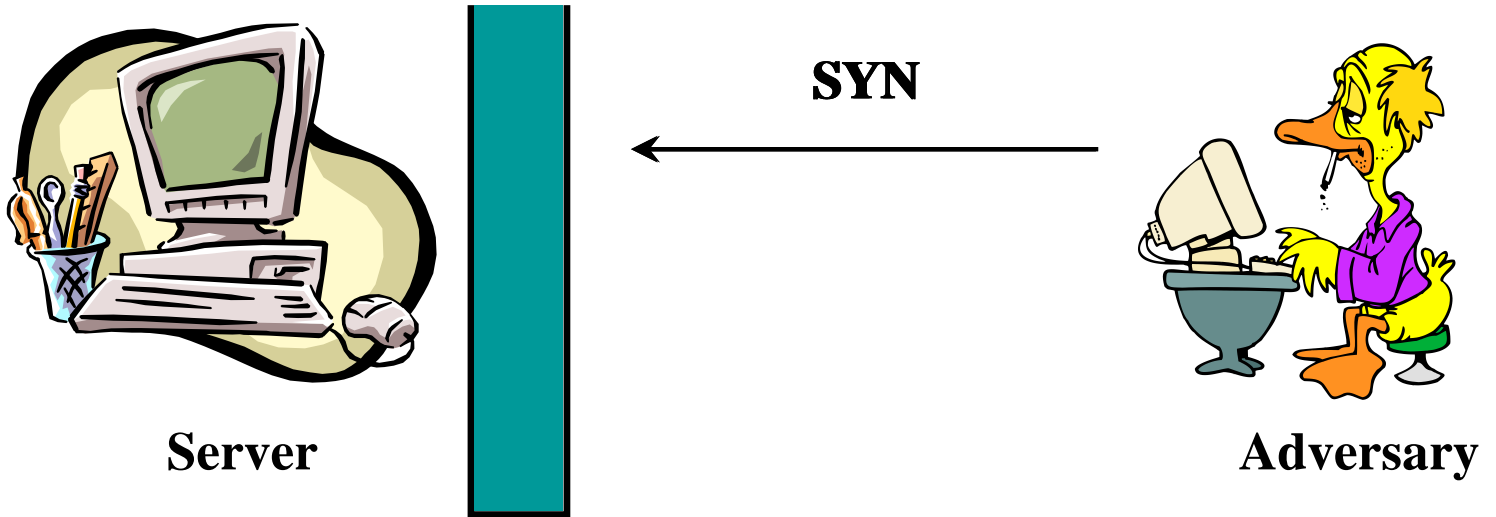
# Syn-flooding!



# Syn-flooding!



# Syn-flooding!





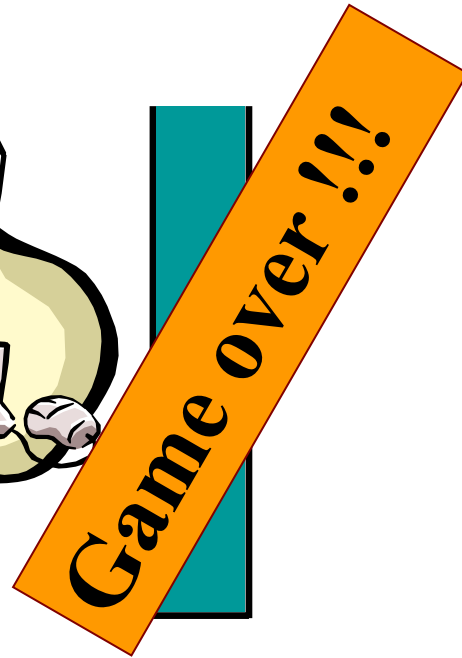
# Syn-flooding!



# Syn-flooding!



Server



Adversary

# Attack Surfaces

- Reachable and exploitable vulnerabilities
- General categories:
  - Network surface: e.g., open ports, services on the inside of a firewall
  - Software surface: e.g., code processing incoming data
  - Human surface: gullible employee access to sensitive data

# Threats

- Unauthorized disclosure
  - Exposure, Interception, Inference, Intrusion
- Deception (false data accepted as true)
  - Masquerade, falsification, repudiation
- Disruption (aiming at availability or integrity)
  - Incapacitation (physically disable system), corruption (system modification), obstruction (interfere with communication)
- Usurpation (unauthorized system control)
  - Misappropriation (theft of service), misuse (unauthorized system access)

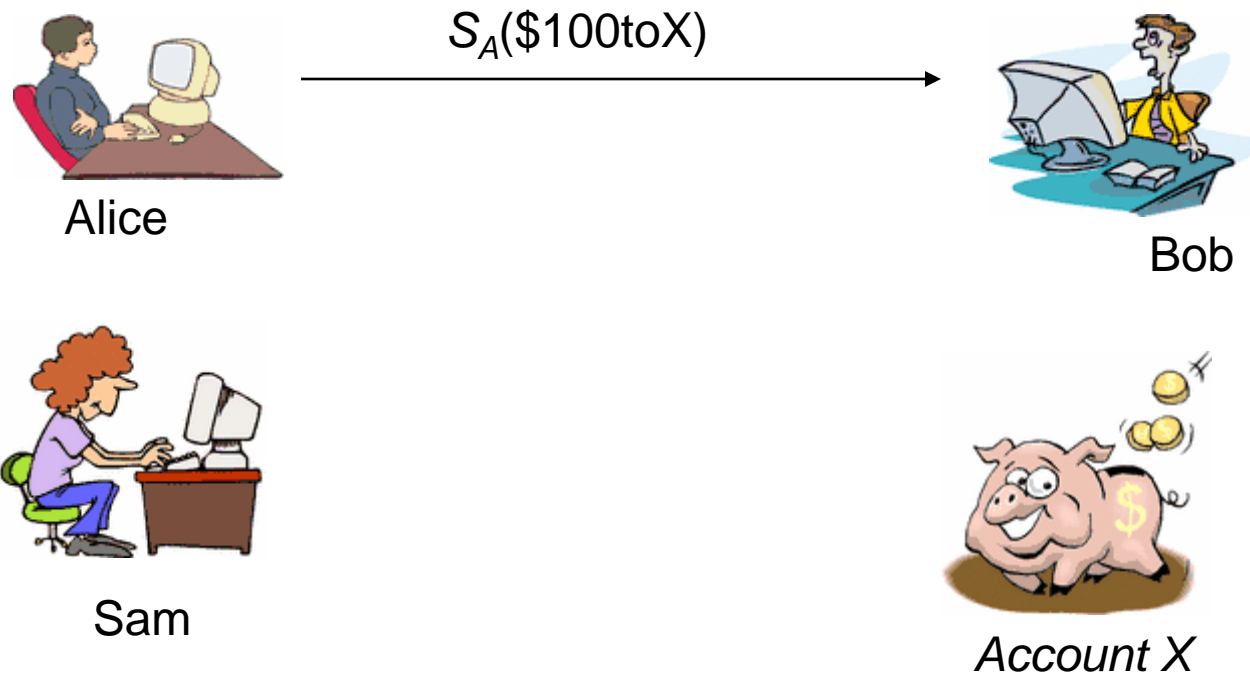
# Threat Examples

- Interception
  - Unauthorized access to assets
  - e.g., someone gets to know my salary
- Obstruction
  - Make assets unavailable
  - e.g., someone prevents me from getting my pay checks
- Fabrication
  - Tamper with assets or even create counterfeit objects
  - e.g., someone changes the amount on my pay check to 100,000,000 won!

# Attacks

- From the way attack is carried out
  - Active attack: affect a target system's operation
  - Passive attack: learn information without affecting system
- From the origin of the attack
  - Insider attack: authorized users do bad things
  - Outsider attack: unauthorized parties gain access

# Active Attack Example: Replay



# Active Attack Example: Replay



Alice



Sam



Bob

\$100



*Account X*



# Active Attack Example: Replay



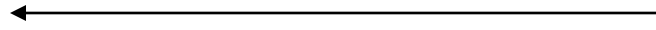
Alice



Bob



Sam

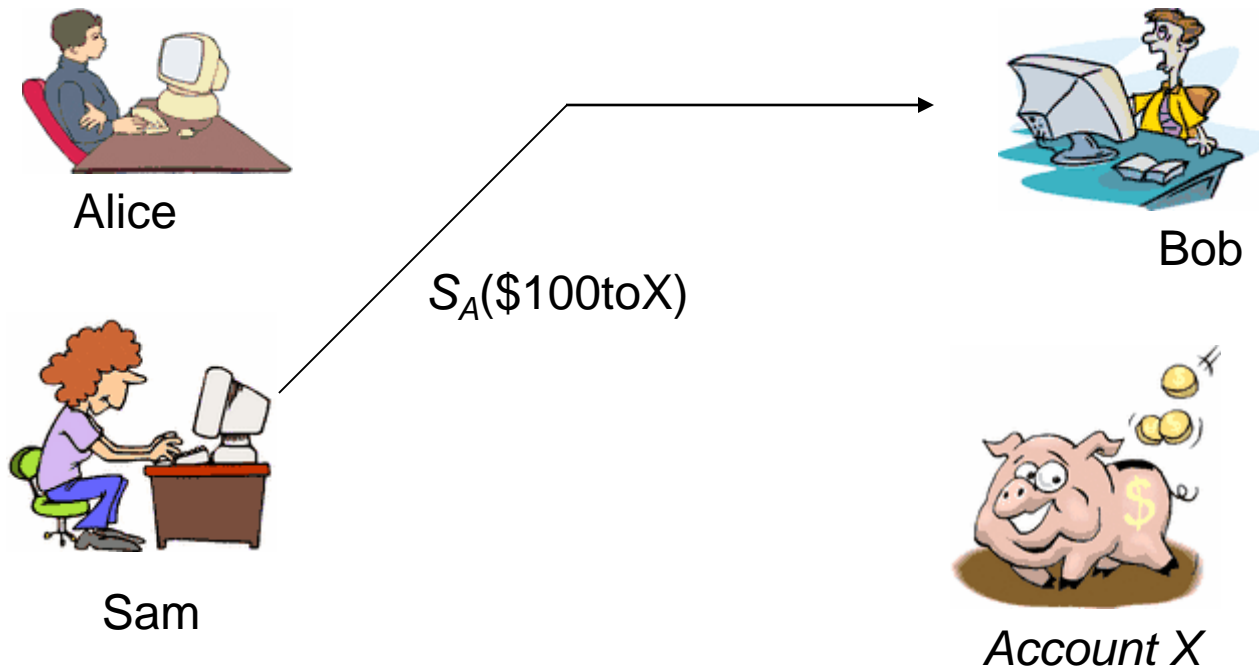


\$100



Account X

# Active Attack Example: Replay



# Active Attack Example: Replay



Alice



Sam



Bob

\$100



*Account X*

# Active Attack Example: Replay



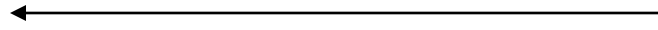
Alice



Bob



Sam



\$100



Account X

# Passive Attack Example: Inference

- Side-channel leaks in encrypted wireless communication

<http://www.youtube.com/watch?v=3sGH9KpYOJk>

- Side-channel leaks in online health information systems

[http://www.youtube.com/watch?v=Aklb4\\_ibB64](http://www.youtube.com/watch?v=Aklb4_ibB64)

# Security Goals: CIA Triad

- Confidentiality: information is protected from unintended disclosure
  - Data: information is not disclosed to unauthorized parties
  - Privacy: control of one's own information disclosure
- Integrity: system and data are maintained in a correct and consistent condition
  - Data: information and code only changed by authorized parties
  - System: system operates without unauthorized inference
- Availability: systems and data are usable when needed

# Security Goals (cont'd)

- A secure system needs to balance confidentiality, integrity and availability
- These goals may overlap or be exclusive, dependent on the situations
  - E.g. Dividing data into  $n$  shares increases confidentiality but reduces the availability

# Additional Security Goals

- Authenticity

- Property of being verified and trusted
- E.g., authentication

- Accountability

- Action uniquely traced back to the responsible party
- E.g., nonrepudiation, deterrence, fault isolation, intrusion detection prevention, etc.



# How to achieve security goals?

- Security controls: including policy and mechanism
- Security Policy
  - A formal statement of rules and practices
  - Specify how information assets are protected
- Security Mechanism
  - Method, tool or procedure for enforcing the security policy

# Security mechanisms

- Cryptographic primitives
  - Encryption helps achieve confidentiality
  - Digital signature helps achieve integrity
  - Client puzzle may helps achieve availability
- Security protocols
  - Authentication
  - Access control

# Security mechanisms (cont'd)

- Security systems
  - Software security
  - Network security
  - Privacy preserving system
- Incentive engineering
  - Consider human factors

# How to choose security control?

- There is no free lunch:
  - Security control introduces costs
  - e.g., performance or payments
- Risk: the chance of attacks
- Tradeoff
  - Assess the loss of an attack
  - Assess the risk
  - Assess the value of assets
  - Assess effectiveness of a security control



# Pitfalls

- Identify incorrect threats
- Incorrect mapping of:
  - Threats → policy
  - Policy → mechanisms
- Changing environment invalidates assumptions!

# Trust

- A *trusted* system is one whose failure can break the security policy
- A *trustworthy* system is one that won't fail

# Assurance

- According to NIST Computer Security Handbook:

Assurance is degree of confidence that security measures work as intended to protect the system and information it processes

- Does security system design meet requirements?
- Does security system implementation meet specifications?



# Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation/Encapsulation/Modularity/Layering
- Least astonishment

# Proposal

- Proposal Deadline: 10/7 11:59pm
- Proposal Format
  - Single column
  - Single spacing
  - Font type: 바탕체
  - Font size: 10
  - Layout: 좌/우/위/아래 모두 20mm
  - Page limit: 2 pages
- Final Report Deadline: 11/24 11:59pm.
- Final Report template will be uploaded by 10/11.