Introduction to Computer Security

(ECE 458)

Vijay Ganesh

Spring 2014

Online Resources, Books, Notes,...

- Books
  - Introduction to Computer Security by Matt Bishop
  - Computer Security: Art and Science by Matt Bishop
  - Hacking: The Art of Exploitation by Jon Erickson
- Notes and slides
  - Course notes/lectures by Prof. Dan Boneh (Stanford)
  - Course notes/lectures by Prof. John Mitchell (Stanford)
  - Course notes/lectures by Prof. Bill Young (UT, Austin)
  - Course notes/lectures by Prof. Matt Bishop (UC, Davis)
- Websites
  - Website by Dan Bernstein (http://cr.yp.to/djb.html)
  - Website by Schneier (http://www.schneier.com/)

Goals of this Course (Syllabus)

- Theory
  - Foundational concepts in security (e.g., confidentiality, integrity,...)
  - Security policies (e.g., access control,...)
  - Basic crypto (e.g., public key cryptography, key management,...)
  - Principles of secure design (e.g., least privilege, fail-safe,...)

- Practice
  - Authentication (e.g., password schemes)
  - Forms of attack, Malware (e.g., viruses, worms, buffer overflow attacks)
  - Mechanisms to prevent/detect/recover from attacks (e.g., layout randomization)
  - Software engineering tools to improve security (e.g., vulnerability and information flow analysis, pen testing, language design)

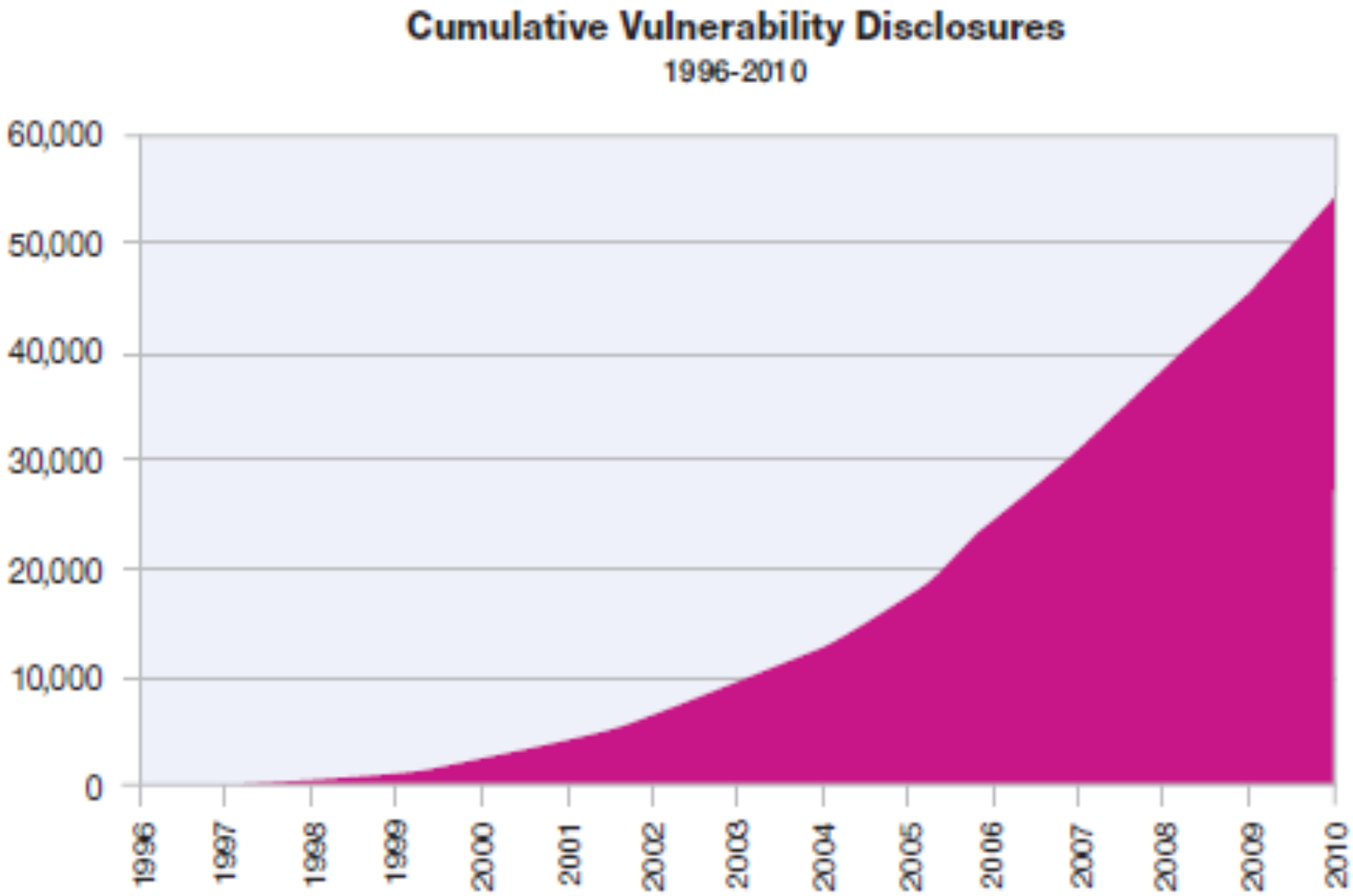
Topics covered in this Lecture

- Basic components of computer security
  - Confidentiality
  - Integrity
  - Availability
- Classes of threats
  - Disclosure
  - Deception
  - Disruption
  - Usurpation
- Policy vs. mechanism
  - Security policies, e.g., access control
  - Mechanism to implement the policy
- Goals of security
  - Prevention
  - Detection
  - Recovery
- Trust and assumptions

What is Security? Why is it Important?

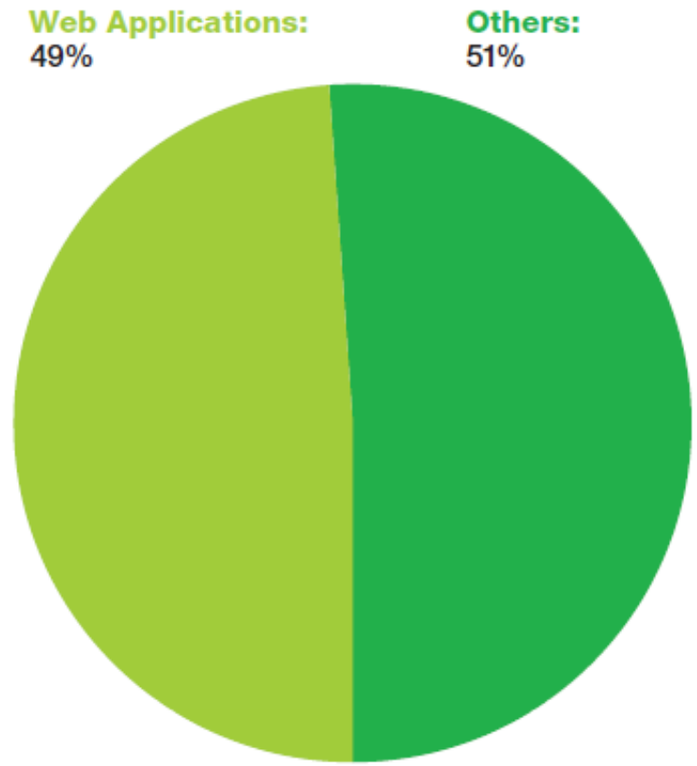
- What is computer security?
  - Often hard to define a field, esp. an evolving one
  - Techniques and mechanisms to "protect" systems and data from "threats"
  - Techniques to prevent, detect and recover from "threats" and "attacks"
  - Requires understanding of threat/attack models, policies, trust, assumptions, properties
- Motivation to study security
  - National defense
  - Espionage by corporations and nations
  - Increasing societal reliance on computers
  - Financial transactions are primarily electronic
  - Privacy issues related to health/financial records
  - Technically challenging (both theory and practice)

Lots of Vulnerable Applications



Source: IBM X-Force, Mar 2011

Percentage from Web applications



Data: http://cve.mitre.org/

Why is Security Hard?

- Thinking through all possible threat scenarios is difficult
  - Future-proofing a system is hard
  - Information systems are heterogenous, target-rich
  - Difficult to impose a uniform security policy
- Security often comes with a price, requiring trade-offs
  - Balancing security with system usability and efficiency
  - Designing, implementing and deploying security features is costly
  - Lots of buggy software that is expensive to fix
- Security ultimately is about risk management
  - Risk assessment (what are the threats, how much would they cost?)
  - How much are you willing to pay
  - Continuous re-assessment

Security Properties of Systems

- **Confidentiality**
  Concealment of information or resources

- **Integrity**
  Trustworthiness of data or resources (provenance)

- **Availability**
  Ability to use information or resource by "authorized" parties only

- **Authentication**
  Mechanisms to establish identity

- **Appropriate control**
  Mechanisms to unauthorized access and control of resources

- **Non-repudiation**
  Non-deniability of actions

Wait, what about...?

- Cryptography
- Digital signatures
- Access control
- Firewalls
  - Authentication through passwords
  - Digital certificates,...

These are mechanisms for providing confidentiality, integrity, availability, authentication,....

Confidentiality

- Concealment of information or resources
  - System makes it infeasible for unauthorized parties to "learn" concealed data or "access" resources
- Mechanisms to enforce confidentiality
  - Access control mechanisms support confidentiality
  - Encryption of data (decryption feasible only if key is available)
  - Data maybe in the clear, but resource requires authentication
  - Sometime even the existence of data (or occurrence of event) needs concealing
  - "Need to know" principle

Integrity

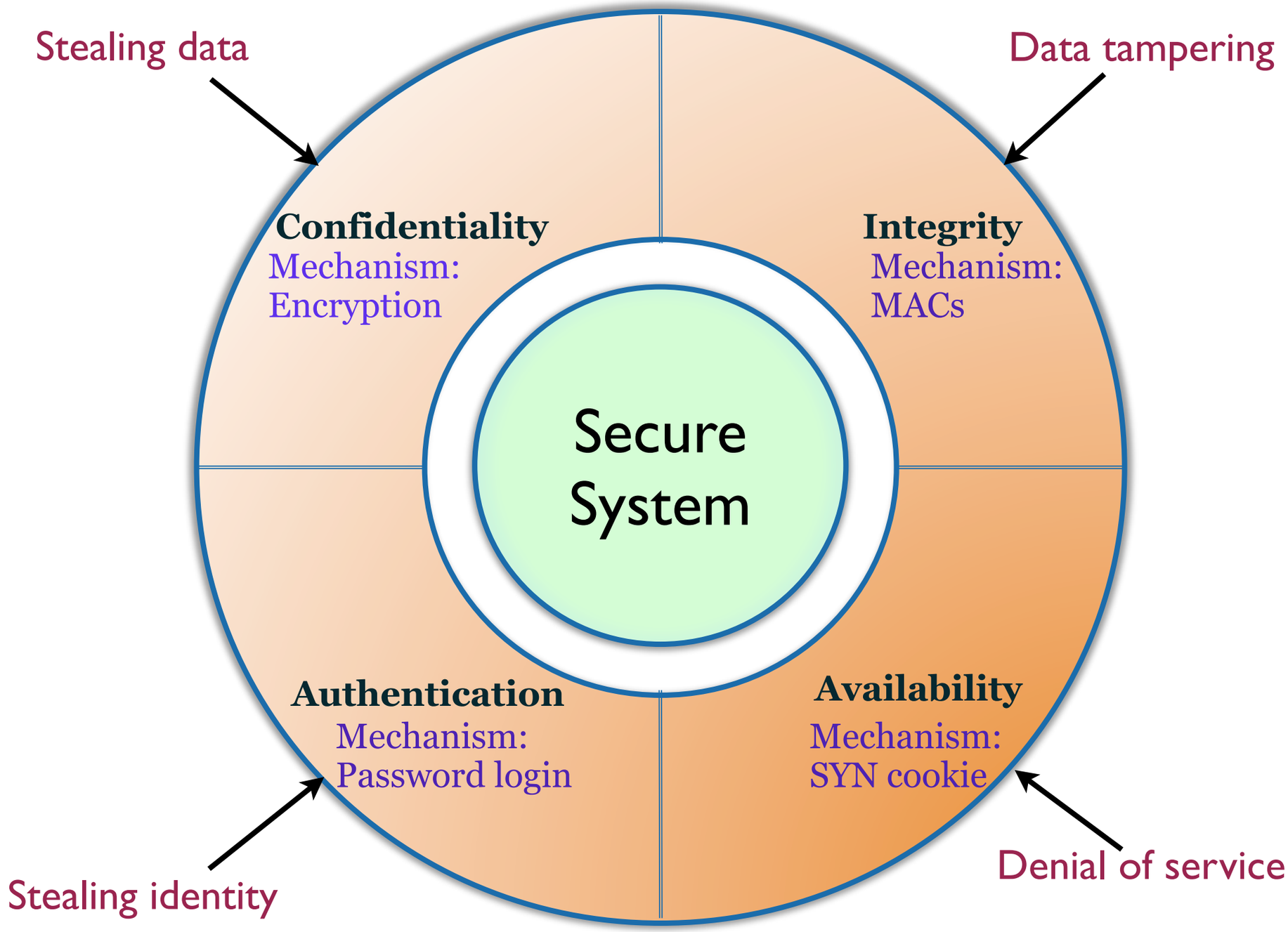
- Trustworthiness of data or resources
  - System prevents improper or unauthorized change to data
  - Data integrity: Data has not been "tampered" with
  - Origin integrity: The source of the data is "verifiable"
- Mechanisms to enforce integrity
  - Prevention mechanisms
    - Block unauthorized attempts to change data (e.g., password protection)
    - Block attempts to change data in unauthorized ways (e.g., change policy)
  - Detection mechanisms
    - Detect unauthorized attempts to change data (e.g., MACs)
    - Detect attempts to change data in unauthorized ways (e.g.,MACs)

Availability

- Ability to use the information or resource by authorized parties only
  - System ensures availability of information or resource
  - Attacker may attempt denial-of-service (DOS)
  - Attacker may exploit hidden assumptions to force DOS
  - Attacker may exploit vulnerabilities to take control of resource and make it unavailable to authorized users (e.g., control-hijacks)
- Mechanisms to ensure availability with high probability
  - Force attacker to pay a price for every DOS attack attempt (e.g., use of SYN cookies to protect against simple DOS attack)
  - Detection mechanisms: statistical models of normal behavior
- Hard to detect/prevent DOS attacks(esp. distributed)

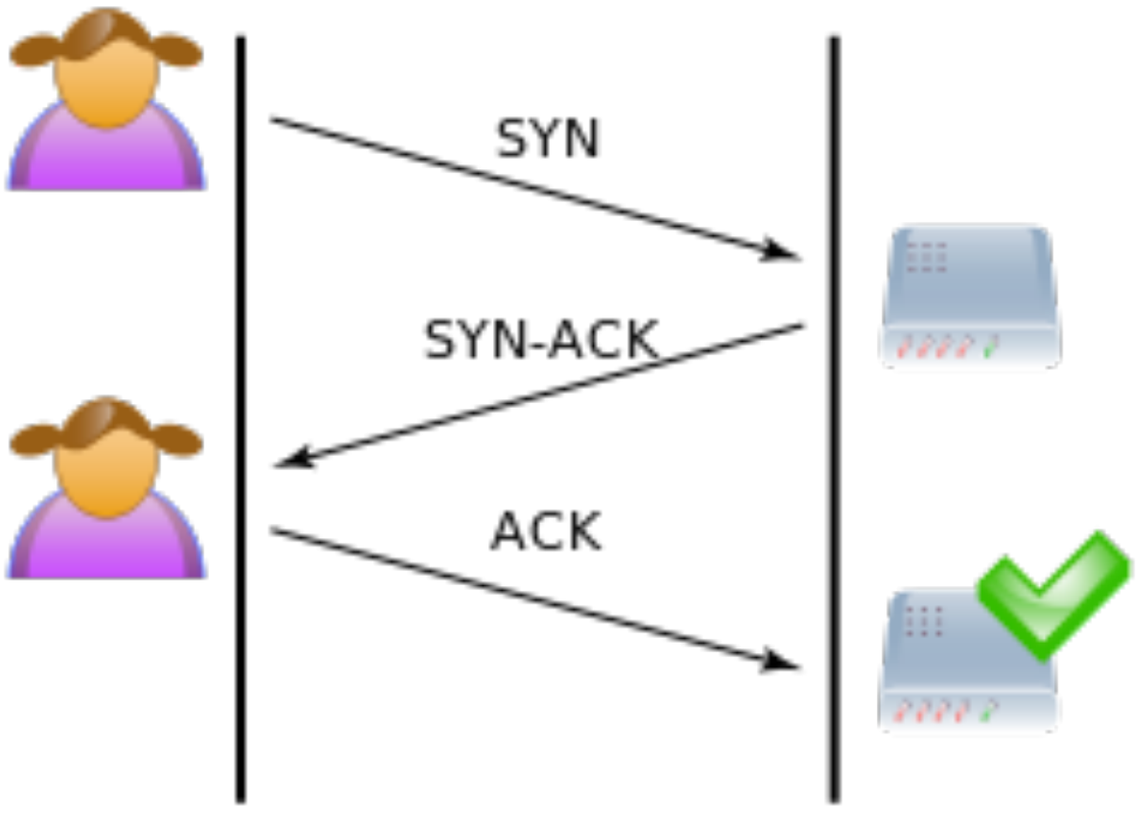
What is Computer Security?

Prevent, Detect and Recover

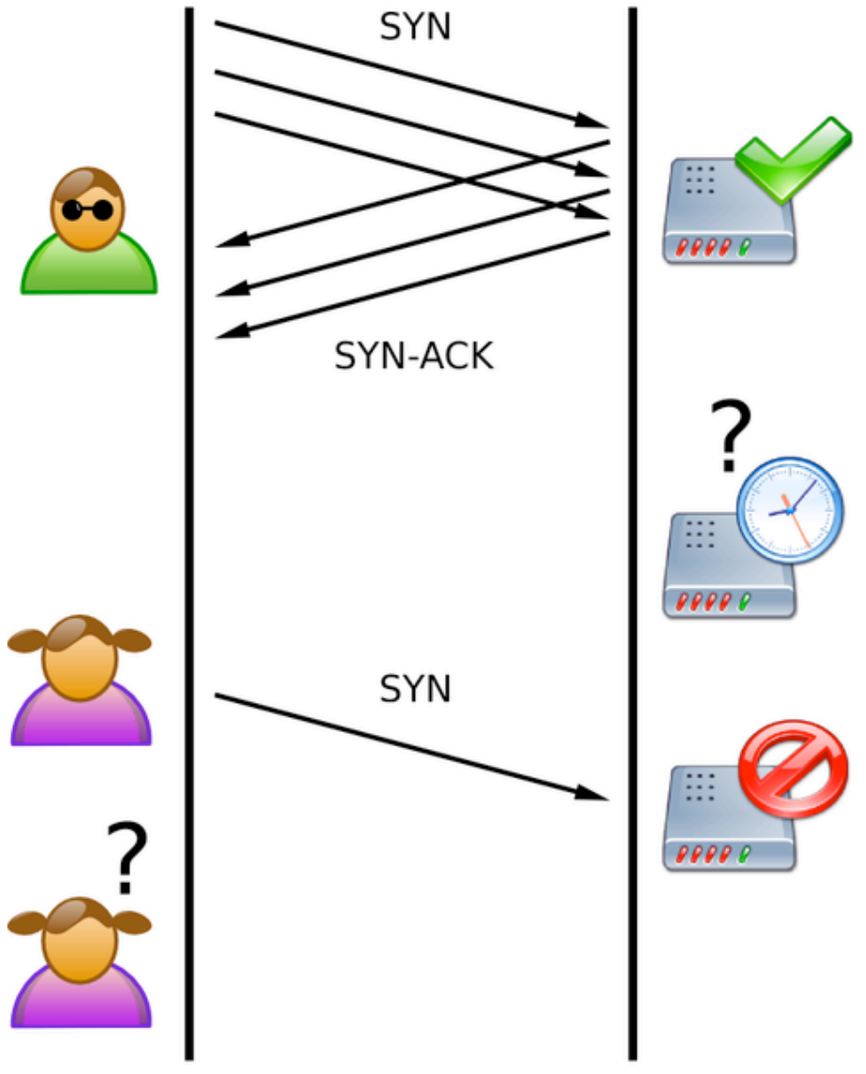


SYN Flooding DOS Attack

Attack on Availability



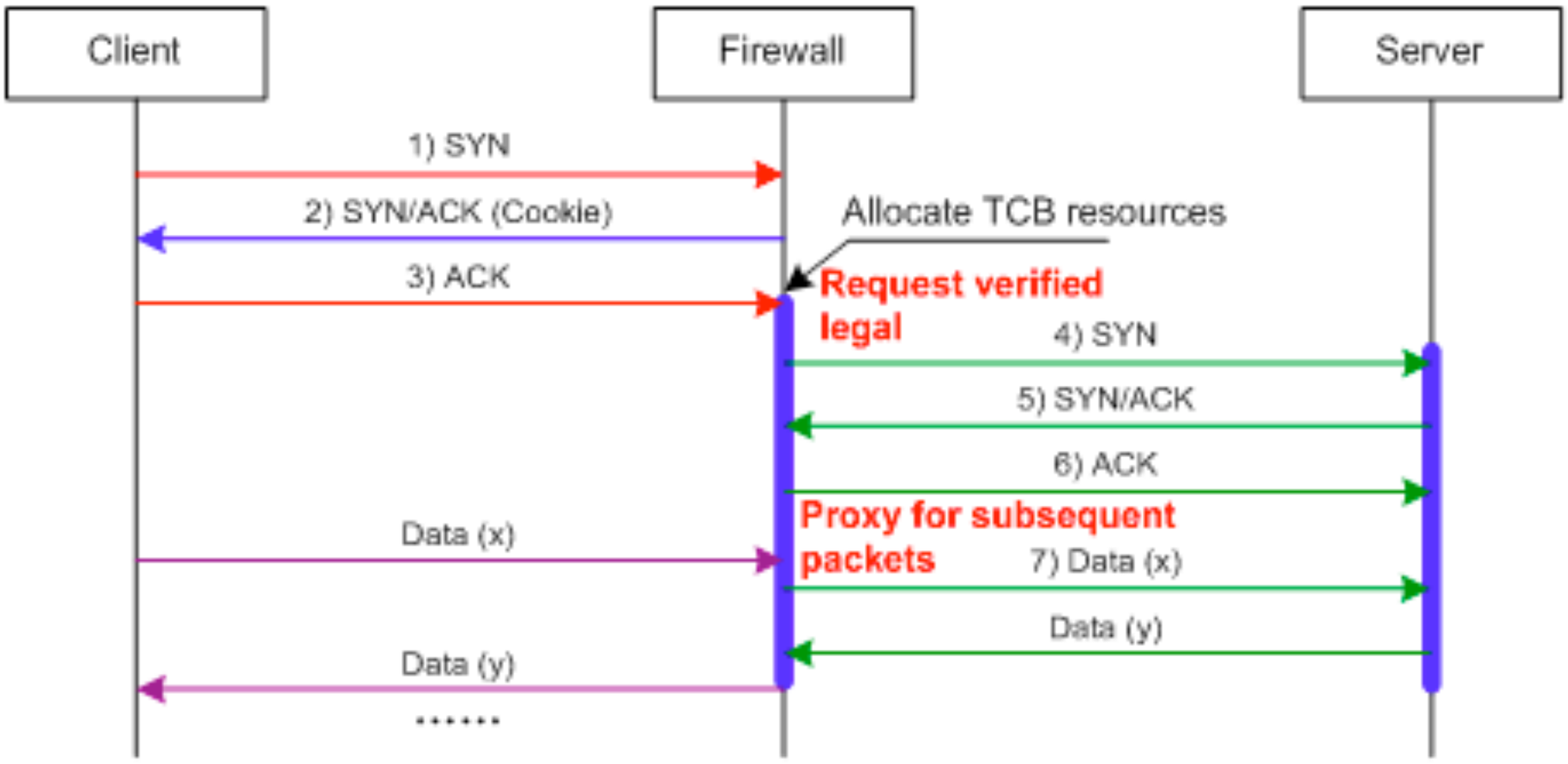
Normal TCP Operation



SYN Flooding Attack

SYN Flooding DOS Attack

SYN Cookies to the Rescue



Original idea: Dan Bernstein (http://cr.yp.to/djb.html)
Picture source: http://www.h3c.com

Authentication and Non-repudiation

- Authentication: Mechanism to establish identity
  - Password-based login implemented using cryptographic hash-functions
  - Collision-resistant and pre-image attack-resistant
  - MD5, SHA256,...
- Non-repudiation: Non-deniability of actions
  - Always ask for a receipt (proof of service provided)
  - Digital signatures (sender cannot deny sending message)

Threats

- A threat is a potential "violation" of security
- Actions leading to violations are called "attacks"
- Confidentiality, Integrity, Availability (CIA) counter threats
- Some types of threats
  - Disclosure: unauthorized access to information (e.g., Stalin knew of the Bomb)
  - Deception: acceptance of false data (e.g., Honey Pots)
  - Disruption: interruption of correct system operation (e.g., DOS attacks, Stuxnet)
  - Usurpation: unauthorized control of system (e.g., Control-hijack, Botnets)

Snooping (Disclosure threat)

- Attacker is listening in, recording, monitoring the network

- Governments do this all the time

- How to protect against such a threat?

Snooping (Disclosure threat)

- Attacker is listening in, recording, monitoring the network

- Governments do this all the time

- How to protect against such a threat?

  - Confidentiality services to rescue
  - Encryption
  - Need-to-know principle

Unauthorized Data Modification

- Can result in a variety of threats
  - Deception
  - Disruption
  - Usurpation
- Examples
  - Use buffer overflow to stack smash resulting in malicious code execution
  - Man in the middle attack
  - Privilege escalation in Web browsers due to software errors

Policy and Mechanism

- Policy
  - An unambiguous statement of what is, and is not, allowed
  - Security is very context-dependent
  - A policy, therefore, helps pin down what security means in a specific context
  - Policy may focus on one or more of a system's security properties (CIAA)
- Mechanism
  - A procedure or tool to enforce a security policy
  - E.g., password-based login is a mechanism to implement access control policy

Trust and Assumptions

- Assumptions
  - Assuming crypto systems are unbreakable can be dangerous
  - Crypto guarantees can be side-stepped by stepping outside the crypto model
  - Side-channel attacks
  - Attacker may learn key by analyzing power consumption or cache behavior
- Trust
  - Very hard to quantify
  - Processors are manufactured in a variety of nations
  - How do you know that the computer manufacturer didn't put some backdoor?
  - Read "Reflections on Trusting Trust" paper by Ken Thompson
    - "You cannot trust code you didn't create yourself"

Design and Verification

- Principles of Secure Design
  - Principle of least privilege (e.g., user gets only essential privileges)
  - Principle of privilege separation (e.g., programs are split into two and granted separate privileges)
  - Principle of fail-safe defaults (e.g., access to resources only through explicit authority)
- Verification
  - PenetrationTesting
  - Formal methods (e.g., model-checking)
  - Information-flow analysis

Putting it all Together

Computer Security: Prevent, Detect and Recover