CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Network Security Principles

Chris Samayoa

Week 4 – 2nd Lecture
2/10/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm
  - Other times by appointment only

Objectives

- Overview of Network Security fundamentals
- Attacker motivations and types
- Common security terminology
- Cryptography introduction
- Authentication basics

Three Aspects of Security

- Confidentiality
  - Keep data private
- Integrity
  - Keep data from being modified by unauthorized individuals/processes
- Availability
  - Keep the system running and reachable

Policy vs. Mechanism

- A **security policy** defines what is and is not allowed on a network or system
  - Needed for organizations of all sizes
- **Security mechanism** is a method or tool for enforcing security policy
  - Prevention
  - Detection
  - Response
- Types of mechanisms:
  - Identification
  - Authentication
  - Audit
  - Containment

Considerations

- Risk analysis and risk management
  - Impact of loss of data
  - Impact of disclosure
  - Legislation may play a role
- Human factors
  - The weakest link

Considerations (cont'd)

- What to protect?
  - System, network, data
- Risk considerations
  - Balance cost to protect against cost of compromise
  - What is attackers level of motivation? Cost to execute attack?
- Security vs. Risk Management
  - Prevent successful attacks or mitigate consequences
- These non-technical issues need to be incorporated into policy and mechanisms

Attackers

- Motivation(s)
  - Bragging Rights
  - Revenge / to inflict damage
  - Terrorism and extortion
  - Financial / criminal enterprises
  - Nation State objectives
- Risk to attacker
  - Organizations can play defensive roles
  - Effective attribution

Attacker Type: Published Attack Tools

- Attacker has specific tools
  - Casts the tool widely to see what can be caught.
  - Sometimes described as script-kiddies
    - Gets them into systems with specific vulnerabilities
    - Gets them account access to susceptible employees
  - They gather what they find, exfiltrate or modify, and stop there
- Strong security posture is effective
  - Sound security practices
  - Systems up to date
  - Least privilege

Attacker Type: Opportunistic

- Looks for a weak link
  - Uses tools to scan for vulnerabilities
  - Once in, repeats the process
    - This time starting with elevated access because of the system or user ID already compromised.
  - They gather what they find, exfiltrate or modify, and stop there
- Good containment architecture can be effective
  - Administrators need to be aware of what paths might be used to reach sensitive data

Attacker Type: Goal Oriented and Top Down

- Researches your organization and system
  - Goal is to compromise some component of your system or access specific data.
  - Learns precursor activities that must be achieved to meet that goal.
  - Often applies APT – Advanced Persistent Threat tactics
  - Will wait for threat vector to propagate
- Defense requires comprehensive strategy:
  - Strong security posture
  - Training of privileged employees
  - Containment Architecture
  - Strong defenses to subversion

Monetary Motivations

- Botnets
  - Controlled machines for sale
- “Protection” or “recovery” for sale
- Attack software for sale
- Stolen data for sale
- Intermediaries used to convert online balances to cash
  - These are the pawns and the ones that are most easily caught

Principle of Least Privilege

- Defined
  - A subject should only be given those privileges that are needed in order to complete its specific task(s)
  - e.g. Log aggregation service only needs ‘read’ privileges specifically to device log files
- In practice
  - Do not consistently use administrator privileges on systems
  - Any temporary elevation of privileges should be relinquished as soon as possible
  - Do not run services as root/admin users
- Issues
  - Makes configuration and administration much more difficult
  - Systems and software design must factor in the ability to granularly assign privileges

Terminology

- Vulnerability
  - A weakness in a system, program, procedure, or configuration that could allow an adversary to violate the intended policies of a system
- Threat
  - Tools or knowledge (capabilities) that are capable of exploiting a vulnerability to violate the intended policies of a system
- Attack
  - An attempt to exploit a vulnerability to violate the intended policies of a system
- Compromise
  - The successful actions that violate the intended polices of a system

Terminology (cont'd)

- Penetration
  - A successful attack (intrusion) that exploits a vulnerability in the code base of a system or its configuration. The result will often be to install a subversion
- Denial of Service
  - An attack that prevents authorized access to a resource, by destroying a target or overwhelming it with undesired requests
- Subversion
  - An intentional change to the code base or configuration of a system that alters the proper enforcement of policy. This includes the installation of backdoors and other control channels in violation of the policy relevant to the system
- Subversion vectors
  - The methods by which subversions are introduced into a system. Often the vectors take the form of malicious code

Terminology (cont'd)

- Secure
  - A system is secure if it correctly enforces a correctly stated policy for a system. A system can only be secure with respect to a particular set of policies and under a set of stated assumptions. There is no system that is absolutely secure.
- Attack Surface
  - The accumulation of all parts of a system that are exposed to an adversary against which the adversary can try to find and exploit a vulnerability that will render the system insecure (i.e. violate the security policies of the system).

Common Issue

- Loosely managed systems
- Security is made even more difficult to implement since today's systems lack a central point of control
  - Home machines unmanaged
  - Networks managed by different organizations.
  - A single function touches machines managed by different parties.
    - Cloud
  - Who is in control?

General Security Concerns

- Buggy code
- Protocol design failures
- Weak crypto
- Social engineering
- Insider threats
- Poor configuration
- Incorrect policy specification
- Stolen keys or identities
- Denial of service

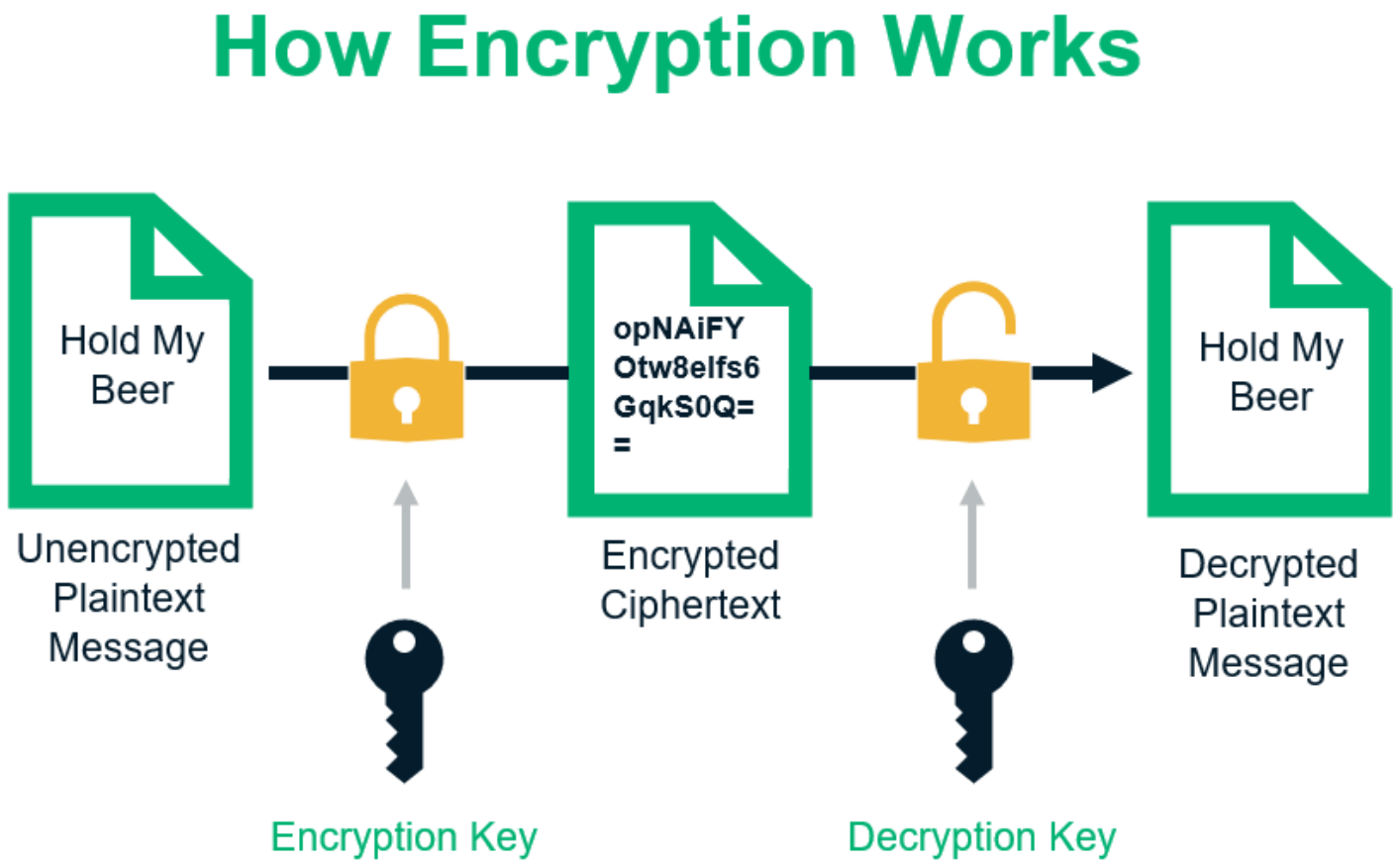
Security Mechanisms

- Encryption
- Checksums
- Key management
- Authentication
- Authorization
- Audit logs
- Firewalls
- Virtual Private Nets (VPNs)
- Intrusion detection
- Intrusion response
- Development tools
- Virus Scanners
- Policy managers
- Trusted hardware

Cryptography

- Cryptography underlies many fundamental security services
  - Confidentiality
  - Data integrity
  - Authentication
- Functions as a basic building block for security services

Cryptography

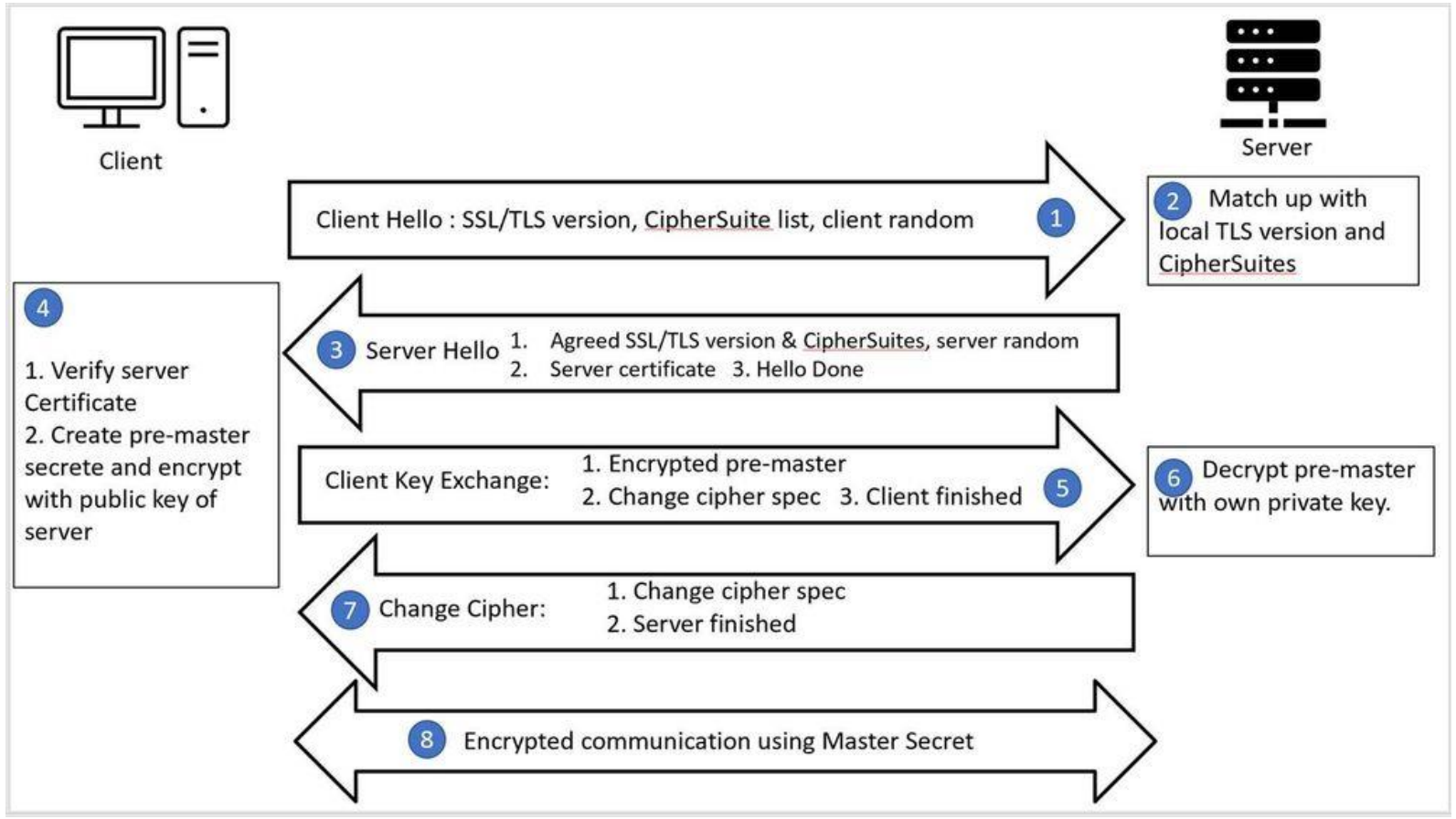


Source: https://sectigostore.com/blog/what-is-asymmetric-encryption-how-does-it-work/

Substitution Ciphers

- Symmetric-key (conventional)
  - Single key used for both encryption and decryption
  - Keys are typically short, because key space is densely filled
  - Ex: AES, DES, 3DES, RC4, Blowfish, IDEA, etc.
- Asymmetric keys (public-private)
  - Two keys: one for encryption, one for decryption
  - Keys are typically long, because key space is sparsely filled
  - Ex: RSA, El Gamal, DSA, etc
- Often used in combination
  - e.g. Diffie-Hellman in TLS to exchange AES cipher

TLS



Source: Microsoft

Identification vs Authentication

- Identification
  - Associating an identify with an individual, process, or request
- Authentication
  - Verification of a claimed identity
  - Ideally
    - Who you are
  - Practically
    - Something you know
    - Something you have
    - Something you are
- Often used in combination
  - e.g. Diffie-Hellman in TLS to exchange AES cipher

Something You Know

- Password or Algorithm
  - e.g. Encryption key derived from password
- Issues
  - How to keep it secret?
    - Find it, sniff it, social engineer it
  - You need to remember it
  - How is it stored and checked?
- Potential attacks
  - Brute force
  - Dictionary
  - Pre-computed Dictionary
  - Guessing
  - Finding elsewhere

Passwords

- Can have too many password or too few passwords
  - Can lead to reuse of passwords
  - People are lazy
  - Can be mitigated by password vaults
- Passwords need to be presented
  - Relies on uncompromised verifier
- Password recommendations changed
  - Length over special characters at this point

Something You Have

- Cards
  - Mag stripe
  - Smart Card
  - USB Key
  - Time varying password
- Issues
  - How to validate?
    - Verifier can be compromised
  - Need special infrastructure
  - e.g. RSA SecureID (https://www.wired.com/2011/06/rsa-replaces-securid-tokens/)

Something You Are

- Biometrics
  - Iris scan
  - Fingerprint
  - Picture
  - Voice
- Issues
  - Need to prevent spoofing

Summary

- Security Triad = Confidentiality, Integrity, and Availability (CIA)
- Security policy defines acceptable use of system
- Security mechanisms enforce the policy
- Attackers have various different motivations
- Terminology is important for communication
- Cryptography is a building block for network security
- Authentication
  - Something you know
  - Something you have
  - Something you are