Data and Network Security

- ***Instructor : Dr. Arash Kosari***

- ***References:***

1. Matt Bishop. Computer Security. Addison-Wesley, 2017.
2. John Erickson. The Art of Exploitation 2nd Edition, No Starch Press, 2008.
3 . Robert C. Seacord. Secure Coding in C and C++. 2nd Edition, Pearson Education, 2005.
4. A. Sotirov. Bypassing Browser Memory Protections. 2008.
5. T. Garfinkel. Traps and Pitfalls: Practical Problems in System Call Interposition Based Security Tools. NDSS, 2003.
6. Adam Barth, Collin Jackson, and John C. Mitchell. Securing Browser Frame Communication. Usenix, 2008.
7. Adam Barth, Collin Jackson, Charles Reis, and the Google Chrome Team. The Security Architecture of the Chromium Browser. 2008.
8. Bortz et al. Origin Cookies: Session Integrity for Web Applications. 2011.
9. Enck, Ongtang, and McDaniel. Understanding Android Security. 2009.
10. Allan Tomlinson. Introduction to the TPM: Smart Cards, Tokens, Security and Applications. 2008.
11. Andrew Baumann, Marcus Peinado, and Galen Hunt. Shielding Applications from an Untrusted Cloud with Haven. OSDI 2014.

- **Basic concepts and definitions**
  - Security policy and access control models
  - Hidden channels, information flow control
  - optional models (DAC) and mandatory models (MAC)
  - role-based models (RBAC)
- **System security**
  - How to run software and their interactions with the system and weaknesses
  - Attacks and defense methods (control hijacking)
  - Safe management of old codes in use (sandbox, virtualization, isolation in different layers)
  - Existing methods for safe code development (static analysis, dynamic analysis)
  - Methods of security breach and Fuzzing
- **Web security model**
  - Web application security (sql, XSS, CSRF)
  - Web meeting management (Cookies)
  - Concepts of symmetric and asymmetric cryptography
  - Message authentication codes and hashing functions
  - Security of web information during exchange (Https/SSL)
  - Defense mechanisms on the browser side (SOP, CSP, CORS)

● Network Security

- Security threats in network protocols (etc, routing, BGP, DNS, TCP)
- Defense tools in the network (etc, IDS, VPN, Firewall)
- Denial of service attacks and defense solutions
- Trusted Computing and SGX
- Mobile security
- Security of mobile platforms (iOS, Android)
- Threats in the field of mobile

•SESSION 1

What are access control security models?

- An access control security model is a formally defined definition of a set of access control rules that is independent of technology or implementation platform. Access control security models are implemented within operating systems, networks, database management systems and back office, application and web server software. Various access control security models have been devised over the years to match access control policies to business or organizational rules and changes in technology.
- Three main types of access control systems are: Discretionary Access Control (DAC), Role Based Access Control (RBAC), and Mandatory Access Control (MAC).

- Discretionary access control (DAC)

کنترل دسترسی اختیاری

  - With discretionary access control, access to resources or functions is constrained based upon users or named groups of users. Owners of resources or functions have the ability to assign or delegate access permissions to users. This model is highly granular with access rights defined to an individual resource or function and user. Consequently the model can become very complex to design and manage.

- Mandatory access control (MAC)

کنترل دسترسی اجباری

  - Mandatory access control is a centrally controlled system of access control in which access to some object (a file or other resource) by a subject is constrained. Significantly, unlike DAC the users and owners of resources have no capability to delegate or modify access rights for their resources. This model is often associated with military clearance-based systems.

Role Based Access Control (RBAC)

- **Role-Based Access Control (RBAC)** is the model and practice of restricting network access based on the roles of individual users across the enterprise. RBAC gives employees access rights only to the information they need to accomplish their assigned tasks based on their job role and prevents them from accessing information that is not relevant to them or necessary to complete their tasks.
- ----------
- **Here are some typical examples of where RBAC controls access for specific roles/positions:**

- An employee in the finance department would like access to the accounting or payroll system such as Xero and/or ADP

- Software engineer roles could be assigned access to the Google Cloud Platform, Amazon Web Services, or GitHub

- The human resources director would be assigned access to Oracle HCM or Zenefits.

- Marketing directors may be assigned access to a marketing automation system such as Marketo and Google Analytics or manage Facebook ads and Google pay-per-click accounts.

- **DAC**: A company may use DAC to control access to a shared folder on a network drive.

The owner of the folder can set permissions for individual users and groups to access the folder and its contents.

- **MAC**: A government agency may use MAC to control access to classified information.

The agency may assign security labels to documents and individuals, and
only those with the appropriate clearance and compartmentalization may access the information.

- **RBAC**: A hospital may use RBAC to control access to electronic medical records.

The hospital may assign roles to users based on their job functions,
such as “Doctor,” “Nurse,” or “Administrator,” and grant access rights based on those roles[1].

What are the benefits of RBAC?

- **Minimize the risk of data breaches -** Implementing RBAC not only reduces the risk of cyber threats and abuse by malicious insiders, but it can also be crucial in limiting the damage from an attacker who has compromised an employee's user credentials.
- **Demonstrate and enforce compliance** - As regulations continue to grow at every level of government from the Federal level to state and industry-specific mandates, RBAC helps organizations meet regulatory and statutory requirements. Financial institutions and healthcare companies are under significant pressure to show how they use, manage, and protect sensitive data.
- **Improve operational productivity and efficiency –** RBAC enables organizations to reduce paperwork and password change requests when hiring and onboarding new employees or switching roles for existing employees. With RBAC, you automate the process to quickly add and change roles and put them into effect across platforms, operating systems (OS), and applications.
- **Provide greater visibility for administrators -** RBAC gives network administrators and managers more visibility and oversight into the business while also guaranteeing that authorized users and guests on the system are only given access to what they need to do their jobs.
- **Conserve resources -** Restricting user access to specific processes and applications conserves network resources and keeps employees focused on the task at hand.

- **What Does Security Policy Mean?**

- A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.

- **Defining a cybersecurity policy**

Cybersecurity procedures explain the rules for how employees, consultants, partners, board members, and other end-users access online applications and internet resources, send data over networks, and otherwise practice responsible security.

- For small organizations, however, a security policy might be only a few pages and cover basic safety practices. Such practices might include:

- Rules for using email encryption
- Steps for accessing work applications remotely
- Guidelines for creating and safeguarding passwords
- Rules on use of social media

Four reasons a security policy is important :

- **1. Guides the implementation of technical controls**

A security policy doesn't provide specific low-level technical guidance, but it does spell out the intentions and expectations of senior management in regard to security.

- **2. Sets clear expectations**

Without a security policy, each employee or user will be left to his or her own judgment in deciding what's appropriate and what's not. This can lead to disaster when different employees apply different standards.

3. Helps meet regulatory and compliance requirements

Documented security policies are a requirement of legislation like HIPAA and Sarbanes-Oxley, as well as regulations and standards like PCI-DSS, ISO 27001, and SOC2.

- **4. Improves organizational efficiency and helps meet business objectives**

A good security policy can enhance an organization's efficiency. Its policies get everyone on the same page, avoid duplication of effort, and provide consistency in monitoring and enforcing compliance.

Seven elements of an effective security policy

1. Clear purpose and objectives
2. Scope and applicability
3. Commitment from senior management
4. Realistic and enforceable policies
5. Clear definitions of important terms
6. Tailored to the organization's risk appetite
7. Up-to-date information

- **Information flow control (IFC)** is a developing concept where a system can monitor the flow of information from one place to another and prevent the flow if it is not wanted. It is a security measure that monitors information propagation between a system and the world, otherwise known as the Internet. Users want to keep their credentials confidential and so IFC uses type-systems and enforces this through compile-time type checking.

The basic model has data assigned a security label of confidential (high) or public (low) where the system will make sure no high data flows to a low context. If IFC can be implemented into existing and future phone/web applications, guaranteeing protection of user privacy would be much easier.

Applications of IFC :

- Protecting Private Information.
- Protecting Against Covert Channels.
- Making privacy easier to use .
- IFC Opponents .

CIA Triad

Confidentiality – restrict access to authorized individuals

Integrity – data has not been altered in an unauthorized manner

Availability – information can be accessed and modified by authorized individuals in an appropriate timeframe

Tools for Information Security

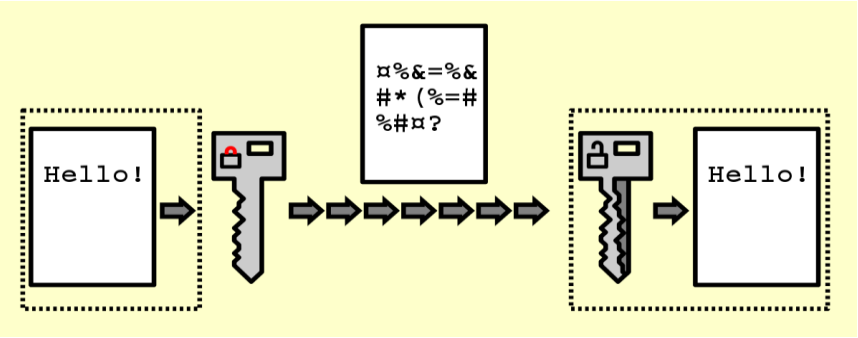
- Authentication
- Access Control
- Encryption
- Passwords
- Backup
- Firewalls
- Virtual Private Networks (VPN)
- Physical Security
- Security Policies

Access Control

- Once authenticated – only provide access to information necessary to perform their job duties to read, modify, add, and/or delete information by:
  - Access control list (ACL) created for each resource (information)
    - List of users that can read, write, delete or add information
    - Difficult to maintain all the lists
  - Role-based access control (RBAC)
    - Rather than individual lists
    - Users are assigned to roles
    - Roles define what they can access
    - Simplifies administration

Encryption

- An algorithm (program) encodes or scrambles information during transmission or storage
- Decoded/unscrambled by only authorized individuals to read it



- How is this done?
  - Both parties agree on the encryption method (there are many) using keys
    - Symmetric key – sender and receiver have the key which can be risky
    - Public Key – use a public and private key where the public key is used to send an encrypted message and a private key that the receiver uses to decode the message

Passwords

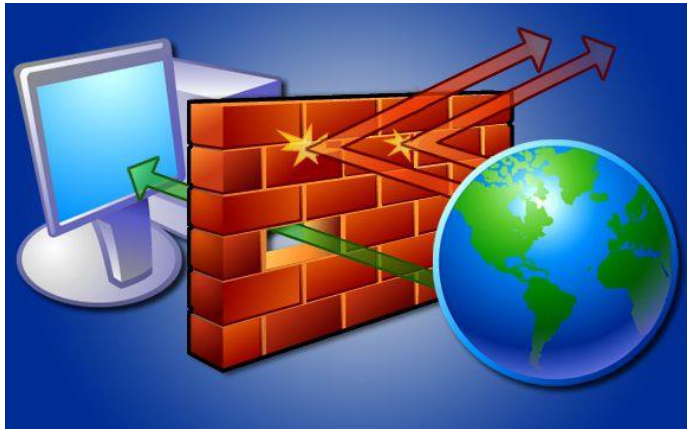
- Single-factor authentication (user ID/password) is the easiest to break
- Password policies ensure that this risk is minimized by requiring:
  - A certain length to make it harder to guess
  - Contain certain characters – such as upper and lower case, one number, and a special character
  - Changing passwords regularly and do not a password to be reused
  - Employees do not share their password
  - Notifying the security department if they feel their password has been compromised.
  - Yearly confirmation from employees that they understand their responsibilities

Backup

- Important information should be backed up and store in a separate location
  - Very useful in the event that the primary computer systems become unavailable
- A good backup plan requires:
  - Understanding of the organizational information resources
  - Regular backups of all data
  - Offsite storage of backups
  - Test of the data restoration
- Complementary practices:
  - UPS systems
  - Backup processing sites

Firewalls

- Can be a piece of hardware and/or software
- Inspects and stops packets of information that don't apply to a strict set of rules
  - Inbound and outbound
- Hardware firewalls are connected to the network
- Software firewalls run on the operating system and intercepts packets as they arrive to a computer
- Can implement multiple firewalls to allow segments of the network to be partially secured to conduct business
- Intrusion Detection Systems (IDS) watch for specific types of activities to alert security personnel of potential network attack



Virtual Private Networks (VPN)

- Some systems can be made private using an internal network to limit access to them
  - Can't be accessed remotely and are more secure
  - Requires specific connections such as being onsite
- VPN allows users to remotely access these systems over a public network like the Internet
  - Bypasses the firewall
  - Encrypts the communication or the data exchanged
- CPP students have this ability for:
  - Exchange services from your Outlook client
  - Mapping a drive or mounting a file share
  - Instructions to establish a VPN connection can be found at https://ehelp.wiki.cpp.edu/VPN_(Virtual_Private_Network):_Requirements

Physical Security

- Protection of the actual equipment
  - Hardware
  - Networking components
- Organizations need to identify assets that need to be physically secured:
  - Locked doors
  - Physical intrusion detection - e.g., using security cameras
  - Secured equipment
  - Environmental monitoring – temperature, humidity, and airflow for computer equipment
  - Employee training

Security Policies

- Starting point in developing an overall security plan
- Formal, brief, and high-level statement issued by senior management
  - Guidelines for employee use of the information resources
  - Embraces general beliefs, goals, objectives, and acceptable procedures
  - Includes company recourse if employees violate the policy
- Security policies focus on confidentiality, integrity, and availability
  - Includes applicable government or industry regulations
- Bring Your Own Device (BYOD) policies for mobile devices
  - Use when accessing/storing company information
  - Intellectual property implications
- Difficult to balance the need for security and users' needs

Personal Information Security

- Simple steps that individuals can take to be more secure:
  - Keep your software up to date
  - Install antivirus software
  - Use public networks carefully
  - Backup your data
  - Secure your accounts with two-factor authentication
  - Make your passwords long, unique, and strong
  - Be suspicious of strange links and attachments

- For more information on personal information security, visit the Stop, Think, Connect website at http://www.stopthinkconnect.org/

- GOOD LOCK