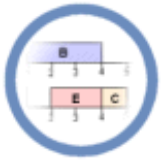




Lecture 10
Security (Part 2)

<lecturer, date>

Outline

- Securing computer systems
  - Cryptography
  - Virtual Private Networks (VPN)
  - Access controls
    - Mandatory access control
    - Discretionary access control
    - Role based access control
- Role based access control

Cryptography

- Kryptos- hidden secret and graphein- writing
- Study of techniques for securing information in the presence of adversaries
  - to secure online credit card transactions
  - to secure data stored online, like in Google drive
- Encryption
  - process of encoding messages such that only authorized people can use it
  - technique of transforming information into an unusable form
  - e.g., replace A by 1, B by 2, C by 3, and so on…
- Relies on the assumption of computational hardness
  - Theoretically possible to ‘break’ such systems
  - Hard to do in practice by any known means

Cryptography

1. Symmetric key cryptography
   - Encryption and decryption happens using the same key (rule)
   - The receiver need to have the same key in order to read (make use of) the information
   - An example is the Data Encryption Standard (DES) (reference 3)
   - e.g., Suppose Bob and Alice want to communicate securely
     - Bob replaces every alphabet by the following alphabet, i.e., to CAT becomes DBU
     - Alice need to know this rule to decrypt DBU

2. Public key cryptography
   - Encryption and decryption happens using different keys
   - The sender need to know the receiver's public key in order to encrypt information so that the receiver can decrypt it using his private key
   - An example is the RSA encryption algorithm (reference 4)
   - e.g., Suppose Alice's private key is A and public key is B
     - Bob encrypts the message using B and sends it to Alice
     - Alice decrypts the message using her private key A

Outline

- Securing computer systems
  - Cryptography
  - Virtual Private Networks (VPN)
  - Access controls
    - Mandatory access control
    - Discretionary access control
    - Role based access control
- Role based access control

Virtual Private Networks (VPN)

- A private network that is a part of a larger network (e.g., internet) that is composed of a selected set of members of the larger network.
- Example: OpenVPN
- Encrypts data between the members of the private network so that third party members (e.g., somebody in the larger network) cannot access the communication.
- Private because the traffic is ‘visible’ only to the members
- One way of ensuring secure communication through e.g., internet
- Interesting in the context of internet of things since private networks connecting personal devices can be constructed on top of the internet

Outline

- Securing computer systems
  - Cryptography
  - Virtual Private Networks (VPN)
  - Access controls
    - Mandatory access control
    - Discretionary access control
    - Role based access control
- Role based access control

Access Controls

Restricting access to resources and information on a selective basis

- Discretionary access control: individual users can set access controls to resources and information without restrictions
- Mandatory access control: individuals can set access controls to resources and information as long as it is consistent with the system wide policy
- Role based access control: individuals can set access controls to resources and information only if it is consistent with their role

Outline

- Securing computer systems
  - Cryptography
  - Virtual Private Networks (VPN)
  - Access controls
    - Mandatory access control
    - Discretionary access control
    - Role based access control
- Role based access control

Role Based Access Control

Role based access control: individuals can set access controls to resources and information only if it is consistent with their role.

Common terminology:

- Subject: A person or a software service, e.g., an employee
- Role: The function in the organization that corresponds to an authority level, e.g., system admin
- Permissions: The mode of access to a resource, e.g., full access, restricted access etc
- Transaction: Any activity carried out by the subject.
- …

Role-based permissions

- Each role is associated with a certain set of permissions
- Need to prove identity to be able to use the system

Common methods for validating identity:

- Passwords
- Biometrics such as finger-prints
- Access cards (RFID etc)

Role Based Access Control

Basic rules for RBAC:

1. Role Assignment: Each subject in the system must have an assigned role.

1. Role Authorization: The role must be authorized by some authority, e.g., a system admin.

2. Transaction Authorization: Every transaction carried out by the subject must be authorized, e.g., by a system admin

Advantages of Role Based Access Control

- Easy to administer
  - Every subject can be given permission based on his role e.g., a security guard does not need permissions to see company operations
  - Every subject with the same role has same permissions
  - New roles can be created with customized permissions e.g., during company expansions
- Support for multi-functionality
  - Each subject can be assigned multiple functions
- Seamless transition between roles
  - Subjects can transition between roles without changing their identities
  - Improves security: each subject has a single identity in the system (albeit different roles)

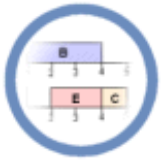
References

1) Basic concepts and taxonomy of dependable and secure computing, Avizienis, A. ; Laprie, J.-C. ; Randell, B. ; Landwehr, C., IEEE Transactions on Dependable and Secure Computing, 2004
2) Industrial Control Systems Cyber Emergency Response Team, https://ics-cert.us-cert.gov/Standards-and-References
3) Data Encryption Standard, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
4) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Rivest, R.; Shamir, A.; Adleman, L., http://people.csail.mit.edu/rivest/Rsapaper.pdf
5) Multiuser cryptographic techniques, Diffie, W. and Hellman, M., AFIPS '76 Proceedings of the national computer conference and exposition.http://www.cin.ufpe.br/~mab/p109-diffie.pdf
6) Virtual Private Networking- an overview, https://technet.microsoft.com/en-us/library/bb742566.aspx
7) OpenVPN, https://openvpn.net/index.php/open-source.html

References

8) Role-Based Access Controls, David F. Ferraiolo and D. Richard Kuhn, http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf





Lab 10
Security (Part 2)

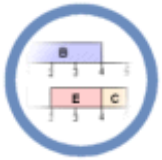
<lecturer, date>

Description

- Implement role based access control for the mobile app that you developed

- Have two roles:
  1. User: can only get readings and monitor for alarms
  2. Admin: can get readings as well as set the values of temperature, water level etc





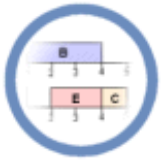
Seminar 10
Security (Part 2)

<lecturer, date>

Description

- Discuss the solutions for the lab.
- Answer the following questions (1 page report):
  - Is this the best solution?
  - Can the security be breached, e.g., using any of the techniques that you learned?
  - How can you further improve security?
  - What are the challenges involved in securing such systems?





Mini-project 10
Security (Part 2)

<lecturer, date>

Description

- Perform a literature survey on encryption techniques, with particular focus on mobile devices and embedded systems:
  - State of the art
  - Impact on size, weight and power constraints
  - Emerging challenges
  - Open problems