Topic 4
Access Control

Dr Diarmuid Ó Briain

8 Oct 2024

setu.ie
INSPIRING FUTURES

Version: 2.0

Licence

Learning objectives

By the end of this topic you will be able to:

- Define access control and explain its importance.
- Analyse the different types of access control and their strengths and weaknesses.
- Describe the principles of layered access control and how they work together to protect resources.
- Assess the importance of password security and the risks of weak passwords.
- Discuss the responsibilities of access control administrators and their role in implementing, managing, and monitoring access control policies and procedures.

Access Controls

- Group exercise
- Discuss these access controls

Group 1

- Preventive
- Deterrent
- Detective

Group 2

- Corrective
- Recovery
- Compensation
- Directive

Group 3

- Administrative
- Logical / technical
- Physical

Access Controls

- **Preventive**
- **Deterrent**
- **Detective**
- **Corrective**
- **Recovery**
- **Compensation**
- **Directive**
- **Administrative**
- **Logical** or **technical**
- **Physical**

Access Control in a Layered Environment

- **Layered / Defence in Depth**
  - The use of several forms of access control.
- **Identification**
  - Subject authentic, accredited and held accountable.
- **Authentication**
  - This is the process of verifying that a given identity is valid.
    - Type 1 – "**Something you know**", i.e. Password
    - Type 2 – "**Something you have**", i.e. Token
    - Type 3 – "**Something you are**", i.e. Biometric
    - "Something you do"
    - "Somewhere you are"
    - Multi-factor Authentication.

Access Control in a Layered Environment

- **Authorisation**
  - Determining the types and extent of activities that are permissible to established users or groups on a system.
- **Auditing and Accountability**
  - Formally examining and reviewing activities, applications and processes initiated by subjects on a system.

Identification and Authentication techniques

- **Identification**
  - Subject must provide an identity to a system to start the Authentication, Authorisation and Accountability process.
  - The Identity correlates an authentication factor with a subject:
    - Typing a username
    - Swiping a Smart Card
    - Waving a Token Device
    - Speaking a Phrase
    - Positioning Face, Hand or Finger for camera/scanner.
- **Authentication**
  - Authentication verifies the Identity of a Subject, thus Identification and Authentication are always a two step process, one useless without the other.

Passwords

- Poor security mechanism for the following reasons:
  - Users typically use passwords they can easily remember
  - Random generated passwords are difficult to remember so the Subject tends to write them down
  - Passwords are easily shared, written down, forgotten
  - Passwords are easily stolen through observation, recording, playback, social engineering and security database theft
  - Passwords often transmitted in clear or shrouded in simple to break encryption
  - Short passwords can be discovered quickly by brute force attacks.

Password Manager

- Help individuals create, store, and manage strong, unique passwords for all of their online accounts
  - An example is the service provided by Bitwarden which gives the user the power to create and manage unique passwords, strengthening privacy and boosting productivity online from any device or location.

bitwarden

Password selection

- Passwords are broken into two groups:
  - Static
    - Always remain the same
  - Dynamic
    - One-time passwords, single-use passwords
    - Cognitive password
    - What is your date of birth?
    - What is your first pet's name?
    - What is your mother's maiden name?

Password policies

- Password policies should at a minimum force:
  - Change the password regularly, minimum and maximum age
  - Password characters should be dictated by the object during creation.
    - Not all letters
    - No number or letter sequences
    - Does not contain the Identification name
    - Minimum length
    - Mix of letters and numbers, upper and lower case
    - No password reuse.

Password security

- Password theft methods include:
  - Network Traffic Analysis
  - Password file access
  - Brute-force attacks
  - Dictionary attacks
  - Social Engineering.

Biometrics

- Uniquely recognising humans based upon one or more intrinsic physical or behavioural traits.
  - Fingerprints.
  - Face scans.
  - Iris Scans - Coloured area around pupil.
  - Retina scans - Pattern of blood vessels in back of eye
    - Most unacceptable by subjects as it can determine medical conditions (pregnancy, blood pressure) and it also blows air into the subjects eye.
  - Palm scans (Palm Topography).
  - Hand geometry
  - Signature dynamics - Recognition of how a subject signs a set of characters.
  - Keystroke patterns (keystroke dynamics) - Flight time and Dwell time.

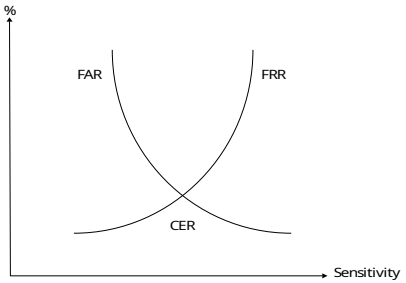
Biometric factor ratings

Errors can occur with biometrics and are categorised as follows:

- **Type 1 - False Rejection Rate (FRR)**
  - Valid subject is not authenticated
  - Percent of valid inputs which are incorrectly rejected.
- **Type 2 - False Acceptance Rate (FAR)**
  - Invalid subject authenticated
  - Percent of invalid inputs which are incorrectly accepted.

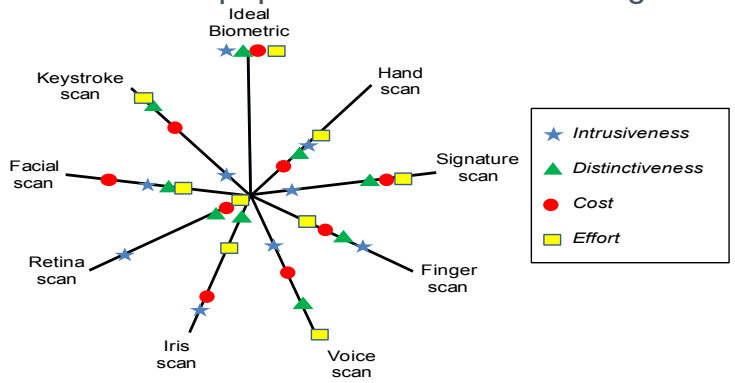
Biometric factor ratings

- Crossover Error Rate (CER) is point of intersection between FRR and FAR.
- The lower the CER rate the more accurate is the system.



Biometric usage, acceptance & cost

- Zephyr analysis chart shows the relation between ideal biometrics and most popular biometric technologies.



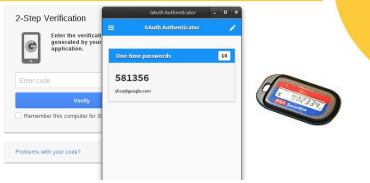
Biometric typical CER rates

Biometric	CER
Iris recognition	0.001% - 0.01%
Fingerprint	0.001% - 0.1%
Palm vein recognition	0.01% - 0.1%
Facial recognition	0.1% - 1%
Voice recognition	1% - 5%

Tokens

There are four types of token:

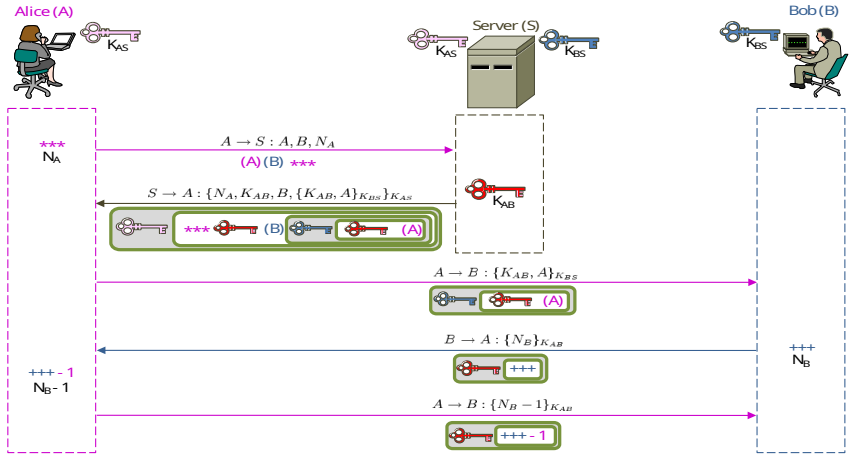
- **Static Tokens**
  - Swipe card, disk, USB RAM Key or a physical key.
- **Synchronous dynamic** password tokens
  - Device that generates new passwords at fixed time intervals.
  - Subject enters generated password with PIN and passphrase/password.
    - Example: Google Authenticator
- **Asynchronous dynamic** password tokens
  - Device that generates new passwords on the occurrence of an event
  - Press a key on the token and the server for example, advances next password
  - Subject enters generated password with PIN and passphrase/password.
- **Challenge-response** tokens
  - Passwords are generated by the token in response to instructions from the object.



Tickets

- Single Sign On (SSO), this means is a mechanism where multiple applications use one place to authenticate.
- A very common example of this will be Google, a single login permits access to Gmail, Google Calendar and other Google applications.
- Google uses Security Assertion Markup Language (SAML) Single Sign-On (SSO) service.

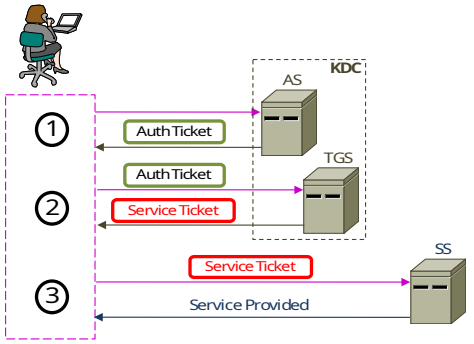
Needham-Schroeder Symmetric Key Protocol



Kerberos

- Kerberos is a computer network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

- Authentication Server (AS)
- Ticket Granting Server (TGS)
- Service Server (SS)



Access Control Techniques

- Discretionary Access Controls (DAC)
  - *a type of access control in which the owner of an object determines who can access that object and what operations they can perform on it.* CC

- Mandatory Access Controls (MAC)
  - *a type of access control in which the system determines whether an access request is allowed based on a set of rules that are defined by a security administrator.* CC

Mandatory Access Controls (MAC)

- **Role-based Access Control (RBAC)**
  - Permissions to perform certain operations are assigned to specific roles
  - RBAC is attractive to organisations with a high rate of turnover.
- **Attribute-based Access Control (ABAC)**
  - Decisions about access to systems and resources based on attributes such as user, resource, action, or environment
  - Particularly suited to OT offering the benefits of Flexibility, Scalability, Expressiveness and Improved security.
- **Lattice-based Access Control (LBAC)**
  - Complex access control based on the interaction between any combination of objects (such as resources, computers, and applications) and subjects
  - Subjects are only allowed to access an object if the security level of the subject is greater than or equal to that of the object.

Mandatory Access Controls (MAC)

Mechanism	Uses	Strengths	Weaknesses
Role-based Access Control (RBAC)	Organisations with high turnover of employees	Easy to manage	Can be difficult to ensure that users are assigned to the correct roles and that they only have the permissions they need
Attribute-based Access Control (ABAC)	OT organisations	Flexible	Can be complex to implement and manage
Lattice-based Access Control (LBAC)	Military, Intelligence, Financial	Fine-grained control	Complex to implement and manage

Centralised Access Control

- Advantages
  - Managed by small team or individual
  - Administrative overhead is low
  - Single changes impact the complete system.
- Disadvantages
  - Single point of failure
  - If elements cannot access centralised access control system then subjects cannot access objects.

Centralised Access Control - RADIUS

- Remote Access Dial-in User Service (RADIUS)
  - Centralised Authentication, Authorisation, and Accounting (AAA) management for computers to connect and use a network service
  - Developed by Livingston Enterprises, Inc., in 1991 as an AAA protocol and later became IETF standard
  - Client/server protocol that runs in the application layer, using UDP as transport
  - RADIUS serves three functions:
    - Authenticate users or devices before granting them access to a network
    - Authorise users or devices for certain network services
    - Account for usage of services.
- Diameter
  - Successor to RADIUS however a lot of the features of Diameter have been included in upgrades of RADIUS
  - Uses Reliable transport protocols TCP or SCTP instead of UDP.

Centralised Access Control - TACACS

- Terminal Access Controller Access Control System (TACACS)
  - Remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks
  - Uses TCP for transport.
- TACACS+
  - TACACS+ is based on TACACS, but, in spite of its name, it is an entirely new protocol which is incompatible with any previous version of TACACS
  - Whereas RADIUS combines Authentication and Authorisation in a user profile, TACACS+ separates the two operations.

De-centralised Access Control

- Advantages
  - No single point of failure.
- Disadvantages
  - Large administrative overhead
  - Maintaining homogeneity becomes difficult.
- A domain is a realm of trust created were a collection of subjects and objects share a common security policy.
- Between these domains a security bridge called a trust can be established to allow subjects in one to access objects in the other.

Access Control Administration

- Responsibilities
  - User Account Management.
  - Activity Tracking.
  - Access rights and permission management.
- User Accounts
  - **User** (Subject)
  - **Owner**
    - Responsibility for classification and labelling an Object.
  - **Custodian**
    - Responsibility of properly storing and protecting Objects.

Access Control Administration - Enrolment

- **Enrolment** function of creating and amending user accounts protected through organisation policies
- User Accounts cannot be created without HR department request on new-hire or promotion
- Formal request from HR department:
  - User details
  - Security classification.
- Users/Security manager verify/approve the assignment
- User training on the organisations security policies
- User should sign a document agreeing to comply with the policies.

Access Control Administration

- Account Maintenance
  - New hire
  - Role changes
  - Employee leaves or retires
- Account, Log and Journal Monitoring
- Access rights and permissions
- Principle of Least Privilege
  - Role changes
- Creeping Privileges

Separation of Duties (SoD)

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database Administrator	Network Administrator	Systems Administrator	Security Administrator	Systems Programmer	Quality Assurance
Control Group		x	x	x		x	x	x	x	x		x	
Systems Analyst	x			x	x		x				x		x
Application Programmer	x			x	x	x	x	x	x	x	x	x	x
Help Desk and Support Manager	x	x	x		x	x		x	x	x		x	
End User		x	x	x			x	x	x			x	x
Data Entry	x		x	x			x	x	x	x	x	x	
Computer Operator	x	x	x		x	x		x	x	x	x	x	
Database Administrator	x		x	x	x	x	x		x	x		x	
Network Administrator	x		x	x	x	x	x	x					
System Administrator	x		x	x		x	x	x				x	
Security Administrator		x	x			x	x					x	
Systems Programmer	x		x	x	x	x	x	x		x	x		x
Quality Assurance		x	x		x							x	

Monitoring - Intrusion Detection System (IDS)

- Sensors which generate security events
- Console to monitor events and alerts and control the sensors
- Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

- **Host**-based IDS (HIDS)
- **Network**-based IDS (NIDS).

- Detection types
  - **Knowledge** (**Signature**) Based Detection
  - **Behaviour** (**Statistical anomaly**) Based Detection.

Security Information and Event Management (SIEM)

- Security solution that helps organisations detect, analyse, and respond to potential security threats and vulnerabilities before they have a chance to disrupt business operations
- SIEM systems collect and analyse data from a variety of sources, including security logs, system logs, and network traffic, to identify patterns and anomalies that may indicate a security incident.

SEIM Systems

- **Improve security visibility**
  - Collect data from a variety of sources, which gives security teams a more comprehensive view of their IT environment and the security threats that it faces
- **Detect security threats**
  - Used to detect a wide range of security threats, including malware, intrusions, and insider threats
- **Respond to security incidents**
  - Help security teams to respond to security incidents more quickly and effectively.

SEIM System benefits

- Improve security visibility
- Reduced risk of data breaches
- Improved compliance

SEIM System benefits

Feature	SIEM	IDS
Purpose	Collect and analyse security data from a variety of sources to identify threats and security incidents	Detect suspicious activity on a network or system
Use cases	Monitoring OT networks and systems for security threats and incidents	Detecting and responding to network intrusions
Deployment	Typically deployed on a centralised server	Typically deployed on individual devices or networks
Data sources	Event logs, network traffic, security alerts, etc.	Network traffic
Capabilities	Can identify threats and incidents by correlating data from multiple sources, generate alerts, and provide insights into security risks	Can detect suspicious activity, such as unusual traffic patterns or known attack signatures

IDS/IPS and SIEM

- Complimentary systems
  - IDS/IPS system detects a suspicious IP address trying to access a critical server
  - IDS/IPS system generates an alert and blocks the traffic
  - Alert is sent to the SIEM system
  - SIEM correlates the alert with firewall logs and server logs
  - SIEM identifies a potential security incident and alerts to the security team
  - Security team investigates the alert and determines a malicious attack
  - Security team takes action to mitigate the attack.

Monitoring – IDS tools

- **Honey Pot**
  - A trap set to detect, deflect, or in some manner counteract attempts at unauthorised use of information systems
  - **Enticement**
    - A Honey Pot placed with open security vulnerabilities and services with known exploits is enticement
    - Perpetrator makes their own decision to perform the exploit.
  - **Entrapment**
    - If the honey pot actively solicits subjects to access it and then the owner charges them with unauthorised intrusion
    - Typically llegal.

Vulnerability scanner

- Search for and map systems for weaknesses
  1) Look for active IP addresses, open ports, OS's and any applications running
  2) Create a report or move to the next step
  3) Attempt to determine the patch level of the OS or applications.
     - Can cause an exploit such as crash the OS or application
  4) Attempt to exploit the vulnerability.
- Scanners may either be malicious or friendly. Friendly scanners usually stop at step 2 and occasionally step 3 but never go to step 4.

Vulnerability scanner types

- **Port Scanner**
  - NMAP.
- **Network Scanner**
  - OpenVAS, Metasploit.
- **Web Application Security Scanner**
  - OWASP Zed Attack Proxy (ZAP).
- **Computer worm**
  - Self-replicating computer program that replicates itself to other nodes
  - Unlike a virus, it does not need to attach itself to an existing program
  - Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.

Penetration testing

- Penetration testing is a method of evaluating security by simulating an attack, (Black Hat Hacker, or Cracker)
  - Active analysis of the system
  - Analysis from the position of a potential attacker
  - Active exploitation of security vulnerabilities.
- Security issues found are presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution
- Penetration testing determines the feasibility of an attack and the business impact of a successful exploit
- It is a component of a full security audit.

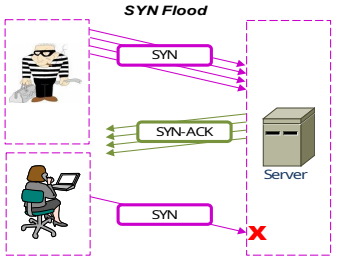
Padded cell

- A padded cell is like a honey pot but is used for intruder isolation.
- When the IDS detects an intruder he/she is transferred to the padded cell.
- The padded cell has the look of an actual system but with fake programs and data, a simulated environment of sorts.

Methods of Attack

- Brute Force Attack
- Dictionary Attack
- DoS attacks
- DDoS attack
- Smurf attack (ping)
- Spoofing
- MitM Attack
- Spamming
- Sniffers.

- DoS Attack



- Password cracker

Learning objectives

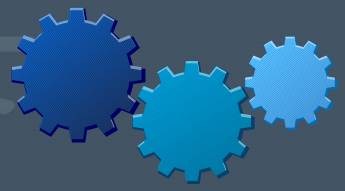
You should now be able to:

- Define access control and explain its importance ✓
- Analyse the different types of access control and their strengths and weaknesses ✓
- Describe the principles of layered access control and how they work together to protect resources ✓
- Assess the importance of password security and the risks of weak passwords ✓
- Discuss the responsibilities of access control administrators and their role in implementing, managing, and monitoring access control policies and procedures ✓

Exercise #4

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Scenario



Worksheet

Resource:

Type of Access Control:

Strengths	Weaknesses

TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An tIarthar Láir
Technological University of the Shannon: Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CEng, FIEI

CISSP®

Thank you

TUS