Sviluppo di Software Sicuro - S^3
Tokeneer ID Station (TIS)
Software Requirements Specification (SRS)

Corso di Laurea Magistrale in
Sicurezza Informatica: Infrastrutture e Applicazioni
Università di Pisa – Polo di La Spezia
C. Montangero
Anno accademico 2009/10

Sommario

- Introduzione
- Supporto alla sicurezza
- Scenari d'uso
- Proprietà di sicurezza

S^3 2009/10 – TIS - SRS

INTRODUZIONE

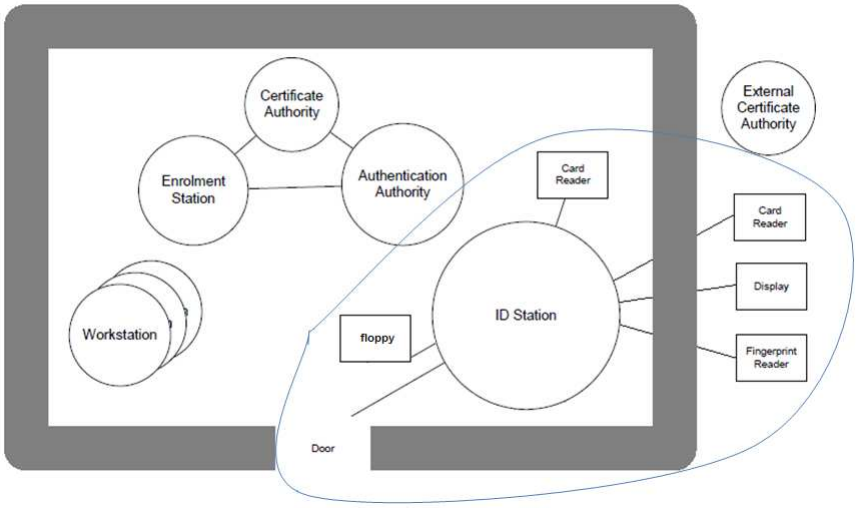
Contesto del progetto

- To demonstrate that developing highly secure systems to the level of rigour required by the higher assurance levels of the Common Criteria is possible
- NSA has asked Praxis High Integrity Systems to develop a high integrity variant of part of an existing secure system (the Tokeneer System)

Scopo dell'applicazione

- Proteggere l'accesso a un *enclave sicuro*
  - contiene workstation ad accesso controllato:
    - utente presenta un token (smartcard) per entrare
    - il sistema usa i dati
      - per un esame biometrico (e.g. verificare l'impronta digitale)
      - per impostare sul token i diritti dell'utente nell'uso delle workstation
  - la porta si apre solo se l'utente passa il test
    - proprietà essenziale da assicurare

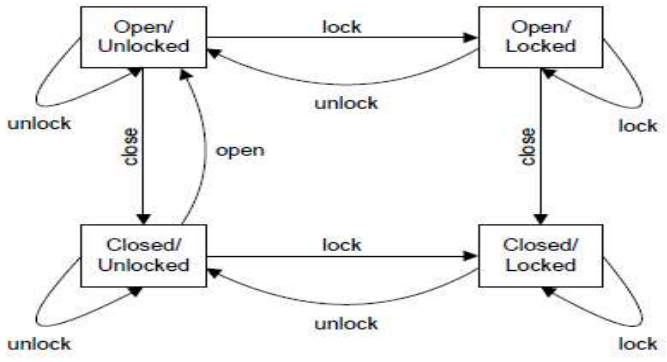
Il contesto del sistema



L'interfaccia

- The ID Station interfaces to 5 different physical devices:
  - Fingerprint reader
  - Smartcard reader
    - external to grant access to the enclave
    - internal to grant access to admin operations
  - Door
  - Visual display
  - An interface to some read/write, removable media
    - to take initialization data from the Enrolment Station
    - to take configuration data in
    - to take audit data out

La porta latch



- Quasi tutte le possibili combinazioni

S3 2009/10 – TIS - SRS

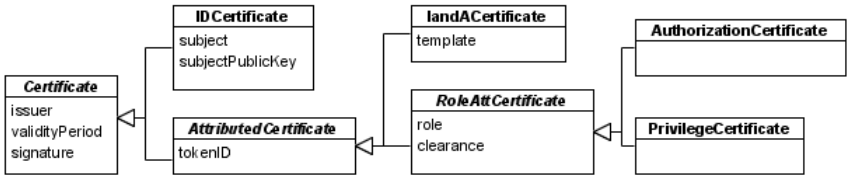
SUPPORTO ALLA SICUREZZA

Diritti e Classi

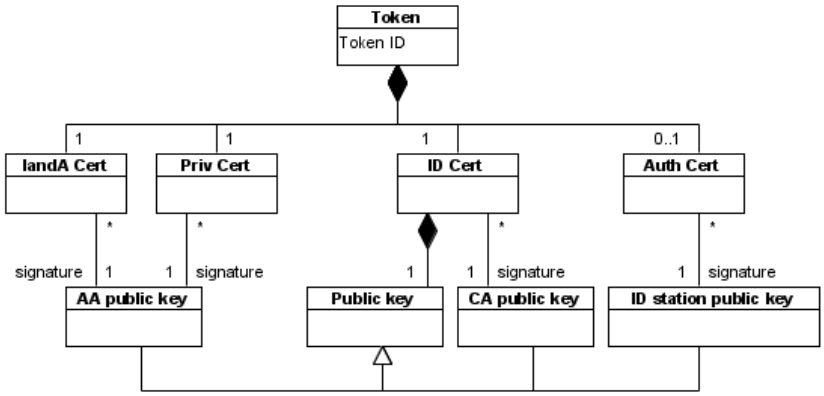
- *PRIVILEGE*
  - *userOnly | guard | securityOfficer | auditManager*
    - *ultimi tre: amministratori*
- *CLASS*
  - *unmarked |*
    unclassified |
    restricted | confidential | secret | topsecret

I certificati

- nome e firma del rilasciante, periodo validità
  - ID: nome e chiave pubblica
  - Attributed: nome del token cui appartengono
    - I&A: modello dell'impronta digitale
    - ruoli: ruolo e clearance del portatore del token
      - privilege: in quanto portatore
      - authorization: per il particolare accesso



Token (smart card)



Autorità: AA=Attributii, CA=Certificati

Enrolment data

- The ID Certificate of this ID Station
  - signed by a CA
- The ID Certificates of the other Issuers. They belong to
  - CAs, who authenticate AAs (Attribute Authorities) and ID Stations (self signed)
  - AAs, who authenticate privilege and I&A certificates

S^3 2009/10 – TIS - SRS

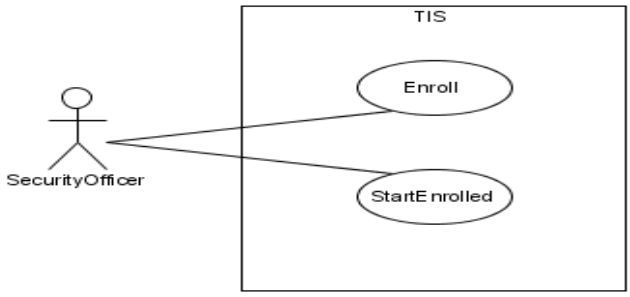
SCENARI D'USO

Formato degli scenari

- Description
- Stimulus
- Assumptions
- Success End-conditions
- Failure Conditions
- Constraints
- Rationale
- Issues

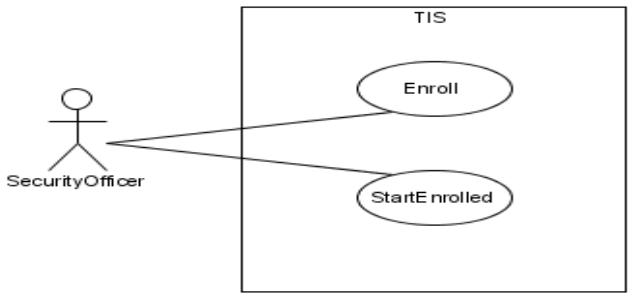
- Parenti dei casi d'uso
  - *no interazioni esplicite*
  - *eventi di audit nelle condizioni successo/fallimento*

Scenari startup



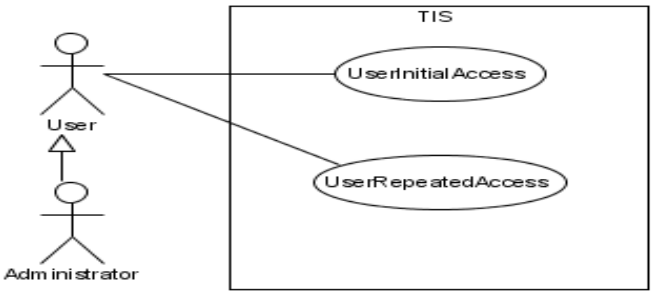
- Enroll: A person powers up the ID Station system, and loads the initialisation data from the Enrolment Station via a floppy disk.
  - Come garantire che la persona che ha accesso senza TIS, sia un SecurityOfficer, e abbia i privilegi necessari?
  - Procedure apposite

Scenari startup



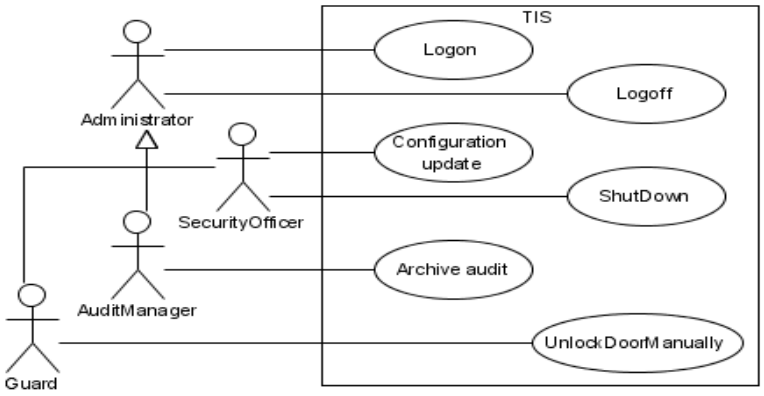
- StartEnrolled: A person powers up the ID Station system, and the ID Station becomes available for use, as it has previously been enrolled.
  - Come garantire che la persona che ha accesso senza TIS, sia un SecurityOfficer, e abbia i privilegi necessari?
  - Procedure apposite

Scenari utente



- *Initial:* A User who should be allowed access to the enclave is given access, making use of biometric authentication.
- *Repeated: nell'intervallo di validità di un accesso precedente*
- *NB: non si considera l'uscita.*

Scenari amministratore



Logon: An Administrator logs onto the ID Station by inserting their Token in the Admin Token Reader.
Logoff: Dual

ID Station is started and enrolled with input from the Enrolment Station

- Description
  - A person powers up the ID Station system, and loads the initialisation data from the Enrolment Station via a floppy disk.
- Stimulus
  - Launching the ID Station application from the Windows interface.
- Assumptions
  - Enrolment data for the ID Station is unavailable internally to the system.
  - A floppy disk has been inserted into the drive, and the data on the floppy disk from the Enrolment Station is correct.
  - The door is closed and locked.

ID Station is started and … (2)

- Success End-conditions
  - The ID Station is running and ready for use, with the data as supplied from the floppy.
  - The door is closed and locked.
  - The following events have been recorded in the Audit Log (in any order), and the existing audit records are preserved:
    - System start-up
    - New enrolment data

ID Station is started and … (3)

- Failure Conditions
  - The data from the Enrolment floppy is not successfully read.
    - Result: the Door is locked and the system is shutdown.
  - Audit files cannot be successfully written.
    - Result: the Door is locked and the system is shutdown.
  - Space for audit files has been exhausted.
    - Results:
      - the oldest audit records are overwritten with the new audit records, and
      - an alarm is raised to the Guard.

ID Station is started and … (4)

- Constraints
  - Not allowed during this scenario:
    - ID Station Configuration data changes
    - User use
- Issues
  - How do we distinguish between authorised and non-authorised people? Do we intend that only authorised people will be able to start up the system? (Email from NSA, 24/2/2003).
  - Answer: ?

ID Station is started and … (5)

  - we cannot distinguish between authorised and unauthorised people without enrolment data, because it is the presence of the data that defines “authorised” as “known and accepted by the specified authority, which I define for you by giving you keys to check with”.
- Ergo: procedure d'accesso per inizializzazione
  - al di fuori della portata del sistema.

ID Station is started already enrolled

- Description
  - A person powers up the ID Station system, and the ID Station becomes available for use, as it has previously been enrolled.
- Stimulus
  - Launching the ID Station application from the Windows interface.
- Assumptions
  - Enrolment data for the ID Station *is available* internally to the system.
  - The door is closed and locked.

ID Station is shut down

- Description
  - An authorised person powers down the ID Station system.
- Stimulus
  - Command to shut down is typed into the console.
- Assumptions
  - The door is closed and locked.
  - A Security Officer is currently logged onto the ID Station.

ID Station is shut down (2)

- Success End-conditions
  - The ID Station is no longer running and responds to no inputs
  - *The door is closed and locked*
  - The following events have been recorded in the Audit Log (in any order), and the existing audit records are preserved:
    - Invocation of command to shutdown
    - System shutdown

Configuration data

- Durations for internal timeouts.
  - These effect how long the system waits before raising an audible alarm, how long the system leaves the door unlocked for, and how long the system waits for a successful token removal.
- The security classification of the enclave.

Configuration data (2)

- The rules for allocating validity periods to authorisation certificates.
  - They depend on the time at which the certificate was issued, and may also depend on the role of the user, e.g., some roles may not be given use of the workstations “out of hours”
- The rules for allowing entry to the enclave.
  - These rules will depend on the role and security classification of the user, e.g., as above

Configuration data (3)

- The minimum size of the audit log before truncation may occur
  - within the available file store capacity of the TIS
- The size of the audit log at which an alarm is raised
  - a slightly smaller value
  - with the intention that the audit log will be archived and cleared before the truncation occurs

Security Officer updates the configuration of the ID Station Description

- Description
  - A Security Officer updates the ID Station configuration data with a completely new set of data, from a floppy.
- Stimulus
  - Command to re-configure is typed into the console.
- Assumptions
  - The door is closed and locked.
  - A Security Officer is currently logged onto the ID Station.

Security Officer updates … (2)

- Success End-conditions
  - The ID Station is available for use with its configuration identical to that specified on the floppy.
  - The door is closed and locked.
  - The following events have been recorded in the Audit Log (in any order), and the existing audit records are preserved:
    - invocation of command to modify configuration
    - modification of ID Station configuration data values

Security Officer updates … (3)

- Failure Conditions
  - The configuration data cannot be successfully read from the floppy.
  - Audit files cannot be successfully written.
    - Result: the Door is locked and the system is shutdown.
  - Space for audit files has been exhausted.
    - Result:
      - the oldest audit records are overwritten with the new audit records
      - an alarm is raised to the Guard.
- Constraints
  - No ID Station shutdown or User use will be allowed during this scenario.

User gains allowed initial access to Enclave

- Description
  - A User who should be allowed access to the enclave is given access, making use of biometric authentication.
- Stimulus
  - User inserts a smartcard into the smartcard reader.

User gains allowed initial access to Enclave (2)

- Assumptions
  - The ID Station has valid start-up data.
  - The ID Station has a valid data configuration.
  - The ID Station is quiescent (no other access attempts, configuration changes or start-up activities are in progress).
  - The User is outside the enclave; the door is closed and locked.

User gains allowed initial access to Enclave (3)

- Assumptions (2)
  - The card inserted by the User has
    - a valid ID Certificate,
    - I&A Certificate, and
    - Privilege Certificate,
    - a valid fingerprint template that matches the fingerprint of the User's finger.
  - The card inserted by the User does not have a valid, current AuthCertificate

User gains allowed initial access to Enclave (4)

- Success End-conditions
  - The User has possession of the card he originally inserted.
  - The card inserted by the User contains a current, valid Authorisation Certificate with
    - validity time: from now until now+(length of time specified in ID Station configuration data)
    - security level: equal to the minimum of
      - the security level defined in the ID Station configuration data
      - the security level in the Permission Certificate on the User card

User gains allowed initial access to Enclave (5)

- Failure Conditions
  - The card inserted by the User does not allow all its data to be successfully read, possibly due to
    - being incorrectly inserted in the first place;
    - being a faulty card;
    - having the incorrect information on it;
    - being removed before all the information has been read.
    - The set of data to be read is at least:
      - ID Certificate
      - I&A Certificate
      - Privilege Certificate
      - Fingerprint Template (contained in the I&A Certificate)

User gains allowed initial access to Enclave (6)

- Failure Conditions (2)
  - A matching fingerprint has not been read, possibly due to
    - no finger being presented to the fingerprint reader within X seconds of the display requesting a fingerprint;
    - the fingerprint not being successfully read within X seconds of the display requesting a fingerprint;
      - The value X shall be taken from configuration data of the ID Station.
    - the fingerprint that was successfully read not being successfully matched to the template read from the card.

User gains allowed initial access to Enclave (7)

- Failure Conditions (3)
  - The card originally inserted by the User does not allow a new Authorisation Certificate to be successfully written, possibly due to
    - being incorrectly inserted in the first place;
    - being a faulty card;
    - being removed before all the information has been written.
  - The User is too slow in opening the door, so the door locks with the user still outside the enclave
  - The user opens the door, but chooses not to pass through, closing the door again
    - come si distingue dal caso in cui entra?

User gains allowed initial access to Enclave (8)

- Failure Conditions (4)
  - Once the door has been opened, it is not allowed to close (it is propped open).
  - Audit files cannot be successfully written.
    - Result: the Door is locked and the system is shutdown.
  - Space for audit files has been exhausted.
    - Result: the oldest audit records are overwritten with the new audit records, and
    - an alarm is raised to the Guard.
- Constraints
  - No ID Station restart or Configuration data changes will be allowed during this scenario.

Issue

- What is the value of “X” above?
- Problem: someone could swap a different card into the card reader while the fingerprint is being taken
  - need to detect the card being removed and reinserted
- Solutions:
  - once the Auth Cert is written, read all the information off again and compare it with the originally values
    - may be an unacceptable performance
  - sufficiently frequent polling of the state of the card reader will ensure that no card swap will have occurred

S3 2009/10 – TIS - SRS

PROPRIETÀ DI SICUREZZA

Property 1: Unlock with Token

- *If the latch is unlocked by the TIS, then*
  - *the TIS must be in possession of either a User Token or an Admin Token.*
  - *The User Token must have*
    - *either a valid Authorisation Certificate,*
    - *or valid ID, Privilege, and I&A Certificates, together with a template that allowed the TIS to successfully validate the user's fingerprint.*
  - *Or, if the User Token does not meet this, the Admin Token must have*
    - *a valid Authorisation Certificate, with role of "guard".*

Property 2: Unlock at allowed time

- *If the latch is unlocked automatically by the TIS, then*
  - *the current time must be close to being within the allowed entry period defined for the User requesting access.*
    - "close" is intended to allow a period of grace between checking that access is allowed and actually unlocking the latch.
    - "automatically" refers to the latch being unlocked by the system in response to a user token insertion, rather than being manually unlocked by the guard.

Property 3 & 4

- Alarm when insecure:
  - *An alarm will be raised whenever the door/latch is insecure.*
    - "insecure" : the latch is locked, the door is open, and too much time has passed since the last explicit request to lock the latch.
- No loss of audit:
  - *No audit data is lost without an audit alarm being raised.*

S^3 2009/10 – TIS - SRS

PROSSIMO ARGOMENTO:
TIS - ARCHITETTURA