Information and Network Security

Access Control -2

Access Control

- Access Control Mechanisms
  - Rule based Access Control
  - Constrained User Interfaces
  - Access Control Matrix
  - Capabilities and ACL
  - Content and Context Based Access Control
- Access Control Administration
- Network Access Control
  - Firewalls
  - IDS
- Single Sign-On Systems

Rule Based Access Control

- uses specific rules that indicate what can and cannot happen between a subject and an object
- based on the simple concept of “if X then Y” i.e propositional logic
- Rule-based access control is NOT necessarily identity-based
  - Tom can use 5 MB attachments
  - Finance officer can use 6 MB attachments
  - Every user with secret clearance can use 5 MB attachments

Constrained User Interfaces

- Database Views

Harris, D	$45,000	8am-5pm
Torkelson, T	$60,000	6pm-2am
Kowtko, J	$45,000	8am-5pm
Swenson, J	$65,000	6pm-2am

Payroll database view

Harris, D	Work history	8am-5pm
Torkelson, T	Work history	6pm-2am
Kowtko, J	Work history	8am-5pm
Swenson, J	Work history	6pm-2am

Manager database view

- Restricted Shells
- Physical Constraints (ATM)

Access Control Matrix

- Table of **subjects** and **objects** indicating, what actions individual subjects can take upon individual objects
- Usually an attribute of DAC models
- The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs)

Access Control Matrix

- Capabilities
  - specifies the access rights a certain subject possesses pertaining to specific objects.
  - corresponds to the subject's row in the access control matrix
  - capability table bound to a subject
  - Capability can be in the form of a token, ticket, or key

User	File1	File2	File3
Diane	Read and execute	Read, write, and execute	No access
Katie	Read and execute	Read	No access
Chrissy	Read, write, and execute	Read and execute	Read
John	Read and execute	No access	Read and write

Table 3-1 An Example of an Access Control Matrix

Access Control Matrix

- Capabilities
  - specifies the list of subjects authorized to access a specific **object**
  - ACL corresponds to the **object's column** in the access control matrix
  - ACL is bound to an object

Access Control Matrix

	Subject	File 1	File 2	File 3	File 4
	Larry	Read	Read, write	Read	Read, write
Capability	Curly	Full control	No access	Full control	Read
	Mo	Read, write	No access	Read	Full control
	Bob	Full control	Full control	No access	No access
				ACL	

Capability = row in matrix
ACL = column in matrix

Content and Context based Access

- Content dependent Access Control

As the name suggests, with *content-dependent access control*, access to objects is determined by the content within the object. The earlier example pertaining to database views showed how content-dependent access control can work. The content of the database fields dictates which users can see specific information within the database tables.

- Context dependent Access Control
  - Firewalls and Intrusion detection systems

Context-dependent access control differs from content-dependent access control in that it makes access decisions based on the context of a collection of information rather than on the sensitivity of the data. A system that is using context-dependent access control "reviews the situation" and then makes a decision. For example, firewalls make context-based access decisions when they collect state information on a packet before allowing it

Summary

Access Control Techniques

Access control techniques are used to support the access control models.

- **Access control matrix** Table of subjects and objects that outlines their access relationships
- **Access control list** Bound to an object and indicates what subjects can access it and what operations they can carry out
- **Capability table** Bound to a subject and indicates what objects that subject can access and what operations it can carry out
- **Content-based access** Bases access decisions on the sensitivity of the data, not solely on subject identity
- **Context-based access** Bases access decisions on the state of the situation, not solely on identity or content sensitivity
- **Restricted interface** Limits the user's environment within the system, thus limiting access to objects
- **Rule-based access** Restricts subjects' access attempts by predefined rules

Access Control Administration

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password from the RADIUS client to the server.	Encrypts all traffic between the client and server.
AAA support	Combines authentication and authorization services.	Uses the AAA architecture, separating authentication, authorization, and auditing.
Multiprotocol support	Works over PPP connections.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Responses	Uses single-challenge response when authenticating a user, which is used for all AAA activities.	Uses multiple-challenge response for each of the AAA processes. Each AAA activity must be authenticated.

Non-repudiation

- **The goal of non-repudiation is to ensure undeniability of a transaction by any of the parties involved. A trusted third party, such as Trent, can be used to accomplish this.**
- For example, let us say Alice interacted with Bob at some point, and she does not want Bob to deny that she interacted with him. Alice wants to prove to some trusted third party (i.e., Trent) that she did communicate with Bob.

Non-repudiation

- **To summarize, trusted third parties can help conduct non-repudiable transactions.**
- In general, non-repudiation protocols in the world of security are used to ensure that two parties cannot deny that they interacted with each other.
- In most non-repudiation protocols, as Alice and Bob interact, various sets of evidence, such as receipts, are generated.
- The receipts can be digitally signed statements that can be shown to Trent to prove that a transaction took place.

Non-repudiation

- Unfortunately, while non-repudiation protocols sound desirable in theory, they end up being very expensive to implement, and are not used often in practice.

Single Sign On Systems

KERBEROS

- Provides a centralized authentication server to authenticate users to servers and servers to users.
- Relies on conventional encryption, making no use of public-key encryption
- Two versions: version 4 and 5
- Version 4 makes use of DES

Kerberos v4 Dialogue

(1) C → AS $ID_c \parallel ID_{tgs} \parallel TS_1$

(2) AS → C $E(K_c, [K_{c,tgs} \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2 \parallel Ticket_{tgs}])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \parallel ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $ID_v \parallel Ticket_{tgs} \parallel Authenticator_c$

(4) TGS → C $E(K_{c,tgs}, [K_{c,v} \parallel ID_v \parallel TS_4 \parallel Ticket_v])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \parallel ID_C \parallel AD_C \parallel ID_{tgs} \parallel TS_2 \parallel Lifetime_2])$$

$$Ticket_v = E(K_v, [K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4])$$

$$Authenticator_c = E(K_{c,tgs}, [ID_C \parallel AD_C \parallel TS_3])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Ticket_v \parallel Authenticator_c$

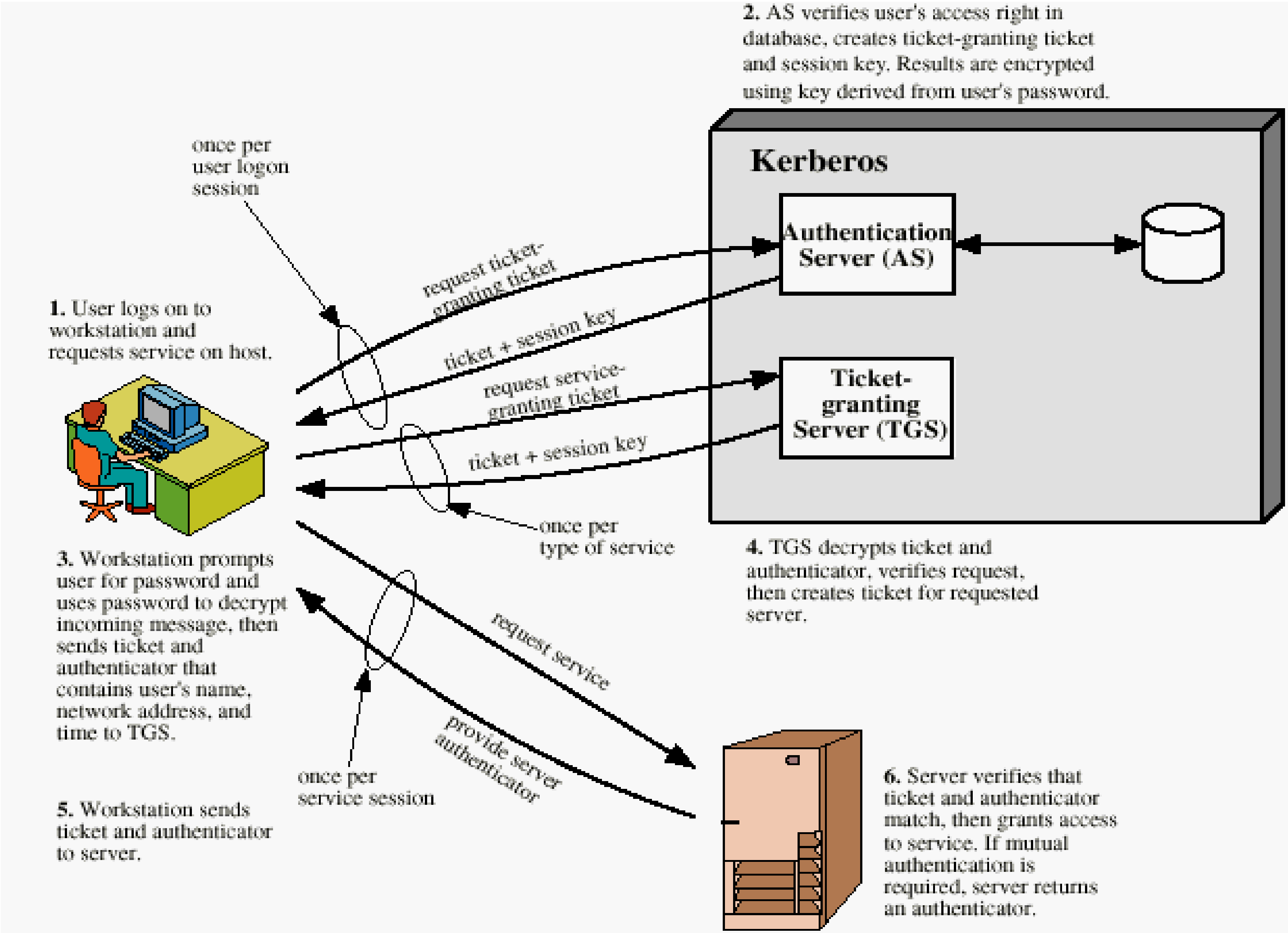
(6) V → C $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$$Ticket_v = E(K_v, [K_{c,v} \parallel ID_C \parallel AD_C \parallel ID_v \parallel TS_4 \parallel Lifetime_4])$$

$$Authenticator_c = E(K_{c,v}, [ID_C \parallel AD_C \parallel TS_5])$$

(c) Client/Server Authentication Exchange to obtain service

Overview of Kerberos



Version 4 Authentication Dialogue

- Problems:
  - Lifetime associated with the ticket-granting ticket
  - If too short → repeatedly asked for password
  - If too long → greater opportunity to replay
- The threat is that an opponent will steal the ticket and use it before it expires

Difference Between Version 4 and 5

- Encryption system dependence (V.4 DES)
- Internet protocol dependence
- Message byte ordering
- Ticket lifetime
- Authentication forwarding
- Inter-realm authentication

Questions?