Distributed Systems
Security – Part 2

Dr Soumyabrata DEV
https://soumyabrata.dev/

School of Computer Science and Informatics
University College Dublin
Ireland

These course slides are adapted from the original course slides prepared by Dr Anca Jurcut, University College Dublin.

Applications of Cryptography

- Digital Certificates
- Access Control
- Capabalities

Certificates

Digital certificates can be viewed as an attachment to an electronic message that is used to verify that a user is who they claim to be.

Issues regarding certificate management.

- What information should a certificate hold?
- How is a certificate created?
- How is a certificate validated?
- What happens when a certificate needs to be revoked?

In general, certificates may only be created by trusted authorities (e.g. a bank, a well-known company).

- Often they must themselves be authorized by a higher authority in order to become a trusted authority.
- This leads to the idea of certification chains - where should it start?

Certificates

- The main problem with digital certificates is revocation.
  - To revoke a certificate, every copy of that certificate would have to be destroyed.
  - This is difficult because certificates are stored in files and files can be copied.
- Often the easy solution is to place a time limit on the certificate.
  - Once it expires, a new certificate must be obtained.
- When this is not enough, the only alternative is to inform all recipients potential that the certificate is now invalid.
  - This is a lot more complex to implement.
- X.509 is the most widely used standard for certificates.

Authentication vs Authorization

- Authentication — Are you who you say you are?
  - Restrictions on who (or what) can access system
- Authorization — Are you allowed to do that?
  - Restrictions on actions of authenticated users
- Authorization is a form of access control
- But first, we look at system certification…

System Certification

- Government attempt to certify “security level” of products
- Of historical interest
  - Sort of like a history of authorization
- Still important today if you want to sell a product to the government
  - Tempting to argue it’s a failure since government is so insecure, but…

Orange Book

- Trusted Computing System Evaluation Criteria (TCSEC), 1983
  - Universally known as the “orange book”
  - Name is due to color of it’s cover
  - About 115 pages
  - Developed by U.S. DoD (NSA)
  - Part of the “rainbow series”
- Orange book generated a pseudo-religious fervor among some people
  - Less and less intensity as time goes by

Orange Book Outline

- Goals
  - Provide way to assess security products
  - Provide general guidance/philosophy on how to build more secure products
- Four divisions labeled D through A
  - D is lowest, A is highest
- Divisions split into numbered classes

EAL 1 through 7

- EAL1 — functionally tested
- EAL2 — structurally tested
- EAL3 — methodically tested, checked
- EAL4 — designed, tested, reviewed
- EAL5 — semiformally designed, tested
- EAL6 — verified, designed, tested
- EAL7 — formally verified

Authentication vs Authorization

- Authentication — Are you who you say you are?
  - Restrictions on who (or what) can access system
- Authorization — Are you allowed to do that?
  - Restrictions on actions of authenticated users
- Authorization is a form of access control
- Classic view of authorization…
  - Access Control Lists (ACLs)
  - Capabilities (C-lists)

Lampson's Access Control Matrix

- **Subjects** (users) index the rows
- **Objects** (resources) index the columns

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	—	—
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

x, r, and w stand for execute, read, and write privileges, respectively.

Are You Allowed to Do That?

- Access control matrix has all relevant info
- Could be 100's of users, 10,000's of resources
  - Then matrix with 1,000,000's of entries
- How to manage such a large matrix?
- Note: We need to check this matrix before access to any resource by any user
- How to make this efficient/practical?

Access Control Lists (ACLs)

- ACL: store access control matrix by column
- Example: ACL for insurance data is in blue

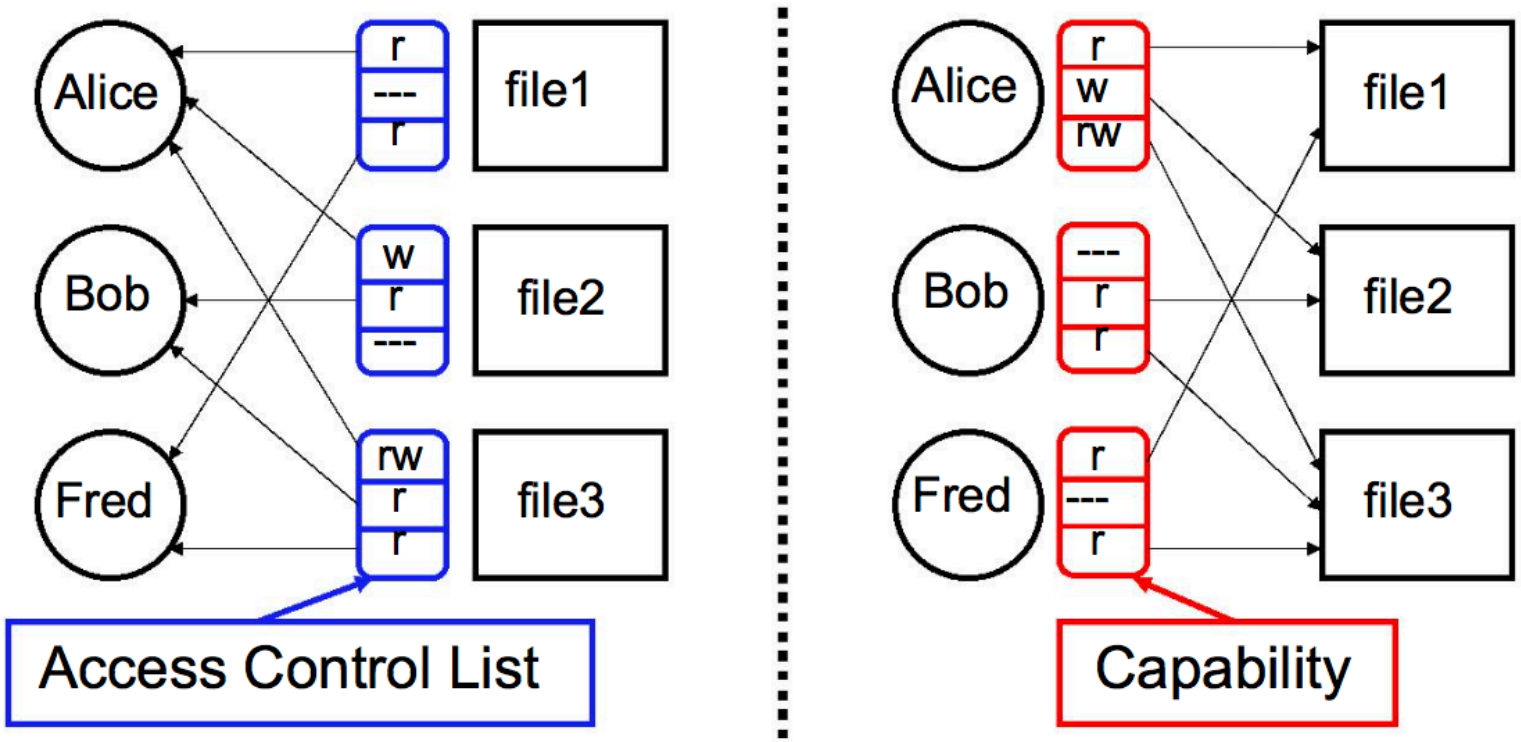
	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	—	—
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

Capabilities (or C-Lists)

- Store access control matrix by row
- Example: Capability for Alice is in red

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	—	—
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

ACLs vs Capabilities



- Note that arrows point in opposite directions…
- With ACLs, still need to associate users to files

ACLs vs Capabilities

- ACLs
  - Good when users manage their own files
  - Protection is data-oriented
  - Easy to change rights to a resource
- Capabilities
  - Easy to delegate — avoid the confused deputy
  - Easy to add/delete users
  - More difficult to implement
  - The “Zen of information security”
- Capabilities loved by academics
  - Capability Myths Demolished

Multilevel Security (MLS) Models

Classifications and Clearances

- Classifications apply to objects
- Clearances apply to subjects
- US Department of Defense (DoD) uses 4 levels:
  - TOP SECRET
  - SECRET
  - CONFIDENTIAL
  - UNCLASSIFIED

Multilevel Security (MLS)

- MLS needed when subjects/objects at different levels access same system
- MLS is a form of Access Control
- Military and government interest in MLS for many decades
  - Lots of research into MLS
  - Strengths and weaknesses of MLS well understood (almost entirely theoretical)
  - Many possible uses of MLS outside military

MLS Applications

- Classified government/military systems
- Business example: info restricted to
  - Senior management only, all management, everyone in company, or general public
- Network firewall
- Confidential medical info, databases, etc.
- Usually, MLS not really a technical system
  - More like part of a legal structure

MLS Security Models

- MLS models explain what needs to be done
- Models do not tell you how to implement
- Models are descriptive, not prescriptive
  - That is, high-level description, not an algorithm
- There are many MLS models
- We'll discuss simplest MLS model
  - Other models are more realistic
  - Other models also more complex, more difficult to enforce, harder to verify, etc.

Bell-LaPadula

- BLP security model designed to express essential requirements for MLS
- BLP deals with confidentiality
  - To prevent unauthorized reading
- Recall that O is an object, S a subject
  - Object O has a classification
  - Subject S has a clearance
  - Security level denoted L(O) and L(S)

BLP: The Bottom Line

- BLP is simple, probably too simple
- BLP is one of the few security models that can be used to prove things about systems
- BLP has inspired other security models
  - Most other models try to be more realistic
  - Other security models are more complex
  - Models difficult to analyze, apply in practice

Biba's Model

- BLP for confidentiality, Biba for integrity
  - Biba is to prevent unauthorized writing
- Biba is (in a sense) the dual of BLP
- Integrity model
  - Suppose you trust the integrity of O but not O
  - If object O includes O and O then you cannot trust the integrity of O
- Integrity level of O is minimum of the integrity of any object in O
- Low water mark principle for integrity

Distributed Systems: Case Study: Kerberos

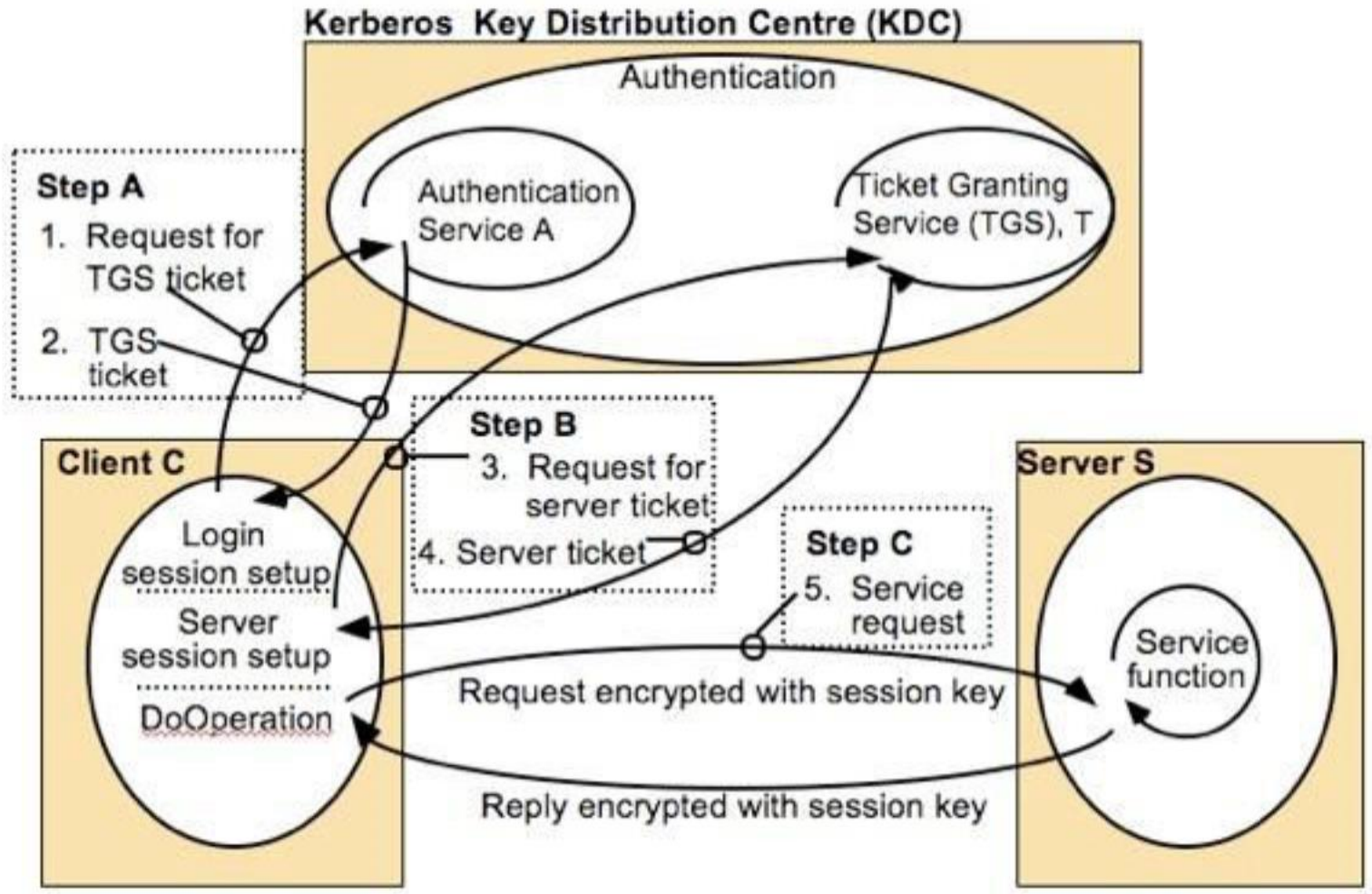
Introduction

- Kerberos is a computer network authentication protocol
  - allows nodes to communicate over non-secure network to prove their identity to one another in a secure manner
- Developed by MIT in the 1980's and soon to become an Internet Standard.
  - The default authentication service for Windows 2000.
- Shared secret-based strong 3rd party authentication
- provides single sign-on capability
- Passwords never sent across network

Adopts Mediated Authentication

- A trusted third party mediates the authentication process -
  - called the Key Distribution Centre (KDC)
- Each user and service shares a secret key with the KDC
- KDC generates a session key - securely distributes it to the communicating parties
- communicating parties prove to each other that they know each other

Kerberos System Architecture



Thank you

For general enquries, contact:

Please contact the Head Teaching Assistant: Xingyu Pan (Star), Xingyu.Pan@ucdconnect.ie