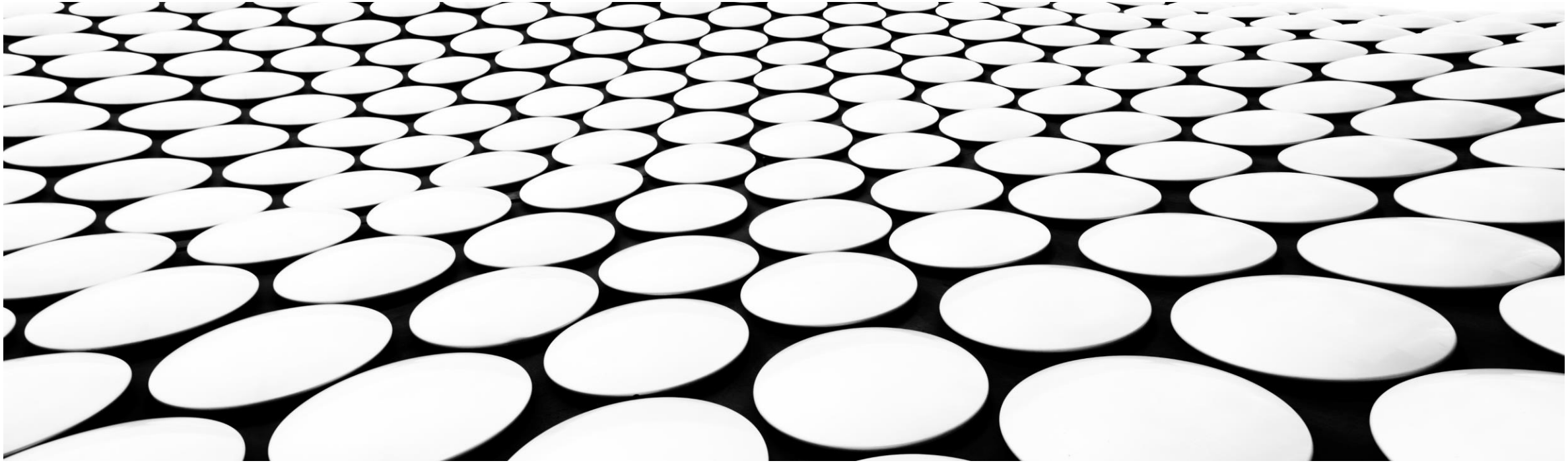
Security in distributed systems

COEN-317: Distributed Systems
Robert Bruce
Department of Computer Science and Engineering
Santa Clara University



Why implement security in distributed systems?

Scenarios:

- A distributed system contains compute nodes that are physically distant to each other and connected via a public internet.
- A distributed system uses sensitive data (such as medical records) or classified data that must be protected.

In these scenarios:

- How can you ensure data will not be tampered with?
- How can you ensure data will not be accessible by unauthorized users?
- How can you ensure the integrity of the distributed system?

Security threats

Interception: refers to access to communication by an unauthorized third-party [1].

Interruption: refers to denial of service attack which effectively makes a distributed system unusable and/or unavailable [1].

Modification: refers to unauthorized tampering with data or services in a distributed system [1].

Fabrication: refers to creating bogus data in a distributed system [1].

[1] pp. 502-503, *Distributed Systems* (3rd edition) by Maarten van Steen and Andrew S. Tanenbaum.

Security mechanisms

Encryption: refers to scrambling data to make it unreadable by an unauthorized third-party [1].

Authentication: refers to a form of identity verification prior to performing a transaction in a distributed system [1].

Authorization: refers to access privileges for authenticated users in a distributed system [1].

Auditing: refers to creation of transactional logs for every event in a distributed system [1].

[1] pp. 503-504, *Distributed Systems* (3rd edition) by Maarten van Steen and Andrew S. Tanenbaum.

Suggested security strategies

Use encryption everywhere:

- All network socket communication in the distributed system is encrypted via Secure Socket Layer (SSL).
- Database tables are encrypted.
- The native operating system filesystem is encrypted.

Identify the vulnerabilities of encryption:

- The encryption password is too weak or easily guessable (e.g. dictionary word or something simple like "123abc").
- The unencrypted data is stored in random access memory or in the CPU cache.
- The encryption algorithm used has known vulnerabilities or uses weak encryption.

Kerebos

What is Kerebos?

"...a security system that assists clients in setting up a secure channel with any server that is part of a distributed system" [1].

Where was Kerebos developed?

Kerebos was developed at Massachusetts Institute of Technology (MIT) [1].

How is security implemented?

Simply put, Kerebos uses an "Authentication Server" and a "Ticket Granting Service"

[1] p. 527, *Distributed Systems* (3rd edition) by Maarten van Steen and Andrew S. Tanenbaum.

Are full-proof secure distributed systems possible?

No distributed system is ever truly secure.

- There could be undiscovered vulnerabilities in the underlying security system software.
- A distributed system is only as secure as its authorized users: people are the weakest link in the security chain!

What can be done to minimize a security breach?

- Encrypt everything (filesystems, database tables, network communication sockets, etc.)
- Utilize strong passphrases instead of dictionary passwords.
- Identify the vulnerabilities of encryption (e.g. weak encryption algorithm, unencrypted data stored in RAM or CPU cache, etc.)
- Utilize modern, strong encryption standards.
- Utilize Kerebos.
- Utilize Blockchain technology for transaction logs.

Utilizing blockchain technology

Blockchain technology is an effective technique for storing transaction logs (audit logs).

- Unless an attacker can delete the blockchain-based transaction logs, the logs will be difficult to modify.
- The transaction log won't stop a data breach but could be highly beneficial during the investigation.

Transactions logs can identify:

- How an attacker successfully breached the system
- What areas were compromised

Non-accessible server nodes (air-gap)

Are non-networked (air-gapped) distributed systems a viable alternative?

- For remote attacks, such systems are certainly more difficult to penetrate. However, such systems are still vulnerable:

An air-gapped system can be compromised by an unsuspecting individual who has physical access to the distributed system and a usb flash drive.

- Real-world example: STUXNET penetrated a distributed system used for nuclear enrichment in Iran.
- This was a very sophisticated attack using USB flash drive to deliver the malware.

For further reading

Kerberos

https://web.mit.edu/Kerberos/

Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon by Kim Zetter

https://archive.org/details/countdowntozerod0000zett