Distributed and Edge Computing

Distributed Systems Security

Contents

Security issues and techniques in distributed system

Security challenges in edge computing

Introduction to digital forensics

Security issues and techniques in distributed system

Characteristics of Distributed Systems

Multiple entities

Heterogeneity

Concurrency

Resource sharing

Openness

Scalability

Transparency

Challenges of Distributed System

Synchronization

Fault Tolerance

Security

Distributed Systems Security

Distributed Systems Security

Securing distributed systems is crucial for ensuring data integrity, confidentiality, and availability across interconnected networks

In the past, security was typically handled on an end-to-end basis, since all the work involved in ensuring safety occurred “within” a single system and was controlled by one or two or few administrators

The distributed systems has created a new ecosystem that brings with it unique challenges to security

As they have multiple nodes working together to achieve a common goal

Distributed Systems Security

Security in a distributed system poses unique challenges that need to be considered when designing and implementing systems

A compromised computer or network may not be the only location where data is at risk; other systems or segments may also be infected with malicious code

As any threat can occur anywhere, even across distances in networks with few connections between them

Distributed Systems Security

Security Threats

Security Policy

Security Mechanisms

Security Threats

Different types of security threats:

- Interception
- Interruption
- Modification
- Fabrication

Interception

Refers to the situation that an unauthorized party has gained access to a service or data

It also happens when data are illegally copied

Interruption

Refers to the situation in which services or data become unavailable, unstable, destroyed and so on

Example: Denial of service attacks

Modification

Involves unauthorized changing of data or tampering with a service so that it no longer adheres to its original specifications

Fabrication

Refers to the situation in which additional data or activity are generated that would normally not exist

Security Policy

A description of security requirements, is needed that is known as security policy

A security policy describes precisely which action the entities in a system are allowed to take and which ones are prohibited

Entities include users, services, data, machines, and so on

Security Mechanisms

Important security mechanisms:

- Encryption
- Authentication
- Authorization
- Auditing

Encryption

Fundamental to computer security and important to protect data

Essential for ensuring confidentiality and integrity of the sensitive data

Need to protect sensitive data from unauthorized access, modification, or theft as well as ensure the privacy of data

Transforms plaintext data into ciphertext using algorithms (e.g., RSA, AES) so that attacker cannot understand

Ensures data confidentiality during transmission and storage

Encryption

Allows us to check whether data have been modified unauthentically ⇒ supports for integrity checks

Transport Layer Security (TLS) / SSL be used as standard protocol to encrypt data exchanged between clients and servers. Establishes a secure communication channels to prevent eavesdropping and tampering

Key Management: Manages encryption keys used to encrypt and decrypt data, that ensures secure storage, rotation, and distribution of keys to authorized entities

Authentication

The process of recognizing a user's identity

Used to verify the claimed identity of a user, client, server, host or other entity

The mechanism of associating an incoming request with a set of identifying credentials

The credential often takes the form of a password, which is a secret and known only to the individual and the system

Typically, users are authenticated by means of passwords, but there are many other ways to authenticate clients

Authentication Mechanisms

Password-based Authentication: Users authenticate with a username and password, commonly used approach but vulnerable to password breaches and phishing attacks

Multi-factor Authentication: Uses two or more authentication factors (e.g., password + OTP, fingerprint etc.), that enhances security by adding an extra layer of verification

Biometric Authentication: Uses unique biological parameters (e.g., fingerprints, facial recognition) for authentication, and it provides strong authentication but may require specialized hardware

Certificate-based Authentication: Uses digital certificates to authenticate clients and servers. Certificates are issued by trusted Certificate Authorities (CAs)

Authorization

After a client has been authenticated, it is necessary to whether that client is authorized to perform the action requested

A security mechanism to determine access levels or user/client privileges related to system resources

Process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity

Authorization Controls

Role-Based Access Control: Assigns permissions based on roles (e.g., admin, user, manager). Simplifies access management by grouping users with similar responsibilities

Attribute-Based Access Control: Grants access based on attributes (e.g., user properties, resource properties l·yŘ ǎƨ ƨy)

Access Control Lists (ACLs): ¦ǎŜǎ fists of permissions associated with users or groups. Lű ƛǎ l·LJLJfƛŜŘ Řirectly to resources to specify who can access them and what actions they can perform

Policy-Based Access Control: Uses policies to define access rules based on conditions & attributes, it offers flexibility to adapt access controls dynamically based on changing conditions

Auditing

Auditing tools are used to trace access contents and ways

Audit logs can be very useful for the analysis of a security breach, and subsequently taking measures against intruders

For this reason, attackers are generally keen not to leave any traces that could eventually lead to exposing their identity

In this sense, logging accesses makes attacking sometimes a riskier business

Why Security Audit ?

To verify that the current security strategy is adequate or not

To check that the security training efforts are working

To uncover any extraneous hardware and software

To uncover the flaws introduced by new technology or processes

To prove the organization is compliant with regulations

Security Challenges in Edge Computing

Edge computing

Latency is a problem where nearly instantaneous transfer of information is necessary

Edge computing addresses this problem by:

- Moving the task of initial data processing to connected devices
- Using edge data centers in place of central servers

Security Issues in Edge Computing

Data Security and Privacy Requirements

Confidentiality

Integrity

Availability

Authentication and access control

Privacy requirement

Data Security and Privacy Challenges

Edge computing utilizes different technologies to put the computing in the proximity of data sources

The data security and privacy-preserving have become the basic requirements to protect end users in their business, economics, and daily life

We must admit that security and privacy should be addressed in every layer in designing edge computing systems

Challenges in edge computing

Core Infrastructure:

- Privacy leakage
- Data tampering
- Denial of service
- Service manipulation

Edge Network

- Denial of service
- Man-in-the-middle

Edge Servers:

- Privacy leakage
- Denial of service
- Service manipulation
- Physical damage

Mobile Edge Devices

- Injection of information
- Service manipulation

Data Security and Privacy Mechanisms

Data confidentiality

Data integrity

Secure data computation

Authentication

Access control

Privacy preserving

Introduction to digital forensics

Forensic

Forensic Science is the application of scientific methods to establish factual answers to legal problems

Crime reconstruction is the determination of the actions and events surrounding the commission of a crime

An investigation is a systematic examination, typically with the purpose of identifying or verifying facts

A key objective during investigations is to identify key facts related to a crime or incident, and a common methodology used is referred to as 5WH

What is digital forensics?

Emerging discipline in computer security

Investigation that takes place after an incident has happened

Try to answer questions: Who, what, when, where, why, and how

Determine what the incident was and get back to a working state

Internal investigation

Criminal investigation

Support for “real world” investigations

Digital Forensics

Conventionally the forensics was limited to the recovery and analysis of biological and chemical evidence during criminal investigations

There is an increased adoption of digital devices and growing incidence of cyber crime

The art of recovering and analysing the contents found on digital devices such as desktops, laptops, tablets, smartphones, etc. for the purpose of investigation whenever an incident is happened

Digital Forensics

Digital forensics refers to forensic science applied to digital information, whereas a digital investigation refers to investigations in the digital domain

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations

Digital Forensics

The practice of collecting, analysing and reporting on digital data in a way that is legally admissible

Can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally

Use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage

Digital Forensic Requirements

Requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel

Similar to all forms of forensic science, it is comprised of the application of the law to computer science

Deals with the preservation, identification, extraction, and documentation of computer evidence

Digital Forensic Requirements

Also involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing

Uses specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed

Forensic Process

Forensic Process

Defines a structured investigation of digital evidence from any device capable of storing or processing data in a digital form

Many similarities to physical investigation processes

But the evidence of interest is digital in this case

Traditional forensics processes are challenged by how to gather what evidence to support a hypothesis of a crime or incident

The process needs to ensure that whatever digital evidence is identified, it must be managed properly for it to prove a case

Forensic Process

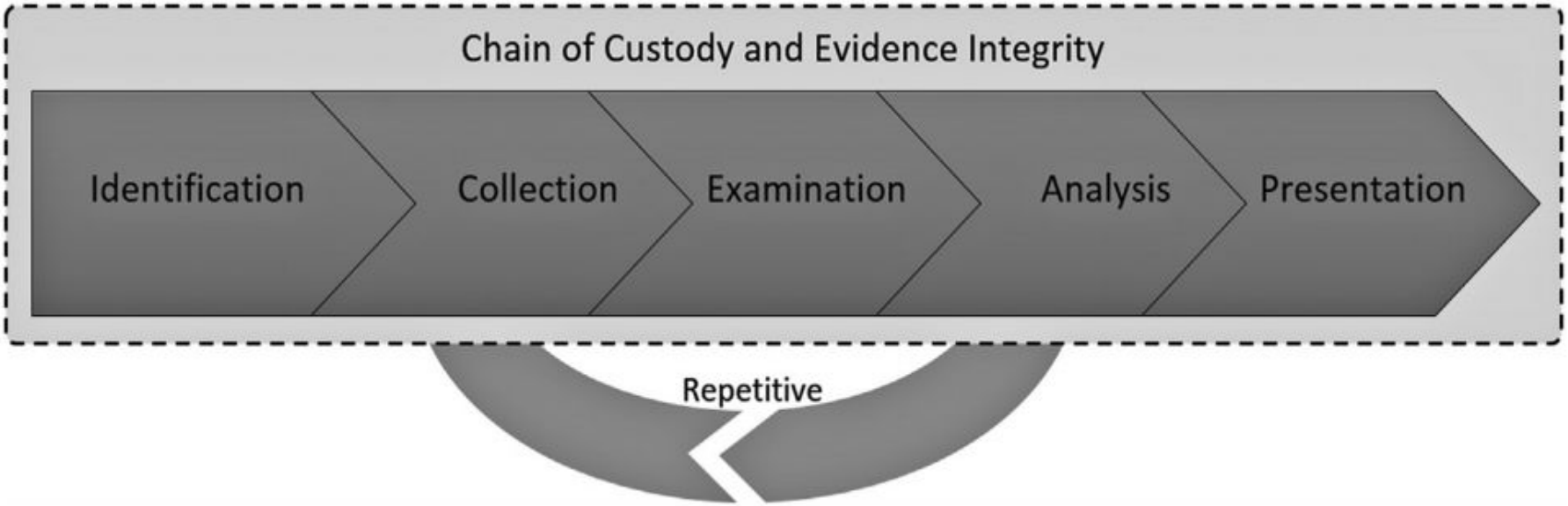
Accused murderers, robbers, and other criminals may have their electronic devices analyzed in an investigation to identify evidence about a crime

Such evidence can provide answers to the 5WH questions of investigations

Evidence may be found in diverse places like in a chat session, communication log, or any other digital traces. In the case of corporate investigations, loss or misuse of corporate confidential information is typically discovered by employees, customers, partners, or incident management analysts using security solutions and tools

The digital forensics process can thus be used in criminal investigations, corporate investigations, or even private investigations

The Digital Forensics Process



Identification Phase

Basis for all the following phases or activities during the digital investigation

Task of detecting, recognizing, and determining the incident or crime to investigate

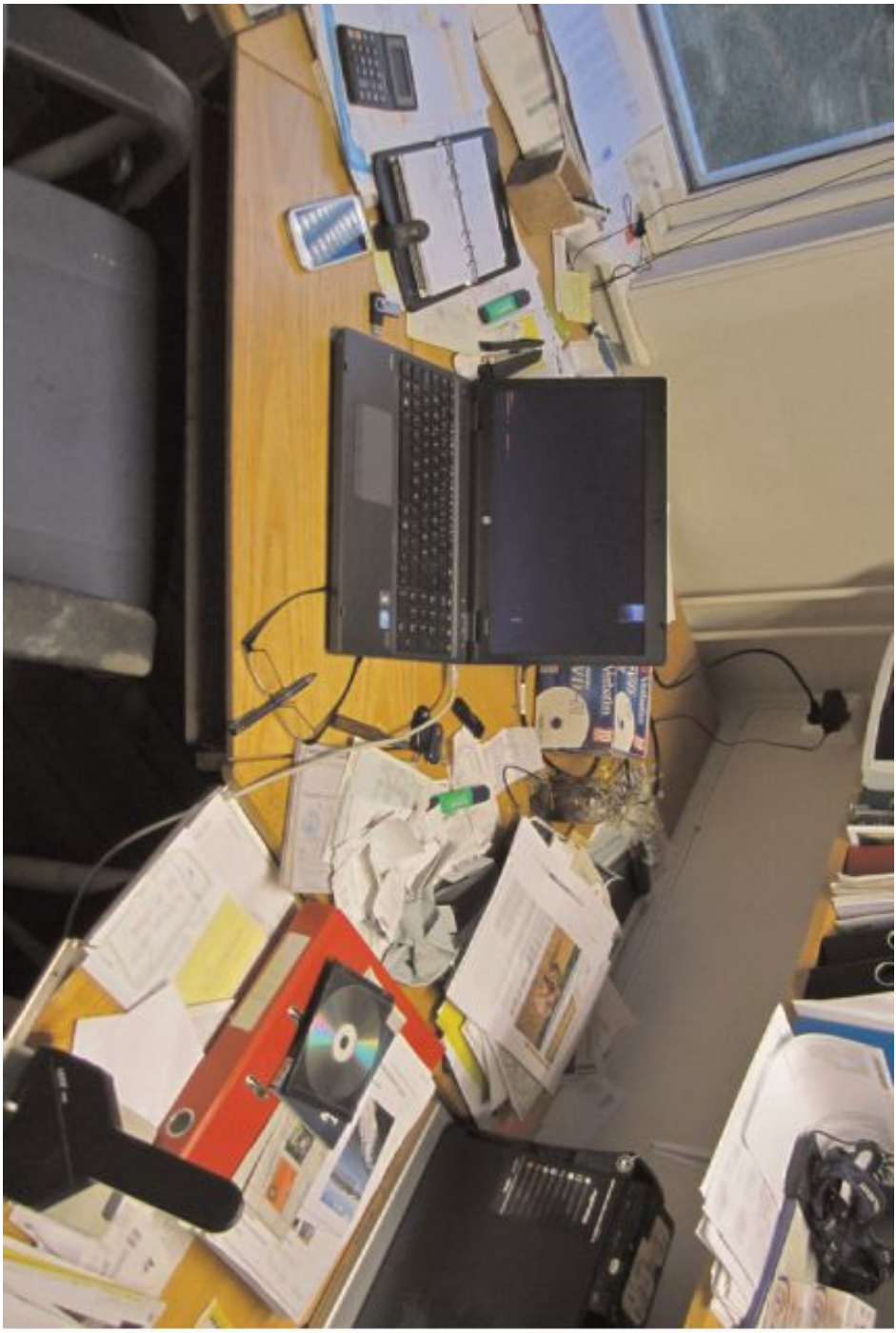
Incidents can be identified based on complaints, alerts, or other indications

Can be used to identify which evidence or objects to look for the investigation

The identification of an incident or a crime leads to the formation of a hypothesis about what might have happened

A digital forensics investigation is a response to an observed incident and the first responder must act accordingly

Example crime scene with multiple digital devices



Collection Phase

Refers to the acquisition or copying of the data

Collection of data from digital devices to make a digital copy using forensically sound methods and techniques

This is when a forensic investigator gains access to the electronic device(s) containing raw data that has been identified as relevant for the specific case

The collection phase of the digital forensics process is common to most literature and scientific research in digital forensics

Sources of Digital Evidence

Examples of order of volatility.

Type of storage media and data	Typical storage lifespan and longevity (dependent on usage)
System registers, peripheral memory, and caches	Nanoseconds
RAM	Ten nanoseconds
Network state	Milliseconds
Running system processes	Seconds
Data on disk (cache)	Minutes
Cloud storage	Months to years
HDD data storage	Years
Floppies and other magnetic tape–based media	Years to decades
CD-ROMs, DVDs, print-outs,	Decades
Read-only memory; flash and SSD data storage	Decades to centuries

Examination Phase

Preparation and extraction of potential digital evidence from collected data sources

Collected data must be examined and prepared for later analysis as part of the examination phase

it is important to document the actions and handling of the data to support the chain of custody

The examination often requires restructuring, parsing, and preprocessing of raw data to make it understandable for a forensic investigator in the upcoming analysis

To facilitate this phase, an analyst typically uses forensic tools and techniques appropriate for extracting relevant information

Analysis Phase

In this phase forensic investigators determine the digital objects to be used as digital evidence to support or refute a hypothesis of a crime, incident, or event

The processing of information that addresses the objective of the investigation with the purpose of determining the facts about an event, the significance of the evidence, and the person(s) responsible

Statistical methods manual analysis, techniques for understanding protocols and data formats, linking of multiple data objects (e.g., through the use of data mining), and timelining are some of the techniques that are used for analysis

As for all other investigative phases, the chain of custody is also important for the preservation and traceability of the collected data in the analysis phase

Presentation Phase

The process by which the examiner shares results from the analysis phase in the form of reports to the interested party or parties

The presentation phase involves the final documentation and presentation of the results of the investigation to a court of law or other applicable audiences, such as a corporation’s top management or crisis management team

The presentation is based on objective findings with a sufficient level of certainty, based on the analysis of digital evidence

It is important that the findings are summarized and that all actions performed during the investigation are accounted for and described in a fashion understandable by the audience

Wish you all the best for your final examination