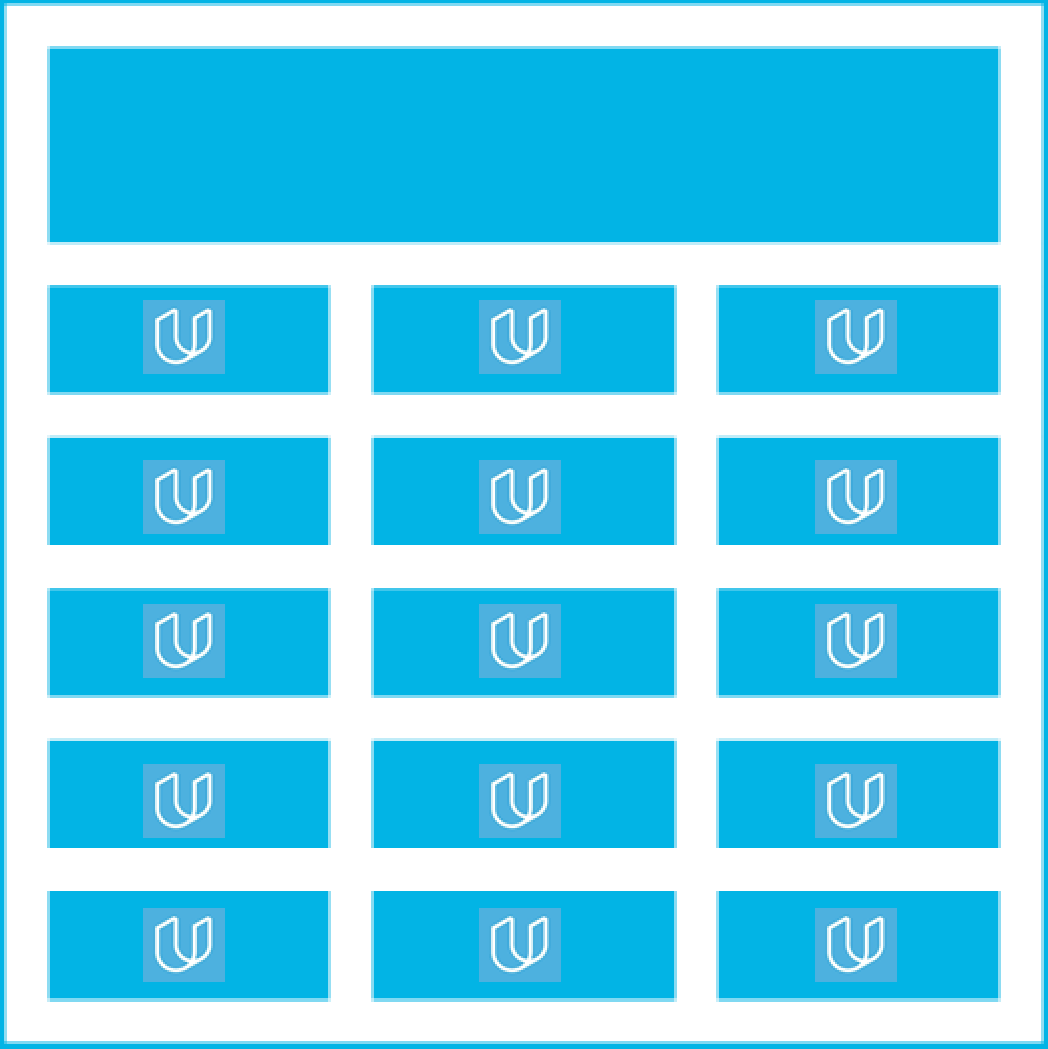
TimeSheets:
Threat Report



Rawan Amr Abdelsattar

30/3/2024

Purpose of this Report:

This is a threat model report for **TimeSheets**. The report will describe the threats facing TimeSheets. The model will cover the following:

- Threat Assessment
    - Scoping out Asset Inventory
    - Architecture Audit
    - Threat Model Diagram
    - Threats to the Organization
    - Identifying Threat Actors
- Vulnerability Analysis
- Risk Analysis
- Mitigation Plan

Section 1

Initial Threat Assessment

Completed Asset Inventory

Components and Functions

- ***TimeSheets Web Server:*** The web server's primary role is to serve static content to a requesting client through the http protocol.
- ***TimeSheets Application Server:*** The application server handles all the business logic process and serves dynamic content.
- ***TimeSheetsDB:*** The database server stores employee data and will be queried from the application server.
- ***AuthDB:*** Stores user authentication data (credentials) and will be queried from the application server.

Completed Asset Inventory

Overview of Application Functionality

TimeSheets is used by employees to track their hours worked. Users will login to the TimeSheets application from their device.

Data Flow

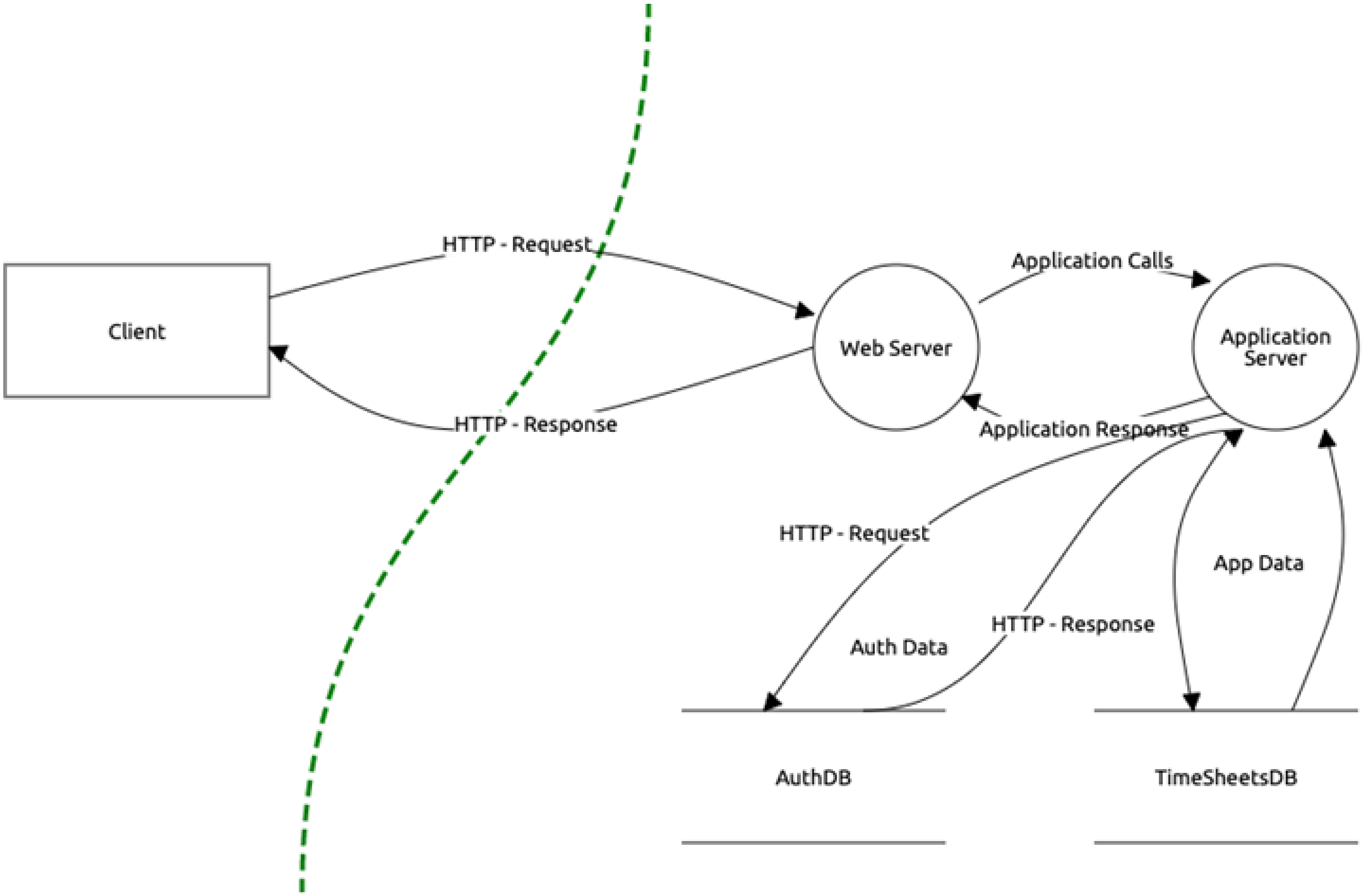
Request is generated from the client via the Internet. The request arrives at the TimeSheets web server which serves static content to the user (HTML, images, etc). Dynamic data is retrieved from the database and served to the client.

Completed Architecture Audit

Flaws

- *There is a lack of encryption at rest - database servers are storing data on unencrypted disks.*
- *There is lack of redundancy.*
- *There is no firewall that is filtering traffic coming from the Internet*

Completed Threat Model



- Employee Data Unencrypted at Rest
- Authentication data is using reversible encryption
- Authentication requests are not encrypted in transit
- Sensitive data is encrypted using DES algorithm

Completed Threat Analysis

What Type of Attack Caused the Login Alerts?

Man in the Middle (MitM)

What Proves Your Theory?

There is lack of encryption between the client and the application. A malicious actor is sniffing traffic and intercepting the requests with a valid username/password in the request. Additionally, the logs show successful login attempts from the expected IP, but also a different location at the same time.

Completed Threat Actor Analysis

Who is the Most Likely Threat Actor?

Internal User

What Proves Your Theory?

The IP address of the unexpected login matches that of an internal user. Additionally, there was no data leaked from the company, and no data changed. Just data accessed that the legitimate user typically doesn't access.

Section 2

Vulnerability Analysis

2.1 Employee Data Unencrypted at Rest

Discovery:

During the threat model the SRE team confirmed that the database is on a server that does not have encryption at rest.

Why is this an issue?

Not encrypting database on the server at rest poses a great security risk to the company and can have disastrous consequences, including:

- **Risk of unauthorized access:** as it threatens the confidentiality and the integrity of the data in case of a breach/ data leak posing threats like information disclosure and tampering (according to the STRIDE model).
- **Regulatory Compliance issues:** most regulations mandate encrypting database data at rest. Non-compliance with those regulations can cause financial penalties or lead to legal consequences.
- **Data theft/manipulation:** non-encrypted database data could be stolen and/or tampered with.

2.2 Authentication Data Stored Using Reversible Encryption

Discovery:

During the threat model the DBA team confirmed that the database is storing authentication data (credentials) encrypted.

Why is this an issue?

Storing authentication data in such way means that it can be decrypted as encryption is a two-way function.

This is a big security issue, as a knowledgeable attacker can reverse the encryption of/decrypt the authentication data, potentially leading to:

- **Identity theft:** successfully managing to access credentials of employees can lead to identity theft posing a security risk as a result of threats like spoofing and repudiation (in terms of STRIDE model)
- **Escalation of privilege:** having breached a system and accessed authentication data can enable the attacker to further try to attack other systems/applications within the network exploiting those credentials in various ways.

2.3 Authentication Requests are Unencrypted in Transit

Discovery:

During the threat model the security team confirmed that authentication requests are being transmitted in plaintext.

Why is this an issue?

According to **NIST SP 800-123** standard regarding general server security : *"Sensitive information transmitted unencrypted or weakly encrypted between the server and the client may be intercepted."* and this is because of the likelihood of attacks like **man-in-the-middle** and **spoofing** attacks where the attacker can intercept the communications and sniff packets violating confidentiality and integrity of data in transit.

These intercepted authentication data can lead to **identity theft** and/or **escalation of privilege** as mentioned earlier.

Also, according to the MITRE corporation, this is considered a weakness as in **"CWE-319: Cleartext Transmission of Sensitive Information"** with a likelihood of exploit of **"high"** and a scope of "Integrity" and "Confidentiality" and an impact of *"Anyone can read the information by gaining access to the channel being used for communication"***.**

2.DES Algorithm in Use

Discovery:

During the threat model the security team identified sensitive data being stored using the DES algorithm.

Why is this an issue?

Key Length: DES has a relatively short key length of 56 bits, making it vulnerable to brute-force attacks

Vulnerable Algorithm Design: DES has been shown to have vulnerabilities to various cryptographic attacks, including differential cryptanalysis and linear cryptanalysis, which can exploit weaknesses in the algorithm's design.

Standardization Issues: DES is a standardized encryption algorithm, but concerns have been raised regarding the National Security Agency's involvement in its development, leading to suspicions about potential backdoors or weaknesses intentionally introduced into the algorithm.

Furthermore, on June 02, 2005, on the news page of NIST official website it said, *"Adopted in 1977 for federal agencies to use in protecting sensitive, unclassified information, the DES is being withdrawn because it no longer provides the security that is needed to protect federal government information."*

Optional Task:

Examine the threat model diagram from Section 1 and answer:

What non-encryption issues can you identify?

What recommendation would you give to solve those issues?

Why do you recommend those solutions?

- **Communication between the client and the web server is done using HTTP:** HTTP messages are plaintext, which means that an attacker can intercept the communication potentially accessing and/or altering the data.
- **Recommendation:** Enforce using HTTPs to access web server
- **Justification:** HTTPs uses TLS to encrypt requests and responses, and to digitally sign those requests and

Section 3

Risk Analysis

3.1 Scoring Risks

Risk	**Score** ***(1 is most dangerous, 4 is least dangerous)***
Unencrypted at Rest	**2**
Reversible Encryption	**4**
Unencrypted in Transit	**1**
Outdated Algorithm	**3**

3.2 Risk Rationale

Why Did You Choose That Ranking? Make sure to include your risk ranking methodology. *(Did you use a tool or defined risk scoring system?)*

The risk scoring process was done using logical thinking, supported by my security knowledge.

Noticeably, the four risks provided are regarding data encryption. So, prioritizing them can be based on the risk of accessing the plaintext form of the data.

Logically thinking, we can divide the four risks into two groups in which one group includes two risks regarding unencrypted data (riskier) and the other regarding encrypted ones (less risky).

First, we have the two risks mentioning unencrypted data , however, comparing the two risks , unencrypted data in transit is considered to be riskier as it's exposed to interception and eavesdropping during transmission.

Second, we have the two risks mentioning encrypted data. undoubtedly, the risk of an outdated algorithm is more than that of a reversible encryption, both are reversible, but outdated algorithms are easier to break.

Section 4

Mitigation Plan

4.1 Employee Data Unencrypted at Rest

What is Your Recommended Mitigation Plan?

As guided by CIS, my recommendation is to enable encryption, often called full-disk encryption, on the server. A strong encryption algorithm as AES256 is recommended.

Why Did you Recommend This Course of Action?

Full Disk Encryption(FDE) encrypts the entire storage medium, such as HDD or SSD, at sector level. This means that every bit on the disk will be encrypted, providing a transparent layer of security, with encryption and decryption happening in the background.

AES 256 is an industry standard for data encryption, with a 256-bit key, operating on fixed-size blocks of data and encrypting them using a series of mathematical operations.

Combining both, we can ensure that our data remains protected even in the case of a breach or data leak.

4.2 Authentication Data Stored Using Reversible Encryption

What is Your Recommended Mitigation Plan?

Authentication data such as key and passwords should be stored as hashes not encrypted using reversible encryption. A secure hashing algorithm as **SHA-256** is recommended. Salting data may be a plus.

Why Did you Recommend This Course of Action?

While reversible encryption is a two-way function, which can be reversed and decrypted again retrieving the plaintext form of data, hashing is a one-way function which can NOT be reversed.

Hashing authentication data can help us protect it in case of a breach or a leak.

When performing authentication, user input can be hashed and compared with the original hashed data stored, ensuring that even if communication is intercepted or data is leaked it's still protected, not readable and irreversible.

4.3 Authentication Requests are Not Encrypted in Transit

What is Your Recommended Mitigation Plan?

As mentioned in **NIST SP 800-123**, Use secure protocols that can provide encryption of both passwords and data (e.g., SSH, HTTPS); do not use less secure protocols (e.g., telnet, FTP, NFS, HTTP) unless absolutely required and tunneled over an encrypted protocol, such as SSH, SSL, or IPsec.

Why Did you Recommend This Course of Action?

According to NIST SP 800-123 :

"Organizations should implement authentication and encryption technologies, such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH), or virtual private networks using IPsec or SSL/TLS, to protect passwords during transmission over untrusted networks. Requiring server authentication to be used with encryption technologies reduces the likelihood of successful man-in-the-middle and spoofing attacks."

4.4 DES Algorithm in Use

What is Your Recommended Mitigation Plan?

Use **AES-256** instead of **DES** to encrypt data

Why Did you Recommend This Course of Action?

According to **NIST**, The Advanced Encryption Standard (AES) specifies a **FIPS-approved** cryptographic algorithm.

Why use AES-256:

- **Security:** AES-256 is highly secure and has undergone extensive analysis.
- **Key Size:** AES-256 uses a 256-bit key, making it computationally infeasible to break.
- **Performance:** AES-256 is efficient and fast on modern computer systems.
- **Standardization:** AES-256 is an internationally recognized encryption standard.
- **Trustworthiness:** AES-256 is widely used by government agencies and trusted organizations.

4.5 Security Audit

The audit team has been made aware of the systemic issue and wants to ensure your recommendations are followed. What steps can the audit team take?

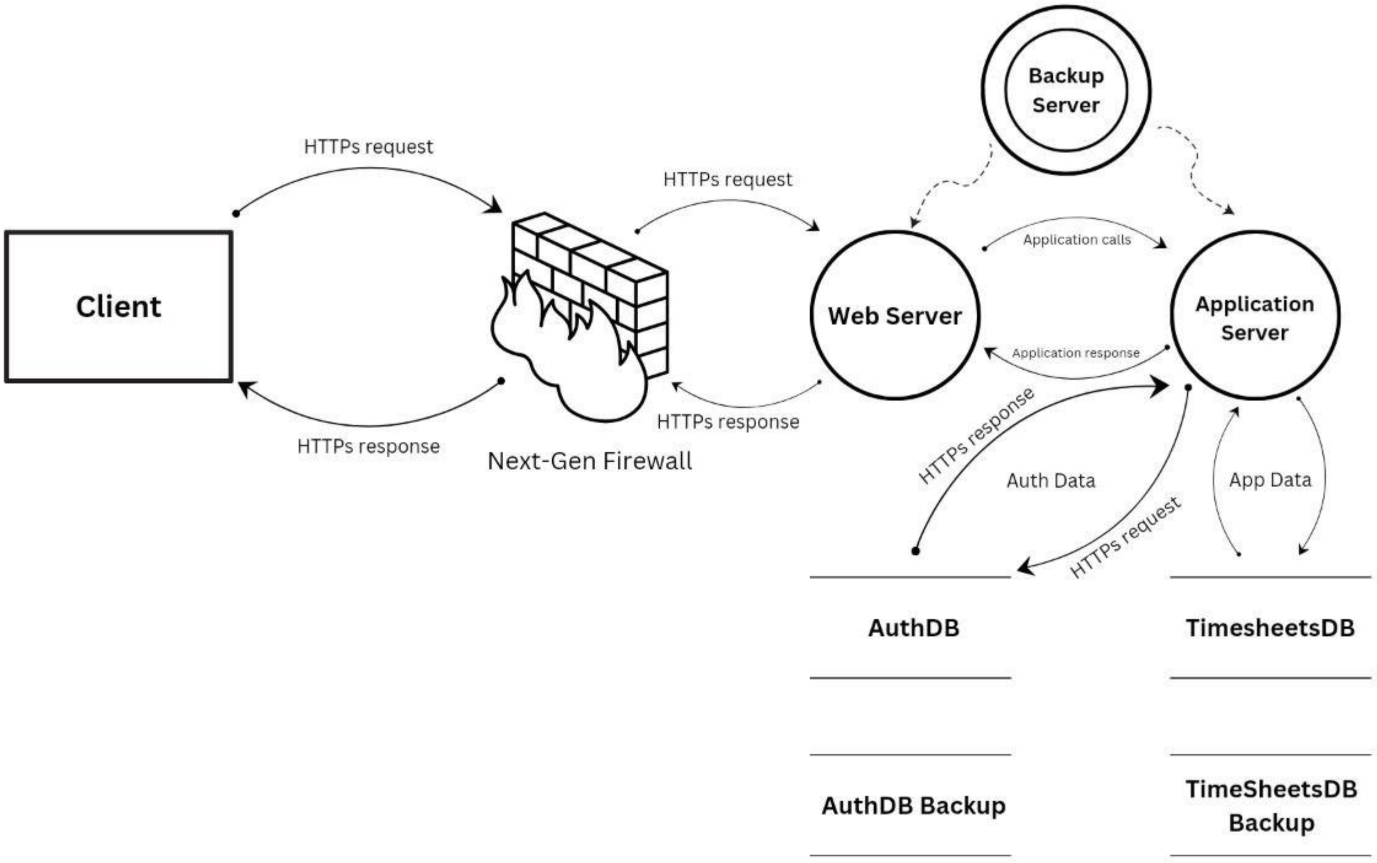
Since we have four main issues provided in the initial threat assessment, I recommend some main steps to be taken to help the audit team make sure recommendations are followed:

- **Technical Testing:** Conduct vulnerability scanning and penetration testing to test encryption configurations and protocols.
- **Interviews and Meetings:** Engage with stakeholders to discuss encryption practices and clarify implementation details.
- **Review Encryption Key Management:** Assess key management practices for compliance with standards and best practices.
- **Documentation Verification:** Check system configurations and encryption key management policies for evidence of encryption implementation.
- **Continuous Monitoring:** Implement ongoing monitoring to track adherence to encryption requirements over time.

Optional Task:

Create an architecture diagram of a secure system.

Image of your secure architecture:



For a high-quality version of my secure design architecture : [View My Design]

Optional Task *(Continued)*:

Additional Steps Would You Recommend to Prevent the Attack as well as Future Issues:

In addition to the issues mentioned in the initial threat report, I recommend some additional but important steps including:

- **Taking Backups and implementing redundancy:** To ensure availability, backups from the DBs should be taken regularly, these backups should be encrypted as well. An additional server should be put as a standby-server or in a load-balancing mode in case of failure of one of the main servers.

- **Implement a Firewall:** A next-gen firewall standing at the perimeter of the network to intelligently filter traffic providing an additional layer of defense and implementing the defense-in-depth design principle.

- **Security awareness training for employees:** even with a secure design architecture and hardened systems , human is one of the most exploitable vulnerabilities. Training employees is essential to make them aware and less vulnerable to social engineering or digital fraud.

- **Security Policies:** security policies supporting the company's security strategy must be put and properly communicated to stakeholders and audited regularly.