**Module Exam**

|  |  |
| --- | --- |
| **Module code and Name** | **ELEC0138 Security and Privacy** |
| **Student Number** |  |
|  |  |
| **Assessment date** | **4pm Fri 25/04/2025** |
|  |  |

**Presentation URL (publicly accessible link):**

**Happy to share the video on twitter/course YouTube? Yes/No**

**Code & Data (publicly accessible link):**

**Coursework 1: Threat Modeling & Attack Simulation (up to 5 pages)**

1. Introduction and objectives

This coursework focuses on a web-based control plane for a home IoT system, where users authenticate to manage connected devices (e.g. smart locks, cameras) within their households.

[picture of web]

The system’s complexity—spanning user interfaces, backend services, device communications, and sensitive data flows—introduces multifaceted security risks. To safeguard user privacy and ensure reliable device operations, this threat modeling and attack simulation aims to systematically identify vulnerabilities, assess risks, and validate defenses.

Sensitive data in this system including user data and IoT system data as shown in table 1:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** Category | **Description** | **Data** Type | **Sensitivity** Level | **Potential** Risks |
| User Credentials    Personal Information    Payment Data     User Activity Logs     Session Tokens    loT Device Data    Backups/Archives | Sensitive information for user authentication   User identity and contact details    Financial information and transaction records    Records of user actions    Temporary credentials for authenticated sessions   Device identifiers, configurations,and real- time status   Historical data stored for recovery or auditing | Passwords,  biometric information   Names,emails, home addresses, phone numbers   Credit card numbers ,billing history    Structured logs (JSON/text)    JWT tokens,OAuth tokens   Device IDs,JSON configurations, status update packets   Compressed logs, database snapshots | High  Medium  High     Medium    High    High    High | Account takeover,  unauthorized device control   Privacy breaches,  phishing attacks  Financial fraud, payment tampering  Behavioral analysis attacks,exposure of sensitive operations  Session hijacking,  man-in- the-middle attacks, privilege escalation   Device spoofing, configuration tampering, physical security threats   Historical data leaks, audit trail destruction, arge-scale data exposure |
|

Table 1 Critical data

Sensitive Data Flow:

Input: Collected via web/mobile interfaces and APIs.

Transmission: Secured by HTTPS/MQTT encryption (prevent protocol downgrades, MITM attacks).

Authentication: Protect credentials and tokens.

Access Controls: Restrict API/device pairing to authorized users.

1. Threat model

**Threat Model 1: Unauthorized Access via Phishing & Brute-Force Attacks**

Attack Vectors & Details:

* Phishing Attacks:

Attackers impersonate legitimate login pages or send deceptive emails to steal credentials.

Example: Phishing links redirecting users to cloned login interfaces.

* Brute-Force Login:

Automated tools target login endpoints with high-volume password guessing.

Example: Credential stuffing attacks exploiting reused passwords.

* Affected Assets: User credentials, session tokens, MFA services.

**Threat Model 2: Data Breaches via SQL/XSS Injections**

Attack Vectors & Details:

* SQL Injections:

Malicious SQL payloads injected into API parameters to extract sensitive database records.

* XSS Injections:

Injecting scripts into user-input fields to hijack sessions or redirect users.

* Affected Assets: Databases, web frontend, user activity logs.

**Threat Model 3: Service Disruption via DDoS & DNS Exploits**

Attack Vectors & Details:

* DDoS Attacks:

Overwhelm servers with traffic floods targeting APIs or authentication services.

Example: Botnets leveraging compromised IoT devices to amplify attack volume.

* DNS Cache Poisoning:

Spoof DNS responses to redirect users/devices to malicious servers.

* Affected Assets: Network infrastructure, DNS servers, API endpoints.

**Threat Model 4: MITM Attacks & Protocol Exploits**

Attack Vectors & Details:

* MITM Attacks:

Intercept unencrypted HTTP/MQTT traffic to alter device commands.

Example: Eavesdropping on public Wi-Fi to capture user-device communications.

* DNS Hijacking:

Redirect device update requests to attacker-controlled servers hosting malicious firmware.

* Affected Assets: Device communication channels, DNS configurations.

**Threat Model 5: Insider Threats & Insecure Firmware Updates**

Attack Vectors & Details:

* Authorized personnel exfiltrate sensitive data.

Example: Database admins selling customer data to third parties.

* Malicious Firmware Uploads:

Exploit unsigned firmware update processes to deploy backdoors

* Affected Assets: Databases, firmware repositories, audit logs.

1. Assess impact and prioritize threats

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Priority** | **Threat** | **Likelihood** | **Impact** | **Risk Level** |
| **1** | Unauthorized Access | 5 | 5 | **25** |
| **2** | Data Breaches | 4 | 5 | **20** |
| **3** | Firmware & Emerging Tech Risks | 3 | 4 | **12** |
| **4** | Device Communication Interception | 3 | 3 | **9** |
| **5** | Insider Threats | 2 | 2 | **4** |

[heat map]

|  |  |  |
| --- | --- | --- |
| **Attack Type** | **Critical Assets Impacted** | **Mitigation Priority** |
| Phishing/Brute-Force | User accounts, MFA systems | Highest |
| SQL/XSS | Databases, web applications | High |
| DDoS/DNS | Network infrastructure, APIs | Medium-High |
| MITM | Device communications, DNS | High |
| Insider Threats | Internal systems, firmware updates | Medium |

1. Data Sources and attacks set-up

**Coursework 2: Security & Privacy Defense Strategy (up to 5 pages)**

1. Security (or Privacy or both) Interaction/visualisation/actuation system
2. Threats inferences and insights
3. Access controls & authentication

Targeted Threat Models:

* TM1 (Phishing/Brute-Force)
* TM5 (Insider Threats)

Targeted Sensitive Data:

* User Credentials
* Session Tokens

Key Solutions:

* Zero Trust Architecture (ZTA):

Enforce strict identity verification for every access request, regardless of origin (user, device, or admin).

Example: Device-to-cloud mutual TLS (mTLS) ensures both parties authenticate before communication.

* Multi-Factor Authentication (MFA):

Combine hardware security keys with behavioral biometrics (typing patterns) to block credential theft.

* Least Privilege Access:

Grant permissions based on context (user role, device location, time).

Example: Admins can only access logs during business hours from approved IP ranges.

1. Data security & encryption mechanisms

Targeted Threat Models:

* TM2 (SQL/XSS Data Breaches)
* TM4 (MITM Attacks)

Targeted Sensitive Data:

* Payment Data
* IoT Device Configurations
* Backups

Key Solutions:

* End-to-End Encryption:

Encrypt data in transit (TLS 1.3) and at rest (AES-256). Use certificate pinning to prevent MITM.

* Input Validation & Tokenization:

Sanitize user inputs with allowlists to neutralize SQLi/XSS (TM2). Tokenize sensitive fields (e.g., credit cards) to render stolen data useless.

1. Network protection & monitoring

Targeted Threat Models:

* TM3 (DDoS/DNS Exploits)
* TM4 (DNS Hijacking)

Targeted Sensitive Data:

* User Activity Logs
* Real-Time Device Status

Key Solutions:

* AI-Powered Anomaly Detection:

Train ML models on normal traffic patterns to flag DDoS spikes (TM3) or abnormal DNS queries (TM4).

* Honeypot Deception:

Deploy decoy devices and fake API endpoints to divert attackers probing for vulnerabilities.

* DNSSEC & Rate Limiting:

Sign DNS records to prevent cache poisoning (TM4). Throttle excessive requests to mitigate DDoS (TM3).

1. Resilience against emerging threats

Targeted Threat Models:

* TM4
* TM5
* Future Quantum Risks

Key Solutions:

* Quantum-Safe Cryptography:

Migrate to NIST-approved algorithms to protect against quantum decryption.

* Secure Firmware Updates:

Mandate code signing with hardware-rooted keys to block unauthorized updates.

* Adversarial AI Defense:

Harden ML models against data poisoning (e.g., detect manipulated training data).

5)Critical Insights：

* Context-Aware Protection:

Security cannot be static. Adaptive controls, such as dynamically adjusting encryption levels based on data sensitivity, ensure resources are allocated efficiently without compromising protection.

* Privacy Design Trade-offs:

Techniques like differential privacy add noise to logs to prevent behavioral profiling but may impact data utility. Striking this balance requires transparent user consent and granular controls.

* Emerging Threat:

Proactive adoption of post-quantum cryptography and adversarial AI defenses highlights the need for future-proofing. However, transitioning legacy systems to quantum-safe protocols remains a logistical and financial challenge for many households.

* Human-Centric Security:

Even advanced defenses fail, phishing-resistant MFA reduces reliance on human vigilance, while clear consent workflows ensure users understand data-sharing implications.

1. Regulation and Ethical considerations

|  |  |  |
| --- | --- | --- |
| **Regulation** | **Key Requirements** | **Solution Alignment** |
| GDPR(EU) | - Data minimization, user consent, and breach notification.  -Right to access/delete data. | -Encrypt personal data (e.g., emails, addresses).  - Granular user consent workflows for data collection.  - Automated breach alerts within 72 hours. |
| CRA | - Secure-by-design IoT devices.  -Vulnerability disclosure and patching. | -Integrate secure firmware signing and OTA updates.  -Establish a vulnerability management program for devices/APIs. |
| PSTI(UK) | - Ban default passwords.  -Provide clear vulnerability reporting channels. | - Enforce strong password policies during device pairing.  -Public-facing security@ email for reporting issues. |
| CCPA(US) | -Opt-out of data sales.  -Disclose data collection purposes. | User dashboard to manage data-sharing preferences |

The design and operation of a home IoT control plane raise critical ethical challenges that must be addressed to ensure user trust and regulatory compliance. Below are key ethical risks and strategies to mitigate them:

1)Surveillance Risks

Scenario: Continuous data collection from IoT devices may enable unwarranted surveillance, exposing users to privacy violations or misuse of sensitive information .

Mitigation:

* Local Data Processing: Implement edge computing to store and process sensitive data directly on devices or local hubs, minimizing centralized storage.
* Data Anonymization: Strip metadata (e.g., blur faces in video logs) and aggregate behavioral data to prevent individual identification.

2)User Consent

Scenario: Users may unknowingly consent to broad data-sharing practices due to complex or opaque privacy policies (e.g., sharing device usage data with third-party advertisers).

Mitigation:

* Granular Consent Management: Provide user-friendly dashboards with toggle options for specific data types.
* Plain-Language Disclosures: Replace legal jargon with concise explanations of data usage.

3)AI-Driven Bias

Scenario: AI-powered security systems might disproportionately flag certain user groups as “suspicious” due to biased training data .

Mitigation:

* Bias Audits: Regularly test AI models with diverse datasets and third-party audits to identify discriminatory patterns.
* User Appeals: Allow users to challenge automated decisions through transparent review processes.

4)Autonomous Device Actions

Scenario: Overly aggressive automation (e.g., AI-driven locks autonomously denying entry based on perceived threats) could lead to safety risks or user alienation.

Mitigation:

* Human-in-the-Loop: Require manual confirmation for critical actions (e.g., overriding door locks during emergencies).
* Explainable AI: Provide users with clear reasoning for automated decisions (e.g., “Door unlocked denied due to unrecognized face”).

By proactively addressing these dilemmas, the IoT control plane can balance security, usability, and ethical responsibility, fostering long-term user confidence and regulatory alignment.

1. Scalability, Innovation & Enterprise Considerations

1)Scalability for Enterprise Adoption

* Architecture:

Multi-Tenancy: Support isolated environments for enterprise clients (e.g., property managers overseeing multiple homes).

Hybrid Cloud: Deploy control plane across public/private clouds for resilience and low-latency device interactions.

* Performance:

Edge Computing: Process device data locally (e.g., smart hubs) to reduce cloud dependency and latency.

Load Balancing: Auto-scale API servers during traffic spikes (e.g., DDoS attacks).

1. Innovation Opportunities

* AI-Powered Threat Hunting

Unlike conventional signature-based tools that rely on known attack patterns, this solution leverages behavioral analytics to proactively detect zero-day attacks. By analyzing anomalies in device behavior—such as unexpected thermostat adjustments at unusual hours—the system identifies potential threats before they escalate. This approach reduces false positives and adapts to evolving attack techniques.

* Blockchain for Audits

Traditional centralized databases are vulnerable to tampering, complicating compliance audits. By implementing blockchain technology, the solution ensures immutable logs of device actions and user consent records. For example, during GDPR audits, organizations can transparently prove compliance with data access requests, enhancing accountability and trust.

* Quantum-Safe Cryptography

While most systems still rely on RSA encryption, this solution adopts lattice-based cryptography to prepare for quantum computing threats. Quantum-safe algorithms future-proof critical communications, such as firmware updates and API interactions, ensuring long-term protection against decryption by quantum-powered attackers.

----------[WIP⬇]--------

3)Long-Term Viability & Cost

The proposed IoT security solution is designed to balance upfront investments with scalable, cost-efficient operations while ensuring adaptability to future technological shifts. An initial investment of 50k–100k covers the deployment of core capabilities, such as AI/ML integration for advanced threat detection and a zero-trust architecture to enforce granular access controls. Ongoing operational costs, estimated at approximately $10k per month, include cloud hosting for real-time data processing, subscription to threat intelligence feeds for proactive defense, and regular compliance audits to meet evolving regulatory standards. To future-proof the system, the architecture adopts a modular design, decoupling critical components like authentication microservices. This approach enables seamless upgrades—for instance, swapping multi-factor authentication (MFA) providers without disrupting the entire infrastructure. Additionally, reliance on open standards such as MQTT for lightweight device communication, TLS 1.3 for robust encryption, and OAuth 2.1 for secure authorization ensures interoperability and avoids vendor lock-in, simplifying integration with third-party tools and platforms.

4)Strategic recommendations

To solidify the solution’s resilience and market relevance, strategic priorities include automating compliance workflows to align with regulations like GDPR. By implementing automated data mapping and real-time monitoring, organizations can streamline audits, reduce legal exposure, and dynamically adapt to regulatory changes. Ethical governance is equally critical; establishing an independent ethics review board ensures AI/ML models are audited for bias, transparency, and fairness, particularly in high-stakes scenarios like automated access denials. Partnerships with cloud providers such as AWS or Azure further enhance scalability by leveraging their IoT-optimized infrastructure and security services, enabling seamless global deployment. Cost efficiency is achieved through serverless architectures like AWS Lambda, which aligns expenses with actual usage—paying only for active API calls or data processing—while maintaining high availability. By integrating these strategies, the solution not only addresses immediate security challenges but also positions itself as a forward-thinking platform capable of evolving with emerging threats, regulatory landscapes, and technological advancements, ultimately fostering secure and sustainable IoT ecosystems.

**Section explaining contribution (up to 200 words)**