Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***EPMwDC***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***Modeling According to the Principles of Privacy by Design and Privacy by Default: Architectural Requirements***

Modeling According to the Principles of Privacy by Design and Privacy by Default: Architectural Requirements

Table of Contents

Introduction

The project “Research and development of an Espionage Prevention Monitor with Detection Capabilities (EPMwDC)” seeks to develop a unique product consisting of hardware and software modules, which would enable government and private organisations to prevent sensitive data leaks when a picture is taken of the screen, displaying confidential data, detecting and reporting to authorities if such incident is realised.

To successfully embed the principles of "Privacy by Design" (PbD) and "Security by Design" (SbD) into a system, its foundational architecture must be engineered to comply with stringent dual-use (civilian and defense) regulatory frameworks, such as the GDPR, EU AI Act, Cyber Resilience Act, and NATO policies. During the architectural design of a system like the Espionage Prevention Monitor with Detection Capabilities (EPMwDC), specific hardware, software, communication, and structural requirements must be systematically mapped and integrated.

Below is a detailed elaboration of the specific requirements, key stages, and critical aspects that must be taken into account during system architecture.

1. Key Stages in Architectural Design and Implementation

The architectural lifecycle must follow a phased implementation strategy to ensure that privacy and security requirements are validated before deployment.

Stage 1: System Integration (Architectural Unification)

The architecture must seamlessly combine hardware and software modules into a unified system. This stage involves ensuring interoperability with existing IT and defense infrastructures, aligning with mandates like the EDA Cyber Defence Framework to ensure the architecture functions within established networks.

Stage 2: Testing and Validation (Simulated Environments)

The architecture must be rigorously tested in simulated threat environments. This validates the system's structural ability to detect and prevent unauthorized visual capture without compromising the system's data minimization principles.

Stage 3: Architectural Certification

Before deployment, the hardware and software architecture must be certified against electromagnetic security standards (e.g., NATO's TEMPEST standards) to ensure the physical architecture itself does not emit exploitable signals.

Stage 4: Isolated/On-Premise Deployment Modeling

The system must be architected for deployment within protected, closed, or segmented customer infrastructures. The architecture must not rely on continuous third-party cloud processing, ensuring that the end-user maintains absolute control over personal data and system operations.

2. Specific Architectural Requirements and Key Aspects

1. Unified "Security by Design" Architecture

To avoid maintaining entirely separate technological bases for civilian and military markets, developers should build a "Unified Architecture". This means creating a core secure baseline that inherently meets the strictest standards across domains (e.g., combining NATO Reliability requirements with EU Cybersecurity and NIS2 mandates). For defense alignment, the architecture should be modeled on a "Data Centric Reference Architecture" (DCRA) utilizing standards like STANAG 5636 to ensure secure semantic interoperability.

2. Edge AI and Local Inference Architecture (Data Minimization)

The primary architectural mechanism for achieving Privacy by Design is the implementation of "Edge Computing".

- **Local Processing:** The architecture must process video frames locally on the workstation's hardware (e.g., utilizing an NVIDIA Jetson platform) rather than streaming continuous video to a central server.
- **Alert-Based Data Transfer:** The system must be designed so that normal, compliant employee behavior is never transmitted or recorded. Only when the local AI inference engine detects a positive threat (e.g., a camera lens) does the architecture permit the creation of a "frozen" alert package containing the raw image, AI annotation, and metadata.

3. Hardware Module Specifications

The physical architecture of the system must be designed to mitigate risks without causing interference:

- **Preventative Hardware Module:** This module must incorporate IR noise emitters operating specifically within the 850 nm to 940 nm spectrum. This architectural choice ensures the noise disrupts unauthorized camera sensors while remaining completely invisible to the human eye, complying with requirements to not interfere with normal human operations.
- **Detective Hardware Module:** The architecture must utilize advanced, laser-based sensors and machine learning algorithms capable of distinguishing between benign reflections (like a user's eyeglasses or eyes) and actual optical threats (like smartphone lenses).

4. Cryptographic and Communications Architecture

All data in transit and at rest must be architected with state-of-the-art encryption to comply with GDPR Article 32 and NIS2 Article 21.

- **Secure Channels:** The communications module must use AES-256 encryption and HTTPS/TLS-secured communication protocols to securely transmit incident data to the remote server. For military applications, this architecture must comply with NATO’s Secure Communications Protocol (SCP).

5. Remote Server and Access Architecture

The central server architecture receiving the alerts must be designed to strictly control data access and maintain forensic integrity.

- **Multi-Tier Access Controls:** The server architecture must implement Role-Based Access Control (RBAC) and multi-factor authentication, ensuring that only authorized security personnel or analysts can view the decrypted incident alerts.
- **Immutable Audit Logging:** The server must maintain immutable audit logs that record all system access, user actions, alert status changes, and data processing activities. This satisfies the requirement for "full traceability".

6. Software Architecture and Cyber Resilience

The software stack must be architected to remain resilient against emerging vulnerabilities and adversarial attacks.

- **Software Bill of Materials (SBOM):** To comply with the EU Cyber Resilience Act, the software architecture must incorporate a managed SBOM to continuously track and secure all third-party dependencies and libraries used within the system.
- **Secure OTA Updates:** The architecture must technically support secure, automated Over-The-Air (OTA) updates to patch vulnerabilities continuously throughout the product's lifecycle.
- **Explainability Logs:** The AI inference engine must be structurally encapsulated with explainability logs. This architectural feature ensures that the logic behind every automated decision (classifying an object as a "threat" or "non-threat") is recorded and auditable, fulfilling transparency requirements under the EU AI Act.

Annexes: Architectural Requirements (Modeling Privacy and Security)

Annex 1. Key Stages in Architecture Design

Key Stages in Architecture Design	
Architectural Unification (System Integration)	• Seamlessly combining hardware and software modules into a cohesive architecture that interoperates securely with existing IT and defense infrastructures.
Simulated Threat Validation	• Rigorously testing the architecture in simulated environments to ensure detection mechanisms and preventative IR noise emissions function accurately.
Hardware Certification	• Reviewing and certifying the physical architecture against electromagnetic security standards (e.g., TEMPEST).
Isolated Deployment Modeling	• Designing the software architecture for on-premise execution, ensuring the system does not rely on third-party data processors or continuous cloud environments.

Annex 2. Compliance Checklist

Compliance Checklist	**[ ]**	• Implement a unified "Security by Design" baseline meeting both NATO Reliability and EU Cybersecurity standards.
	[ ]	• Embed End-to-End Encryption (AES-256 or quantum-resistant algorithms) for all data at rest and in transit.
	[ ]	• Ensure the hardware complies with the Cyber Resilience Act, utilizing secure boot mechanisms, hardened firmware, and automated over-the-air (OTA) update capabilities.
	[ ]	• Maintain an automated Software Bill of Materials (SBOM) for all third-party components.
	[ ]	• Implement Role-Based Access Control (RBAC) and immutable audit logging mechanisms within the remote server architecture.

Annex 3. Challenge Overcoming

Challenges	Suggestions to Overcome Challenges
• **Over-Engineering Costs:** Building a single architecture that meets the strictest military and NATO standards can significantly increase development costs for the civilian market.	• **Adopt a Unified Secure Baseline:** Develop a single core secure hardware architecture to reduce long-term R&D fragmentation, but differentiate the software and compliance layers for different markets.
• **Compatibility with Segmented Networks:** Defense systems often operate on isolated	• **Local Inference & Edge Computing:** Process all video feeds directly on the local

networks (like Lithuania's *Saugusis tinklas*), which restricts internet connectivity and complicates remote OTA updates.	hardware device, mitigating the need for continuous internet connections and drastically reducing data exposure.
• **Electromagnetic Emissions:** Designing hardware that emits IR noise without causing electromagnetic interference that could compromise other sensitive operational equipment.	• **Pursue Early TEMPEST Certification:** Embed electromagnetic shielding and rigorous EMI testing early in the hardware design phase to satisfy strict military procurement rules.

References

1. Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
2. CJEU Case C-511/18 - La Quadrature du Net and Others, 2020. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
3. The Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847
4. Digital Operational Resilience Act: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
5. General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
6. NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
7. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
8. NATO AI Strategy, 2024. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy
9. Treaty on European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012M/TXT
10. CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
11. Data Strategy for the Alliance, 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance
12. NATO's Data and Artificial Intelligence Review Board, 2022: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/10/13/natos-data-and-artificial-intelligence-review-board
13. CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
14. NATO Digital Backbone, 2024: https://www.nato.int/en/news-and-events/articles/news/2024/12/13/nato-digital-backbone
15. White Paper on Export Controls COM(2024) 25 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025
16. Dual-Use Regulation (2021/821): https://eur-lex.europa.eu/eli/reg/2021/821/2024-11-08/eng
17. European Commission. AI Act Single Information Platform: https://ai-act-service-desk.ec.europa.eu/en
18. Action Plan on synergies between civil, defence and space industries. COM(2021) 70 final. https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/action-plan-synergies-between-civil-defence-and-space-industries

Finansuoja Europos Sąjunga
NextGenerationEU
Mykolo Romerio universitetas
NAUJOS KARTOS LIETUVA

Editor
<<Main Editor>>

Contributors
Evaldas Bruze (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Reviewers
Evaldas Bružė (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Disclaimer