



Task 9: Writing Conclusions and Recommendations

Prepared by

ALI MMADI, PhD student-Midocean University



Research Issues (2)

Task 9

Introduction and link with the previous task

Hello,

We are arriving at Task 9, the final synthesis: writing the conclusions and recommendations. This step is crucial because it transforms the interpretations from our discussion (Task 8) into actionable knowledge and roadmaps for the future.

If the discussion explained the "why" of our results, the conclusions extract the essence, and the recommendations chart the path toward application and future research.

Today, I will evaluate two theses on innovative topics in cybersecurity: threat analysis in medical IoT and the security of software supply chains.

Thesis 1 - Security of IoT Medical Devices (Title: "Conclusions: Risk Assessment in Connected Hospitals")

Subject: Analysis of Vulnerabilities in Insulin Pumps and Connected Heart Monitors in 5 Hospitals.

Key Findings (Clarity):

1. Main Result Confirmed:

78% of devices use unencrypted communication protocols (unsecured BLE).

Impact: Risk of drug dose tampering or theft of health data.

2. Key Interpretation:

The vulnerability does not stem from the technology itself, but from the time gap between lifecycle cycles: medical devices certified for 10 years vs. security standards that evolve every 18 months.

3. Impact of the Results:

This situation creates a "scissor effect" where exposure increases over time, compromising patient safety and GDPR/HIPAA compliance.

Memo 1 - Recommendations (Realism)

Recommendations for future research:

Develop retrofit security modules for existing devices (realistic since prototypes exist in labs).
Study "quantum-safe" protocols for new long-lived devices.

Recommendations for practitioners:

Implement a network quarantine zone for all medical IoT devices (feasible with VLAN segmentation).
Adopt a pre-purchase security checklist inspired by the MITRE framework for hospital procurement.

Recommendations for policymakers:

Amend FDA/EU MDR regulations to include mandatory security updates in initial certification.

Create a targeted bug bounty program funded by public health agencies.

Realism: These recommendations are phased (short/medium/long term) and combine technical solutions with regulatory frameworks.

Thesis 2 - Security of Software Supply Chains (Title: "Conclusions: Analysis of Attacks through Compromised Dependencies")

Subject: Study of transitive vulnerabilities in npm, PyPI, and Docker Hub ecosystems.

Key Findings (Clarity):

1. Major quantitative result:

1 vulnerable package out of 12 in npm, with an average cascading impact on 85 downstream packages.
The most effective attack: typosquatting (35% of cases).

2. Systemic interpretation:

The problem is structural, not accidental: the open-source package economy prioritizes speed and functionality over security. Implicit trust is exploited.

3. Economic impact:

A single malicious dependency can contaminate a value chain averaging €2.3M in commercial software development.

Memo 2 - Recommendations (Realism)

Recommendations for future research:

Develop anomaly detection algorithms specific to package metadata (behavioral signatures).

Create a 'supply chain hygiene' score inspired by CVSS but for dependency ecosystems.

Recommendations for practitioners (realistic and immediate): Implement 'SLSA Level 1' (Google framework) in all CI/CD pipelines within 6 months. Adopt Sigstore for artifact signing and verification starting today. Maintain a mandatory dynamic SBOM (Software Bill of Materials) for every project. Recommendations for policymakers: Develop a 'cyber' equivalent of food traceability (mandatory SBOM regulation for software publishers).

Realism: Each recommendation is associated with a clear actor (DevOps, CISO, regulator) and a defined time frame.

Summary of key strengths

Characteristics of clear conclusions:

Prioritized: From most to least important

Evidence-based: Directly linked to the findings

Nuanced: Acknowledge limitations and uncertainties

Forward-looking: Open up future perspectives

Characteristics of realistic recommendations:

Actionable: Start with a verb

Targeted: Specific audience identified

Phased: Short, medium, long term

Resourced: Take into account required costs/skills

Essential link to Task 8: Recommendations are directly derived from the explanatory mechanisms identified in the discussion, not just from the raw results.

Conclusion

In evaluating these two theses, we see that:

The clarity of the conclusions is judged by their ability to synthesize without oversimplifying, to extract the essence without losing nuance.

The realism of the recommendations is measured by their feasibility: are they targeted at the right level (technical, organizational, policy)?

Are they proportional to the problems identified?

These two criteria ensure that the research does not remain an academic exercise, but becomes a transformative force in the practical field of cybersecurity.

Thank you for your attention.

Bibliographic References

1. IoT Medical Device Security

Food and Drug Administration (FDA). (2022). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. FDA Guidance Document.

Annotation: The primary regulatory framework for medical device security in the US. It is essential for discussing policy recommendations, certification requirements, and the mandatory security updates mentioned in the conclusions. It directly supports the analysis of the lifecycle mismatch problem.

Hei, X., Du, X., & Lin, S. (2020). *Medical IoT Security: A Survey*. *IEEE Internet of Things Journal*, 7(2).

Annotation: A comprehensive academic survey that catalogs vulnerabilities in medical IoT, including unencrypted BLE protocols. It provides the evidence base for the statistical claim about unsecured communications and discusses retrofit security solutions.

MITRE Corporation. (2023). *Medical Device Cybersecurity: Playbook for Healthcare Delivery Organizations*. Retrieved from <https://www.mitre.org/>.

Annotation: A practical framework from a leading cybersecurity R&D organization. It offers actionable guidelines for network segmentation (zones of trust/quarantine) and pre-procurement checklists, validating the realism of the practitioner recommendations.

European Union Agency for Cybersecurity (ENISA). (2021). *Good Practices for Security of Internet of Things in the context of Smart Manufacturing and Logistics*.

Annotation: While focused on manufacturing, ENISA's guidelines on secure IoT lifecycle management and the integration of security from design are directly transferable to the medical context and support the policy-level recommendations for regulatory updates.

2. Software Supply Chain Security

Google. (2023). *Supply-chain Levels for Software Artifacts (SLSA) Framework*. <https://slsa.dev/>.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

