MarCaS

Threat Hunting and Security Analysis for Maritime Vessels

Simon Yusuf Enoch, **Hyunjae Kang**, Huy Kang Kim,
Dan Dongseong Kim

Whitecliffe

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

KOREA UNIVERSITY

Maritime Vessels & Cyber Threats

- Maritime IT/OT systems (navigation, communications, cargo management, etc.) face a rising number of cyber incidents.
  - e.g., Marlink SOC reported 14.8 B events in 2024.

Main cyber threats and motivations

During the latter half of the year, cybercriminals targeting the maritime sector were driven by several key motivations:

Financial gain

Cybercriminals take advantage of vulnerabilities in maritime systems or personnel to carry out financial fraud or theft, frequently focusing on monetary transactions, contracts, and confidential financial information.

1

Corporate espionage

Cyber adversaries conduct espionage to acquire sensitive or confidential information, typically for competitive advantage, political leverage, or military intelligence purposes.

2

Hacktivism

Threat actors seek to interfere with or damage essential systems, leading to major disruptions in business operations, often with the goal of debilitating an organisation or industry.

3

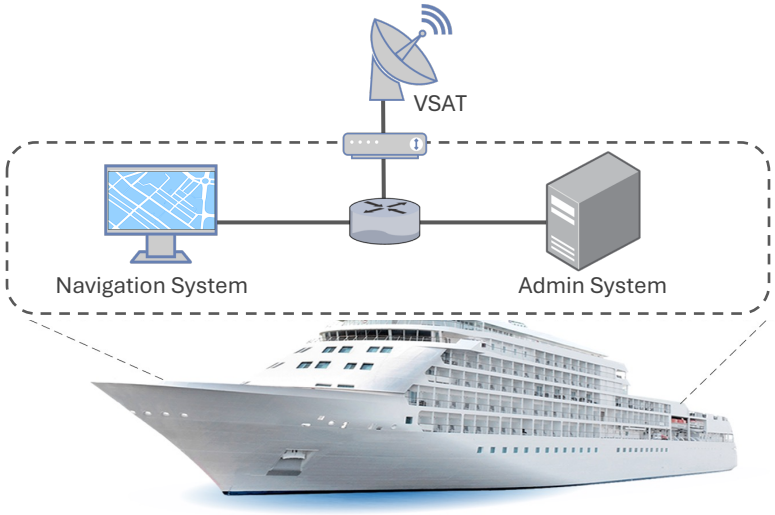
Intellectual property theft

Cyber attackers engage in intellectual property theft to steal proprietary designs, trade secrets, and confidential business information, often aiming to gain a competitive edge, disrupt innovation, or sell valuable data to third parties.

4

Source: Marlink Global Maritime Cyber Threat Report H2 2024

Related Work - Cybersecurity Assessment

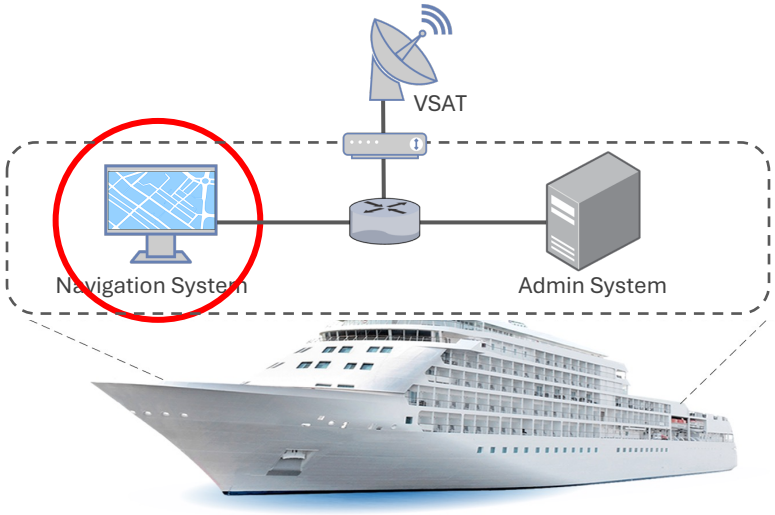


Related Work - Cybersecurity Assessment

Vulnerability Scanning & Threat Analysis

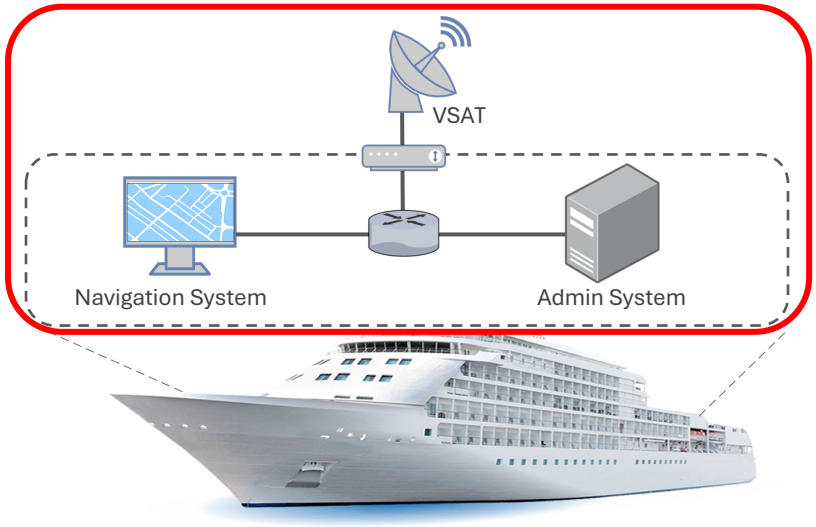
- Tools/Frameworks: Nessus, OpenVAS, STRIDE, ATT&CK, etc.
- Ref: Svilicic et al. (2019), Kavallieratos et al. (2019), Goudossis et al. (2019)

Vulnerabilities on vessel systems in isolation



Related Work - Cybersecurity Assessment

Research Gap: More systematic, but still the possibility of multi-step or multi-host attacks remain underexplored.



Model-Based

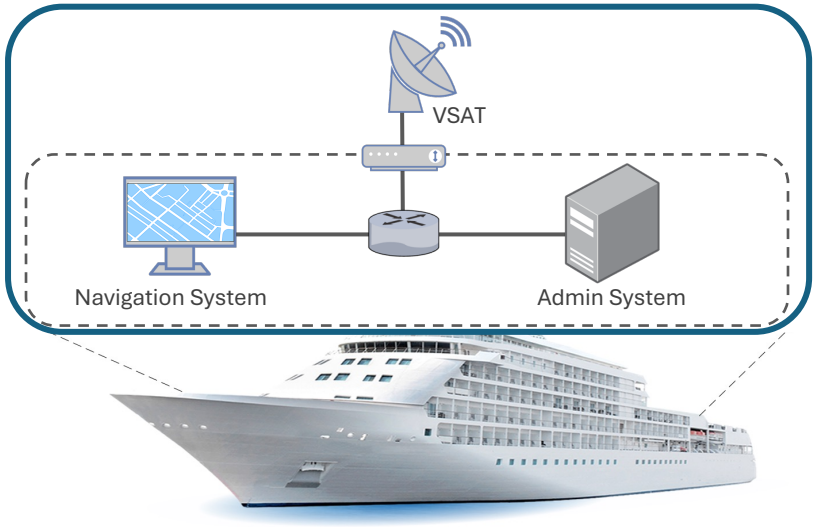
- Methods: MaCRA, fuzzy theory and attack trees, etc.
- Ref: Tam & Jones (2019), Bolbot et al. (2019), Shang et al. (2019)

Related Work - Cybersecurity Assessment

- ***MV-HARM*, Enoch et al. (2021)**

Proposed a formal graphical security model to capture **multi-stage attack paths**, considering a **complete maritime vessel network**.

Model-Based

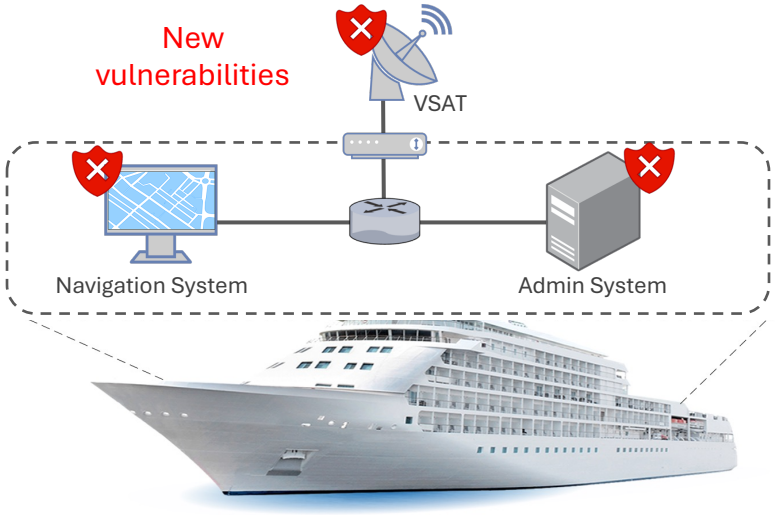


Related Work - Cybersecurity Assessment

- ***MV-HARM*, Enoch et al. (2021)**

However, one of the main drawbacks of MV-HARM is that information on the **vulnerabilities** is **not up-to-date**.

Model-Based



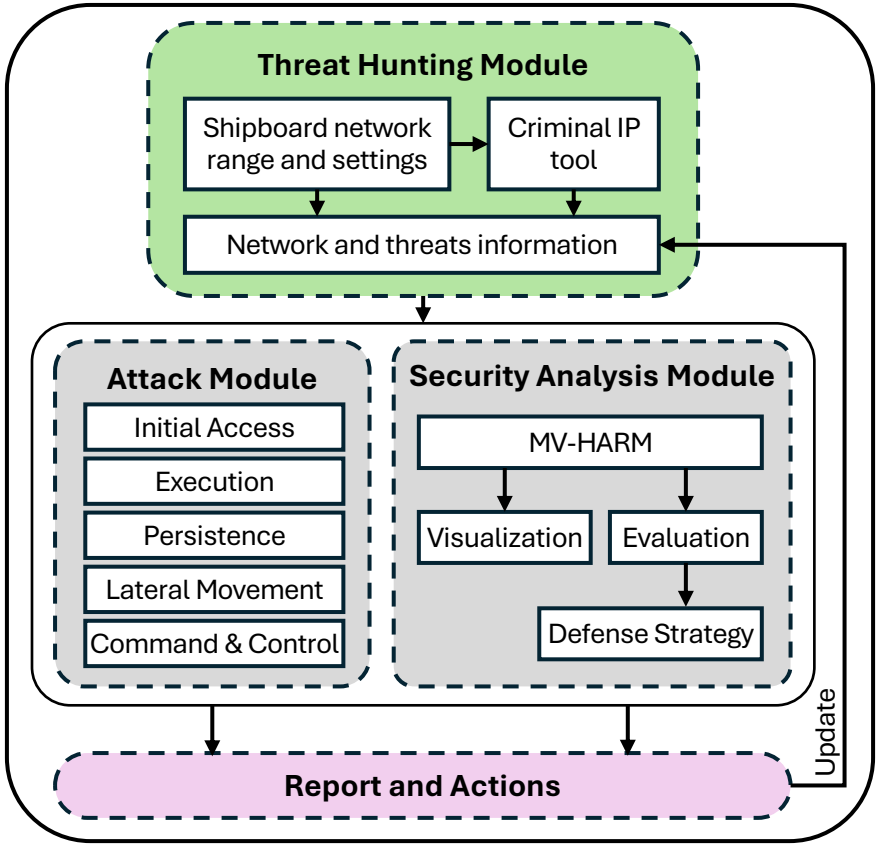
Key Contributions

Propose a framework for **threat-hunting** and **security management** of a vessel's attack surface.

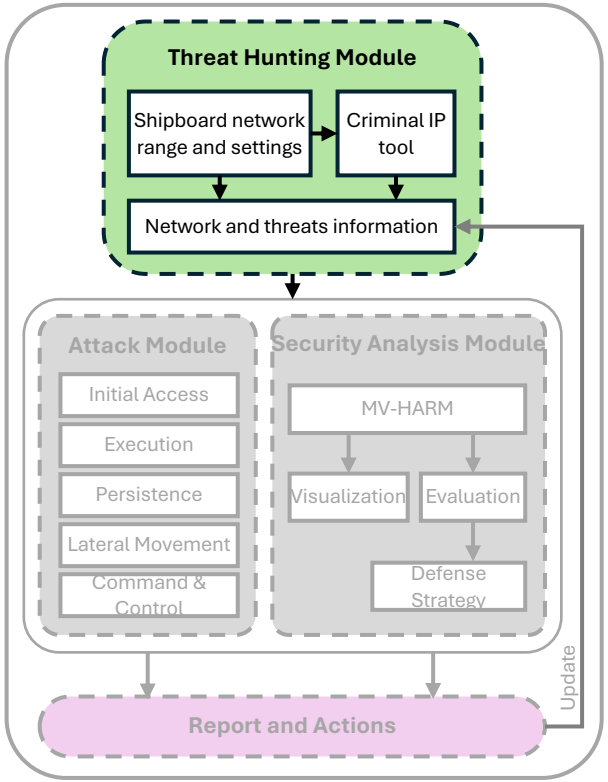
Demonstrate the proposed framework using **operational data from an actual ship** located offshore.

Perform a **risk assessment** using the security model named MV-HARM.

Proposed Framework

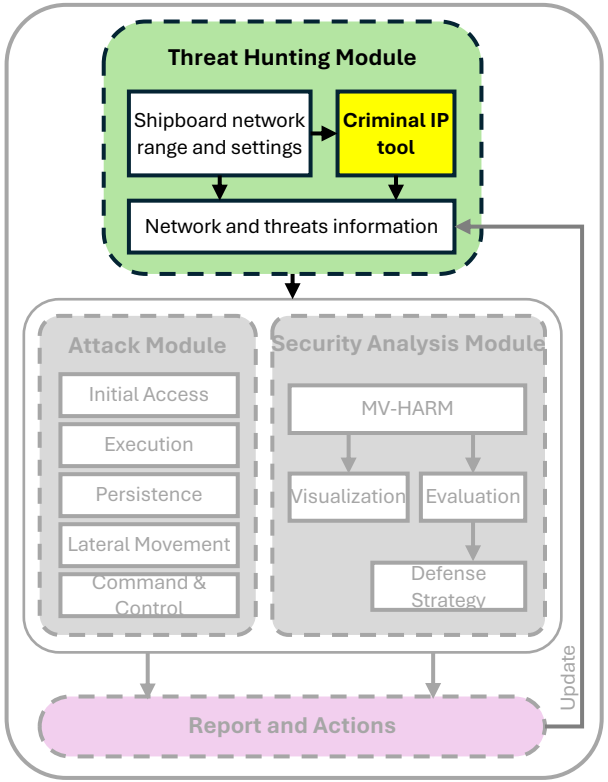


Threat Hunting Module

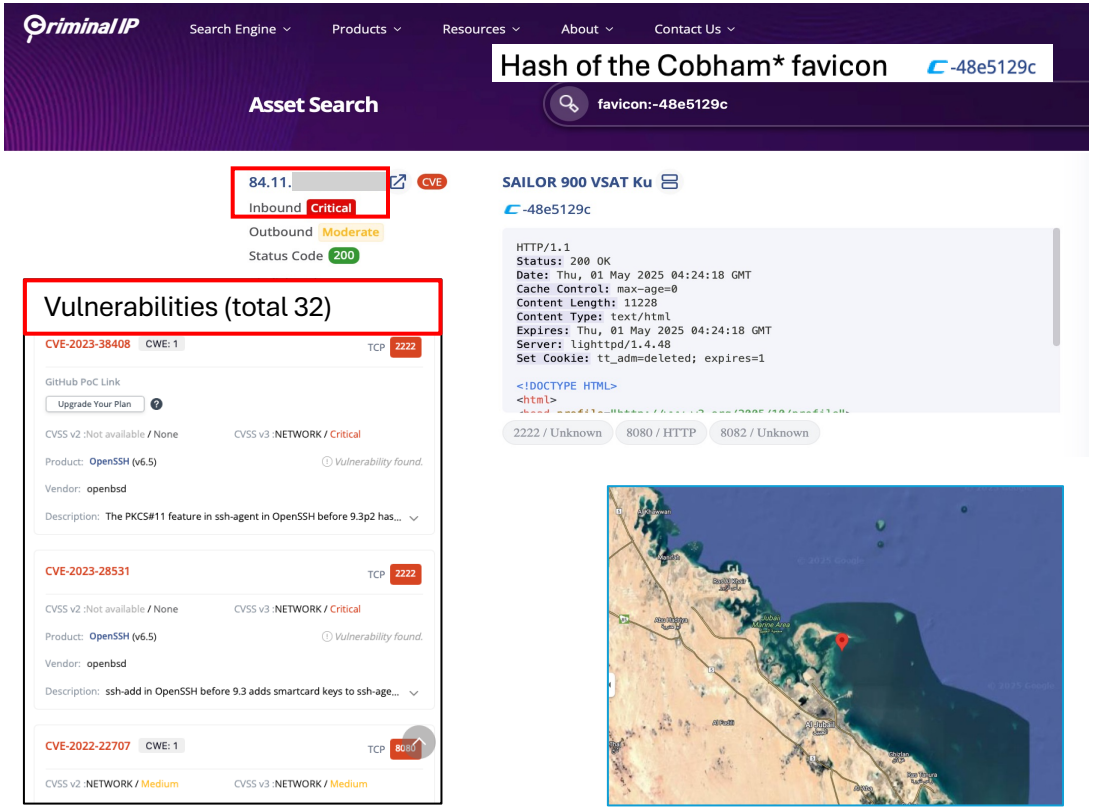


- Uses Criminal IP to collect **real-time** data on **vessel-exposed assets** (IPs, services, vulnerabilities).
- Identifies internet-facing systems (e.g., AIS, SATCOM) and compiles **configuration/ threat** data for risk analysis.

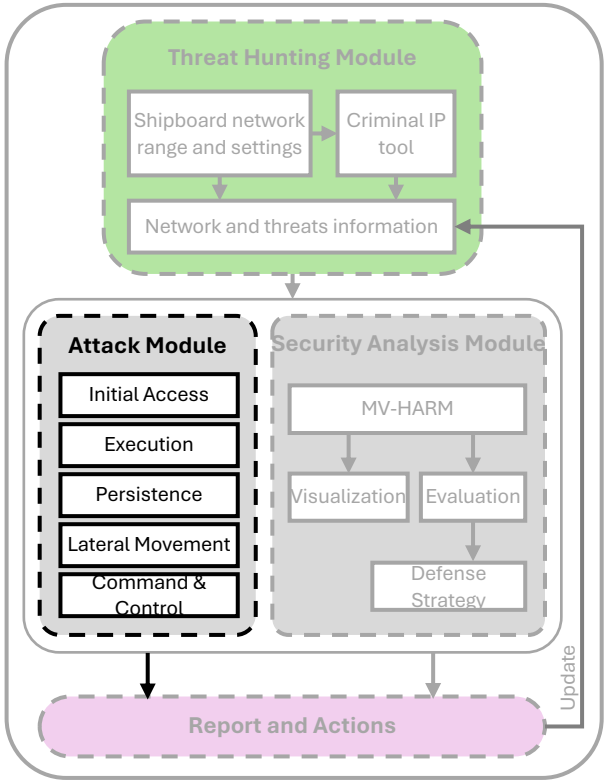
Threat Hunting Module



* Cobham Satcom: A global provider of satellite and radio communication solutions

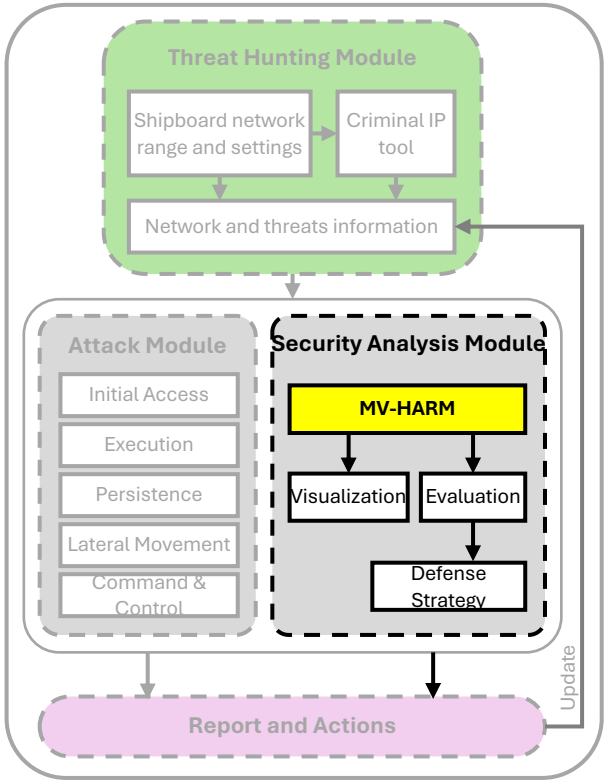


Attack Module



- Emulates adversary behavior via **MITRE ATT&CK**.
- Covers TTPs: Initial Access, Execution, Persistence, Lateral Movement, Command & Control.
- Provides detailed understanding of **potential exploitation paths**.

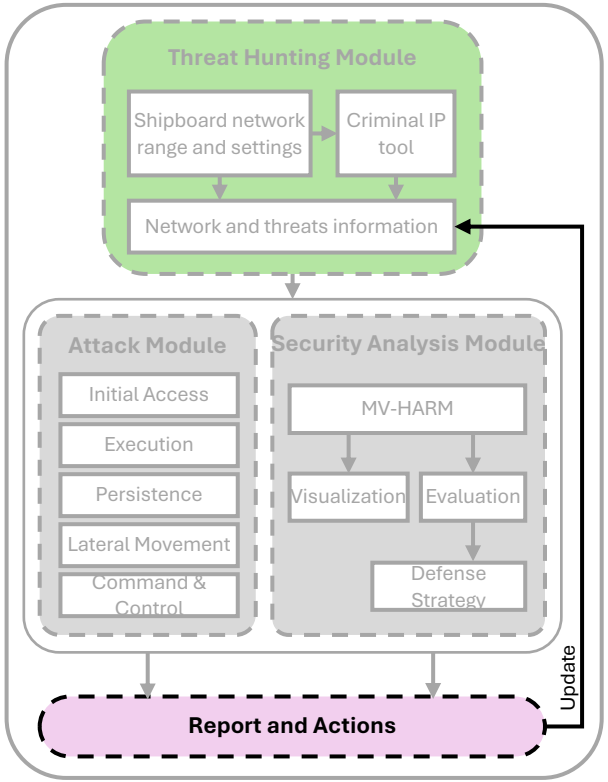
Security Analysis Module



** A graphical security model that visualizes and evaluates multi-layered attack paths*

- Employs **MV-HARM*** for **hierarchical attack modeling**:
  - **Upper** layer – network topology/reachability
  - **Lower** layer – vulnerabilities & threats
- Includes:
  - Evaluation module: computes **security metrics**
    - Risk Metric = Impact × Attack Probability
    - Attack Success Probability (from CVSS)
    - Threat-Specific Risk (using STRIDE categories)
    - Number of Attack Paths
  - Defense strategy module: recommends **mitigations** (segmentation, patching, isolation).

Report and Actions

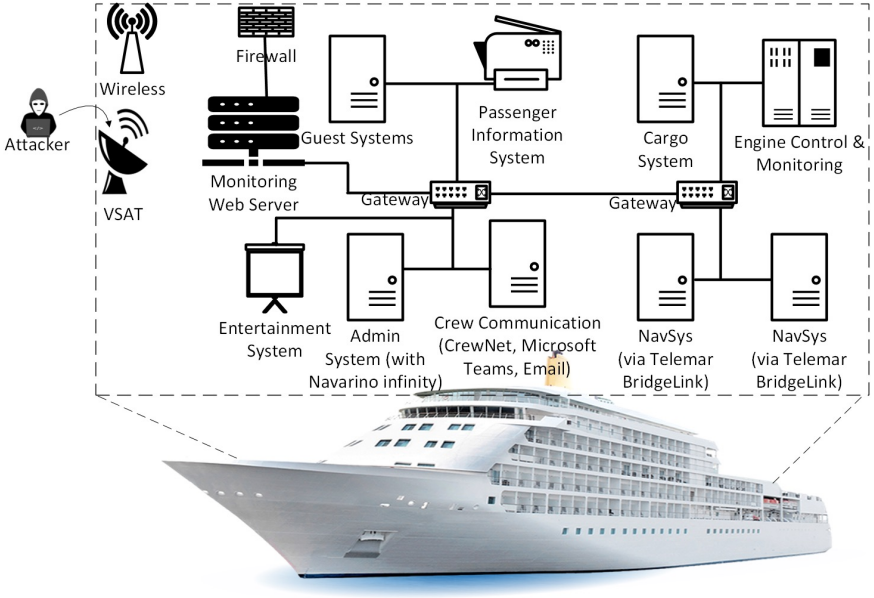


- Generates detailed reports:
  - **Attack paths, vulnerabilities, metric scores, and mitigation advice**
- Supports iterative reassessment as assets or threats evolve.

Application: Case Study

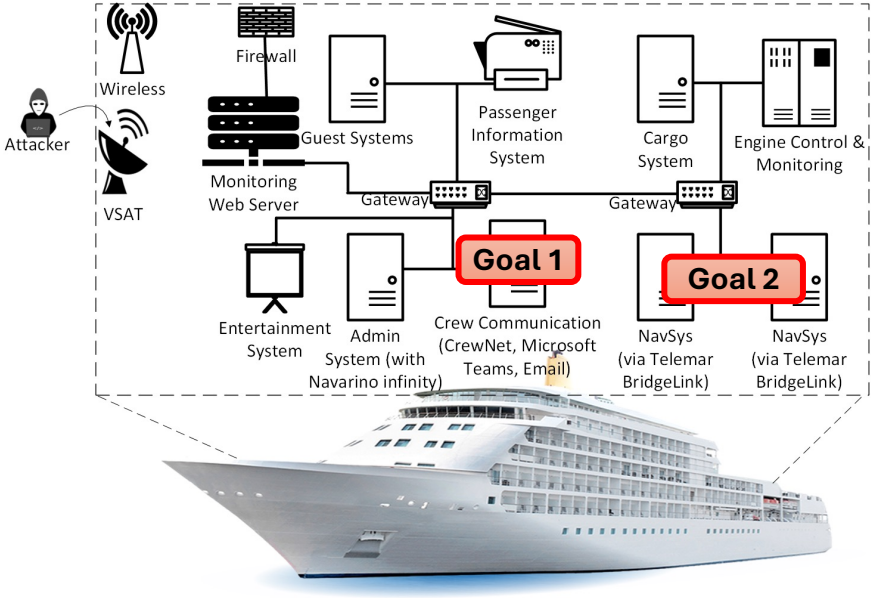
- The **scope** of this case study:
  - Defense, Report and Actions components not included

- **Onboard network of a commercial vessel:**
  - Based on ICS 2021 guidelines.
  - Mixed OT (navigation, engine) + IT (admin, crew comms).
  - Connected via VSAT and coastal networks.



Application: Case Study

- **Attacker model:**
  - Onshore adversary targeting externally connected systems.
  - **Goal 1:** Compromise *Crew Communication portal* (old Apache).
  - **Goal 2:** Hijack *Navigation system* via malicious update to alter vessel route.



Application: Case Study

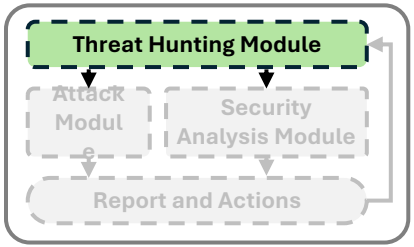


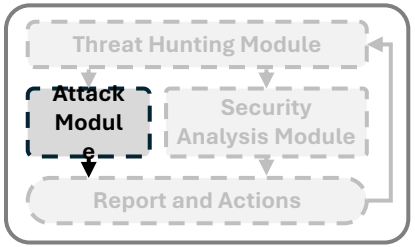
Table. Vulnerabilities Information (Selected)

Asset	CVE-ID	ID	BS	S	T	R	I	D	E
VSAT	CVE-2023-38408	v1	9.8	0.0	0.5	0.3	0.0	0.0	0.2
	CVE-2021-41617	v5	7.0	0.0	0.5	0.3	0.0	0.0	0.2
	CVE-2023-28531	v2	9.8	0.0	0.5	0.3	0.0	0.0	0.2
	CVE-2020-15778	v6	7.8	0.0	0.5	0.3	0.0	0.0	0.2
	CVE-2016-10009	v7	7.3	0.0	0.5	0.3	0.0	0.0	0.2
Admin System	CVE-2019-11072	v3	9.8	0.0	0.5	0.3	0.0	0.1	0.1
Crew Comm.	CVE-2022-22707	v4	5.9	0.2	0.2	0.2	0.2	0.2	0.1
NavSys 1	CVE-2023-38408	v1	9.8	0.0	0.5	0.3	0.0	0.0	0.2
NavSys 2	CVE-2023-28531	v2	9.8	0.0	0.5	0.3	0.0	0.0	0.2
Web Server (Navarino Mon.)	CVE-2019-11072	v3	9.8	0.0	0.5	0.3	0.0	0.1	0.1

BS: CVSS base score

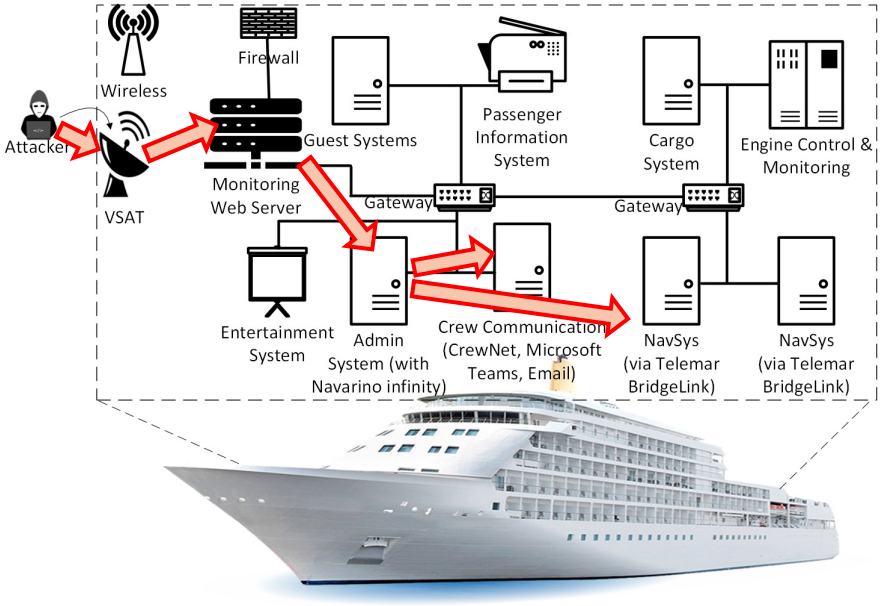
- **Threat Hunting (Criminal IP):**
  - Real-time data collection (Cobham favicon hash = –48e5129c).
  - **58 vulnerabilities** found (critical–low).
  - Example: VSAT interface uses default credentials → high risk.
  - Vulnerabilities mapped to STRIDE threat weights.

Application: Case Study

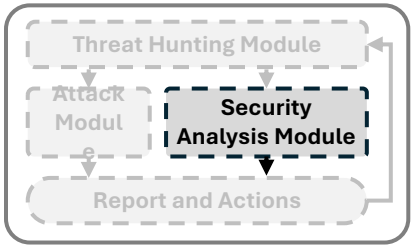


- **Attack Agent Simulation:**
  - **Initial Access:** exploit VSAT via SSH flaws (T1190).
  - **Execution:** run code via ssh-agent bugs (T1059).
  - **Persistence:** reuse credentials, create accounts (T1136).
  - **Lateral Movement:** pivot from VSAT → Web Server → Admin → Crew/Nav Systems (T1021, T1068).
  - **Command & Control:** establish HTTPS C2 over satellite link (T1071).

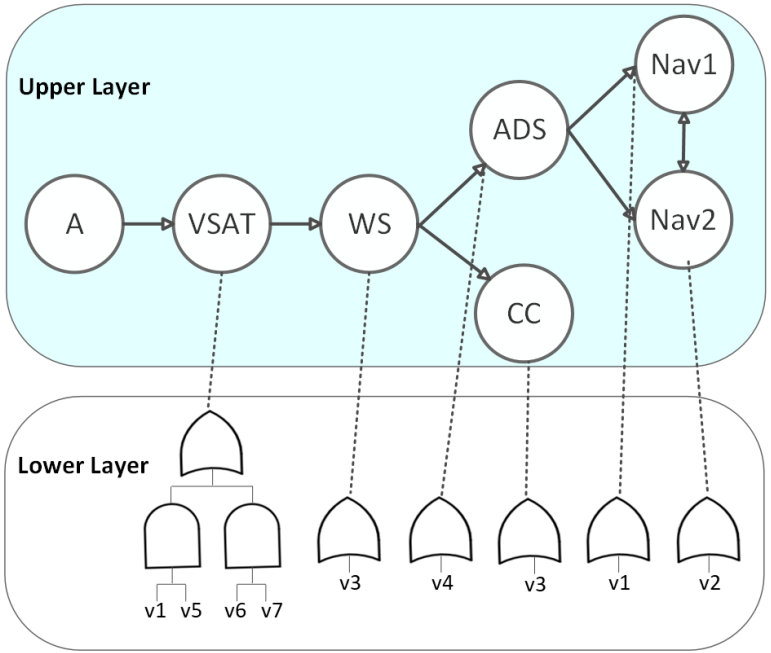
T = MITRE ATT&CK tactic/technique



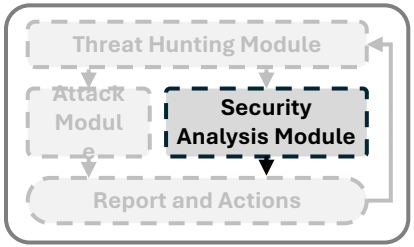
Application: Case Study



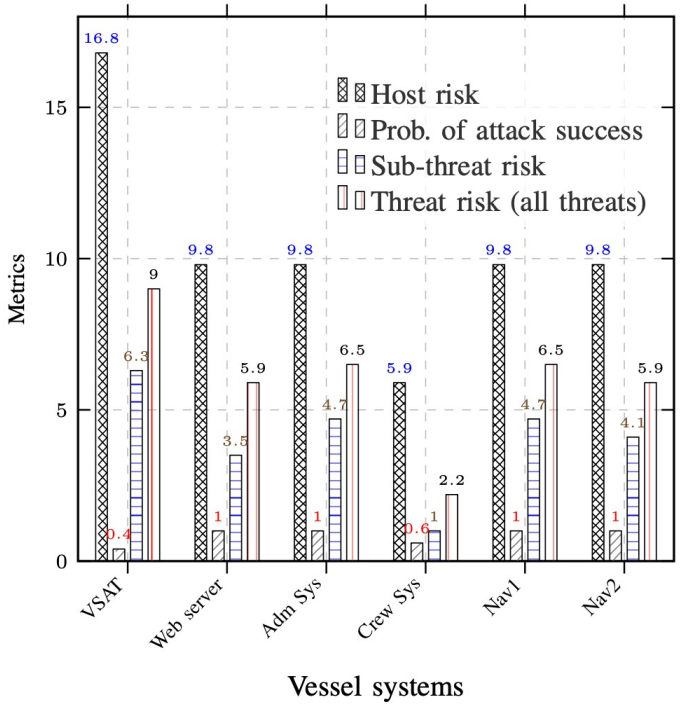
- **Security Analysis (MV-HARM):**
  - Graphical attack paths linking vulnerabilities.



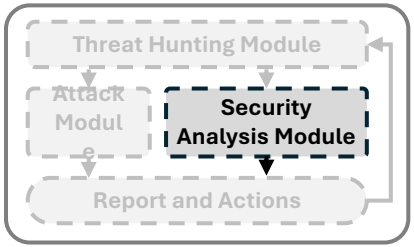
Application: Case Study



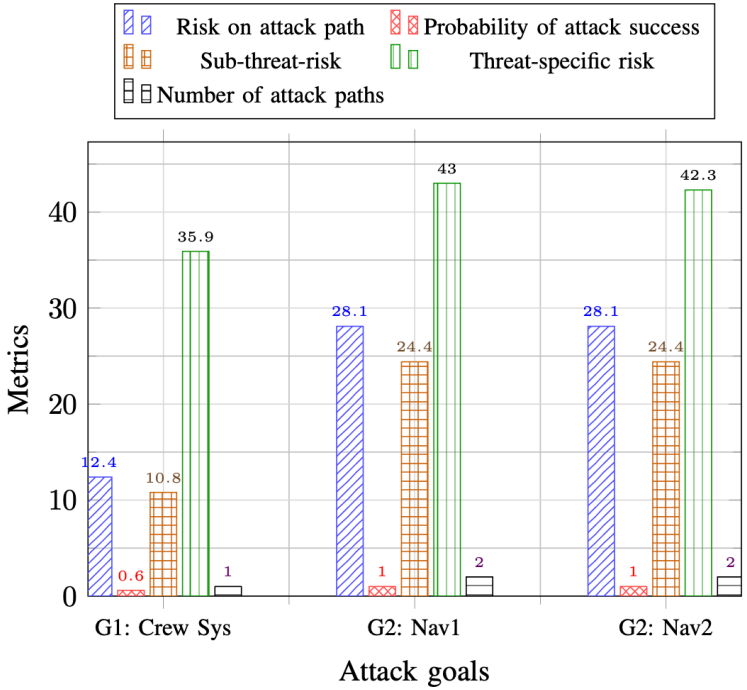
- **Security Analysis (MV-HARM) (cont.):**
  - **Host risk:** VSAT highest due to multiple critical CVEs and external exposure.
  - **Prob. of attack success:** Systems with single critical CVEs → higher attack probability (no chaining).
  - **Sub-treat risk (T, I, E):** VSAT ranks highest across Tampering, Info Disclosure, Elevation.
  - **Threat risk (all threats):** VSAT dominates total risk; Crew minimal.



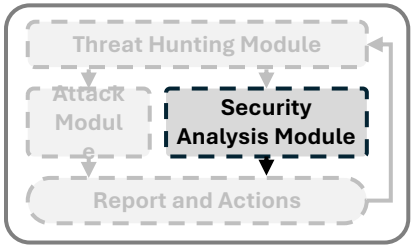
Application: Case Study



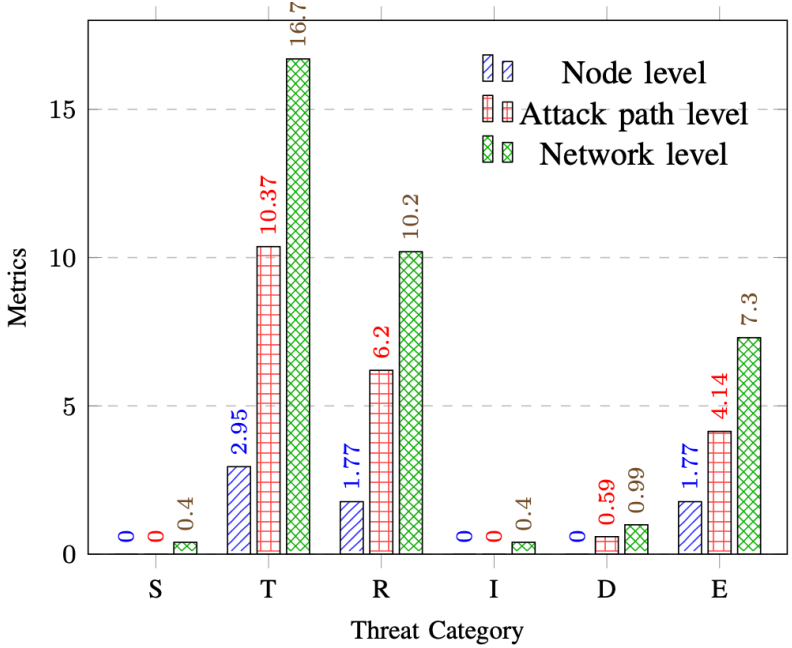
- **Security Evaluation by Attack Goal:**
  - G1 (Crew) → 1 attack path; G2 (Nav) → 2 paths → broader attack surface.
  - G2 shows highest risk & threat-specific risk.
  - Mitigating one navigation system can reduce risk in the other.



Application: Case Study



- **Individual Threat Analysis (Admin System):**
  - ‘Tampering’ (T) → highest risk at node level.
  - ‘Spoofing’ (S) and ‘Information Disclosure’ (I) → lowest risk locally but some network-level exposure.
  - Highlights importance of multi-level contextual evaluation.



Conclusion

- Maritime systems' connectivity increases vulnerability; traditional methods use **outdated** data.
- Our proposed framework combines **real-time threat intelligence + MV-HARM modeling** for **continuous, quantitative risk assessment**.
- Demonstrated effective analysis using **live vessel data** and simulated attacks.
- Enables continuous monitoring and informed security decisions.
- *Future work:* automate the Defense/Reporting/Action phase for onboard response.

Thank you!

Contact: Simon Yusuf Enoch <simony@whitecliffe.ac.nz>
Hyunjae Kang <hyunjae.kang@uq.edu.au>