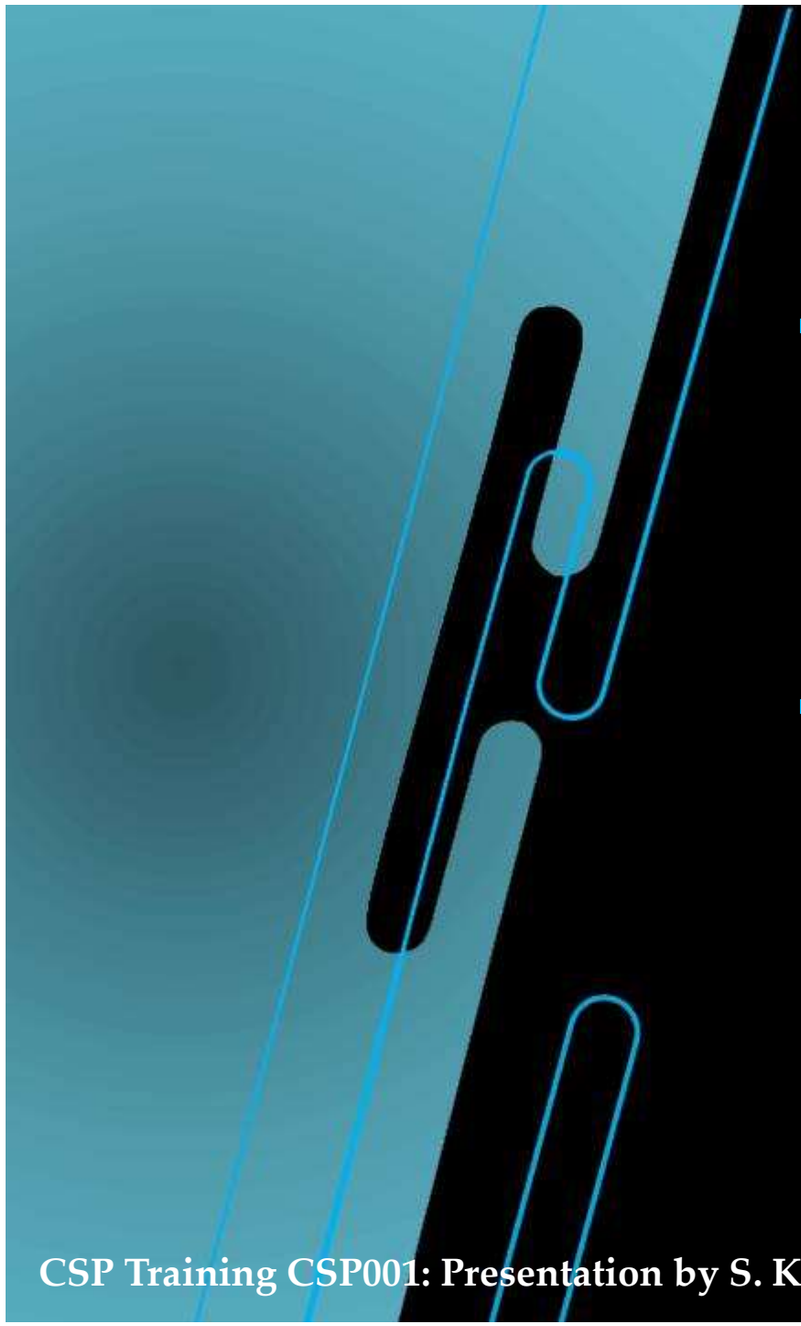
AI and Cybersecurity: Research in Maritime

CSP007

PRESENTATION BY: STYLIANOS KARAGIANNIS, (PDMFC, PORTUGAL)

Tracking and Identification Protocols in Maritime Communication

- **Automatic Identification System (AIS):** Primarily used for vessel tracking and collision avoidance in coastal areas and busy waterways. It operates on VHF frequencies and provides real-time position, course, and speed information.
- **Long Range Identification and Tracking (LRIT):** Designed for long-range identification and tracking of vessels, particularly for regulatory compliance and security purposes. LRIT operates over satellite communication systems, enabling global coverage and tracking capabilities beyond the range of AIS. Example: LRIT data is transmitted via satellite to LRIT data centers for monitoring and compliance purposes.



Emergency Distress and Commercial Communication Solutions at Sea

- **Global Maritime Distress and Safety System (GMDSS):** An internationally recognized system for distress and safety communications at sea. It encompasses various communication technologies such as satellite, HF, VHF, and MF radio, providing redundancy and ensuring reliable communication in emergency situations.
- **Inmarsat:** A commercial satellite communication network provider offering voice, data, and internet services to the maritime industry. While Inmarsat services can be used for distress communication as part of GMDSS compliance, they also provide non-emergency communication and connectivity solutions for vessel operations and crew welfare. Example: Inmarsat FleetBroadband provides high-speed internet access for emails, weather updates, and crew communications.

GMDSS Vulnerabilities (Vendor: Cobham)

Firmware Access Control Vulnerabilities

CVE-2019-9534: The firmware version 1.07 of Cobham EXPLORER 710 lacks validation, allowing an unauthenticated, local attacker to upload custom firmware, potentially leading to various security threats.

CVE-2019-9533: Specific root password across firmware versions up to v1.08, which could be reverse-engineered by attackers to gain unauthorized access.

CVE-2019-9530: The web root directory of Cobham EXPLORER 710 firmware version 1.07 allows unauthenticated, local attackers to access and download any file without restrictions.

CVE-2019-9532: The web application portal of Cobham EXPLORER 710 firmware version 1.07 transmits login passwords in cleartext, facilitating interception by unauthenticated, local attackers.

Inmarsat Vulnerabilities

Satellite Communications

CVE-2017-3221: Inmarsat AmosConnect 8 login form is vulnerable to Blind SQL injection, allowing remote attackers to access usernames and passwords.

CVE-2013-6035: Firmware on various satellite terminals allows remote attackers to execute arbitrary code via TCP port 1827 without authentication.

CVE-2013-6034: Firmware on satellite terminals contains hardcoded credentials, making it easier for attackers to obtain unauthorized login access.

Thank you

Organization: PDMFC

Please send all questions to:
stylianos.karagiannis@pdmfc.com