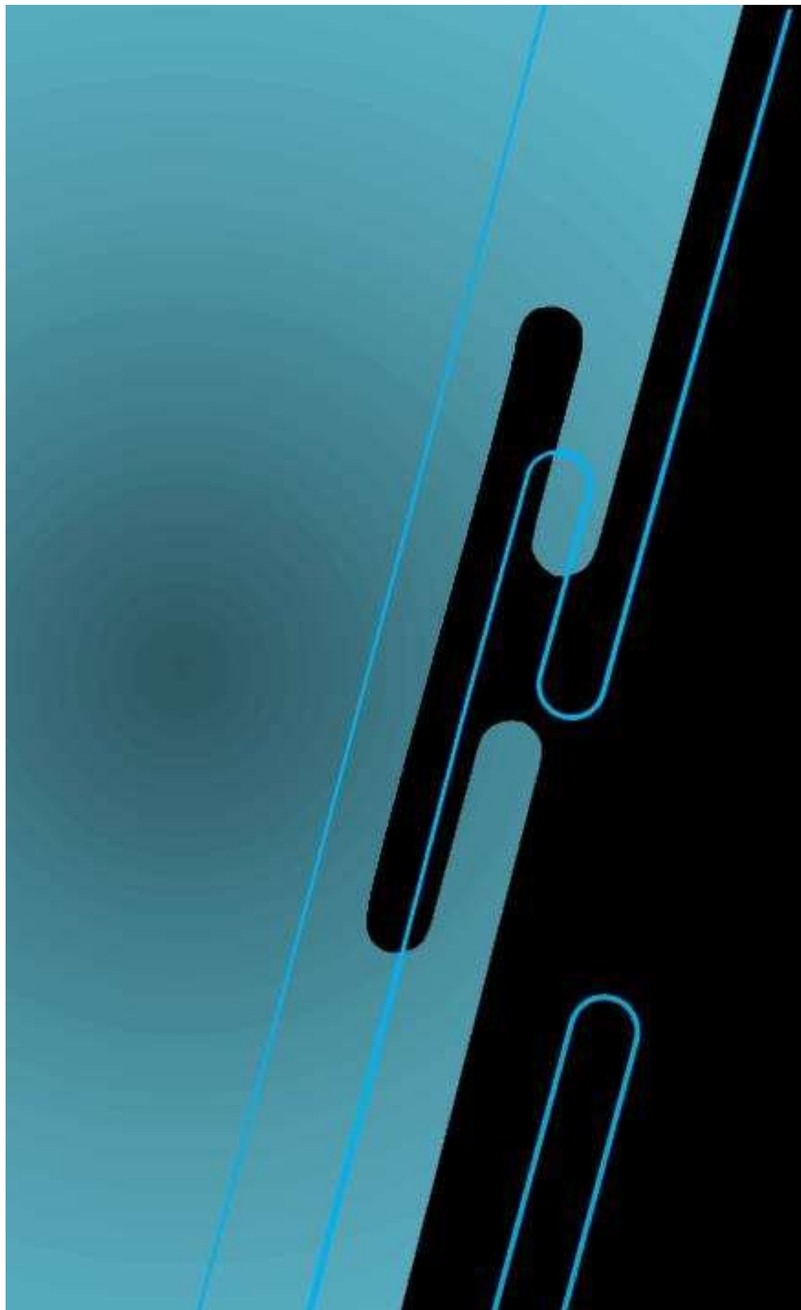
IA e sicurezza informatica: Ricerca in ambito marittimo

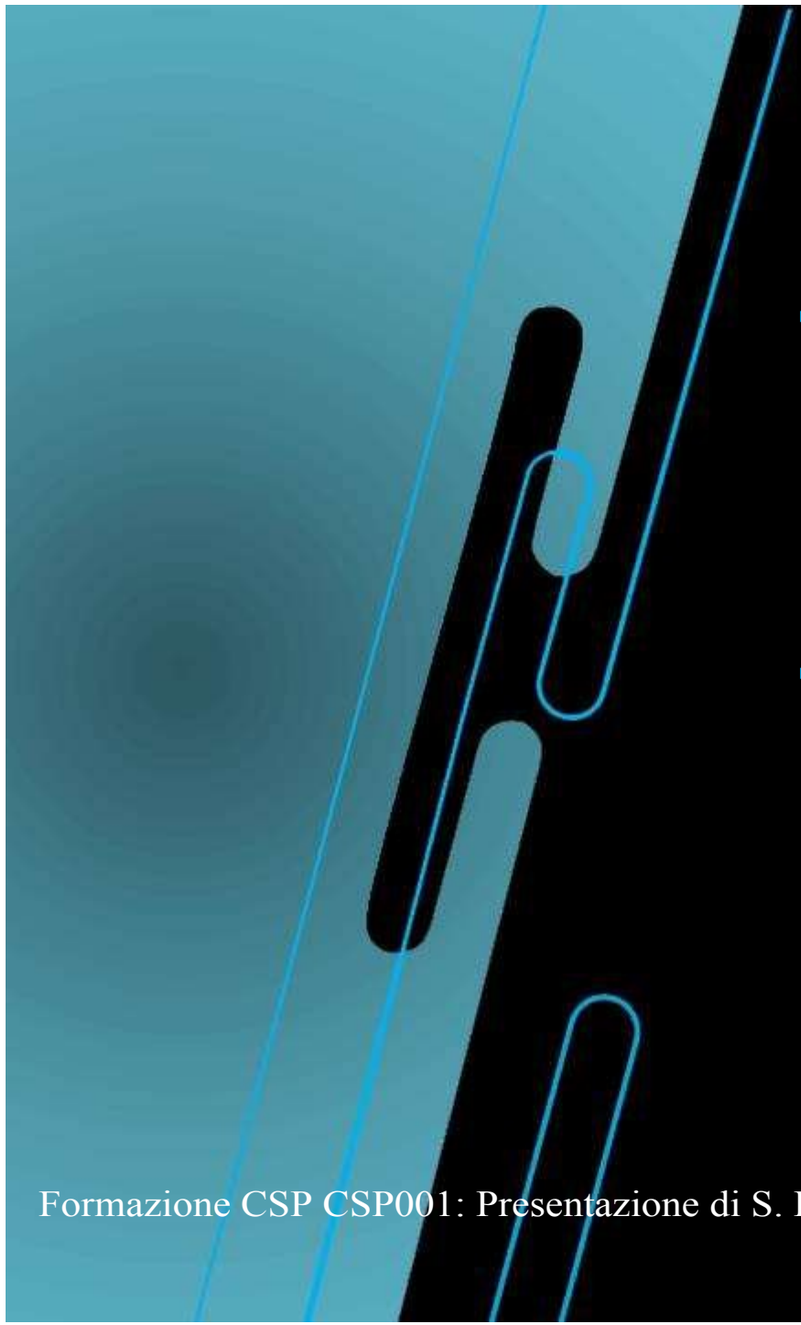
CSP007

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS, (PDMFC, PORTOGALLO)



Protocolli di tracciamento e identificazione nelle comunicazioni marittime

- Sistema di identificazione automatica (AIS): Utilizzato principalmente per la localizzazione delle imbarcazioni e per evitare le collisioni nelle zone costiere e nelle vie d'acqua trafficate. Funziona su frequenze VHF e fornisce informazioni in tempo reale su posizione, rotta e velocità.
- Identificazione e tracciamento a lungo raggio (LRIT): Progettato per l'identificazione e il tracciamento a lungo raggio delle imbarcazioni, in particolare per scopi di conformità normativa e di sicurezza. L'LRIT opera attraverso sistemi di comunicazione satellitare, consentendo una copertura globale e capacità di tracciamento al di là della portata dell'AIS. Esempio: I dati LRIT vengono trasmessi via satellite ai centri dati LRIT per scopi di monitoraggio e conformità.



Soluzioni di comunicazione commerciale e di emergenza in mare

- Sistema globale di soccorso e sicurezza marittima (GMDSS): Un sistema riconosciuto a livello internazionale per le comunicazioni di soccorso e sicurezza in mare. Comprende varie tecnologie di comunicazione, quali satellite, HF, VHF e radio MF, che forniscono ridondanza e garantiscono comunicazioni affidabili in situazioni di emergenza.
- Inmarsat: Fornitore di reti commerciali di comunicazione satellitare che offre servizi voce, dati e Internet all'industria marittima. I servizi Inmarsat possono essere utilizzati per le comunicazioni di soccorso nell'ambito della conformità al GMDSS, ma forniscono anche soluzioni di comunicazione e connettività non di emergenza per le operazioni navali e il benessere dell'equipaggio. Esempio: Inmarsat FleetBroadband fornisce accesso a Internet ad alta velocità per e-mail, aggiornamenti meteo e comunicazioni con l'equipaggio.

Vulnerabilità GMDSS (Fornitore: Cobham)

Vulnerabilità del controllo di accesso al firmware

CVE-2019-9534: la versione 1.07 del firmware di Cobham EXPLORER 710 manca di convalida, consentendo a un aggressore locale non autenticato di caricare un firmware personalizzato, che potrebbe portare a varie minacce alla sicurezza.

CVE-2019-9533: password di root specifica nelle versioni del firmware fino alla v1.08, che potrebbe essere decodificata dagli aggressori per ottenere un accesso non autorizzato.

CVE-2019-9530: La directory web root del firmware Cobham EXPLORER 710 versione 1.07 consente agli aggressori locali non autenticati di accedere e scaricare qualsiasi file senza restrizioni.

CVE-2019-9532: il portale dell'applicazione Web di Cobham EXPLORER 710 versione firmware 1.07 trasmette le password di accesso in chiaro, facilitando l'intercettazione da parte di aggressori locali non autenticati.

Vulnerabilità di Inmarsat

Comunicazioni satellitari

CVE-2017-3221: il modulo di login di Inmarsat AmosConnect 8 è vulnerabile a Blind SQL injection, consentendo agli aggressori remoti di accedere a nomi utente e password.

CVE-2013-6035: Il firmware di diversi terminali satellitari consente agli aggressori remoti di eseguire codice arbitrario tramite la porta TCP 1827 senza autenticazione.

CVE-2013-6034: il firmware dei terminali satellitari contiene credenziali codificate in modo rigido, rendendo più facile per gli aggressori ottenere un accesso non autorizzato.

Grazie

Organizzazione: PDMFC

Si prega di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com