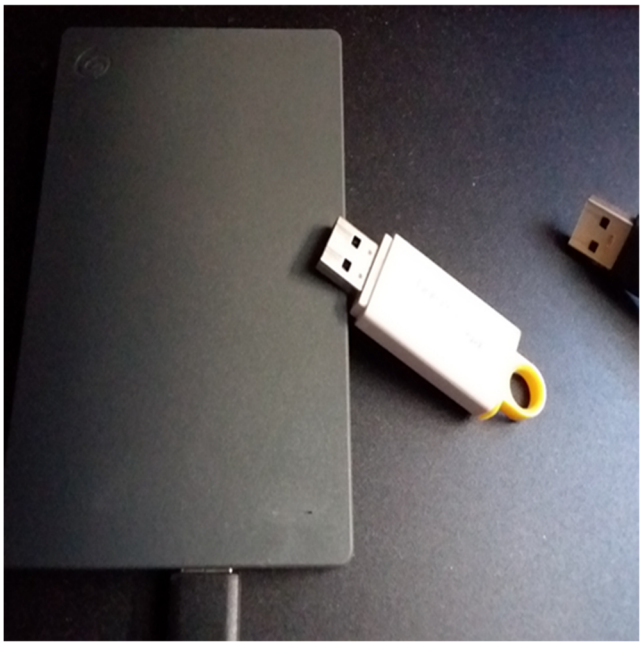
Ministero delle Imprese e del Made in Italy

DIREZIONE GENERALE PER LE TECNOLOGIE DELLE COMUNICAZIONI E LA SICUREZZA INFORMATICA - ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE

Scuola Superiore di Specializzazione in Telecomunicazioni

Sicurezza informatica: protezione dei sistemi OT e dell'hardware

Seminario on line, 19 aprile 2023 ore 09:30 – 12:30



Lo scenario cyber, in ambito nazionale ed internazionale, sta diventando sempre più complesso e caratterizzato da minacce informatiche sempre più pericolose e tecniche di attacco sempre più evolute.
Cittadini, Imprese e Pubbliche Amministrazioni subiscono danni, a volte molto onerosi, che incidono, oltre che sulla sfera personale, sulla funzionalità e sulla operatività delle organizzazioni, con impatto sui servizi forniti, spesso nell'ambito di attività essenziali per lo Stato.
L'ubiquità dei sistemi di calcolo, tipica del paradigma della "Internet of Things", in cui una moltitudine di oggetti dotati di capacità elaborativa si connettono alla rete, infatti, ha drammaticamente aumentato il numero di possibili attacchi cyber. In tale contesto, pur essendo molta l'attenzione rivolta ad attacchi di livello informatico, altrettanto importanti sono gli attacchi che sfruttano le debolezze dell'hardware e, più in generale, per quelle che possono essere le conseguenze qualora l'attacco avesse quale obiettivo i sistemi di controllo industriale.

Il seminario si propone di affrontare le problematiche relative alla sicurezza cyber delle Operational Technologies (OT), con particolare riferimento ai sistemi di controllo industriale (ICS), ovvero dei sistemi informatici utilizzati per monitorare e controllare processi fisici, dispositivi ed infrastrutture, anche critiche, per poi scendere nel dettaglio della sicurezza a livello hardware.

Dopo una introduzione sulle peculiarità dei sistemi OT, verrà descritta l'evoluzione delle minacce da cui occorre difendersi, evidenziando i principali episodi di attacchi a sistemi SCADA, PLC, DCS e SIS. Ci si concentrerà, quindi, sull'illustrazione delle possibili contromisure da adottare, indicando per ciascuna di esse pregi e limiti.

Verranno successivamente introdotte le principali problematiche della sicurezza dell'hardware, quali l'*hardware trust*, ovvero modifiche intenzionali all'hardware che ne compromettono la sicurezza e l'*hardware vulnerability*, ovvero gli attacchi che sfruttano debolezze architetturali dell'hardware. Si analizzeranno, infine, le principali contromisure utilizzate per mitigare il rischio legato alle varie problematiche descritte.

09:30 – Saluti iniziali
Dr.ssa Eva Spina, Direttore DGTCSI – ISCTI, MIMIt

09:40 – Cybersecurity delle Operational Technologies (OT): minacce e contromisure
Prof. Roberto Setola, Facoltà Dip.ale di Ingegneria, Università Campus Bio-Medico, Roma

10:55 – Sessione di Domande e Risposte

11:05 – La sicurezza dell'hardware: problematiche e contromisure
Prof. Marco Ottavi, Dip. di Ingegneria Elettronica, Università degli Studi di Roma Tor Vergata

12:20 - Sessione di Domande e Risposte

12:30 - Conclusioni

La partecipazione è gratuita. Per prenotarsi ed ottenere il link per seguire il seminario on line, inviare una email a:
scuolasuperiore.tlc@mise.gov.it
Sono stati richiesti 3 Crediti Formativi Professionali (cfp) riconosciuti dal Consiglio Nazionale degli Ingegneri