Cybersecurity degli oggetti connessi

Principi di progettazione e configurazione

Edoardo Calia
Vice Direttore
Fondazione LINKS - Torino

La Fondazione LINKS

LA FONDAZIONE LINKS È UN ENTE STRUMENTALE
DELLA **COMPAGNIA DI SAN PAOLO**
E OPERA COME ENTE STRUMENTALE DEL **POLITECNICO DI TORINO**

Al centro dell'ecosistema torinese della ricerca e dell'innovazione la Fondazione LINKS opera all'interno di un consolidato network internazionale con l'obiettivo di contribuire al progresso tecnologico e socio-economico attraverso processi avanzati di ricerca applicata.

160+
RICERCATORI

1º
CONTRIBUTION/RESEARCHERS
Fonte: Elaborazione su dati Commissione Europea

8º
IN ITALIA PER PROGETTI FINANZIATI EU (H2020)
Fonte: Commissione Europea.
Tot. enti valutati (research organizations): 263

900+
PARTNER INDUSTRIALI

17M €
BILANCIO 2020

1600+
PUBBLICAZIONI

24
FAMIGLIE DI BREVETTI

Presidiamo tecnologie per trasferirle al mercato


Antennas Design

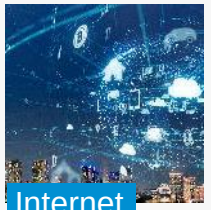

Augmented & Virtual Reality


Blockchain & Distributed Ledger Technology


Communic. Technologies

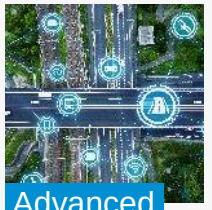

High Performance Computing


Artificial Intelligence & Data Science


Internet Of Things


Navigation Services


Rural Urban & Heritage Development


Advanced Transportation Models

Applications

ASSETS VALORISATION	BUSINESS MODELLING	CIRCULAR ECONOMY	CULTURAL HERITAGE INNOVATION
CYBERSECURITY	DIGITAL FOR WELL-BEING	INDUSTRY 4.0	USER EXPERIENCES

End-Markets

Finance & Insurance

Telecom

Aero, Space & Defense

Logistics & Transport

Manufacturing

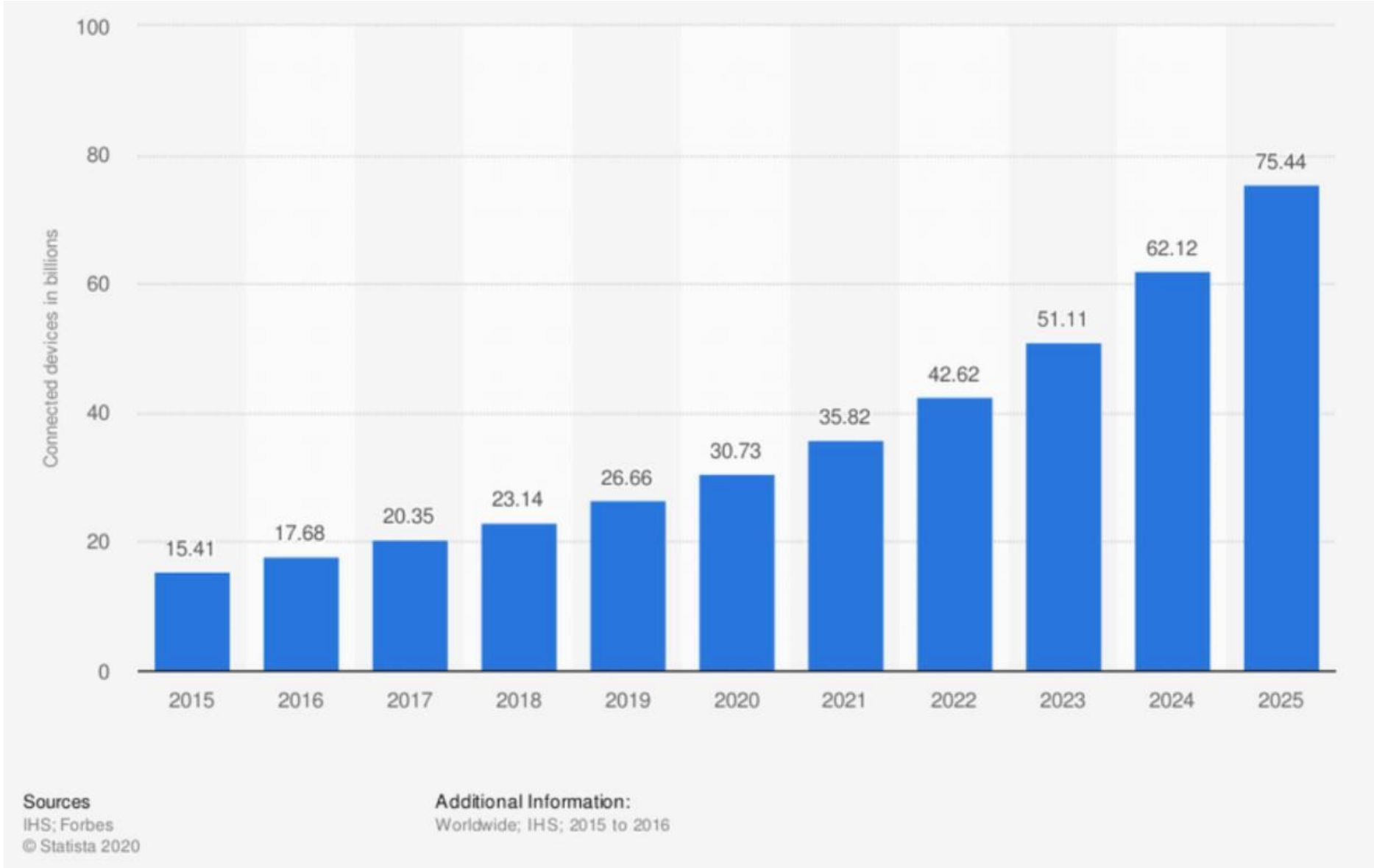
Energy

Agritech Food & Beverage

Public Authorities

Museums & Turism

IoT: numero di oggetti connessi



Oggetti connessi: nuove sfide per la cybersecurity

- Tra gli oggetti connessi figurano anche sistemi elettronici di supervisione e controllo di impianti industriali e altri *sistemi embedded*
- Così come avviene per la cybersecurity dei sistemi informatici tradizionali, un oggetto può essere target o veicolo per nuove tipologie di attacco
  - Attacchi rivolti a sistemi industriali
  - Attacchi che usano gli oggetti comuni installati anche presso le abitazioni degli utenti come veicolo per attacchi (es: DDoS, *Distributed Denial of Service*)

Attacchi verso sistemi industriali

Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

A power cut in western Ukraine last month was caused by a type of hacking known as "spear-phishing", says the US Department of Homeland Security (DHS).

The attack caused a blackout for 80,000 customers of western Ukraine's Prykarpattyaoblenergo utility.

Experts have described the incident as the first known power outage caused by a cyber attack.

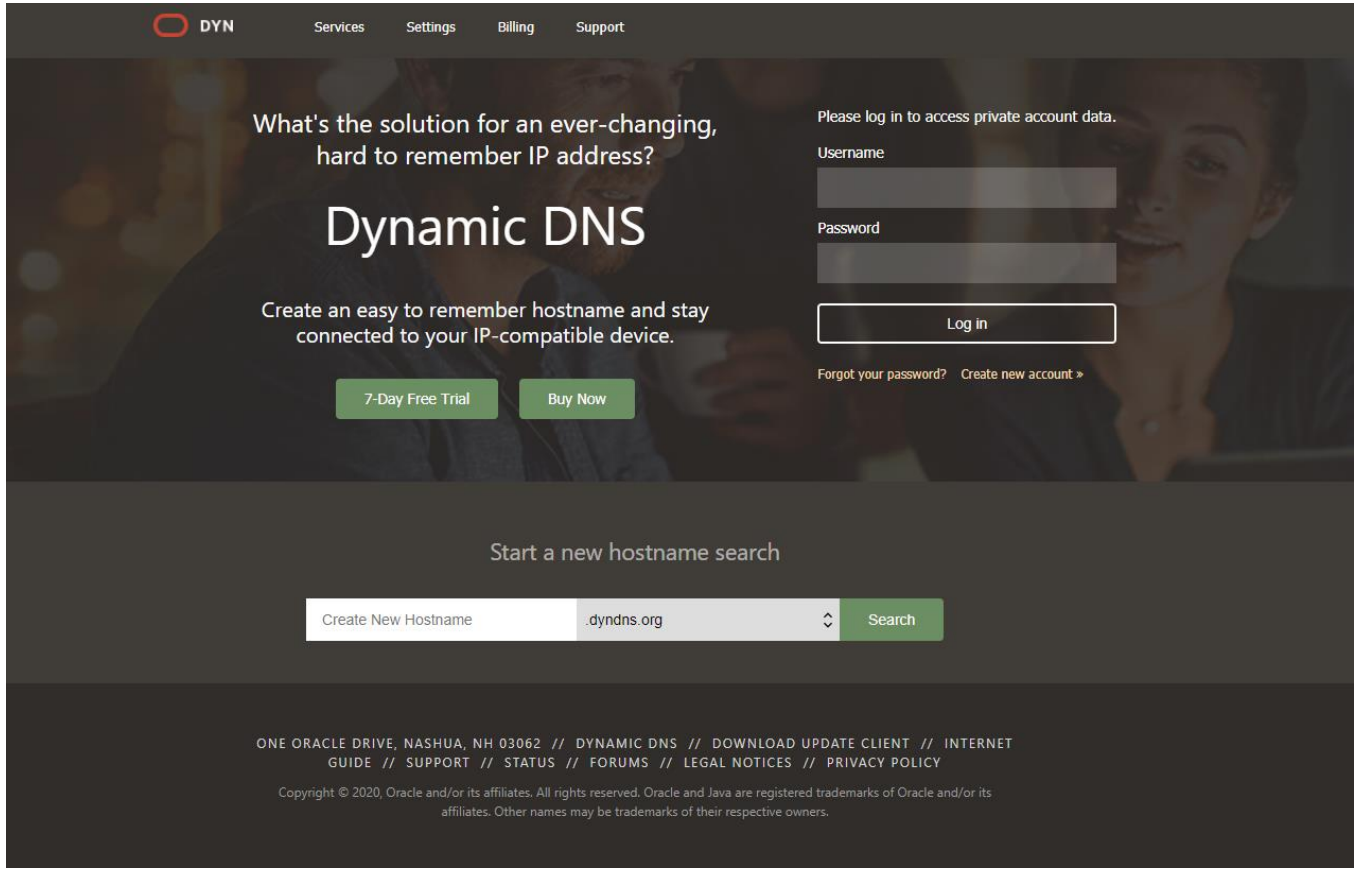
Attacchi verso Sistemi Industriali

- Differiscono dai cyber attacchi tradizionali per alcune peculiarità:
  - Assenza di una motivazione legata al furto di dati, sostituita dall'obiettivo di arrecare danni fisici (nel mondo fisico) a cose, persone o processi (es: processi produttivi)
  - Sono più complessi da mettere a punto perché richiedono una conoscenza del contesto e della organizzazione target (competenze di ingegneria di processo anche molto specifiche). Per la massima efficacia occorre aver eseguito un sopralluogo sul posto.

Attacchi di DDoS

- DDoS: Distributed Denial of Service
- Aumentati in modo significativo nel 2020
- Sfruttano anche la crescente banda disponibile nelle reti moderne: in Olanda si è registrato quest'anno un attacco che ha generato 88Gbps di traffico, e in Italia uno che ha generato 11 milioni di pacchetti di dati al secondo
- Per generare moli di traffico di questo tipo spesso si usano decine o centinaia di migliaia di oggetti, ciascuno in grado di generare una frazione del traffico totale

Attacco DDoS
Dyn (Oracle)



L’attacco a Dyn

- 50,000 – 100,000 oggetti utilizzati prima come target, poi come attaccanti (webcam, router wifi domestici, baby monitors etc)
- È stato utilizzato il malware Mirai (*futuro* in Giapponese), composto da due parti: una dedicata alla propagazione (virus) e una dedicata all’attacco (Command and Control)
- Come target è stato scelto il servizio offerto da Dyn, la società che gestiva la traduzione da nome a indirizzo IP (DNS) di alcuni dei principali servizi Internet

Mirai Botnet

- Componente virus: scansiona costantemente lo spazio degli indirizzi IP (con alcuni *range* espressmente esclusi) alla ricerca di altri dispositivi sui quali installarsi. Tenta l'accesso utilizzando un piccolo dizionario di coppie username - password utilizzate come default sui dispositive più comuni
- Componente Command and Control: al momento opportuno scatena l'attacco, inviando richieste di servizio false all'indirizzo IP scelto come target
- L'attacco non genera danni, ma rende il server preso di mira inutilizzabie dagli utenti reali

Mirai botnet

- Il codice del malware è stato reso pubblico, e molti lo hanno scaricato e utilizzato per perpetrare ulteriori attacchi, eventualmente modificandolo leggermente
- Uno dei più rilevanti si è verificato nel Novembre del 2016, quando 900,000 router di Deutsche Telecom sono stati compromessi utilizzando per accedervi il protocollo utilizzato da DT per la gestione remota degli apparati

Tecniche di difesa: dispositivi domestici

- L'utente non ha molta possibilità di influenzare le caratteristiche di sicurezza degli oggetti connessi acquistabili sul mercato (consumer)
- Buone prassi sono il cambio della password rendendo inutilizzabile quella impostata per default sui dispositivi, e disabilitare (se possibile / semplice) «porte» di accesso che potrebbero rappresentare una vulnerabilità, come quelle associate al servizio UPnP (che consente diversi automatismi di configurazione, ed è normalmente attivo ad esempio su tutti i router domestici)

Gestione attenta delle credenziali

- Gli oggetti connessi, come gli utenti umani, accedono a servizi autenticandosi sulla rete mediante credenziali (oppure offrono servizi ricevendo connessioni autenticate mediante credenziali)
- Molti utilizzano il classico metodo username / password
- L'identità degli oggetti, se non gestita correttamente, costituisce una vulnerabilità
- Il rischio è anche maggiore rispetto ai sistemi informativi classici perché la verifica e aggiornamento delle password viene fatto meno frequentemente

Identità degli oggetti

- Il tema è ampio e complesso, ma il suo studio può contare sulla esperienza maturata in molti anni nel settore della sicurezza dei sistemi informativi
- Ad esempio è allo studio, da parte del W3C, una architettura simile a quella detta PKI (Public Key Infrastructure) che si appoggia su sistemi decentralizzati (DPKI), per evitare colli di bottiglia rappresentati dalla gestione dei certificati

Tecniche di difesa: dispositivi domestici

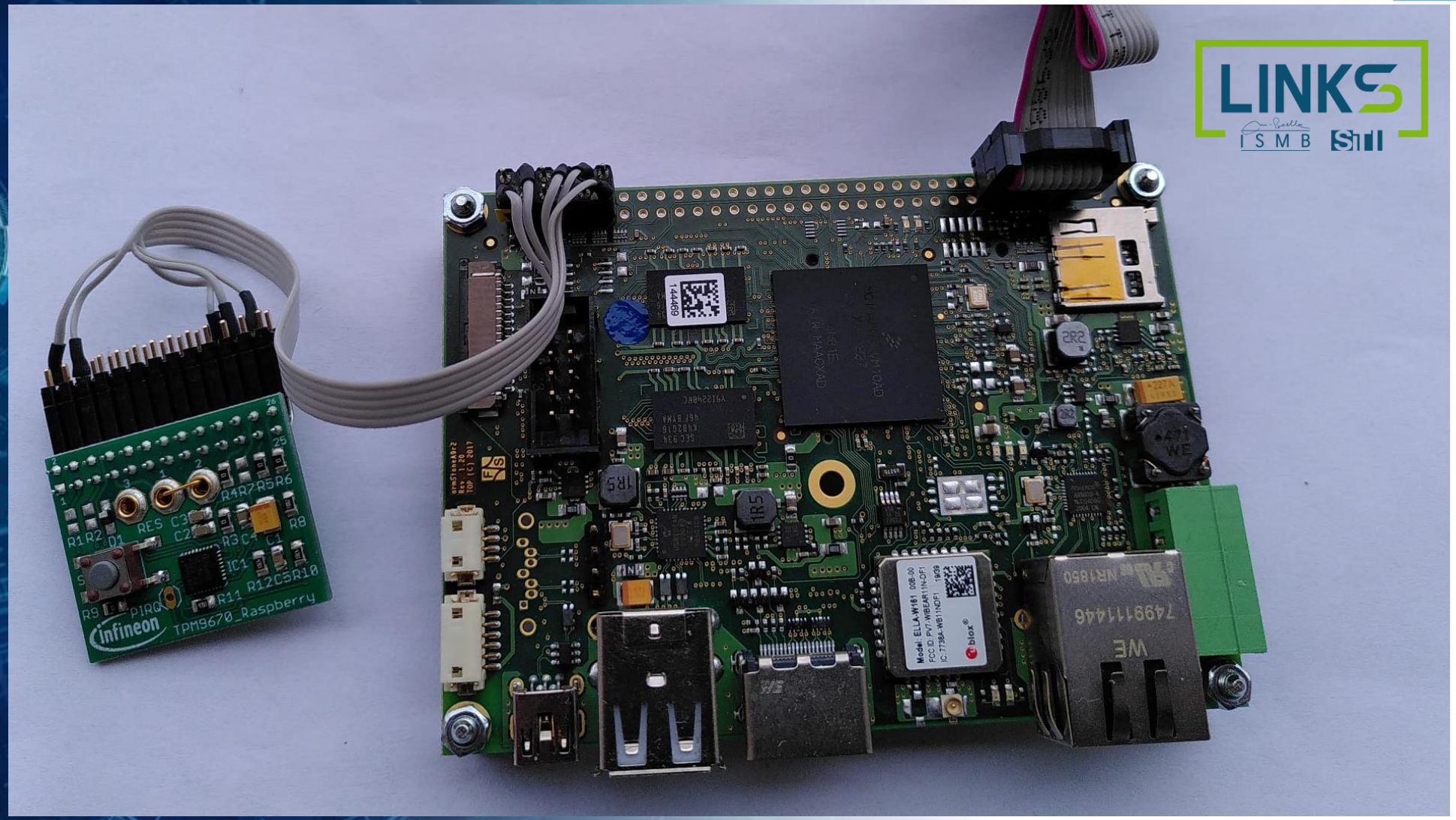
- La quasi totalità della responsabilità sulla sicurezza informatica nel caso dei dispositivi domestici grava sul costruttore, che spesso mette sul mercato oggetti che presentano vulnerabilità significative
- Il compromesso funzionalità – sicurezza non è tuttavia semplice da raggiungere: alcuni oggetti hanno (e devono avere) prestazioni molto basse (ad esempio per contenere il consumo), e questo non consente di utilizzare sistemi sofisticati di sicurezza (ad es. crittografia)
- Parte delle verifiche di sicurezza dovrebbero / potrebbero essere eseguite dagli operatori e ISP, che hanno la possibilità di osservare il traffico di rete e quindi verificare profili / pattern ed eventi sospetti

Sicurezza di dispositivi embedded
Embedded Trusted Computing

Trusted computing

- Tecnologia proposta dal TCG, Trusted Computing Group, che ne ha definito e pubblicato le specifiche
- Obiettivo: garantire che i dispositivi che ne fanno uso non siano stati manomessi (ad esempio modificando il SW o installando SW malevolo)
- Basato su meccanismi di crittografia asimmetrica (chiave pubblica / chiave privata)


LINKS
ISMB


infineon
TPM9670_Raspberry

Cyber Range

- Un *cyber-Poligono di tiro* messo a punto presso LINKS – Politecnico di Torino
- Laboratorio utilizzabile per condurre prove di sicurezza su dispositivi elettronici ed elaboratori
- Una «sandbox» isolata dalla rete aziendale
- Sistemi sofisticati di simulazione e co-simulazione (mista oggetti reali e simulati)
- Progettato in collaborazione con il CINI (Consorzio Interuniversitario Nazionale per l'Informatica) e in particolare con l'Università di Genova

Cyber Range

Luogo ideale per

- Testare le performance di sicurezza di dispositivi (penetration test, vulnerability assessment etc)
- Svolgere esercitazioni e training su cybersecurity
- Ospitare challenge nell'ambito di competizioni per studenti e aziende

Grazie per l'attenzione!

Edoardo Calia
Vice Direttore - Fondazione LINKS
Via Pier Carlo Boggio 61, 10138 Torino


edoardo.calia@linksfoundation.com


@edocalia


https://www.linkedin.com/in/edocalia/