TEST LABORATORIO DI SICUREZZA SUPSI - I risultati

Il laboratorio di sicurezza della SUPSI, con alcuni studenti dell'opzione di specializzazione in cyber-crime, ha investito alcuni giorni per analizzare 4 dispositivi comuni in vendita sul mercato, allo scopo di determinare il livello di sicurezza e le eventuali vulnerabilità.

I dispositivi analizzati sono:
- sistemi di allarme tramite detezione di movimento e contatti per finestre e porte
- serrature elettroniche per porte
- smart TV

Le analisi sono state svolte con studenti anche a scopo didattico, applicando tecniche di analisi dei sistemi, delle tecnolgie utilizzate, di attacchi al software e alle app mobile (reverse code engineering).
Le analisi hanno permesso di apprezzare alcune tecniche di sicurezza dei sistemi e l'efficacia di architetture specifiche per evitare attacchi di jamming RF, spoofing o furto di informazioni tramite attacchi ai protocolli Bluetooth ed NFC.
Dall'altro lato, è stato possibile identificare punti critici dei sistemi analizzati.

In particolare:
Per 2 dispositivi su 4 è stato possibile forzare il sistema e prendere possesso dello stesso.
Per un terzo dispositivo è stato possibile determinare un punto debole dello stesso qualora installato in un ambiente non debitamente protetto (ad esempio in un appartamento con accesso Wi-Fi non sufficientemente robusto).

Il gruppo di sicurezza e cybercrime della SUPSI tiene costantemente monitorato il mondo IoT allo scopo di studiarne le tendenze e proporre correttivi nell'ambito di progetti di ricerca e conferenze internazionali sul tema, allo scopo di stimolare una sensibilizzazione degli attori che porti quanto prima ad una regolamentazione del mercato e delle regole di accesso allo stesso con apparecchi che possono risultare pericolosi dal punto di vista della sicurezza informatica.