CYBER SECURITY

I dispositivi interessati

Bit e Byte e Dintorni ?

- Cos'è un bit
- Cos'è un Byte
- Codice ASCII e UNICODE => ATN messaggi in altra lingua => incomprensibili => potrebbero celare codice maligno
- Come vengono memorizzati ed elaborati i dati
- Come vengono trasmessi i dati: I **PACCHETTI** in chiaro e cifrati
- Multimedia e dati: la telefonata 'classica' cos'è ?

L'Hardware

- **RETI**
  - IP V4 e V6
  - APPARATI
    - SERVER & CLIENT
    - SWITCH CABLATI E WIFI
    - ROUTER
    - FIREWALL
    - NAS E ARCHVIAZIONE
    - PERIFERICHE

- **RETI**
  - SERVIZI
    - WEB E SHARING
    - MESSAGGISTICA
    - VOIP
    - …

I Limiti…

Devono essere alimentati

Possono andare «fuori giri»

Si scaldano e si rompono

Sono passibili di ‘saturazione’

Quali sono I Dispositivi interessati ?

- computer "tradizionali" (desktop, server, notebook, . . .)
- telefoni e tablet
- infrastruttura/servizi: router, NAS, stampanti, . . .
- *smart* TV, lettori bluray, . . . ("smart means exploitable" Mikko Hypponen)
  - Samsung:"Entro il 2020 tutti i nostri prodotti saranno collegati a Internet, ma il 75% delle nostre TV sono gi`a connesse al web" Clicca qui...
- console di ultima generazione
- automobili, aerei, dispositivi medici, . . .
- "Internet of Things (IoT)": frigoriferi, forni, termostati, . . .
  - Clicca qui...

Quali sono I Dispositivi interessati ?

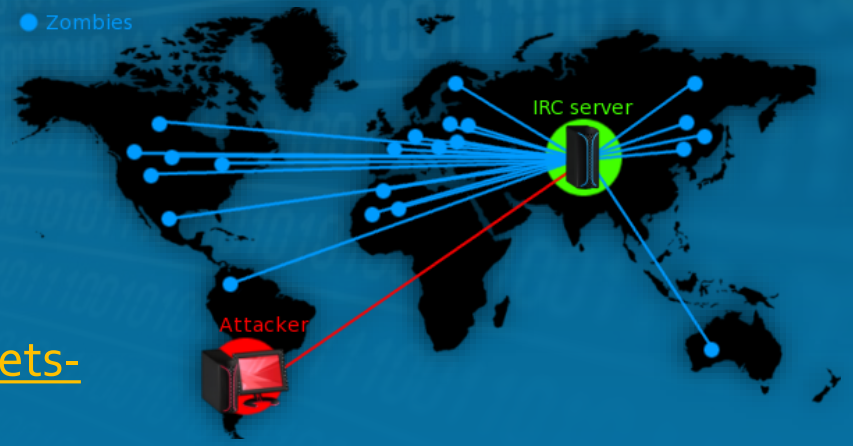
- **computer "tradizionali" (desktop, server, notebook, . . .)**

Febbraio 2013: "La botnet nota come Bamital `e caduta sotto l'azione congiunta di Microsoft, Symantec e delle autorità giudiziarie USA . . . ha infettato più di otto milioni di PC"

http://punto-informatico.it/3712603/PI/News/microsoft-symantec-contro-botnet.aspx

Nine bad botnets and the damage they did:

http://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/



https://www.google.it/search?q=botnet&rlz=1C1EJFA_enIT733IT733&oq=botnet&aqs=chrome..69i57.1815j0j3&sourceid=chrome&ie=UTF-8#q=botnet&tbm=nws&*

Quali sono I Dispositivi interessati ?

- **Infrastruttura/servizi**

Synology Diskstations and Rackstations are being hit by malware dubbed Synolocker . . . similar to the infamous Cryptolocker

. . . encrypts all your files and then demands a ransom to unlock them

http://www.theregister.co.uk/2014/08/05/synologys_synolocker_crisis_its_as_bad_as_you_think/

Have Printers Become a Gateway for Malware?

https://www.opswat.com/blog/have-printers-become-gateway-malware

. . . infects NAS and Digital Video Recorders. . .

http://www.slashgear.com/malware-targets-dvrs-and-synology-nas-to-mine-bitcoin-01323166/

Quali sono I Dispositivi interessati ?

- **Smart TV, . . .**

  LG: . . . collecting usage information. . . better targeted advertising to be shown on the "dashboard" of his TV . . .

  https://blog.malwarebytes.org/online-security/2013/11/snoopy-lg-smart-tv-spies-on-you/

  . . . file name was transmitted unencrypted in HTTP . . .

  http://arstechnica.com/security/2013/11/smart-tv-from-lg-phones-home-with-users-viewing-habits-usb-file-names/

  Samsung: . . . registrare ci`o che viene detto nelle vicinanze della tv . . . e trasmesso a una societ`a terza . . .

  www.ansa.it/sito/notizie/tecnologia/hitech/2015/02/09/samsung-la-smart-tv-ci-ascolta_1ae6133f-84d7-4532-a043-ea38ca34e306.html

  Home Invasion 2.0 - Attacking Network-Controlled Consumer Devices

  https://www.youtube.com/watch?v=eGjrBb1Oscg

Quali sono I Dispositivi interessati ?

- **Dispositivi medici**

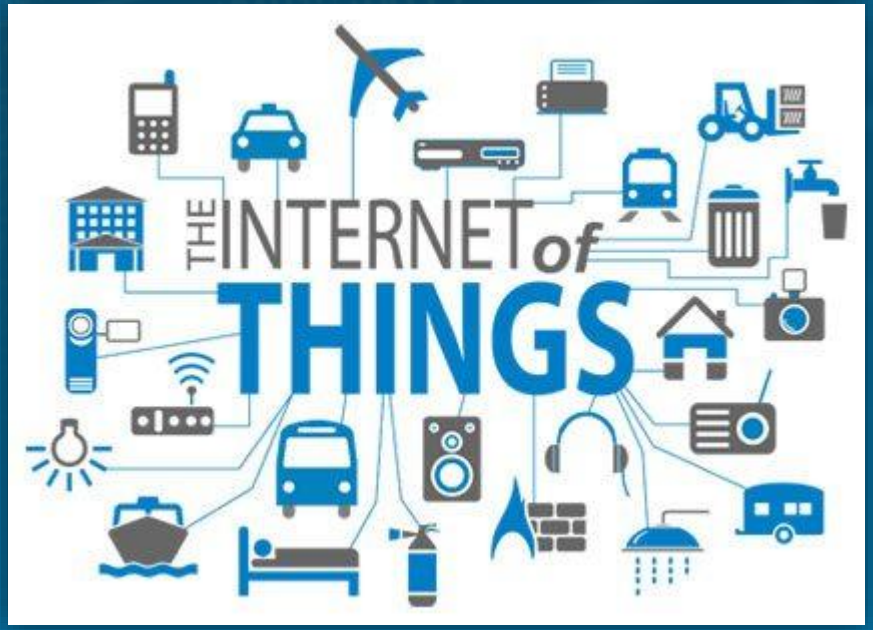
www.washingtonpost.com
Pacemaker
hacked-terminals-capable-of-causing-pacemaker-mass-murder
"Drug Pump's security flaw lets hackers raise dose limits"
drug-pumps-security-flaw-lets-hackers-raise-dose-limits
Medical devices that are vulnerable to life-threatening hacks"
medical-devices-that-are-vulnerable-to-life-threatening-hacks
Interessante video (in inglese):
https://www.youtube.com/watch?v=LRKTnoqUXMo

Quali sono I Dispositivi interessati ?

- **IoT: Internet of Things**

  TV, frigoriferi, termostati, telecamere, . . .
  http://www.welivesecurity.com/2014/11/24/smart-home-security/

  Shodan, a search engine for IoT, . . . lets users easily browse vulnerable webcams
  http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/



Quali sono I Dispositivi interessati ?

- **Varie ed eventuali**

Controllo di automobili

www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
www.welivesecurity.com/2015/11/13/7-things-need-know-car-hacking/
www.hackaday.com/2015/01/21/remotely-controlling-automobiles-via-insecure-dongles/
www.welivesecurity.com/2015/02/03/bmw-fixes-security-flaw-left-2-million-cars-unlocked/

Treni

http://www.theregister.co.uk/2016/01/04/irked_train_hackers_talk_derailment_flaws_drop_scada_password_list/

Manomettere il traffico aereo

www.businessinsider.com/hacker-wreak-havoc-air-travel-faa-2013-6

Baby-monitor:

www.welivesecurity.com/2015/04/22/hackers-spy-kansas-family-unsecured-baby-monitor/

Il Software

- **SISTEMI OPERATIVI**
  - WINDOWS
  - LINUX
  - IOs
  - ANDROID
  - …
- **SERVIZI**
  - DNS
  - IIS, APACHE, …
  - FILE SHARING
  - …
- **APPLICAZIONI**
  - MS OFFICE
  - AUTOCAD
  - SICUREZZA
  - TOOL DI SVILUPPO
  - …
  - HACKING
- **ALTRI**
  - FIRMWARE
  - DRIVER

Il Software: CLASSIFICAZIONE

I software possono essere classificati in base a diverse loro caratteristiche:

- grado di permissività della licenza (software libero o software proprietario);
- da installare o portabile o fruibile come servizio (SaaS);
- sistema operativo su cui possono essere utilizzati (OS ecc.);
- tipo di interfaccia utente visiva (testuale o grafica, modalità touch screen);
- modalità di esecuzione, batch quando i lavori sono impostati in modo che possano essere eseguiti fino al completamento senza l'intervento umano, online (o programmi interattivi) che invece richiedono l'intervento umano per l'immissione dati ed il controllo del lavoro;

Il Software: CLASSIFICAZIONE

- funzione (videoscrittura, foglio elettronico, database management system, grafica, sistema operativo, browser, lettore multimediale, posta elettronica e altre migliaia-considerando la variabilità in termini di soluzioni applicative);
- campo di applicazione: utilizzo casalingo (*home*) o professionale (*business*). In alcuni casi un prodotto vale per ambo le categorie, in molte altre un prodotto ha versioni specifiche (esempio un sistema operativo o una suite di produttività), in tantissime esiste solo per una delle due, spesso quella aziendale (ad esempio un sistema ERP);

Il Software: CLASSIFICAZIONE

- *stand alone* (ovvero che possono girare completamente autonomi su sistemi isolati) oppure *network* (ovvero che funzionano in un ambito di rete). Il secondo caso può essere a sua volta diviso in software in versione client-server (sul client può essere installato magari solo un *agent* oppure l'intero software che però si appoggia ad una base di dati installato su un server oppure ad un servizio server[9]),
- *terminal-server* oppure cloud (applicazioni web) anche in modalità SaaS[10]. Esempi classici di programma di rete, in ambito aziendale, è il sistema gestionale, la posta elettronica centralizzata (spesso associata ai moduli di pianificazione attività e risorse), il firewall della LAN.

MA CHE GIRO FANNO IN DATI IN RETE?

- Com'è fatta allora una rete ?
- Nodi e tratte
- I percorsi dei dati
  - Escono dal nostro IP
  - Rimbalzano di nodo in nodo => possono essere 'ascoltati'
  - Raggiungono il destinatario

- Ping e Traceroute
- https://www.iplocation.net/ip-lookup

Software: il Browser → Cookies

- I cookie sono file di testo che i siti web utilizzano per tenere traccia delle attività degli utenti sulle loro pagine.
- I cookie possono essere utilizzati per personalizzare l'esperienza dell'utente e migliorare la navigazione sul sito.
- I cookie possono anche essere utilizzati per raccogliere informazioni sulle abitudini di navigazione dell'utente e creare profili di utenti.

Software: il Browser → Cookies

- Rischi per la Privacy e la Sicurezza
  - Tracciamento: I cookie possono tracciare il comportamento online degli utenti, creando profili dettagliati delle loro abitudini e preferenze1.
  - Accesso non autorizzato: Se non adeguatamente protetti, i cookie possono essere intercettati da malintenzionati, che potrebbero accedere a informazioni sensibili2.
- Regole e Normative
  - Per proteggere la privacy degli utenti, esistono normative specifiche come il GDPR (Regolamento Generale sulla Protezione dei Dati) che regolano l'uso dei cookie. Ad esempio, i siti web devono ottenere il consenso informato degli utenti prima di installare cookie non essenziali3.

Software: il Browser ➔ Cookies

- Consigli per la Sicurezza
  - Gestione dei Cookie: Utilizza le impostazioni del browser per gestire e cancellare i cookie.
  - Consenso Informato: Assicurati che i siti web che visiti rispettino le normative sulla privacy e richiedano il tuo consenso per l'uso dei cookie3.

COOKIES (LINK)

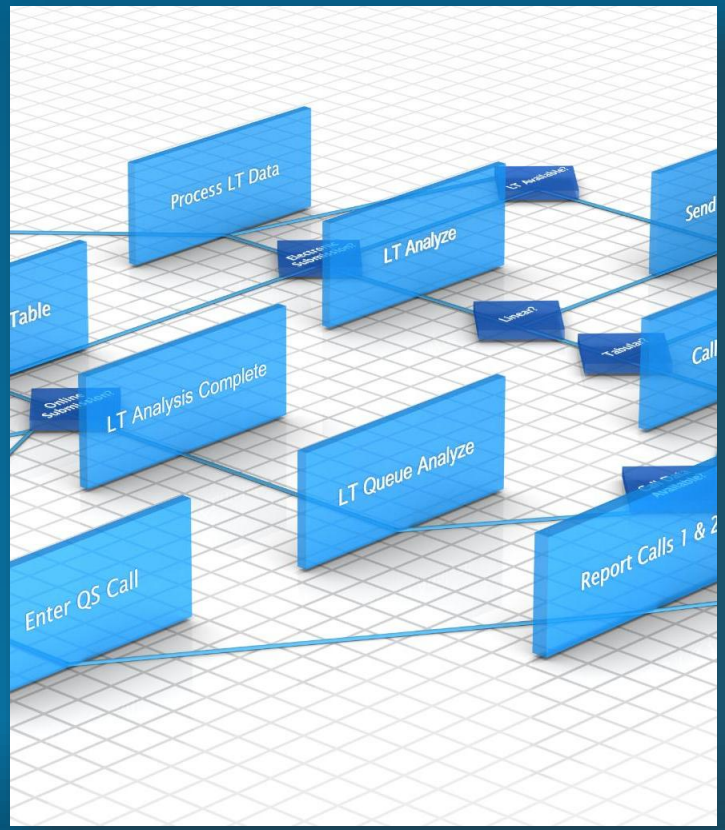
- non è altro che un piccolo file di testo che viene memorizzato sul dispositivo dell'utente quando questo naviga su determinati siti web tramite l'utilizzo del proprio browser preferito.
- utilizzati per ricordare alcune informazioni che l'utente ha precedentemente inserito nei campi di testo di un sito, come ad esempio il nome, l'indirizzo, la password, l'email e/o i numeri delle carte di credito.
- accettare i cookie in linea di massima non è pericoloso in quanto questi servono solo a semplificare un po' le cose quando si naviga su Internet.
- pandasecurity ➔ cookie-pericolosi

COOKIES ELIMINAZIONE

- Chrome ➔ Estensione per visualizzarli
  - Cerca ed Installa «edit this cookie»
- Brave, Firefox, etc.
- Cancellazione di tutti i dati di navigazione
  - Impostazioni => Cancella dati di Navigazione

Plugin del browser

- I plugin del browser sono programmi software che estendono la funzionalità di un browser web.
- I plugin possono aggiungere nuove funzionalità come l'accessibilità, la sicurezza e l'interfaccia utente.
- I plugin possono essere utilizzati per visualizzare contenuti multimediali come video e audio, o per migliorare la navigazione sui siti web.

Come funzionano i plugin del browser

- I plugin del browser sono eseguiti all'interno di un sandbox separato dal browser principale.
- I plugin comunicano con il browser principale attraverso un'interfaccia definita dal browser.
- I plugin possono accedere a risorse esterne del sistema operativo, come il file system locale, solo se l'utente ha dato il consenso.