Sicurezza Informatica

Una breve introduzione

Giovanni Lagorio

DIBRIS - Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi
Università di Genova

12 giugno 2017

Chi sono io?

Giovanni Lagorio

- appassionato di tecnologia, programmatore, "smanettone" ☺
- ricercatore presso il Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi

  `http://www.dibris.unige.it`
- docente di "(Computer and Network) Security" del Corso di Laurea magistrale in Informatica

  `http://computerscience.dibris.unige.it/`

  `http://informatica.dibris.unige.it`
- membro del comitato organizzativo e docente del Master Universitario di II livello in "Cyber Security and Data Protection"

  `http://www.mastercybersecurity.it`
- (un) fondatore e membro del ZenHack team

  `http://zenhack.team/`

Oggi

Argomento vastissimo, solo una *chiacchierata* per:

- informarvi su possibili pericoli
- stimolare il vostro interesse
  - nel caso: `http://informatica.dibris.unige.it` ☺
- fornirvi spunti per approfondimenti

Troverete il link al PDF di questa presentazione alla fine

Attenzione

Descriverò degli attacchi perché è importante *capire* come funzionano (per *difendersi*! . . . e perché è divertente ☺)
Attaccare un sistema altrui senza esplicita autorizzazione è *illegale*

Contenuti

Cosa ci interessa difendere?

In un sistema informatico, cos'è che ha valore per noi?

- Hardware/Software
  - Tipicamente, facilmente sostituibili
- Dati
  - Il valore varia da persona a persona, e può variare anche nel tempo

Tre importanti proprietà: CIA

Cos'è, secondo voi, una violazione della sicurezza?

Cosa vi viene in mente?

Tre importanti proprietà:

- Confidentiality, segretezza
- Integrity, integrità
- Availability, disponibilità

Quindi, cosa vuol dire sicuro?

Quando un sistema/programma è corretto? Quando è sicuro?

Sistema corretto

(Se usato "bene") fa quello che deve fare

Sistema sicuro

(Anche se usato *arbitrariamente* "male") non fa quello che non deve fare

Compromesso

Un programma che non fa nulla è sicuro. . . inutile, ma sicuro ☺
(computer spento, acceso ma isolato, connesso in una rete isolata, connesso al resto del mondo, . . .)

Sicuro rispetto a cosa?

La sicurezza non è mai assoluta

Quali sono i possibili attacchi/attaccanti (interni/esterni)?

https://www.flickr.com/photos/28804910@N06/3207495054/

Mentalità

Dal libro "Thinking Security" di Steven M. Bellovin

the purpose of computer security is not security for its own sake, but to enable some other operation to function properly and (in some cases) profitably.

Let me stress that: the purpose of an organization — a business, a school, a government agency, a hospital — is not to be secure; rather, security is an aid to carrying out its real purpose.

. . . defensive technologies cost money and time; are they worth it? . . . is the cost of the defense more or less than the losses from this attack?

This is a crucial point that every security person should memorize and repeat daily: the purpose of security is not to increase security; rather, its purpose is to prevent losses. Any unnecessary expenditure on security is itself a net loss.

Un piccolo quiz...

Esempio: attacchi che sfruttano l'accesso fisico

Hardware keylogger:

- USB: `http://www.irongeek.com/i.php?page=security/usb-hardware-keyloggers-1-keycarbon`
  venduti perfino su Amazon!
  `http://www.amazon.it/getDigital-KeyGrabber-USB/dp/B001M419IA/ref=sr_1_1`
- PS2:
  `http://www.amazon.com/KeyKatcher-64K-PS-Hardware-Keylogger/dp/B004ZLV1UI`

ma anche...

Video Ghost `http://www.keydemon.com/tiny_frame_grabber/`

- Records entire screenshots at regular intervals
- Compatible with all DVI, VGA, and HDMI devices
- Supports resolutions up to Full-HD 1080p
- No power supply necessary (power is drawn from USB)
- 4 Gigabytes of internal memory in all versions

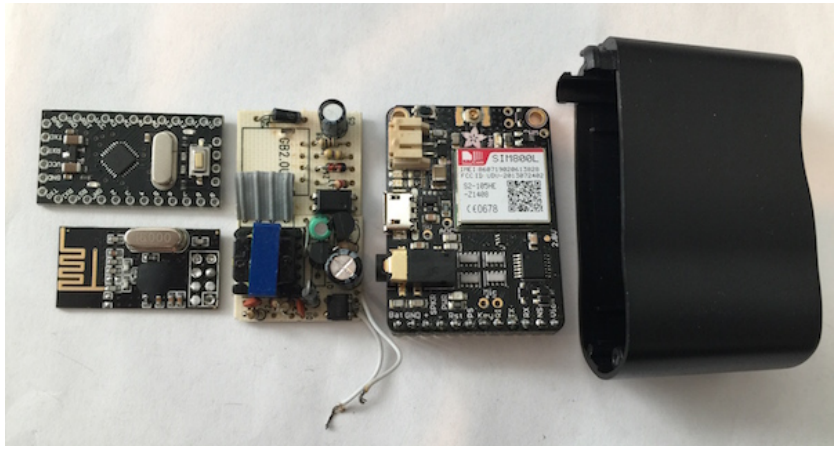
- Embedded time/date-stamping circuit powered by battery, 7 years lifetime!
- No drivers or software necessary, compatible with Windows, Mac, and Linux
- Ultra compact and discrete, looks like an mini-extension cableVideoGhost DVI
- Completely stealthy, undetectable for anti-virus programs
- Available color options: White, Black, Gray, Blue
- Works out of the box, no configuration necessary!

Prendere il controllo tramite...

- USB:
  - Fingendo di essere una tastiera/mouse
    `https://hakshop.com/products/usb-rubber-ducky-deluxe`
  - Sfruttando debolezze dei (di molti?) controller
    `https://nakedsecurity.sophos.com/2014/10/06/badusb-now-with-do-it-yourself-instructions/`
- Thunderbolt (Mac): `http://arstechnica.com/apple/2015/08/thunderstrike-2-rootkit-uses-thunderbolt-accessories-to-infect-mac-firmware/`

Per il resto della presentazione, assumiamo di NON avere accesso fisico

Esempio: KeySweeper, attacco che sfrutta solo la vicinanza



. . . camouflaged as a functioning USB wall charger, that wirelessly and passively sniffs, decrypts, logs and reports back (over GSM) all keystrokes from any MS wireless keyboard in the vicinity

All keystrokes are logged online and locally. SMS alerts are sent upon trigger words, usernames or URLs, exposing passwords. If unplugged . . . continues to operate using its internal battery and auto-recharges upon repowering. A web based tool allows live keystroke monitoring

`http://samy.pl/keysweeper/`

Esempio: attacchi che usano un accesso remoto

Babbo Natale (nel 2014) vi ha portato una Playstation o XBox?

Siete riusciti a giocarci? Online con gli amici? Gli attacchi DDoS a XBox/PSN erano "marketing" per il servizio DDoS venduto (!) dai Lizard Squad :

- `www.welivesecurity.com/2014/12/31/xbox-psn-lizard-squad-ddos/`
- `www.welivesecurity.com/2015/01/13/hacked-routers-used-paid-ddos-attacks/`

Ottobre 2016, DDoS sul DNS

Per alcune ore il traffico Internet è stato "bloccato" (solo il DNS, ma...)

- causato da una *botnet* di dispositivi IoT, come router e telecamere di sorveglianza (!)
- come? Password di default

`www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/`

Anche:

`https://attivissimo.blogspot.it/2016/09/nuove-frontiere-degli-attacchi.html`

Denial Of Service (involontario)

April 21, 2010
Buggy McAfee update whacks Windows XP PCs . . . . . The damage was widespread: the University of Michigan's medical school reported that 8,000 of its 25,000 computers crashed. Police in Lexington, Ky., resorted to hand-writing reports and turned off their patrol car terminals as a precaution. Some jails canceled visitation, and Rhode Island hospitals turned away non-trauma patients at emergency rooms and postponed some elective surgeries. . . .
A report at the Internet Storm Center said the errant McAfee update registered a false positive that flagged the Windows file SVCHOST.EXE as a virus.

`http://www.cnet.com/news/buggy-mcafee-update-whacks-windows-xp-pcs/`

Outline

Un po' di storia

anni '80 virus fase "hobbystica"

1988 primo worm

...

oggi un'economia "underground" di crimine online

`http://on.ted.com/Hypponen`

`https://www.coursera.org/course/malsoftware`

- cybercrime cost ... economy about $450 billion annually

  `http://www.hamiltonplacestrategies.com/news/cybercrime-costs-more-than-you-think`

- industria matura: giorni della settimana vs weekend, riuso del software/componenti, ...

Malware

... contrazione di *malicious* e *software*: "programma malvagio/maligno"

`http://it.wikipedia.org/wiki/Malware`

Virus

Virus

Software in grado di infettare dei file/dischi, in modo da riprodursi facendo copie di se stesso `http://it.wikipedia.org/wiki/Virus_%28informatica%29`

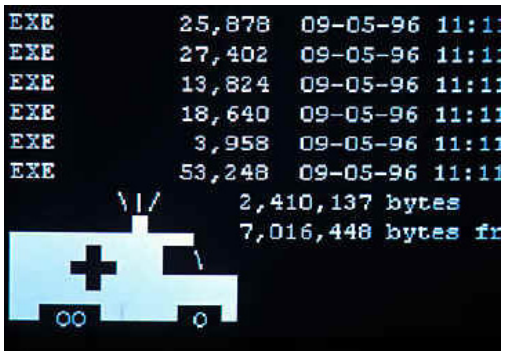
1983 Fred Cohen usa il termine virus

1986 Arriva *Brain*, il primo virus per PC

Tantissime varianti ed evoluzioni arrivano di continuo

Molto carino: `https://archive.org/details/malwaremuseum`

I sintomi di un'infezione erano molto chiari:



`http://enews.storman.com/2012/may/storage.html#sttapart1`

Worm

Worm

. . . malware in grado di autoreplicarsi . . . Il termine deriva dal romanzo di fantascienza del 1975 Codice 4GH . . .

`http://it.wikipedia.org/wiki/Worm`

1988 Robert Morris Jr.,figlio di un alto dirigente della NSA (presso il National Computer Security Center!), crea il primo worm

- colpì tra le 4000 e le 6000 macchine, si stima il 4-6% dei computer collegati

1988–2003 varie evoluzioni

- SQL Slammer ha causato DoS su vari host, quasi 75.000 in 10 minuti, rallentando il traffico di tutta Internet

2004–Aprile 2017 ?

Maggio 2017 WannaCry

oggi ?

Cybercrime

- Bande criminali pagano per l'accesso a computer infetti
  `http://krebsonsecurity.com/tag/gangstabucks/`
  - Vero e proprio listino prezzi `http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf`
- Servizi *Pay-per-install* permettono l'infezione massiva con un malware scelto dal cliente (spambot, finti antivirus, banking trojans, software per rubare le password/carte di credito), con costi che variano a seconda della posizione geografica delle vittime
  `http://www.secureworks.com/cyber-threat-intelligence/threats/ppi/`
  - Un esempio su Android: `http://www.welivesecurity.com/2012/09/12/dancing-penguins-a-case-of-organized-android-pay-per-install/`

Adesso, va “di moda” il *ransomware*

Trend Micro ha presentato il report delle minacce del primo semestre del 2016 segnalando 3.667.384 casi di infezioni provenienti da ransomware solo in Italia.

- `www.hwupgrade.it/news/sicurezza-software/italia-bersagliata-dai-ransomware-3-6-milioni-di-casi-solo-nel-primo-semestre64667.html`
- `www.trendmicro.it/informazioni-sulla-sicurezza/ricerca/trendlabs-1h-2016-security-roundup/index.html`

Ultima perversione: gratis la chiave di decifratura, se riesci a far infettare almeno altre due persone!

`https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/`

Wannacry (Maggio 2017)

- `https://youtu.be/ZqNSoHFtGM0`
- `https://en.wikipedia.org/wiki/WannaCry_ransomware_attack`

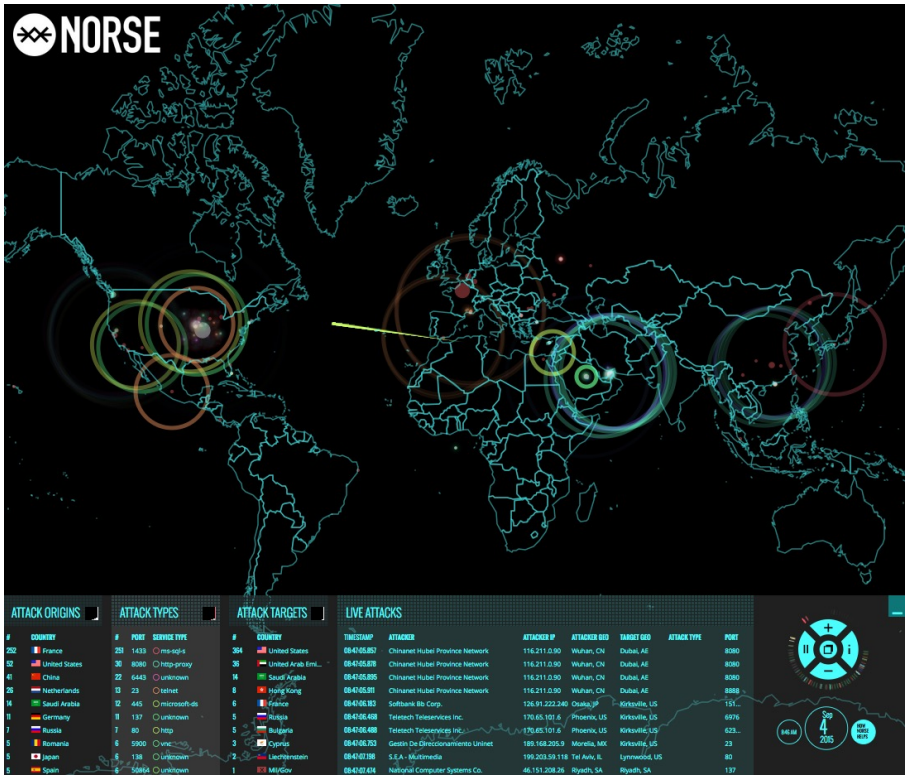
Outline

Con quanti computer hai a che fare?

- 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 già connesse al web"
    `www.ansa.it/sito/notizie/tecnologia/hitech/2015/02/05/samsung-in-2020-tutto-connesso-internet_174162de-bcb2-49ea-8c0b-c49a2d9025b0.html`
- console di ultima generazione
- automobili, aerei, dispositivi medici, . . .
- "Internet of Things (IoT)": frigoriferi, forni, termostati, . . .
  - `http://edition.cnn.com/2013/08/05/tech/mobile/five-hacks/index.html`

Un videogioco di guerra?

Norse ha predisposto una mappa animata che mostra in tempo reale gli attacchi *rilevati* in corso: `map.norsecorp.com`



`attivissimo.blogspot.it/2015/09/un-videogioco-di-guerra-no-il-grafico.html`

Computer “tradizionali”

- Febbraio 2013: “La botnet nota come Bamital è caduta sotto l’azione congiunta di Microsoft, Symantec e delle autorità giudiziarie USA . . . ha infettato più di otto milioni di PC”

  `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/`

`http://en.wikipedia.org/wiki/Botnet`

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/`

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/`

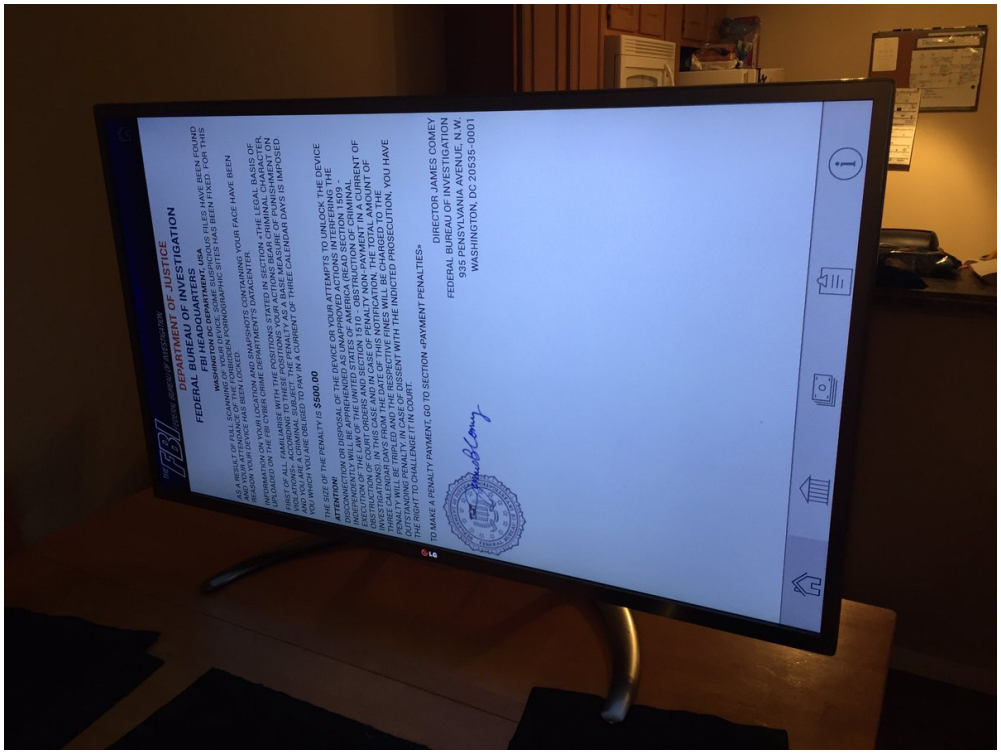
- Samsung: . . . registrare ciò che viene detto nelle vicinanze della tv . . . e trasmesso a una società terza . . .

  `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`

Televisioni che si infettano (ransomware)



`https://attivissimo.blogspot.it/2016/12/si-le-smart-tv-sono-infettabili-e.html`

LG non voleva rivelare la procedura di reset, assente dal manuale, e chiedeva circa 340 dollari per la riparazione (presso un centro assistenza)
Lieto fine: l'immagine è diventata virale e LG ha fornito gratuitamente le istruzioni per il reset

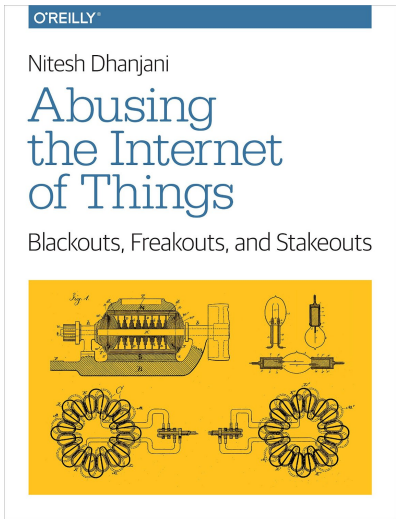
Dispositivi medici

- http://www.washingtonpost.com/national/health-science/facing-cybersecurity-threats-fda-tightens-medical-device-standards/2013/06/12/b79cc0fe-d370-11e2-b05f-3ea3f0e7bb5a_story.html
- Pacemaker (attacchi wireless, in grado di *uccidere*)
  - http://www.itnews.com.au/News/319508,hacked-terminals-capable-of-causing-pacemaker-mass-murder.aspx
  - http://www.theregister.co.uk/2016/12/01/denial_of_life_attacks_on_pacemakers/
- "Drug Pump's security flaw lets hackers raise dose limits" http://www.wired.com/2015/04/drug-pumps-security-flaw-lets-hackers-raise-dose-limits/
- Medical devices that are vulnerable to life-threatening hacks" http://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/
- Interessante video (in inglese): https://www.youtube.com/watch?v=LRKTnoqUXMo

IoT: Internet of Things

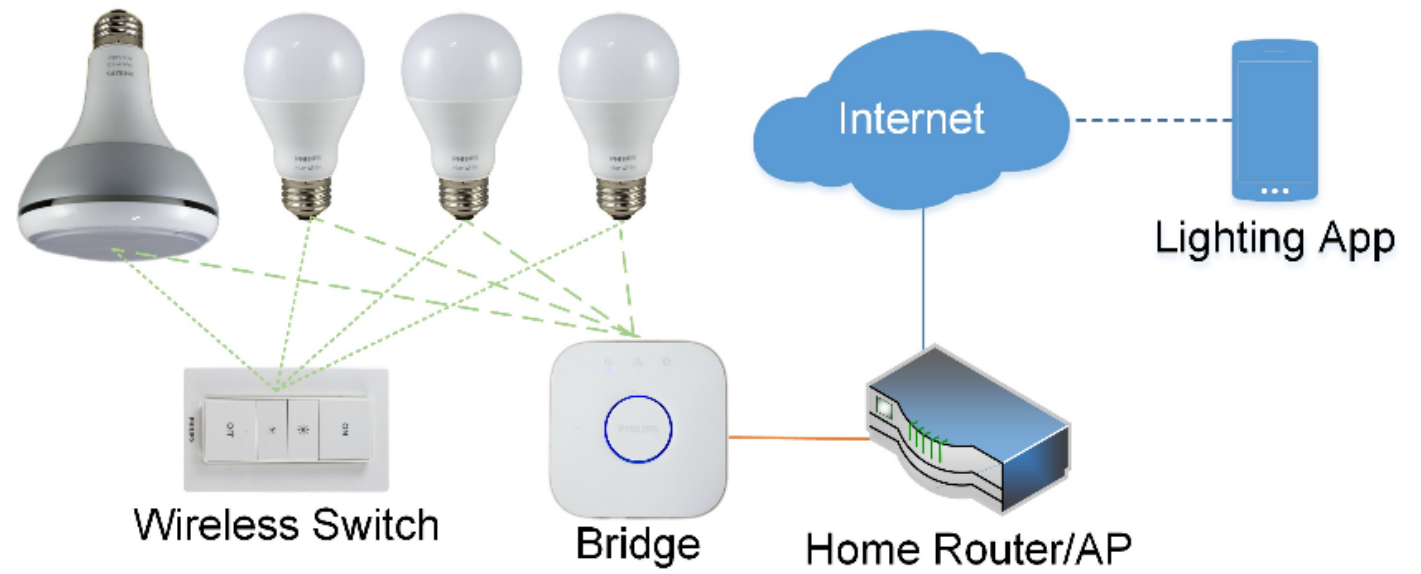
- TV, frigoriferi, termostati, telecamere, . . .

  `http://www.welivesecurity.com/2014/11/24/smart-home-security/`
- Shodan, a search engine for IoT, . . . lets users easily browse vulnerable webcams
  - `arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/`
  - `attivissimo.blogspot.com/2016/03/piccola-demo-di-ordinaria-insicurezza.html`
  - `attivissimo.blogspot.com/2016/03/dj-mette-online-senza-protezioni-il-suo.html`



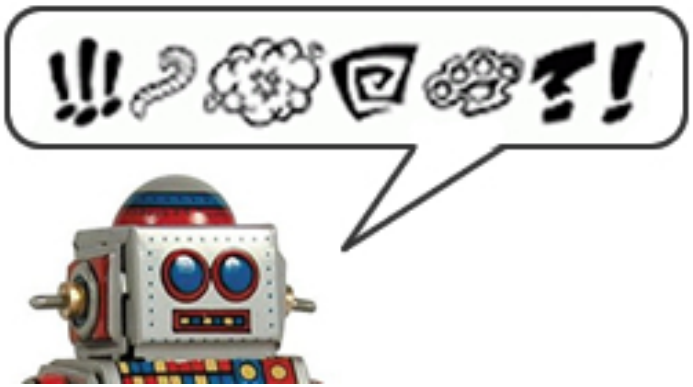
Uscito recentemente (2015): "Abusing the Internet of Things" di Nitesh Dhanjani — O'Reilly

Lampadine che si infettano!



`http://iotworm.eyalro.net/`

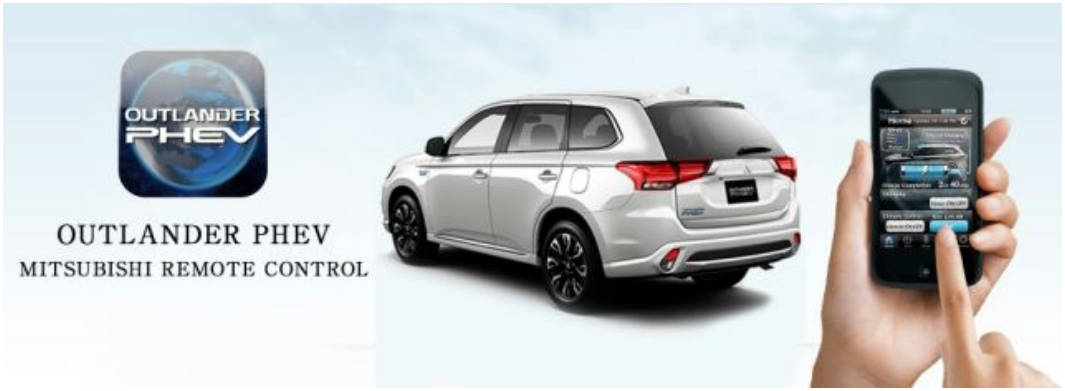
Giocattoli “spia”



https://attivissimo.blogspot.it/2016/12/se-pensavate-di-regalare-giocattoli.html

https://www.pentestpartners.com/blog/making-childrens-toys-swear/

Automobili



attivissimo.blogspot.it/2016/06/la-mitsubishi-outlander-si-ruba-via-wi.html

Anche:

- www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- www.welivesecurity.com/2015/11/13/7-things-need-know-car-hacking/
- 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/

Varie ed eventuali

- 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/`
- Sex toys (sì, davvero!):
  `https://boingboing.net/2017/04/03/gaping-holes.html` . . . IoT sex-toy with a wireless camera . . . once you login to it via the wifi network (default password "88888888"), you can root it and control it from anywhere in the world

Outline

Come trovare dei computer e prenderne il controllo?

Stra-semplificando:

1. Scoprire quali macchine/servizi ci sono "in giro"
   - Scansione attiva; per es., usando `http://nmap.org/`
   - Intercettazione del traffico; per es., usando `https://www.wireshark.org/`
   - Ingegneria sociale: ottenere informazioni sfruttando meccanismi sociali
   - ...
2. Trovare le vulnerabilità (già note); per es., usando `http://www.metasploit.com/` e `http://www.exploit-db.com/`
3. Sferrare l'attacco

Esistono distribuzioni di Linux già belle e pronte con tutti gli strumenti a portata di mano. La più famosa è Kali `https://www.kali.org/`

Ottenere informazioni tramite ingegneria sociale (1/2)

- Spesso basta chiedere: in un sondaggio il 70% delle persone ha rivelato la (propria?) password in cambio di una barretta di cioccolato! `http://news.bbc.co.uk/2/hi/technology/3639679.stm`
- Pennette USB "dimenticate" nel parcheggio

  `https://www.schneier.com/crypto-gram/archives/2006/0615.html#6`
- SPAM (posta indesiderata)/phishing con cose del tipo:
  - Attività sospetta sul suo account Pinco-Pallo, cambia subito la password cliccando QUI...
  - Il tuo computer ha un virus! Scarica il NOSTRO antivirus
  - È morto . . . , clicca QUI per vedere le foto/video/. . .
    - Per esempio, nel 2013 Totti `http://www.ilmessaggero.it/TECNOLOGIA/HITECH/totti_morto_malware_falso_annuncio/notizie/263541.shtml`

  collegamenti a siti che richiedono di installare software o "codec" per vedere un video, una cartolina, ricevere una suoneria, . . . nel 99.9% dei casi, si tratta di trojan

Ottenere informazioni tramite ingegneria sociale (2/2)

Quando siete in giro attenzione a:

- telefonate dalla "reception" che chiedono informazioni (per es.: carta di credito, di identità, informazioni personali)
- wifi (di "hotel", "aeroporti", ...) aperte
- ordinare una pizza (pagando con carta di credito), grazie al volantino che qualcuno vi ha fatto passare sotto la porta
- postazioni di ricarica (spesso la porta è una USB)

  `http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/`
- ...

`http://www.10news.com/money/consumer/thieves-develop-new-way-to-get-credit-card-numbers-at-hotels`

Come forzare l'esecuzione di comportamenti non voluti?

1. Cerchiamo dei bug
2. Fra questi, qualcuno potrebbe essere una vulnerabilità
3. Scriviamo un exploit che la sfrutti, per causare il comportamento voluto (dall'attaccante!)

Esempio: SQL injection (1/2)

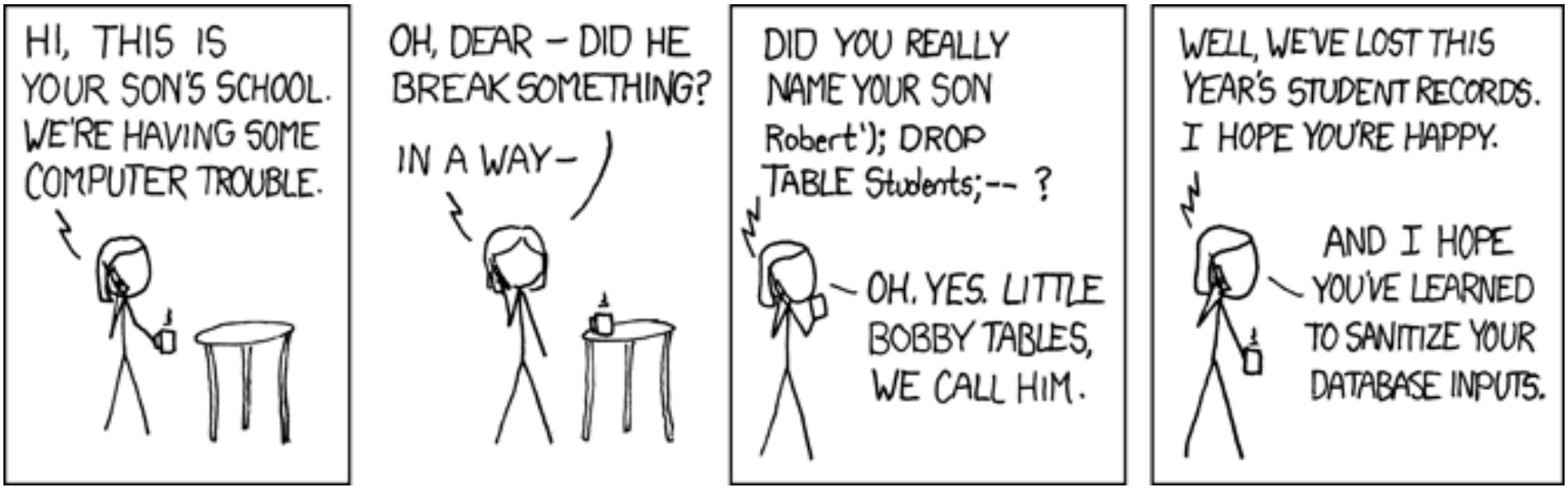
Consideriamo un programma che inserisce un nuovo studente nella tabella "Studenti" di un DB.
I dati da inserire arriveranno da qualche interfaccia utente (una pagina web, una finestra, ecc.) e verranno memorizzati nelle variabili `nomeDaInserire` e `cognomeDaInserire`

```
String comandoSQL="INSERT INTO Studenti(nome, cognome) VALUES('"+
                        nomeDaInserire+"', '"+cognomeDaInserire+"');";
// per es.: INSERT INTO Studenti(nome, cognome)
//                                      VALUES('mario', 'rossi');
executeSQL(comandoSQL); // esegue il comando sul DB server
```

Esempio: SQL injection (2/2)

Cosa succede se:

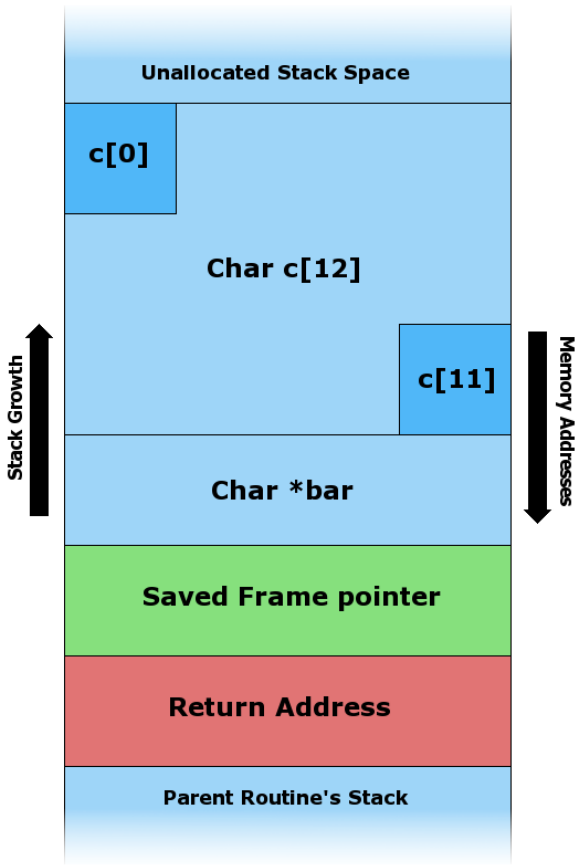
```
nomeDaInserire = "mario', 'rossi'); DROP Studenti; -- ";
cognomeDaInserire = "esempio di SQL Injection";

comandoSQL =
  "INSERT INTO Studenti(nome, cognome) VALUES('mario', 'rossi');
  DROP Studenti; -- ', 'esempio di SQL Injection');"
```



http://xkcd.com/327/

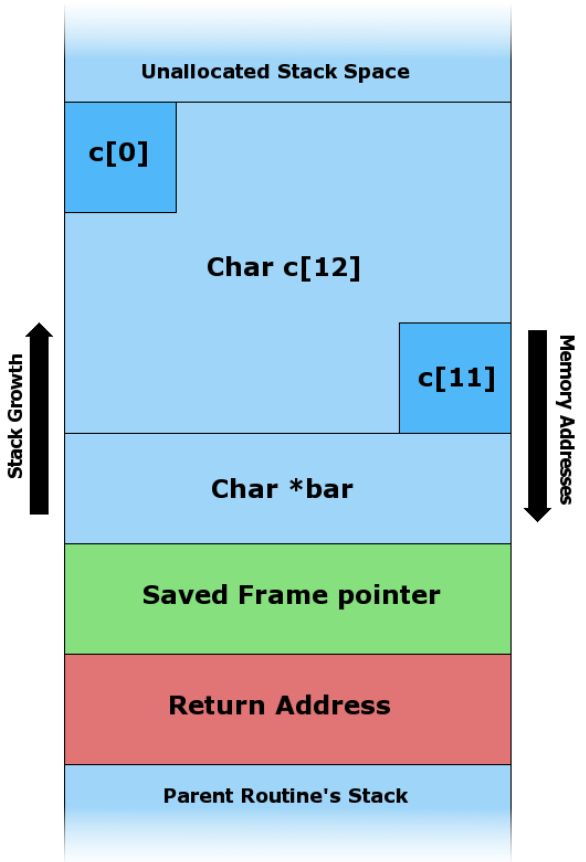
Esempio: Buffer overflow (1/3)

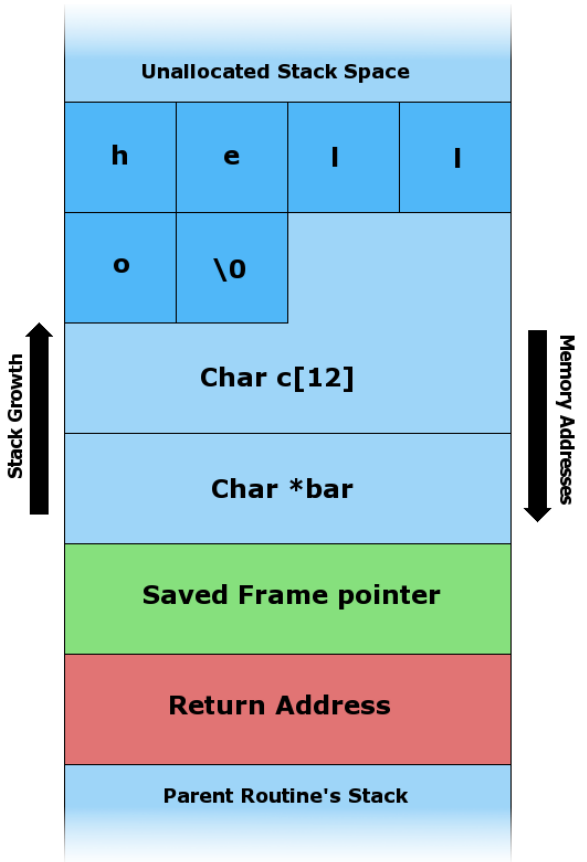
```
#include <string.h>

void foo(char *bar) {
   char  c[12];
   strcpy(c, bar);
}

int main(int argc, char **argv)
   foo(argv[1]);
}
```



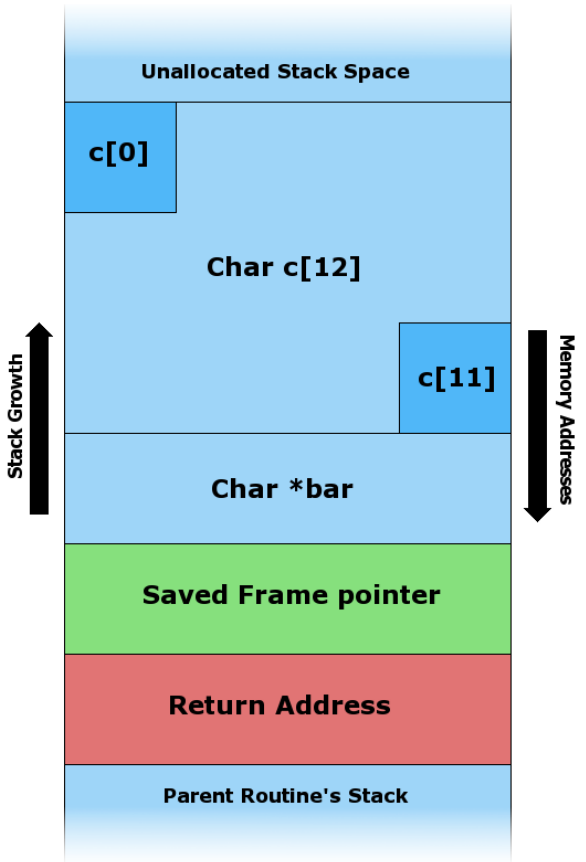
http://en.wikipedia.org/wiki/Stack_buffer_overflow

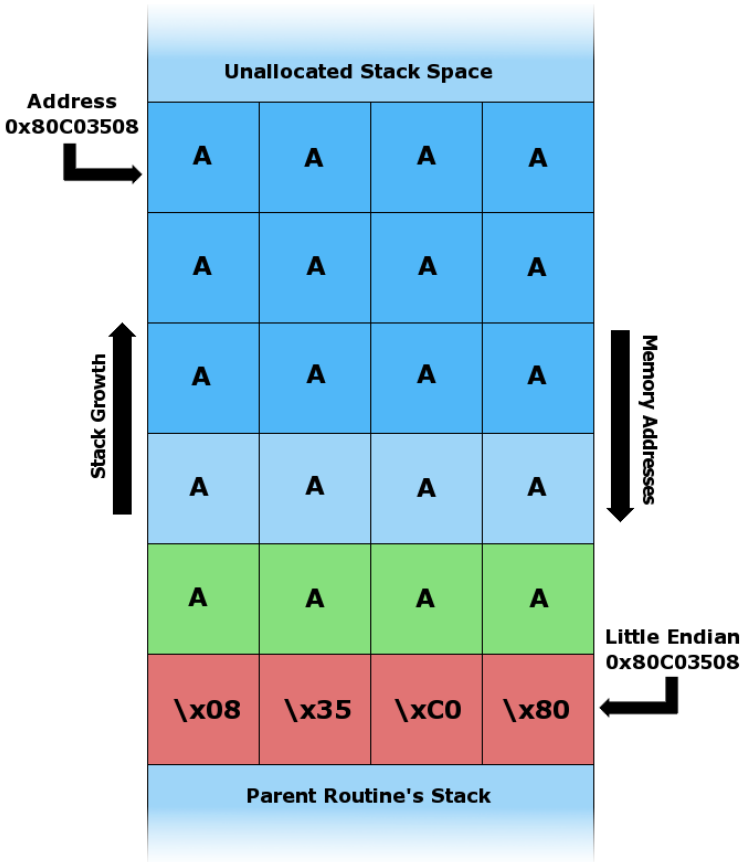
Esempio: Buffer overflow (2/3)





Esempio: Buffer overflow (3/3)





Quindi basta non lanciare “roba strana”?

Sì, ma alle volte è meno facile di quello che sembra...

- Cosa succede quando aprite, per esempio, un PDF? `nakedsecurity.sophos.com/2012/07/17/adobe-reader-vulnerability-pdf-malware-video`
- Didier Stevens spiega come sia possibile sfruttare una vulnerabilità di Adobe Reader senza neppure aprire un PDF!
  “The answer lies in Windows Explorer Shell Extensions. Have you noticed that when you install a program like WinZip, an entry is added to the right-click menu to help you compress and extract files? ...When you install Adobe Acrobat Reader, a Column Handler Shell Extension is installed. A column handler is a special program...”
  `blog.didierstevens.com/2009/03/04/quickpost-jbig2decode-trigger-trio`

Va beh, non siamo più nel 2009!

Vero. . . post del 17 Dicembre 2015: `http://arstechnica.com/security/2015/12/outlook-letterbomb-exploit-could-auto-open-attacks-in-e-mail/`

. . . The winmail.dat file includes instructions on how to handle attachments . . . "When the value . . . will be rendered as an OLE object. " . . . This sort of vulnerability makes for an extremely dangerous phishing attack — the victim doesn't even have to click on anything within the e-mail for it to execute, as it opens automatically when the e-mail is viewed. . . .

Malware nelle pubblicità

Il Javascript contenuto nel codice dell'inserzione era di per sé pulito, ma scaricava un'immagine-banner con variazioni invisibili dei pixel, da cui JS estraeva il codice ostile. Questo sistema ha permesso di eludere i filtri di sicurezza e infettare gli utenti che usavano versioni non aggiornate di Internet Explorer e di Adobe Flash.

- `https://attivissimo.blogspot.it/2016/12/malware-nelle-pubblicita-su-siti.html`
- `https://www.bleepingcomputer.com/news/security/new-stegano-exploit-kit-hides-malvertising-code-in-image-pixels/`
- `http://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-`

Outline

Dispositivi

- Non abbandonate mai un dispositivo accessibile senza *lock-screen*
  - Pericoli: attacchi fisici e locali
- Impostate delle password decenti
  - Sì, anche nei telefonini `http://en.wikipedia.org/wiki/Smudge_attack`
- Dove possibile, cifrate l'intero dispositivo (ne parliamo dopo)

Biometria (1/2)

- Hacking the Samsung Galaxy S8 Irisscanner
  `https://media.ccc.de/v/biometrie-s8-iris-en`
- "Just by casually making a peace sign in front of a camera, fingerprints can become widely available" said Isao Echizen, a researcher from NII
  `https://bgr.com/2017/01/11/is-touch-id-safe-fingerprint-camera/`
- Smartphone fingerprint reader could be hacked using paper and ink
  `https://nakedsecurity.sophos.com/2016/03/08/your-smartphone-fingerprint-reader-could-be-hacked-using-paper-and-in`

Inoltre...

Biometria (2/2)

Le nuove tecnologie promettono...

- Lyrebird: "Record *1 minute* from someone's voice and Lyrebird can compress her/his voice's DNA into a unique key. Use this key to *generate anything* with its corresponding voice."

  `https://lyrebird.ai/`
- Face2Face: "real-time facial reenactment of a monocular target video sequence (e.g., Youtube video)"

  `http://www.graphics.stanford.edu/~niessner/thies2016face.html`

Antivirus

(Installate e) tenete aggiornato un antivirus (per scegliere può essere utile: `https://www.av-test.org/en/antivirus/`)
In caso di file sospetti:

- Fatelo esaminare a `http://www.virustotal.com/`
- Esecuzione in ambienti virtualizzati (per esempio, usando Virtual Box `https://www.virtualbox.org/`)

Se il PC rischia di essere infetto:

- Kaspersky Rescue Disk `http://support.kaspersky.com/8093`
- Una distribuzione *live* di Linux e F-PROT `http://www.f-prot.com/products/home_use/linux/`
- . . . cose analoghe . . .
- tipicamente *inutile* usare qualcosa sul sistema operativo infettato

Software

Tenere aggiornato *tutto* il software

- sistema operativo
- antivirus
- tutte applicazioni
  - rimuovere quelle non usate
- firmware dei vari dispositivi (router, switch, TV, . . .)

Abilitate gli aggiornamenti automatici, dove possibile
Nel

- 2014: "44% of breaches . . . known vulnerabilities, 2–4 years old"
  `www.welivesecurity.com/2015/02/25/`
  `top-10-breaches-2014-attacked-old-vulnerabilities-says-hp/`
- 2017: WannaCry sfruttava vulnerabilità sistemata un paio di mesi prima
  - Presumibilmente trovata dall'NSA, ma saltata fuori ad Aprile per opera del gruppo *Shadow Brokers* `https://en.wikipedia.org/wiki/EternalBlue`

Evitate

Evitate

- programmi/app di dubbia provenienza (crack, keygen, etc)
- marketplace non ufficiali (Android/iOS)
- l'esecuzione automatica di programmi da DVD/USB/...

Fate attenzione

Fate attenzione alle app “del momento”:

- Yup, the Android app store is full of useless, unwanted anti-WannaCry apps

  `https://www.grahamcluley.com/android-wannacry-apps/`

- Pokémon Go: Fake versions of game hit tens of thousands of Android and iPhone users

  `http://www.telegraph.co.uk/technology/2016/07/18/`

  `pokemon-go-fake-versions-of-game-hit-tens-of-androi/`

- Up to two million Android devices may have been affected by a new strain of malware, which poses as fake guides to popular Play Store games

  `http://www.trustedreviews.com/news/`

  `new-android-malware-targets-pokemon-go-and-fifa-players-here-s-how-to-protect`

Password

- MAI usare le stesse credenziali per servizi diversi
  - Per ricordarsele: programmi password-safe; per esempio, KeePass `http://keepass.info/`
  - Ma, da soli, non bastano: `http://arstechnica.com/security/2015/11/hacking-tool-swipes-encrypted-credentials-from-password-manager/`
- Se usate Chrome o Firefox, impostate la *master password*
- Cambiate SEMPRE le password di default dei dispositivi/programmi

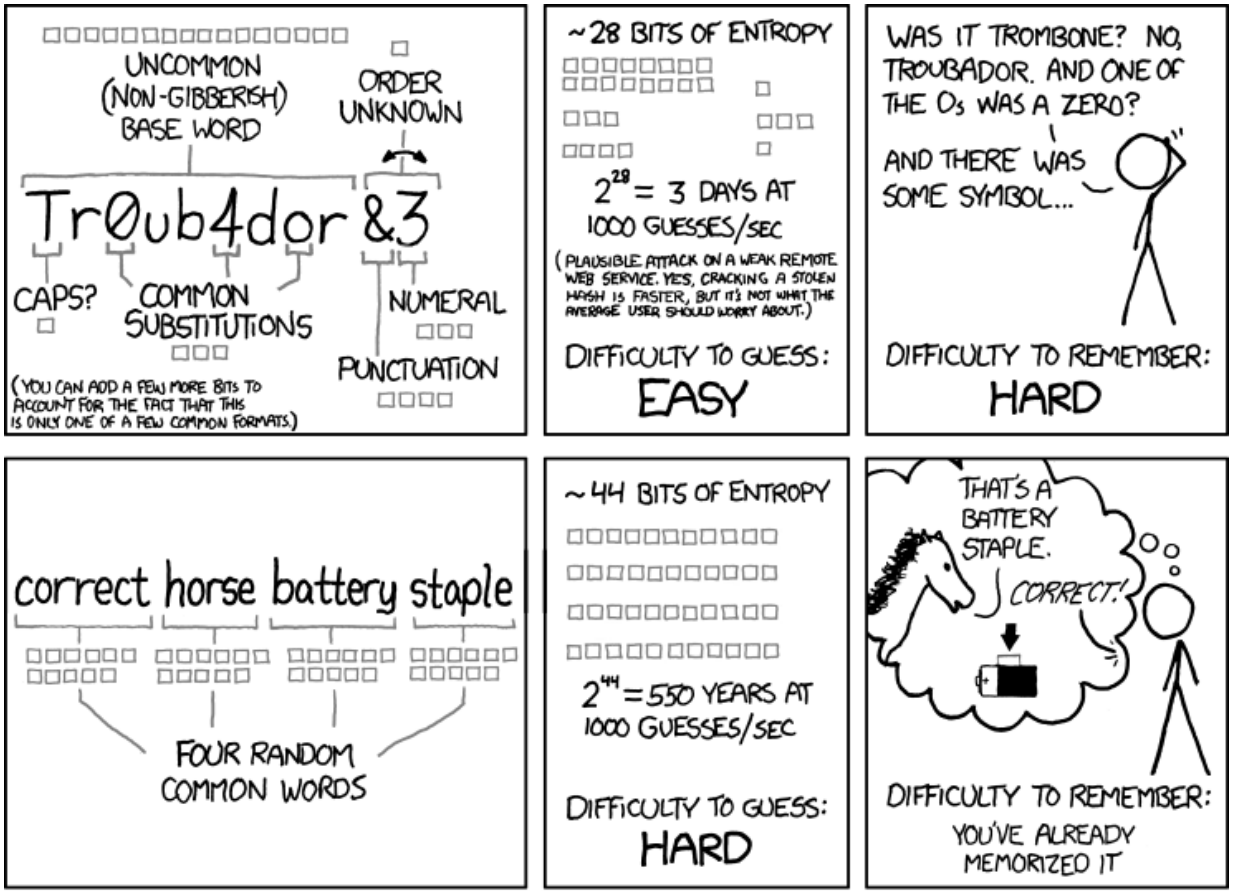
Ovunque possibile, abilitate l'autenticazione in due passi

`http://en.wikipedia.org/wiki/Two-step_verification`

Esempi:

- `https://www.google.com/landing/2step/`
- `https://www.dropbox.com/help/363`

Scelta delle password (1/3)



http://xkcd.com/936/

Scelta delle password (2/3)

Fra le password rubate ad Adobe nel 2013, le più usate sono (sigh!): 123456 (quasi 2 milioni di utenti, su circa 38 milioni), 123456789, password, adobe123, 12345678, qwerty, 1234567, 111111, photoshop e 123123

Nel 2015/16 la situazione non è stata tanto diversa, *anzi*:

- `https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/`
  - in oltre 10M password, 17% erano 123456
  - le 25 più comuni costituiscono oltre il 50%
- `http://arstechnica.com/security/2015/09/new-stats-show-ashley-madison-passwords-are-just-as-weak-as-all-the-rest/`
- `http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514`

Tristemente "Password patetiche nei siti di Polizia e Giustizia italiani":

`http://attivissimo.blogspot.it/2015/07/le-password-patetiche-dei-siti-di.html`

Scelta delle password (3/3)

`hackaday.com/2016/01/27/tp-links-wifi-defaults-to-worst-unique-passwords-ever/`

Vedere anche:

- `www.troyhunt.com/2013/11/adobe-credentials-and-serious.html`
- `www.wired.com/2015/04/snowden-sexy-margaret-thatcher-password-isnt-so-sexy/`

Wi-Fi

- (già detto) cambiate le eventuali password di default su access point
- usate WPA2 (al limite WPA, *mai* WEP)
- usate password lunghe e non comuni (per evitare attacchi a dizionario)
- disabilitate WPS `www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why-you-should-disable-it/`
- su Wi-Fi pubblici
  - cercate di usare solo siti su HTTPS (e controllate che lo siano davvero!)
  - considerate l'uso di una VPN
    - `lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-fo`

SPAM/Phishing

Spesso, basta un po' di buon senso ☺
Fate caso:

- alla grammatica e allo stile
- come si rivolgono a voi ("caro utente" vs il vostro nome e cognome reale, per esempio)

In caso di sospetti, NON:

- rispondere
- cliccare sui collegamenti
  - se siete in dubbio, andate sul sito ufficiale della banca/azienda/etc

Per il web

Cercare di usare sempre HTTPS (controllate la barra degli indirizzi, mettetelo di default ovunque possibile)
Flash è probabilmente la cosa peggiore, disabilitatelo di default:
`attivissimo.blogspot.ch/2015/02/ennesima-falla-in-flash-attacchi-in.html`
Alcuni add-on per i browser:

- per disabilitare selettivamente gli script:
  - uMatrix `https://github.com/gorhill/uMatrix`
  - NoScript `https://noscript.net/`
- HTTPS Everywhere `https://www.eff.org/https-everywhere`
- Privacy Badger, `https://www.eff.org/privacybadger` limita la possibilità di "spiare" la vostra navigazione web
- uBlock Origin, evita di scaricare pubblicità e contenuti potenzialmente dannosi `https://github.com/gorhill/uBlock`

Infine, non fidatevi ciecamente solo perché ci sono dei lucchetti nella pagina! `http://www.troyhunt.com/2011/07/padlock-icon-must-die.html`

Dati: Sicurezza e Privacy

Fate *regolarmente* delle copie di sicurezza

- in almeno due diversi dispositivi, usati a rotazione
- tenete i dispositivi offline (=spenti in un cassetto)
  - possibilmente, in luoghi fisici diversi

`http://www.hanselman.com/blog/TheComputerBackupRuleOfThree.aspx`

Dove possibile, cifrare il sistema, specialmente sui dispositivi mobili

- Opzione offerta dalle moderne distribuzioni Linux (per es. Ubuntu)
- Bitlocker per Windows
- Supportata da (molti dispositivi) Android, dovrebbe essere il default su quelli nuovi
- Default su iOS

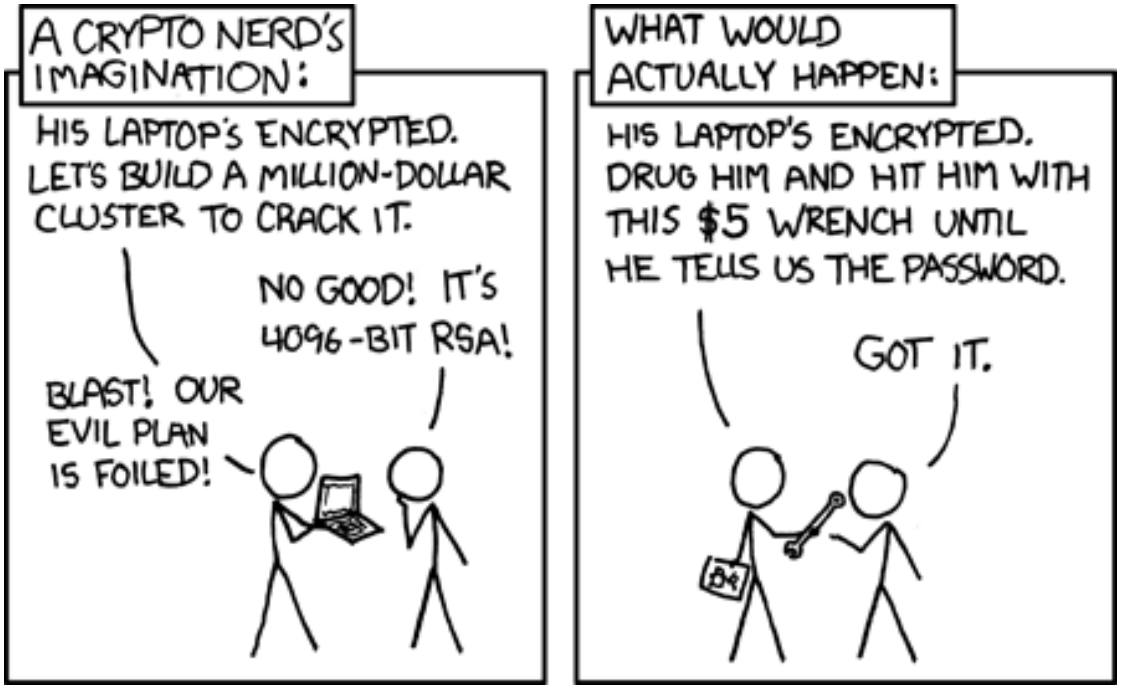
`http://www.pcworld.com/article/2304851/`

`so-long-truecrypt-5-encryption-alternatives-that-can-lock-down-your-data.html`

Outline

Conclusioni

- la sicurezza è un compromesso: sicuro spesso significa inusabile
- tenere i sistemi (e se stessi!) aggiornati è fondamentale
  - conoscere le tecniche di attacco aiuta a difendersi
- un pizzico di paranoia aiuta ☺



`http://xkcd.com/538/`

That's all folks!

Grazie per l'attenzione. Domande?

Il PDF di questi lucidi può essere scaricato da:

- `http://www.disi.unige.it/person/LagorioG/SicurezzaInformatica.pdf`
- `http://tinyurl.com/sic-info` (alias del precedente)

Su `http://informatica.dibris.unige.it/orientamento/eventi.html` troverete informazioni sulle attività offerte