Sicurezza dei sistemi e delle reti

INTRODUZIONE

Argomenti del corso

Sicurezza dei sistemi

- Concetti generali: Proprietà e Standard di sicurezza.
- Minacce, vulnerabilità e attacchi.
- Superficie e alberi di attacco.
- Classificazione del malware: Zero Day, polymorfismo e botnet
- Access control: Politiche di sicurezza (DAC e MAC) e gestione dell'identità (IAM). Politiche di accesso in WIndows e Linux. Studio e lab su setuid e attacco Shellshock
- Autenticazione: Principi di base e metodi di autenticazione. Protocolli challenge-response

Sicurezza delle reti

- Stack ISO/OSI e minacce comuni. Spoofing (lab) Attacchi a TCP/IP, ARP, UDP: Studio e lab su Synflood, TCP Hijacking
- Attività di ricognizione: Network e Port scanning. Metodi e tecniche di scansione.
- Analisi del traffico: Wireshark
- Sicurezza dell'insfrastruttura di rete e del livello trasporto: SSL/TLS
- Sicurezza perimetrale: Firewall, Stateless filtering e Stateful filtering
- Rilevamento delle intrusioni: IDS
- Software security: Cenni su Buffer overflow

Laboratori:

- Wireshark, Iptables
- VM in virtualbox + docker

Materiali e testi

Il sito del corso: su ariel

Testi di riferimento

- Testi di Computer and Network Security:
- Sicurezza dei computer e delle reti, William Stallings, Pearson 2022
- "Security Engineering" R. Anderson, Wiley 2008
  - (Disponibile anche gratuitamente: http://www.cl.cam.ac.uk/~rja14/book.html)
- Computer Security (3rd ed.), Dieter Gollmann. Wiley, 2010
- Computer Networking», Kurose, Ross, Pearson 2005
- «Security in Computing», Pfleeger, Prentice Hall
- Testi Network Security :
- «Network Security Bible» E. Cole – Wiley 2009
- «The practice of network security» R. Bejtlich Pearson
- «Inside Network Perimeter Security» Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey, SAMS 2004
- Articoli scientifici indicati a lezione (e sul sito)

Esame

Esame da 6CFU

- Altri contenuti in Sicurezza II da 6cfu

-Esame scritto

- Domande ed esercizi a risposta aperta
- prova di laboratorio open book

Progettino Facoltativo

Scritto: domande ed esercizi sul programma trattato a lezione e gli approfondimenti indicati.

Laboratorio: esercizi da risolvere con i tool trattati a lezione

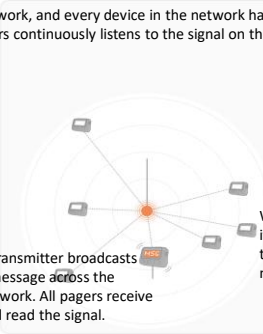
- Wireshark Tabelle di filtraggio traffico

Introduzione

Pagers

How do pagers work?
Pagers operate on a radio frequency network, and every device in the network has a unique code. Each pager within range of the network's transmitters continuously listens to the signal on the network, waiting to read their code.

A transmitter broadcasts a message across the network. All pagers receive and read the signal.



When a pager reads its own code in the transmission, it receives the message.

Hacker russi dietro l'attacco al Gse, indaga

Da Pegasus a Predator, i software hanno spiato

Cybersicurezza, il buco all'Agenzia delle entrate, Lockbit rivendica l'attacco. "Ma l'hacker ha agito da solo"

I criminali informatici sostengono di aver sottratto milioni di dati. Ma si sospetta che chi ha materialmente 'bucato' l'ente pubblico sia un affiliato, non un interno al collettivo dedito alla pirateria online

di Andrea Ossino

stato un

ulakis. L'allarme

Attacchi informatici

"L'attacco hacker alla Regione Lazio legato a quello di Engineering". Ma l'azienda smentisce: "Nessun collegamento"

di Arianna Di Cori

A un mese **dall'attacco hacker** che ha colpito i sistemi informatici della **Regione Lazio** è tempo di un primo bilancio. Sono ancora fermi **13 su 36 servizi** collegati al portale web principale e per cui è prevista la **riattivazione** tra il 3 e il 10 settembre. I problemi, intanto, si stanno facendo sentire in diversi settori collegati al servizio sanitario regionale, dalle farmacie alle forniture ospedaliere, ma anche nel mondo delle professioni e del lavoro.

Utenti iOS e Mac a rischio: attenti a Safari!

26 Agosto 2020

Pawel Wylecial prova ad avvisare **Apple** il 17 aprile.

Quattro giorni dopo ha la soddisfazione di sentirsi dire che ha ragione, ma la grande azienda non fa nulla per porre rimedio al **"bug"**.
In pratica **un difetto nella programmazione del browser Safari** potrebbe consentire ai **pirati informatici** di rubare i **file degli utenti Apple** che adoperano il celeberrimo software di navigazione online.
Apple non avrebbe adottato alcuna iniziativa volta ad eliminare la segnalata **vulnerabilità**.
Le reiterate sollecitazioni sortiscono il solo effetto di chiedere al fastidioso informatico di farla finita e di tenere nascosti i dettagli della propria scoperta fino **"a primavera del 2021"**

Pawel Wylecial che non crede ai suoi occhi. Ci pensa qualche giorno e poi, il 24, decide di "sputare" sul web tutte le informazioni

Il tallone d'Achille risiederebbe nella **API Web Share di Apple**, un nuovo standard per la condivisione di file e altri contenuti, e la dinamica di sottrazione dei file personali descritta da Wylecial nel suo post prevede che la vittima **"collabori"** con i malintenzionati. Allora non c'è da avere paura?

https://blog.redteam.pl/2020/08/stealing-local-files-using-safari-web.html

5G Devices

Opinion

Every Part of the Supply Chain Can Be Attacked

When it comes to 5G technology, we have to build a trustworthy system out of untrustworthy parts.

«Il continuo disaccordo del governo degli Stati Uniti con la società cinese Huawei sottolinea un problema molto più grande con le tecnologie informatiche in generale:

Non abbiamo altra scelta che fidarci completamente di loro ed è impossibile verificare che siano affidabili.

Risolvere questo problema, che è sempre più un problema di sicurezza nazionale, richiederà sia di apportare importanti cambiamenti politici sia di inventare nuove tecnologie…"

Security issues in 5G

Migliaia di persone hanno l'opportunità di infilare una backdoor nel prodotto finale:

- I pacchetti software open source sono sempre più presi di mira dai gruppi che installano backdoor.
- Le app false nel Google Play Store illustrano le vulnerabilità nei nostri sistemi di distribuzione del software.
- Il worm NotPetya è stato distribuito da un aggiornamento fraudolento di un popolare pacchetto di contabilità ucraino, che illustra le vulnerabilità nei nostri sistemi di aggiornamento.
- I chip hardware possono essere sottoposti a backdoor nel punto di fabbricazione, anche se il design è sicuro.
- La National Security Agency ha sfruttato il processo di spedizione per sovvertire i router Cisco destinati alla compagnia telefonica siriana.

Security issues in 5G

Le soluzioni tecniche si dividono in due categorie fondamentali:

- migliorare i processi di ispezione tecnica per i prodotti i cui progettisti forniscono il codice sorgente
- costruire un sistema sicuro, anche se una qualsiasi delle sue parti può essere sovvertita.
- ex vicedirettore della National Intelligence Sue Gordon ha detto del 5G: "Devi presumere una rete sporca".

- Problema
- possiamo risolverlo costruendo sistemi affidabili con parti non affidabili?
- Sembra ridicolo a prima vista, ma Internet stesso era una soluzione a un problema simile: una rete affidabile costruita con parti inaffidabili.

Security

La sicurezza è molto più difficile dell'affidabilità.

- Difficile costruire sistemi sicuri con parti sicure, figuriamoci con parti e processi di cui non possiamo fidarci e che quasi sicuramente vengono sovvertiti dai governi e dai criminali di tutto il mondo.
- Le attuali tecnologie di sicurezza, tuttavia, non sono nemmeno lontanamente sufficienti per difendersi da questi attacchi sempre più sofisticati.
- Allo stesso tempo, tutti questi problemi stanno peggiorando poiché i computer e le reti diventano più critici per la sicurezza personale e nazionale.

Sicurezza e 5G

Il valore del 5G non è per guardare i video più velocemente;

- è per le cose che parlano alle cose senza disturbarti.
- Queste cose – automobili, elettrodomestici, centrali elettriche, città intelligenti – influenzano sempre più il mondo in modo fisico diretto.
- Sono sempre più autonomi, utilizzando l'A.I. e altre tecnologie per prendere decisioni senza intervento umano.

Il rischio delle backdoor cinesi nelle nostre reti e computer non è che il loro governo ascolti le nostre conversazioni; è che spegneranno la corrente o faranno schiantare tutte le auto l'una contro l'altra

Att

Facebook sotto attacco hacker, problemi per quasi 90 milioni di account

29 Settembre 2018 101

Facebook è stato colpito duramente **da un attacco hacker** lo scorso martedì 25 settembre, mettendo **a rischio quasi 50 milioni di account**. Il colosso dei social network ha spiegato in un **comunicato ufficiale**, che le indagini sono ancora nelle fasi iniziali, ma quello che appare molto chiaro è che gli aggressori hanno sfruttato una **vulnerabilità nel codice di Facebook**, attraverso la funzione "Visualizza come", una sorta di anteprima del proprio profilo, visto da una persona con la quale non abbiamo ancora stretto amicizia.

La falla di sicurezza ha permesso ai malintenzionati di rubare diversi token di accesso, in modo da essere utilizzati per prendere possesso degli account. I token di accesso sono l'equivalente di chiavi digitali, che permettono di eseguire il log-in di Facebook senza dover reinserire la propria password ogni volta.

Huawei Mate 20 Pro e Kirin 980 passano su Geekbench: ottimi punteggi, ma non il top

TIM regala 30 Giga al mese ad alcuni clienti via SMS o app MyTIM 49
19 min fa A quanto pare, la

Amazon: Xiaomi Mi A2 Lite, prese smart

Mark Zuckerberg
Homerid

I want to update you on an important security issue we've identified. We patched the issue last night and are taking precautionary measures for those who might have been affected. We're still investigating, but I want to share what we've already found:

On Tuesday, we discovered that an attacker exploited a technical vulnerability to steal access tokens that would allow them to log into about 50 million people's accounts on Facebook.

We do not yet know whether these accounts ... Altro...

Attualità

HACKER IN AZIONE

Rubati e venduti i dati di 500 milioni di utenti Yahoo!

YAHOO! questa volta ha ben poco per cui esultare. Indirizzi email, nomi e date di nascita di 500 milioni di utenti sarebbero stati sottratti all'azienda informatica e messi in vendita nel deep web. Ad agosto era stato il presunto autore del colpo, l'hacker *Peace*, ad annunciare l'impresa. Adesso *Yahoo!*, dopo aver condotto un'indagine interna, sarebbe vicina a svelare i dettagli del maxi-furto. La notizia arriva nel periodo peggiore: il colosso delle telecomunicazioni *Verizon* sta per acquisire *Yahoo!*, ma l'hackeraggio potrebbe mettere a rischio l'operazione. Fra i dati rubati non ci sarebbero informazioni finanziarie, ma il danno d'immagine subito dal gruppo è comunque importante. *Yahoo!*, consapevole dell'attacco, non ha invitato gli utenti a cambiare la password per precauzione, mostrandosi non reattivo. L'attacco è l'ennesimo colpo per Marissa Mayer, l'amministratore delegato di *Yahoo!*, sulla quale erano state riposte le speranze del rilancio. Smentite da anni di tagli ai costi e dall'ultimo capitolo di una pioniera della Silicon Valley: dopo la vendita anche il famoso motore di ricerca cambierà nome.

Attualità

lunedì 19 settembre 2016

di *Alfonso Maruccia*

A A

Commenti (7)

Tor e Firefox, una falla in comune

Gli sviluppatori di Tor aggiornano il browser ufficiale avvertendo dell'esistenza di una falla potenzialmente molto pericolosa. Interviene anche Mozilla, che a sua volta rilancia programmando un update

Roma – Il browser ufficiale di Tor è affetto da una grave vulnerabilità di sicurezza, potenzialmente utilizzabile da "avversari" ben equipaggiati per compromettere le difese a protezione dell'anonimato degli utenti della darknet: l'avvertimento arriva direttamente dagli sviluppatori, che si premurano di chiudere la falla con un nuovo aggiornamento per il software. Firefox, che di Tor costituisce la base, sarà invece ancora vulnerabile per poco.

Il browser di Tor è stato dunque aggiornato alla release 6.0.5, e agli utenti viene caldamente consigliata l'installazione dell'update visto che la vulnerabilità in oggetto permette di "impersonare" un sito web legittimo (es. *addons.mozilla.org*) tramite un certificato crittografico fasullo, installare un aggiornamento potenzialmente malevolo per un componente aggiuntivo del browser e da lì "bucare" il sistema dell'utente – magari tramite l'esecuzione di codice malevolo da remoto.

Un **attacco di tipo man-in-the-middle** (MITM) come quello descritto dai ricercatori è problematico ma non impossibile, ed è già ampiamente documentato nelle cronache di questi anni che ad esempio riguardano la famigerata certificate authority (CA) olandese DigiNotar.

Attualità

martedì 20 settembre 2016

di *Stefano De Carlo*

A A

Commenti (9)

Windows, all'assalto della modalità provvisoria

I laboratori CyberArk espongono alcune debolezze del "Safe Mode" che possono portare al furto di credenziali e all'infezione di altri PC nella rete della vittima. Microsoft non considera valida la vulnerabilità

Roma – La *modalità provvisoria* (**Safe Mode**) è una particolare tipologia di boot disponibile fin dalle prime versioni di Windows che procedere a caricare solo lo stretto indispensabile (driver e sottosistemi critici) alle funzioni del sistema operativo, in modo da ovviare ad eventuali problemi che sorgono durante le normali operazioni. In questi elementi base **non rientrano molti dei controlli di sicurezza** e da qui Doron Naim dei laboratori CyberArk ha tratto spunto, studiando come questo ambiente ridotto può essere sfruttato dai malintenzionati.

L'attacco può essere eseguito se l'attaccante ha accesso fisico o logico alla macchina, e può abilitare al **furto delle credenziali**. Una volta compromessa la prima macchina, l'attaccante imposta l'accesso alla modalità provvisoria al **prossimo riavvio**. A quel punto ha due opzioni. Nel primo caso inietta una **finta schermata di login**, potenzialmente del tutto indistinguibile da quella reale, per sottrarre nome utente e password in chiaro. In alternativa può sfruttare il suo iniziale accesso alla macchina per caricare un **servizio compatibile con il Safe Mode** e pertanto eseguito quando l'utente riavvierà per la prima volta il PC: il servizio può accedere agli hash delle password salvate e sfruttare note debolezze per eseguire attacchi *pass the hash* a sottosistemi di Windows che consentono l'autenticazione conoscendo anche solo

Attualità

"Sicurezza"

Sicurezza in relazioni a guasti provocati.

- Qui non parliamo di incidenti o malfunzionamenti software

In genere in informatica ci si preoccupa di come raggiungere uno scopo

La sicurezza si preoccupa di come prevenire un comportamento non desiderato

- Modo diverso di pensare!
- Un avversario/hacker/nemico cerca attivamente e maliziosamente di superare le misure preventive studiate

Esempio.

Testing Software

Sicurezza è interdisciplinare

Comprende diverse aree della CS

- Crittografia
- Networking
- Operating systems
- Databases
- AI/learning theory
- Computer architecture/hardware
- Programming languages/compilers
- HCI, psychology
- ..e molte altre

Proteggere denaro vs informazioni [Pfl]

Caratteristiche	Denaro in banca	Informazioni da proteggere
Dimensione e portabilità	I siti per depositare denaro sono grandi, non protabili. Edifici richiedono guardie armate, cassaforti, molti livelli di sicurezza	Le informazioni di valore sono piccolo e portabili. I dispositivi fisici sono piccoli
Abilità nell'evitare il contatto fisico	Difficile. Le bache hanno bisogno di presenza fisica e denaro contante.	Semplice. Per le informazioni on è necessario il conttao fisico. Anche moneta elettrobica può essere trasferita via computer, mail, etc.
Valore del bene	Molto alto	Variabile, da molto alto a molto basso

Esempi

- Automotive industry
- Wilshire Associates mail system, gestiva $10 miliardi di investimenti

Terminologia

Un sistema può essere:

- Un singolo prodotto (PC, device, smartcard,…)
- Alcuni prodotti incluso il sistema operativo, di comunicazione, etc.
- Come sopra più le applicazioni
- Come sopra più il personale
- Come sopra più I clienti o utenti esterni

Terminologia

Un soggetto può essere una persona fisica

o una persona legale (una compagnia)

Un “attore” può essere

- Una persona
- Un dispositivo (PC, smartcard)
- Un ruolo (un cliente)
- Un ruolo complesso (Alice or Bob, Bob che finge di essere Alice)

Anche il livello di precisione cambia

- "La smart card di Bob che rappresenta Bob che sostituisce Alice"
- "Bob usa la carta di Alice in sua assenza".

Rete

Una rete è una configurazione di individui interconnessi.

Il termine networking si riferisce alla possibilità di comunicare con o all'interno di un gruppo

Esempi.

- Una rete di vicini (neighborhood watch),
- Una rete di intelligenza (spy networks),
- Una rete di notizie o televisiva
- Un social media come Facebook, Twitter and Instagram.

Rete di computer

Le reti di computer giocano un ruolo chiave nella società moderna

Due prospettive

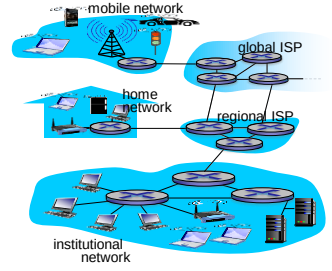
- Fisica

Una rete è una infrastruttura hardware che connette diversi terminali

  - personal computers, personal digital assistants, smart phones, wireless sensors, wireless actuators (e.g. a Philips Hue lamp) and smart televisions.

- Logica

Da un punto di vista software una rete è un sistema che facilita lo scambio di informazioni tra applicazioni che non condividono fisicamente una spazio di memoria



Internet: numeri

Internet è partita con 4 hosts in 1969, nel 1983 gli Internet hosts erano già 500.

Oggi ci sono più macchine connesse a Internet che umani sul pianeta

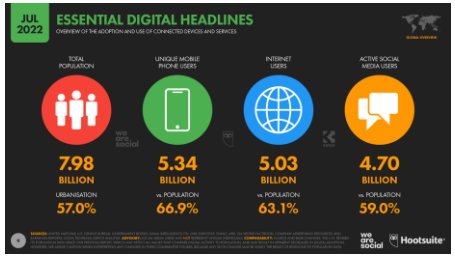
5.03 miliardi di persone usano internet– equivalent al **63.1 %** della popolazione mondiale

Ecommerce: 8,1 trillion USD

Proiezione economica su ecommerce: 24% del commercio mondiale mel 2026

- $14 billion online during 2020's black Friday

Servizi come e-learning: Coursera ha raggiunto 15 milioni di studenti



Internet: numeri

Internet: "network of networks"

- Molteplici Internet Service Provider interconnessi

Protocolli controllano la spedizione ela ricezione dei messaggi

- e.g., TCP, IP, HTTP, Skype, 802.11

Internet standard:

- RFC: Request for comments
- IETF: Internet Engineering Task Force

Internet: una rete di servizi

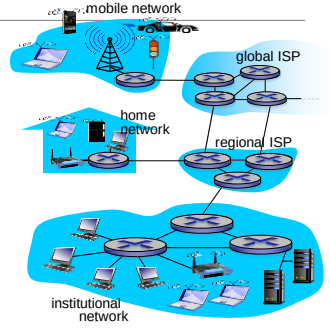
infrastruttura che fornisce servizi alle applicazioni:

- Web, VoIP, email, games, e-commerce, social nets, …

fornisce l'interfaccia di programmazione alle app

- hook che consentono all'invio e alla ricezione di programmi di app di "connettersi" a Internet

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on line
P2P	Peer-to-peer	File sharing



Internet oggi

Fisicamente la più grande rete di computer del nostro tempo

- Utilizza protocolli di comunicazione accettati a livello globale (alcuni anche standardizzati)
  - perinviare e ricevere messaggi tra miliardi di dispositivi finali e milioni di (sotto)reti.

Logicamente

- Internet è una struttura globale
- fornisce servizi di comunicazione ad applicazioni di rete, e-mail, world wide web (www), giochi online, voice over IP (VoIP), Skype, Netflix e molti altri.
- È un mezzo per la consegna dei dati da una sorgente a una destinazione a diversi livelli di astrazione

Internet-connected devices

IP picture frame
http://www.ceiva.com/

Slingbox: watch, control cable TV remotely

Internet refrigerator

sensorized, bed mattress

Web-enabled toaster + weather forecaster

Tweet-a-watt: monitor energy use

Internet phones

Embedded systems

- Standalone embedded systems
- Network-aware embedded systems
  - Permettono l'accesso ad alcune (limitate)funzionalità interne dall'esterno
- Network-connected embedded systems
  - Sono 'on-line' usando protocolli standard aperti al pubblico
- Network-central embedded systems
  - Hanno alcune funzionalità standalone function ma il design di hardware e software è stato fatto per operare in un contesto di rete. Es. smart phone apps, television sets e intelligent lighting
- Fully networked embedded systems

Oggi/Domani: IoT

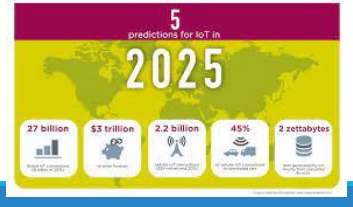
L'IoT è Internet più un'estensione di Internet nel mondo fisico che ci circonda, che è monitorato e influenzato dalle cose Logicamente

È una struttura globale che estende la portata delle applicazioni distribuite a miliardi di dispositivi con scarse risorse. L'IoT offre infinite possibilità per scenari innovativi (ad esempio case intelligenti, assistenza sanitaria intelligente, edifici intelligenti, città intelligenti),

Nel 2021 c'erano più di 10 miliardi di dispositivi IoT attivi.

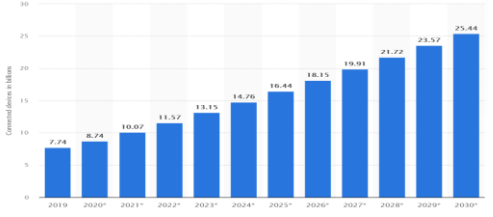
Si stima che il numero di dispositivi IoT attivi supererà i 25,4 miliardi nel 2030.

Entro il 2025, ci saranno 152.200 dispositivi IoT che si connetteranno a Internet al minuto



Numero di IoT devices dal 2019 al 2030

Si prevede che il numero di dispositivi Internet of Things (IoT) in tutto il mondo triplicherà da 8,74 miliardi nel 2020 a oltre 25,4 miliardi di dispositivi IoT nel 2030. Nel 2020, il numero più alto di dispositivi IoT si trova in Cina con 3,17 miliardi di dispositivi.



Il futuro: AI

- **Trasporti**: auto a guida autonoma
- **Manufacturing:** AI powered robot
- **Healthcare:** diagnosi più veloci delle malattie, scoperta di nuovi farmaci, assistenti infermieristici virtuali
- **Education**: tutor virtuali assistono gli istruttori umani e l'analisi facciale misura le emozioni
- **Media:** giornalismo sfrutta l'intelligenza artificiale (Bloomberg genera report per dati finanziari complessi)
- **Customer Service:** assistente AI in grado di effettuare chiamate simili a quelle umane

https://builtin.com/artificial-intelligence/artificial-intelligence-future

Cos'è la sicurezza?

Raggiungere un obiettivo in presenza di un avversario

Un sistema sicuro è un sistema che assolve uno specifico compito, nonostante l'avversario voglia impedirlo o stia operando in qualsiasi modo.

Per discutere di sicurezza consideriamo:

1. Politica
   - Le regole che vuoi che il tuo sistema faccia rispettare
   - L'obiettivo che vuoi raggiungere
     ES. Solo Bob può leggere il file F,
2. Modello di minaccia (threat model)
   - Assunzioni su cosa può fare un attaccante
     Una serie di ipotesi sull'avversario.
   - Alice non conosce la tua password, non può accedere fisicamente al laptop, può indovinare la password
3. Meccanismo.
   - software o hardware o qualsiasi parte della progettazione, implementazione,
   - cerca di assicurare che la politica sia seguita fintanto che il cattivo segue il modello di minaccia.

Perché la sicurezza è difficile da assicurare

Un obiettivo negativo
- assicurare che la politica di sicurezza sia seguita indipendentemente da ciò che l'attaccante può fare
- Al contrario per creare un file system ed essere sicuri che Alice possa accedere al file, basta provare:
  Se Alice può accedere al sistema funziona
- Ma dimostrare che nessun altro oltre ad Alice può accedere al file è un problema molto più difficile da risolvere,
  - scopri cosa potrebbero fare tutte le persone nel mondo per cercare di ottenere il file il file system lo disattiverà, ma l'avversario proverà tutti i tipi di altri attacchi, come indovinare la password, ecc

Un processo iterativo.
- ad ogni iterazione trova l'anello più debole nel sistema.
- modello di minaccia sbagliato.
- Il meccanismo aveva alcuni bug perché è un software
- Difficile per sistemi di grandi dimensioni. aggiustarli.
- cambiare il modello di minaccia iterare e provare a progettare un nuovo sistema, migliorare le cose

Non riesci a raggiungere la sicurezza perfetta? tutto è semplicemente rotto.
- Rinunciare e smettere di usare i computer. Ogni sistema avrà probabilmente un punto di rottura che porterà al compromesso.
- Non significa necessariamente che il sistema non sia utile: dipende dal contesto.
  - Gestire la sicurezza come rischio vs beneficio.

Perchè i sistemi di computer sono poco sicuri?

Le reti di computer sono “sistemi di sistemi”
- Se un sistema è sicuro l’ambiente intorno cambia
- C’è una crescente complessità dovuta al numero di componenti, interazioni complesse

- Alta competitività short “time-to-market”, high ROI
- Si sfruttano le vulnerabilità attraverso il grande numero di connessioni
  - worm outbreaks, botnets
- Lento incident response
  - “incident hiding”, manual handling
- Errori umani

Motivazioni

- Intelligence and military use (5th century BC – 1980's)
  - "security by obscurity", crypto-wars
- Hacker spirit, fun and fame (1980's – 2000's)
  - Pwnie, CCC, CTF
- Cybercrime, monetary gain (2000's – currently)
  - Phishing, botnets, spam
- Political goals, cyberconflict (2007 – currently)
  - Attack on Estonia, Russian-Georgian conflict, Stuxnet
- "Hacktivism" (2011 – currently)

Esempi: Problemi con la policy

Sarah Palin email hack during the 2008 United States presidential election campaign

the Yahoo! personal email account of vice presidential candidate Sarah Palin was hacked

The hacker, David Kernell, had obtained access to Palin's account by looking up biographical details such as her high school and birthdate and using Yahoo!'s account recovery for forgotten passwords.

Policy: login with password or answering QS

Mat Honan.

"In the space of one hour, my entire digital life was destroyed". First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook".

Apple tech support gave the hackers access to my iCloud account. Amazon tech support gave them the ability to see a piece of information – a partial credit card number – that Apple used to release information.

Policy: the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification

https://en.wikipedia.org/wiki/Sarah_Palin_email_hack

Esempi : problemi con threat model

- Fattore umano poco considerato:
  - Phishing
  - Interazione col supporto tecnico (finto) per resettare la password
- Assunzioni computazionali variano col tempo
  - Ex: DES keys, ora bastano 100 dollari per brute force
- CA non affidabili
  - Nel 2011 2 CA (in Iran) sono state compromesse
- Randomness in PRNG
- Hardware poco affidabile

Esempi: problemi con i meccanismi/bugs

Apple iCloud password-guessing limit

La API Find my Phone non aveva il limite

https://bitcoin.org/en/alert/2013-08-11-android

Android Security Vulnerability

11 August 2013

We recently learned that a component of Android responsible for generating secure random numbers contains critical weaknesses, that render all Android wallets generated to date vulnerable to theft. Because the problem lies with Android itself, this problem will affect you if you have a wallet generated by any Android app. An incomplete list would be Bitcoin Wallet, blockchain.info wallet, BitcoinSpinner and Mycelium Wallet.

Esempio: The Linux Backdoor Attempt of 2003

Nel 2003 Linux utilizzava un sistema chiamato BitKeeper per archiviare la copia principale del codice sorgente Linux.

Una seconda copia del codice sorgente è stata conservata in modo che gli sviluppatori potessero ottenere il codice tramite un altro sistema di codifica chiamato CVS.

La copia CVS del codice era una copia della copia BitKeeper primaria.

- Se uno sviluppatore avesse voluto proporre una modifica al codice Linux, avrebbe dovuto presentare la modifica proposta e passare attraverso un processo di approvazione per decidere se la modifica sarebbe stata accettata nel codice principale.
- Ma il 5 novembre 2003, Larry McVoy notò che c'era una modifica al codice nella copia CVS che non conteneva un puntatore a un record di approvazione.
- L'indagine ha dimostrato che la modifica non era mai stata approvata e, cosa ancora più strana, che questa modifica non appariva affatto nel repository primario di BitKeeper.

Esempio: The Linux Backdoor Attempt of 2003

La modifica ha cambiato il codice di una funzione Linux chiamata wait4, che un programma dovrebbe utilizzare per attendere che accada qualcosa.

Nello specifico, ha aggiunto queste due righe di codice:

```
if ((opzioni == (__WCLONE|__WALL)) && (current->uid = 0))

retval = -EINVAL;
```

Impostare l'ID utente su zero è un problema perché l'ID utente numero zero è l'utente "root", a cui è consentito fare assolutamente tutto ciò che vuole:

Mercato delle Vulnerabilità

Opzione 1: bug bounty programs (Programma di Ricompense per la Segnalazione di Vulnerabilità)
- Google: fino a $3133.7 in 2010, adesso fino a $20K per bug
- Facebook: fino a $20K per bug
- Microsoft: fino a $150K per bug
- Pwn2Own competition: $10-15K
- United Airlines

Opzione 2: vulnerability brokers
- ZDI, iDefense: $2-25K

Opzione 3: gray and black markets
- fino a $100-250K
- Uno zero-day per iOS venduto a $500K

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
iOS	$100,000-$250,000

Source: Andy Greenberg (Forbes, 3/23/2012)

It's a Business

Diverse compagnie si sono specializzate nel trovare e rivendere exploit
- ReVuln, Vupen, Netragard, Exodus Intelligence
- Prezzo medio per exploit $35-160K
- Abbonamento annuale $100K

Alcune nazioni sono compratori
- "Israel, Britain, Russia, India and Brazil are some of the biggest spenders. North Korea is in the market, as are some Middle Eastern intelligence services. Countries in the Asian Pacific, including Malaysia and Singapore, are buying, too" -- NY Times (Jul 2013)
- Il caso Hacking-Team

Mercato dei dati rubati

Numero di una singola carta di credito: $4-15 [Dell SecureWorks, 2013]

Numero di una singola carta con dati su nastro manetico: $12-30

"Fullz": $25-40
- Nome, indirizzo, telefono, email con password, data di nascita, SSN, IBAN, credenziali per online banking

Credenziali per un conto bancario online con $70-150K: sotto $300

Mercato per le vittime

Pay-per-install su machine compromesse [Trend Micro, "Russian Underground 101", 2012]
- US: $100-150 / 1000 downloads, "global mix": $12-15
- Usato per spedire spam, portare DOS, click fraud, ospitare scam websites

Botnets in affitto
- DDoS: $10/hour or $150/week
- Spam: da $10/1,000,000 emails

Tools and services
- Basic Trojans ($3-10), Windows rootkits ($300), email, SMS, ICQ spamming tools ($30-50), botnet setup and support ($200/month, etc.)

Sicurezza delle reti

Campi di interessi:
- Attacchl:
  - how bad guys can attack computer networks
- Difesa:
  - how we can defend networks against attacks
- Progettazione:
  - how to design architectures that are immune to attacks

Peccato originale: Internet non è stata pensata considerando la sua sicurezza
- original vision: “a group of mutually trusting users attached to a transparent network”

Bad News

La sicurezza spesso non gode del centro dell’attenzione
- Nello sviluppo ci si focalizza su performance and usability

Implementazioni sono piene di bug
- Buffer overflows sono una delle principali vulnerabilità
- Cross-site scripting e altri attacchi Web

Le reti sono più aperte e accessibili
- Si aumenta il pericolo di attacchi, facile eliminare le tracce

Molti attacchi non sono propriamente “tecnici”
- Phishing, social engineering, etc.

Good News

Ci sono molti meccanismi di difesa

Bene capire le restrizioni
- Crittografia ha dei limiti
- Molti buchi di sicurezza dipendono da fraintendimenti

Consapevolezza della sicurezza

Usabilità e fattori economici

Cosa aspettarsi dal corso

Non copriremo tutti gli argomenti

Principali obiettivi
- Classificazione e discussione di diversi aspetti relativi alla sicurezza
- Diventare familiare con tecniche, protocolli, tool,….
- Diventare un “consumer” educato alla sicurezza
  - Ma possibilmente un security manager
- Mettere le mani in “pasta”
  - Esempi reali e pratica in laboratorio

“hacker”?

Credits

Dan Boneh CS155

Stallings Cap 1

Jonhatan Katz - CMSC 414 Computer and Network Security

Kurose and Rose: *Computer Networking: A Top Down Approach*