Laboratorio di Amministratore di Sistema

9. Sicurezza di rete

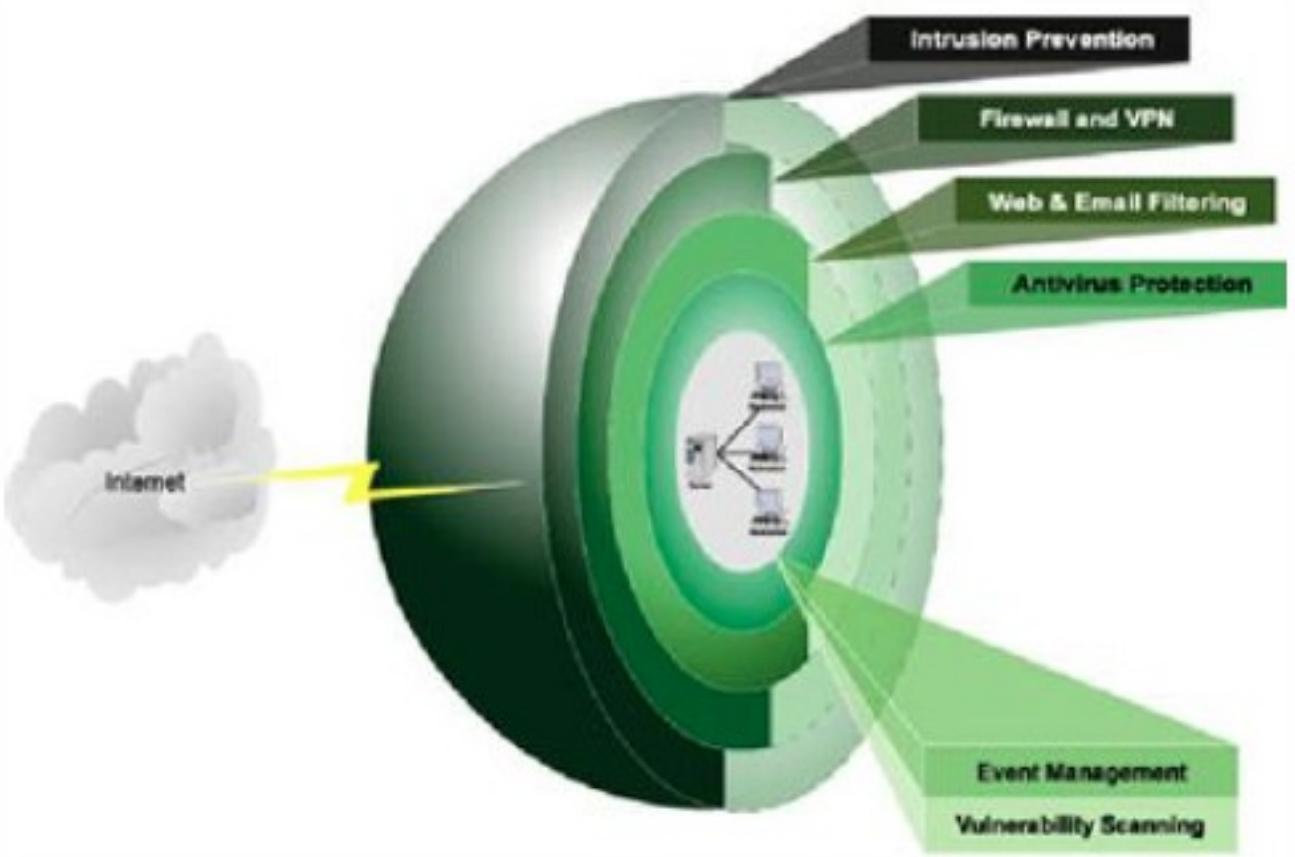
[Cisco ITESS II - Chapter 14]

Università di Venezia – Facoltà di Informatica

feb-mag 2013 - A. Memo

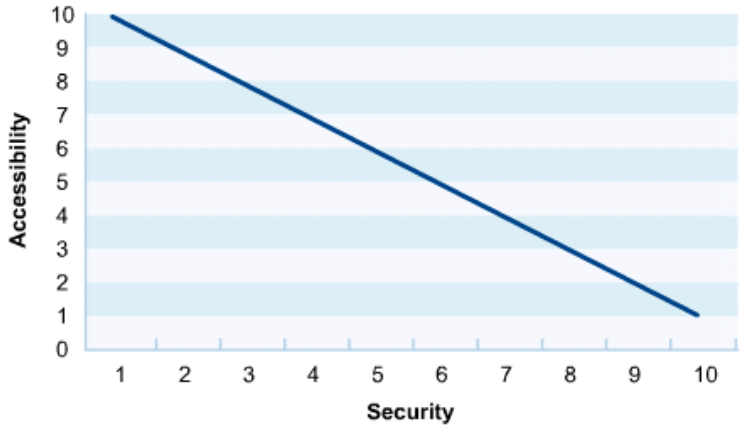
ver 2.1

Developing a Network Security Policy



Accessing Security Needs

- Ci deve essere sempre un delicato equilibrio tra sicurezza e accessibilità.
- più accessibile è una rete è meno sicura è.
- Quando si tratta di un rete di computer, la sicurezza è sufficiente?
- Ci sono diversi fattori da considerare:
  - Il tipo di business in cui l'azienda si impegna
  - Il tipo di dati memorizzati sulla rete
  - La filosofia di gestione dell'organizzazione



Accessing Security Needs

- Tipo di azienda

  -Alcuni affari, come legge e medicina, per la loro natura generano dati riservati. La legge protegge la privacy dei clienti.

- Tipo di dati

  - Alcuni tipi di dati sono considerati privati e dovrebbero essere protetti (libri paga, informazioni personali dei dipendenti, informazioni contabili e fiscali, segreto commerciale, ...)

- filosofia di gestione

  - Se i dati sulla rete non sono soggeti alla legge sulla privacy,il livello di sicurezza potrebbe dipendere dalla filosofia dell'azienda.

Acceptable Use Policy

- Il primo passo nella creazione di una politica di sicurezza per un rete aziendale è quello di definire un Acceptable Use Policy (AUP).

- Un AUP permette agli utenti ciò che è accettabile e consentito della rete aziendale.

- L'AUP può includere informazioni sull'installazione software o hardware.

- Per visualizzare alcuni esempi di AUP, visitare questi siti web:

  - http://www.ja.net/documents/use.html
  - http://www.freeservers.com/policies/acceptable_use.html
  - http://www.rice.edu/armadillo/acceptable.html

Politica di utilizzo accettabile

- è un insieme di regole applicate dal proprietario / gestore di una rete , sito web o sistema di computer di grandi dimensioni che limitano i modi in cui la rete del sito o del sistema può essere utilizzato.
- L'AUP viene definita da società, imprese, università, scuole, fornitori di servizi Internet e proprietari di siti web spesso per ridurre il rischio di azioni legali che possono essere prese da un utente, e spesso con poche prospettive di applicazione.
- L'AUP è parte integrante del quadro generale di sicurezza, ed è spesso pratica comune chiedere ai nuovi membri di una organizzazione di firmare un AUP prima di avere accesso a sistemi informatici.

freeservers POLICIES

ACCEPTABLE USE POLICY

Freeservers has a **zero tolerance** policy for **spam, pornography, and warez**. Any sites found to contain, promote, or link to such content are subject to immediate removal from our service.

By typing in the 4-character security code and clicking the "submit" button at the bottom of the registration page, you accept these terms and conditions and acknowledge that your use of Freeservers is subject to certain limitations set forth below. If you do not accept this agreement, do not proceed with the sign-up process.

I. For the purposes of this agreement, Freeservers, Freeservers.com, and About Web Services may be used interchangeably.

II. Freeservers.com cannot be held responsible for the content of pages hosted under our service. Freeservers does not review pages for content before they are posted and does not verify, endorse, or otherwise take responsibility for the content of any user-created pages. However, we reserve the right to remove any page from our servers which we determine is violating our rules and guidelines. **Users are solely responsible for all files contained in their own directory,** and can be held legally liable for the contents of their Web site.

Penn Computing

Computing : Menu ...

Policy on Acceptable Use of Electronic I

Summary

This policy defines the boundaries of "acceptable use" of lim electronic information sources, as detailed below. It includes information environment evolves.

The policy is based on the principle that the electronic inform and service. Other uses are secondary. Uses that threaten t system; the privacy or actual or perceived safety of others; a

By using University electronic information systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable University policies, as well as City, State and Federal laws and regulations, as detailed below.

The policy defines penalties for infractions, up to and including loss of system access, employment termination or expulsion. In addition some activities may lead to risk of legal liability, both civil and criminal.

Users of electronic information systems are urged in their own interest to review and understand the contents of this policy.

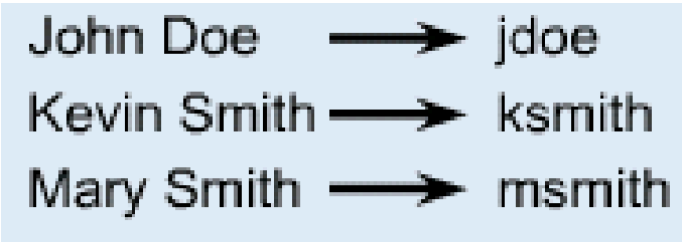
Purposes

The University of Pennsylvania makes computing resources (including, but not limited to, computer facilities and services, computers, networks, electronic mail, electronic information and data, and video and voice services) available to faculty, students, staff, registered guests, and the general public to support the educational, research and service missions of the University.

Username and Password Standards

- Di solito l'amministratore di sistema definisce la denominazione convenzionale per i nomi utente in una rete.

- Un esempio comune è il primo iniziale del nome della persona e poi l'intero cognome.



- Una convenzione di denominazione nomeutente complesso non è così importante quanto avere una password standard complessa.

- Durante l'assegnazione delle password, il livello di password di controllo deve corrispondere al livello di protezione richiesto.

-Password dovrebbe scadere dopo un determinato periodo di tempo

- Le password dovrebbero contenere una combinazione di lettere e numeri in modo da nonessere facilmente individuabile.

Virus Protection Standards

- Alcuni standard richiedono che il software di protezione antivirus sia installato su tutti i sistemi della rete.

- Collocare appositi filtri e liste di accesso su tutto i gateway entranti per proteggere la rete da accessi indesiderati.

- Per evitare i virus, bisogna sviluppare una politica anche sulla posta email in entrata/uscita

University of California Electronic Communications Policy

The University of California Electronic Communications Policy was originally issued November 17, 2000. A revision was issued in 2005.

Policy Issuance Letter

- August 18, 2005 (pdf)

Policy

- Electronic Communications Policy (pdf) (html)
- Attachment 1, ECP User Advisories (pdf) (html)
- Attachment 2, ECP Implementation Guidelines (pd

Major Changes in August 2005 Revision

Key Points on the Use of E-mail at UCOP

Getting the Message, Highlights of the ECP (pdf)

Campus and UCOP ECP Coordinators

Nonconsensual Access Requires Formal Authori

- **Contact your campus ECP coordinator fo**
- **Campuses may adapt and use the UCOP (pdf)**
- **Annual Reports on Nonconsensual Acce**

University Electronic Mail Student Notification Policy (Use of E-mail for Official Correspondence to Students)

Last revised: May 24, 2004 **Last reviewed:** May 24, 2004

Answers to Frequently Asked Questions

A. Policy Statement

Electronic mail (e-mail), like postal mail, is a mechanism for official University communication to students. The University will exercise the right to send e-mail communications to all students, and the University will expect that e-mail communications will be received and read in a timely manner.

B. Scope

This policy applies to all admitted and enrolled students of The University of Texas at Austin. Official communications using e-mail can include e-mail to a group, such as all admitted students, or an e-mail message to only one student.

- http://www.utexas.edu/policies/email/#policy
- http://www.ucop.edu/ucophome/policies/email/email.html
- http://www.onet.on.ca/onetspam.html

Security Policy

SANS (SysAdmin, Audit, Network, Security) Institute

1. Acquisition Assessment Policy

definisce le responsabilità in materia di acquisizioni aziendali, e definisce i requisiti minimi di una valutazione di acquisizione di essere compilato dal gruppo di sicurezza delle informazioni.

2. Bluetooth

Dispositivo di sicurezza comune questa politica prevede più sicure le operazioni di dispositivo Bluetooth. E protegge la società da perdita di identificazione personale Informazioni (PII) e dati aziendali proprietarie.

3. Dial-in

Criteri di accesso definisce adeguato accesso dial-in e il suo utilizzo da parte autorizzato personale.

4. Etica Politica

definisce le modalità per stabilire una cultura di apertura, fiducia e integrità nelle pratiche di business.

Security Policy

SANS (SysAdmin, Audit, Network, Security) Institute

5. Information Sensitivity Policy

definisce i requisiti per la classificazione e il fissaggio del Informazioni di organizzazione in un modo appropriato per la sua sensibilità livello.

6.Internal Lab Security Policy

definisce i requisiti per i laboratori interni per garantire che riservate tecnologie di informazione e non sono compromessi, e che servizi di produzione e degli interessi della organizzazione sono protetti da attività di laboratorio.

7. Personal Communication Devices Policy

descrive i requisiti di sicurezza per le informazioni personali Dispositivi di comunicazione e segreteria telefonica.

Security Policy

SANS (SysAdmin, Audit, Network, Security) Institute

8. Risk Assessment Policy

definisce i requisiti e fornisce l'autorità per la team di sicurezza delle informazioni per identificare, valutare, e risolvere i rischi di infrastruttura informativa dell'organizzazione associata condurre gli affari.

9. Technology Equipment Disposal

definisce le regole per la cessione dei beni tecnologici obsoleti e riciclaggio materiale informatico

10. Web Application Security Assessment Policy

definisce la valutazione di applicazioni Web per identificare potenziali o debolezze realizzate come risultato di involontario mis-configurazione, autenticazione debole, la gestione degli errori insufficienti, le informazioni sensibili perdite, ecc

Online Security Resources

- Alla fine del 1988, uno studente laureato di 23 anni alla Cornell Università rilasciato un worm autoreplicante sulla Internet. Nel giro di poche ore, la rapida diffusione verme causato la chiusura di oltre 60.000 UNIX computer nelle università e strutture militari.

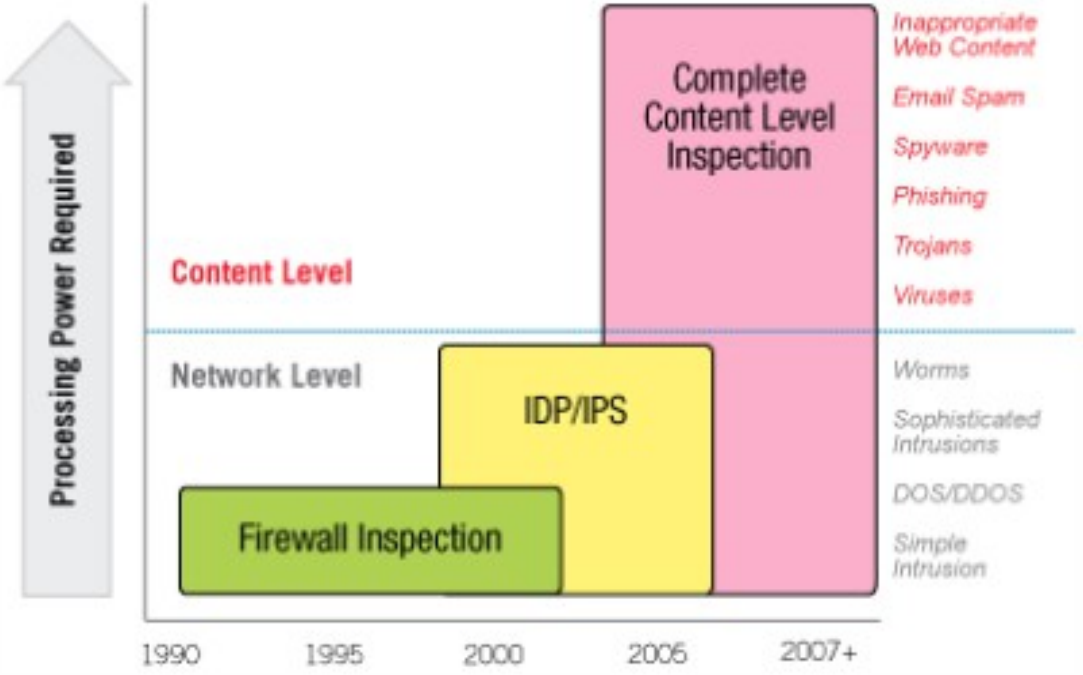
- Risorse basate sul Web offrono informazioni critiche e strumenti potenti che possono essere utilizzati per proteggere una rete. Alcune delle migliori risorse per la sicurezza on-line sono le NOS siti web produttore

http://www.cert.org
http://www.microsoft.com

http://www.redhat.com
http://www.nipc.gov

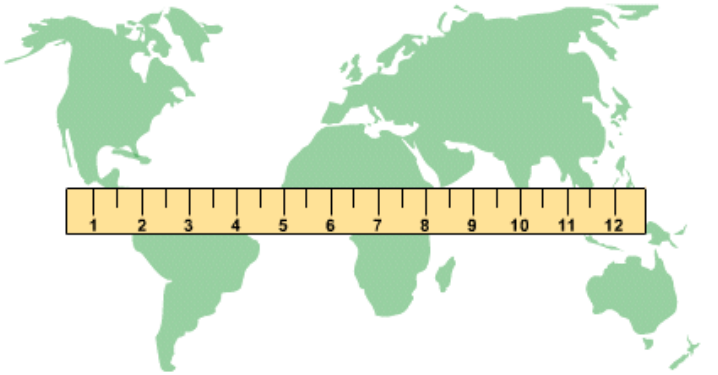
Threats of Network Security

Today's content-based threats, which bypass conventional firewalls, spread faster and do more damage.



Overview: Internal/External Security

- Internet essenzialmente opere di seguito le regole che sono aperti al pubblico.
- Se si studiano le regole abbastanza, si è costretti a trovare lacune e debolezze che possono essere sfruttate.
- Il numero di individui, organizzazioni e istituzioni collegato a Internet sono in crescita.
- Connessione a Internet apre la porta a intrusi di rete.
- Oltre alle minacce esterne provenienti da Internet, aziendali le reti devono affrontare numerosi problemi di sicurezza interna.
- Politiche di sicurezza ben implementate possono ridurre al minimo il rischio che da questi scenari



Network security is essential because the Internet has made networked computers accessible and vulnerable.

Security vulnerabilities within Linux services

The ten more critical internet security vulnerabilities in Linux

1. BIND Domain Name System
2. Remote Procedure Calls (RPC)
3. Apache Web Server
4. General UNIX Authentication Accounts with No Passwords or Weak Passwords
5. Clear Text Services
6. Sendmail
7. Simple Network Management Protocol (SNMP)
8. Secure Shell (SSH)
9. Misconfiguration of Enterprise Services NIS/NFS
10. Open Secure Sockets Layer (SSL)

Security vulnerabilities within Linux services

SANS Top-20 2007 Security Risks (2007 Annual Update)

Client-side Vulnerabilities in:

C1. Web Browsers
C2. Office Software
C3. Email Clients
C4. Media Players

Server-side Vulnerabilities in:

S1. Web Applications
S2. Windows Services
S3. Unix and Mac OS Services
S4. Backup Software
S5. Anti-virus Software
S6. Management Servers
S7. Database Software

Security Policy and Personnel:

H1. Excessive User Rights and Unauthorized Devices
H2. Phishing/Spear Phishing
H3. Unencrypted Laptops and Removable Media

Application Abuse:

A1. Instant Messaging
A2. Peer-to-Peer Programs

Network Devices:

N1. VoIP Servers and Phones

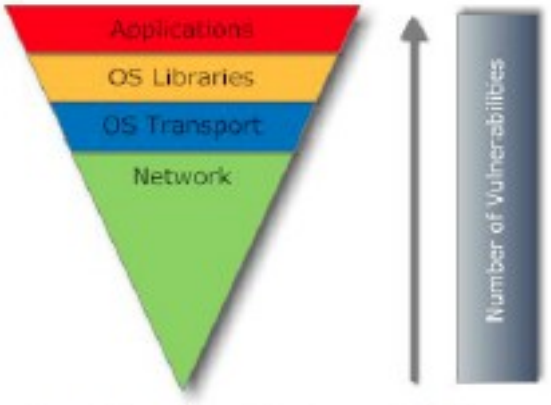
Zero Day Attacks:

Z1. Zero Day Attacks

http://www.sans.org/top-cyber-security-risks/

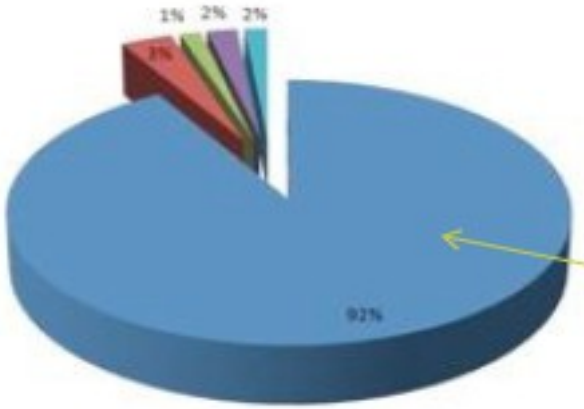
Top Cyber Security Risks

- Priorità Uno: il software lato client che rimane senza patch.
- Priorità Due: Internet rivolte a siti web che sono vulnerabile.
- Sistemi operativi continuano ad avere meno remotelyexploitable vulnerabilità che portano alla massiccia Internet vermi.
- Crescente numero di vulnerabilità zero-day



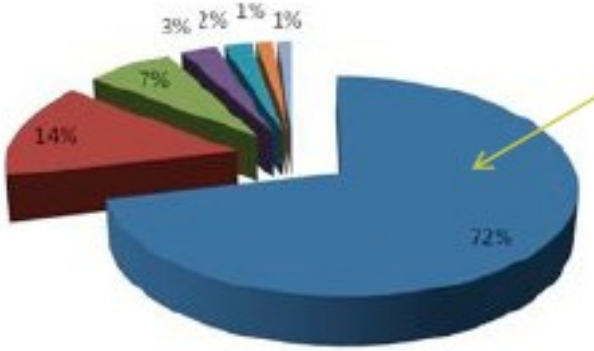
Application Vulnerabilities exceed OS Vulnerabilities

Microsoft OS Attack % For Vulnerabilities



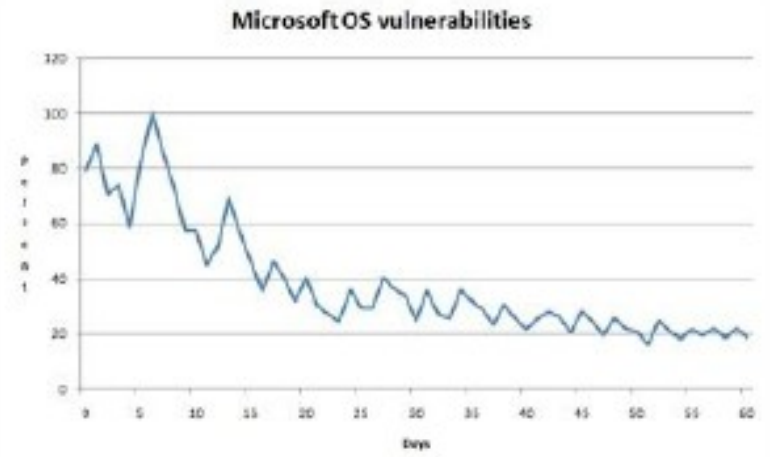
Conficker/ Downadup worm variants based on buffer overflow vulnerability

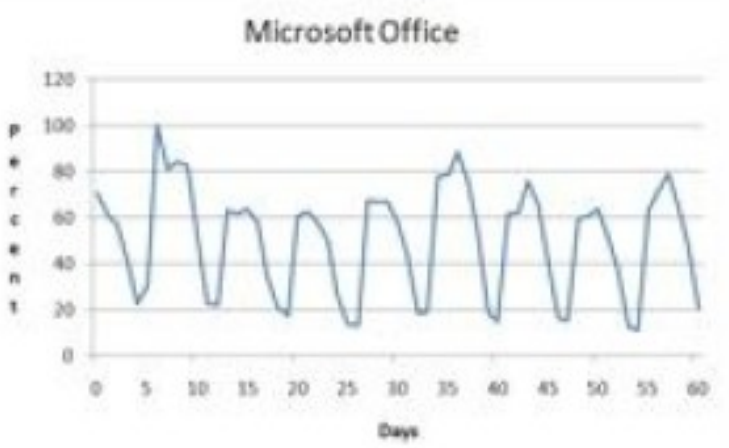
Apple Vulnerabilities Being Exploited

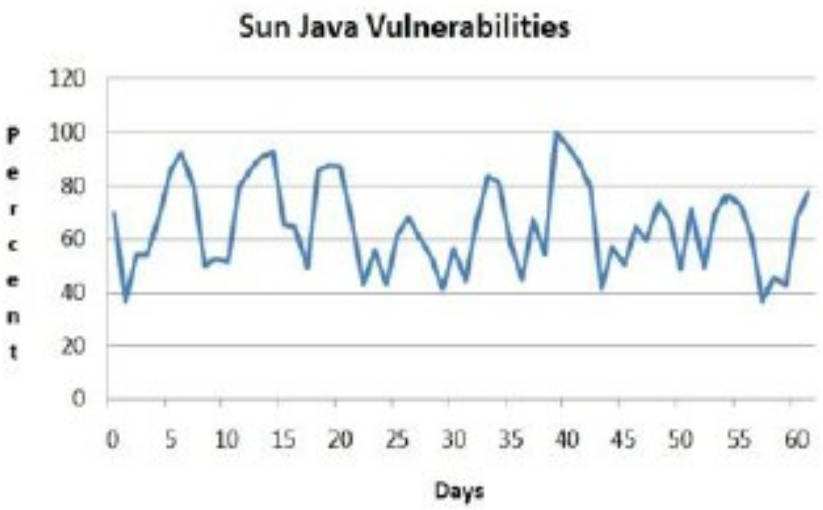


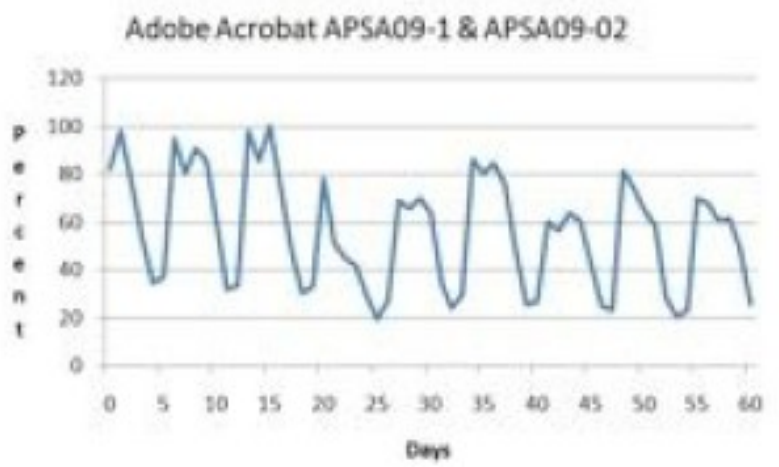
based on QuickTime

Application Patching is Much Slower than Operating System Patching









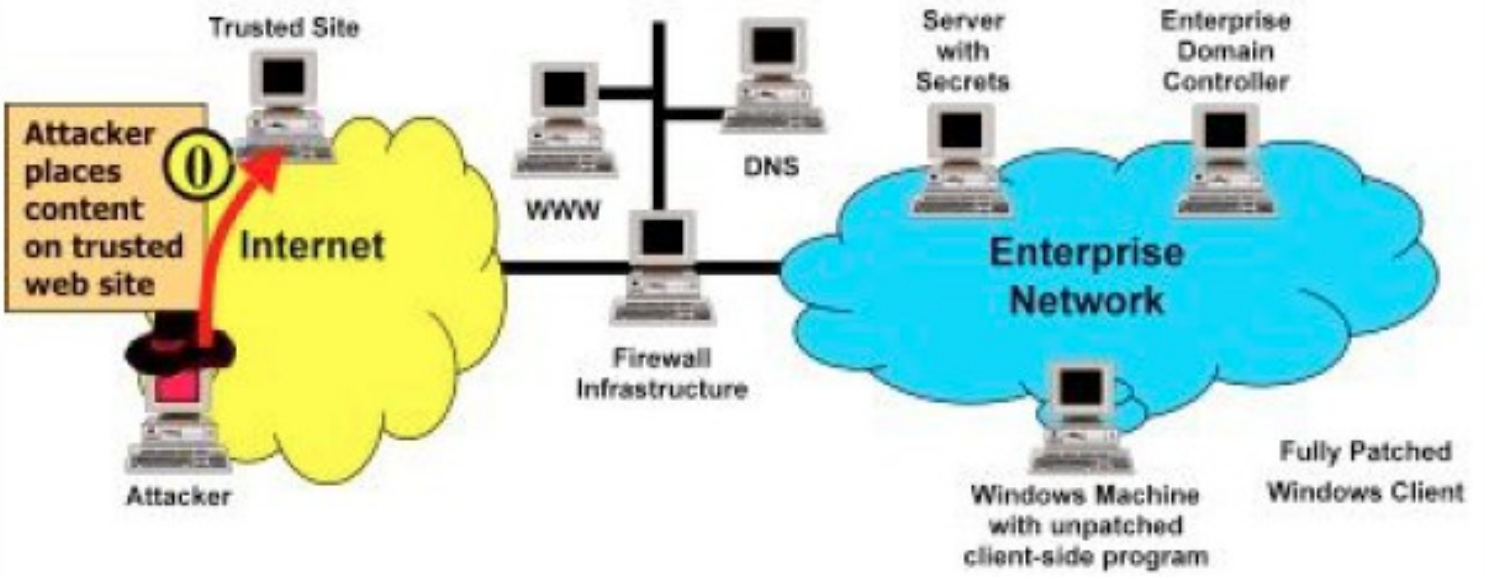
Real-Life HTTP Client-Side Exploitation Example

- Questa sezione illustra un esempio di attacco informatico reale
- In questo attacco, "Widget Acme Corporation" ha subito una grave violazione da pirati informatici che sono stati in grado di compromettere l'intera infrastruttura di rete interna utilizzando due dei più potenti vettori di attacco comunemente usati attualmente: sfruttamento delle lacune del software lato client e attacco *pass-the-hash* contro macchine Windows.

by http://www.sans.org/top-cyber-security-risks/

Step 0: Attacker Places Content on Trusted Site

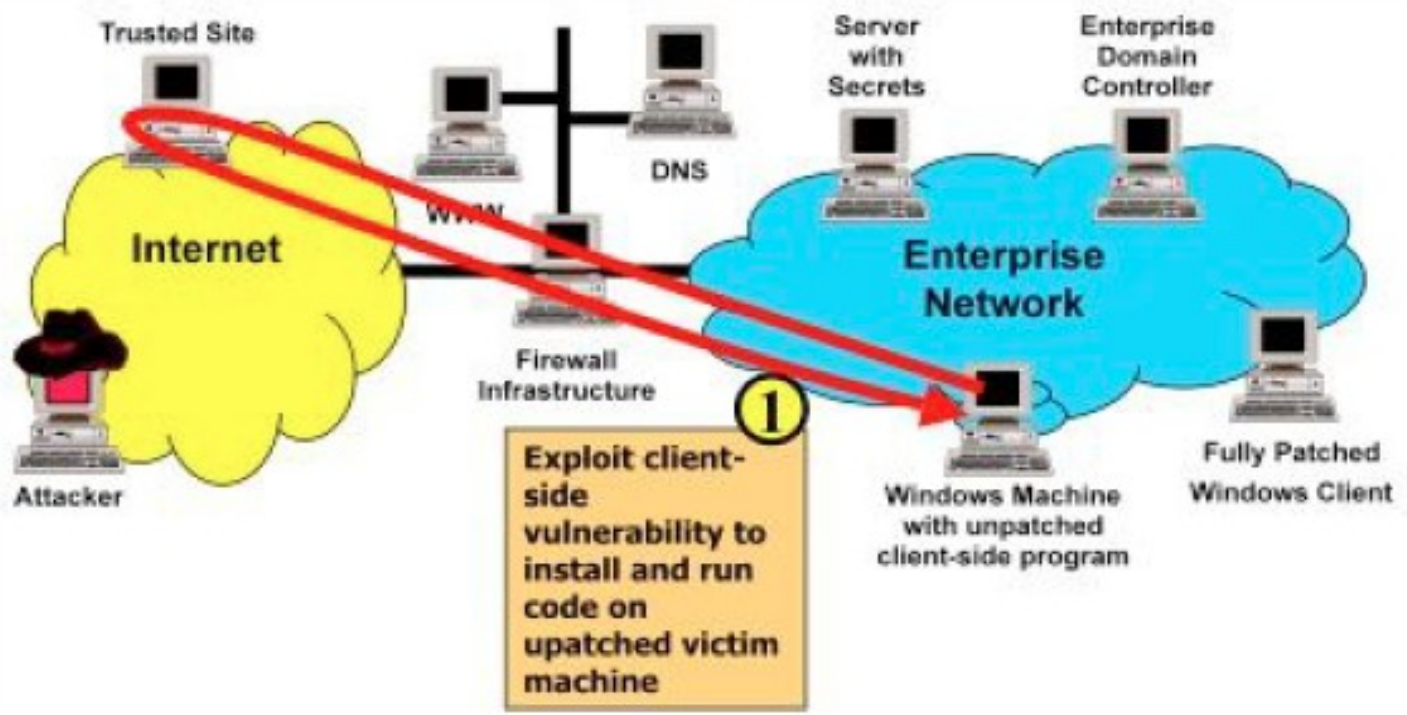
Nella Fase 0, l'attaccante comincia inserendo un contenuto malevolo in un sito web attendibile di terzi, come un social networking, blogging, o qualsiasi altro server web che ospiti contenuti postati da utenti pubblici. Il contenuto immesso dall'attaccante include codice per lo sfruttamento di software lato client non adeguatamente aggiornato.



Step 1: Client-Side Exploitation

Nella Fase 1, un utente sulla rete interna aziendale naviga in Internet da una macchina Windows con software lato client non adeguatamente aggiornato, come ad esempio un lettore multimediale (ad esempio, Real Player, Windows Media Player, iTunes, ecc) , un visualizzatore di documenti (ad esempio, Acrobat Reader), o un componente della suite di Office (ad esempio, Microsoft Word, Excel, Powerpoint, ecc.). Dopo aver caricato il contenuto malevolo dal sito, il browser dell'utente vittima invoca la vulnerabililtà del lato client del programma passandogli il codice exploit dell'attaccante. Questo codice permette all'attaccante di installare o eseguire programmi sulla macchina vittima, utilizzando i privilegi dell'utente che ha lanciato il browser. L'attacco è parzialmente limitato perché questo utente non dispone in generale di credenziali amministrative sul suo sistema. Tuttavia, l'attaccante può eseguire programmi con i privilegi utente.

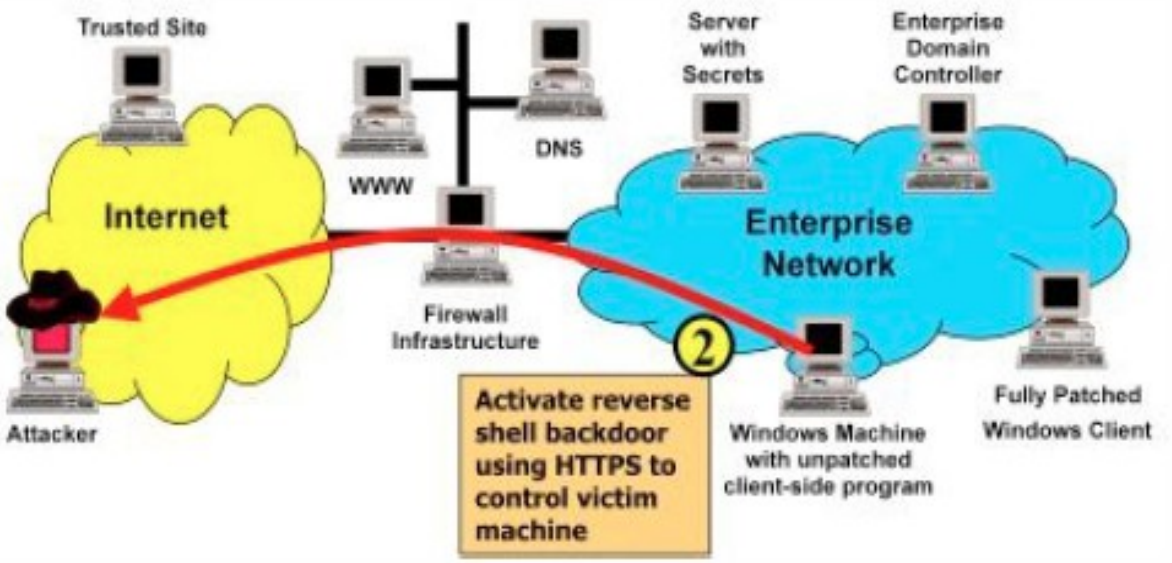
Step 1: Client-Side Exploitation



Step 2: Establish Reverse Shell Backdoor Using HTTPS

Nella Fase 2, il codice dell'attaccante installa un programma *backdoor back connection* sulla macchina vittima. Questo programma permette all'aggressore un accesso alla shell della macchina vittima, utilizzando l'accesso HTTPS dalla macchina attaccante a quella vittima attaccata.

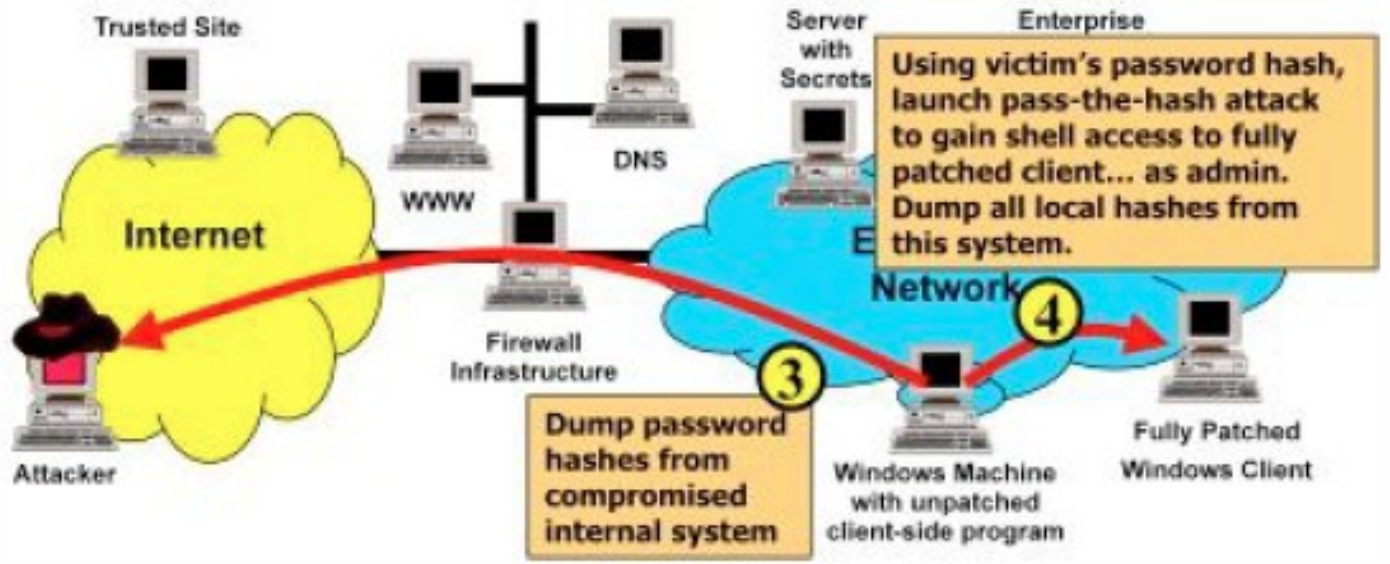
Il traffico *backdoor* sembra quindi essere regolare traffico cifrato web in uscita per quanto riguarda il firewall aziendale a cui la rete è collegata.



Steps 3 & 4: Dump Hashes and Use Pass-the-Hash Attack to Pivot

Nel passaggio 3, l'attaccante usa l'accesso alla shell del sistema vittima per caricare in locale un programma che sfrutti le debolezze della macchina per aumentare gradualmente i propri privilegi. Questo programma permette (o almeno cerca) al malintenzionato di passare su questa macchina dall'account utente con limitati privilegi a quello di totale controllo del sistema. Anche se i venditori spesso rilasciano patch per fermare questi attacchi di aumento di privilegi locali, molte organizzazioni non distribuiscono rapidamente tali patch, perché tendono a concentrarsi esclusivamente sui patch contro gli attacchi da remoto. L'attaccante ora può scaricare gli hash delle password per tutti gli account di questo computer locale, tra cui l'account di amministratore locale sul sistema.

Steps 3 & 4: Dump Hashes and Use Pass-the-Hash Attack to Pivot



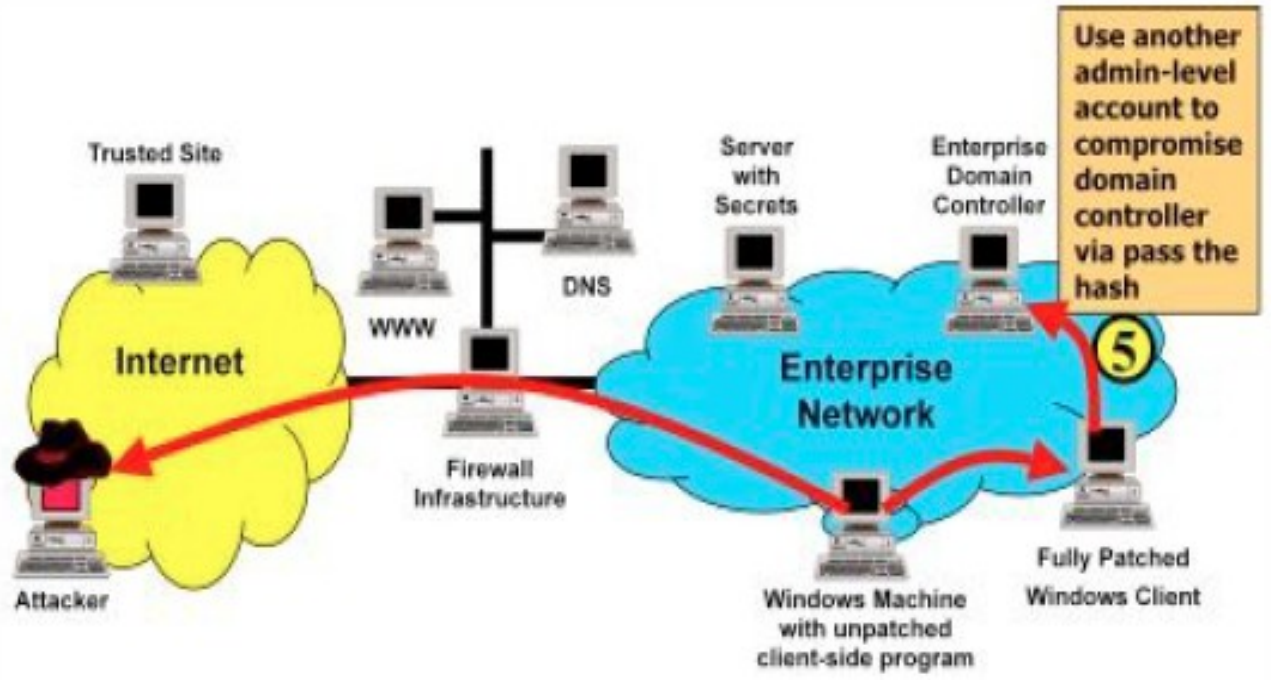
Steps 3 & 4: Dump Hashes and Use Pass-the-Hash Attack to Pivot

Nella fase 4, invece di violare ed utilizzare l'account di amministratore locale, l'attaccante utilizza un programma Windows *pass-the-hash* per scoprire l'autenticazione a un'altra macchina Windows sulla rete aziendale interna, un sistema client completamente aggiornato e protetto su cui il nuovo utente vittima ha privilegi amministrativi completi . Utilizzando NTLMv1 o NTLMv2, le macchine Windows si autenticano per l'accesso alla rete utilizzando Server Message Block (SMB), il protocollo basato sulle hash degli utenti e non sulle loro password, permettendo al malintenzionato di accedere al file system o eseguire programmi sul sistema completamente protetto con privilegi di amministratore locale. Utilizzando questi privilegi, l'attaccante ora scarica anche le hash delle password per tutti gli account locali di questa macchina Windows, che era regolarmente protetta.

Step 5: Pass the Hash to Compromise Domain Controller

Nel passaggio 5, l'attaccante utilizza una chiave hash della password di un account locale sul client Windows perfettamente protetto per accedere al sistema controller di dominio, di nuovo con un attacco pass-the-hash per ottenerne l'accesso alla shell. Poiché la password per l'account amministratore locale è identica alla password di un account amministratore di dominio, gli hash delle password per i due account sono identici. Pertanto, l'utente malintenzionato può accedere al controller di dominio con privilegi completi di amministratore di dominio, avendo il controllo completo su tutti gli altri account e le macchine presenti.

Step 5: Pass the Hash to Compromise Domain Controller



Steps 6 and 7: Exfiltration

Nella fase 6, con i privilegi completi di amministratore di dominio, l'attaccante compromette ora la macchina server che memorizza i dati riservati dell'organizzazione.

Nella fase 7, l'attaccante estrae ed analizza queste informazioni sensibili, composte generalmente da oltre 200 MB di dati. L'attaccante invia dal server questi dati attraverso Internet, sempre utilizzando HTTPS per criptare le informazioni, riducendo al minimo le probabilità di essere scoperto.

Outside Threats **(minacce esterne)**

- Furto di dati si verifica quando un utente non autorizzato o programma software ottiene illegalmente informazioni private che è memorizzata o trasmessa su una rete (packet sniffing e sistema di effrazioni).

- La distruzione dei dati avviene quando un non autorizzata persona o un programma software irrompe in un sistema e eliminazione di dati.

- Un Denial of Service (DoS) è progettato per degradarsi prestazioni del server o rimuoverlo dalla rete completamente.

Outside Threats

Diverse fonti esterne possono causare attacchi:

- Gli hacker - i veri desideri degli hacker di sezionare i sistemi e programmi per vedere come funzionano.
- Crackers - quelli che sfondano a sistemi informatici per manomettere, sottrarre o distruggere i dati.
- Virus - che provoca un po 'di imprevisti e di solito indesiderabile evento.
- Worms - un virus autoreplicante che non altera i file, ma risiede nella memoria attiva e si duplica.
- Cavallo di Troia - è un programma che si presenta come un altro programma per ottenere informazioni

Denial of Service (DoS)

- Nel 1997, una variante del protocollo TCP SYN attacco, chiamato terra, era scoperto. L'attacco di terra utilizza un programma che altera l'IP intestazione della richiesta SYN (spoofing o fucinatura), rendendo la chiedere di essere proveniente dal bersaglio stesso.

- dispositivi di rete possono essere configurate per bloccare gli attacchi TCP SYN da una singola fonte, aumentando il numero di semiaperta connessioni o diminuendo la quantità di tempo di attesa per l' rispondere.

- Teardrop (o attacco frammento) è il nome di un programma che approfitta della via IP gestisce frammentazione, l'invio di frammenti con sovrapposizione informazioni riassemblaggio che confondere il software di destinazione.

Denial of Service (DoS)

- Un attacco DoS si verifica quando il sistema di mira non può servizio legittime richieste efficace rete.

- Come risultato, il sistema è diventato sovraccaricato messaggi illegittimi.

- Gli attacchi DoS hanno origine da un host o un gruppo di host.

- Quando l'attacco proviene da un gruppo coordinato di padroni di casa, questi attacchi sono chiamati Distributed DoS (DDoS).

- Un attacco DoS comune è quello di sovraccaricare un sistema di destinazione per l'invio di più dati di quelli che può gestire.

Denial of Service (DoS)

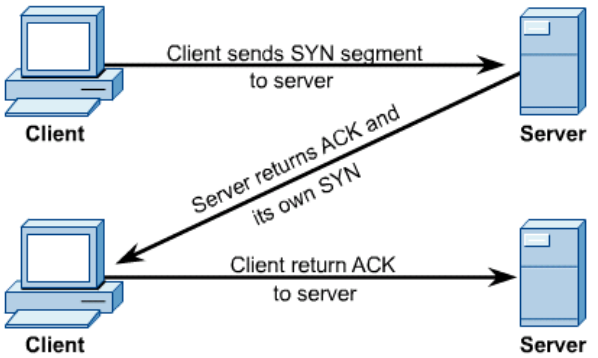
Ci sono diversi tipi di attacchi DoS:

- Un attacco di tipo buffer overflow è stato progettato per sopraffare il software in esecuzione sul sistema di destinazione (buffer overflow).

- Il cosiddetto ping della morte è un buffer overflow ben noto. L'attaccante invia una richiesta di eco ICMP che sono illegalmente grandi al bersaglio. (carenze specifiche nel software NOS)

- La sincronizzazione (SYN) TCP attacco sfrutta il TCP protocollo three-way handshake.

- - L'attaccante invia una grande volume di TCP sincronizzazione SYN richieste senza risposta alle ACK (risultante elevato volume di semiaperta connessioni).



Denial of Service (DoS)

- l'attacco Smurf si basa su spoofing del pacchetto IP. Normalmente le richieste di ping esterni vengono negati e interno sono ammessi. Spoofing l'intestazione IP, le richieste di ping esterni può raggiungere e inondazioni e sovraccaricare la rete interna.

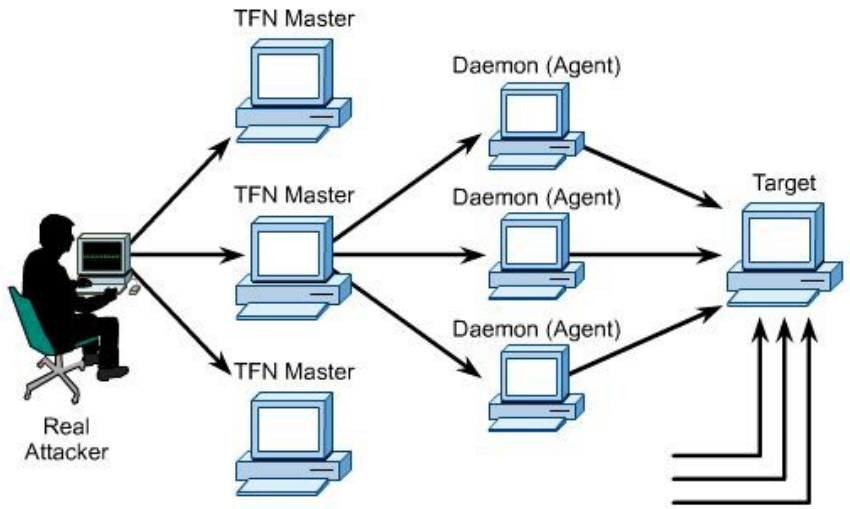
- Gli esempi qui elencati sono tutte le vulnerabilità conosciute. Software OS è ora scritto con questi attacchi in mente. Per esempio, la maggior parte dei sistemi sono ora immuni da terra e Goccia.

- Vulnerabilità note del software rappresentano fori nel sistema. Questi fori possono essere riparati, o rattoppati, con l'installazione di aggiornamenti del software quando sono messi a disposizione da un fornitore.

Distributed Denial of Service (DDoS)

- Prima che l'hacker può attaccare il obiettivo finale, una "flotta" di "zombie" (non protetta host con un connessione permanente a Internet) devono essere coordinati per l' attaccare.

- L'hacker sfrutta la mancanza di sicurezza del zombie.



- L'hacker rompe al sistema o direttamente o attraverso un virus e-mail.

- L'obiettivo della rottura o un virus è quella di installare il software sul sistema di zombie.

- L'hacker utilizza gli zombie per lanciare un attacco DDoS sul obiettivo finale

Well Known Exploits

- Ogni combinazione di NOS e applicazioni software contiene il proprio set unico di vulnerabilità e debolezze.

- Minacce alla sicurezza di rete viene da individui con strumenti sofisticati (e con relativamente debole tecnica abilità).

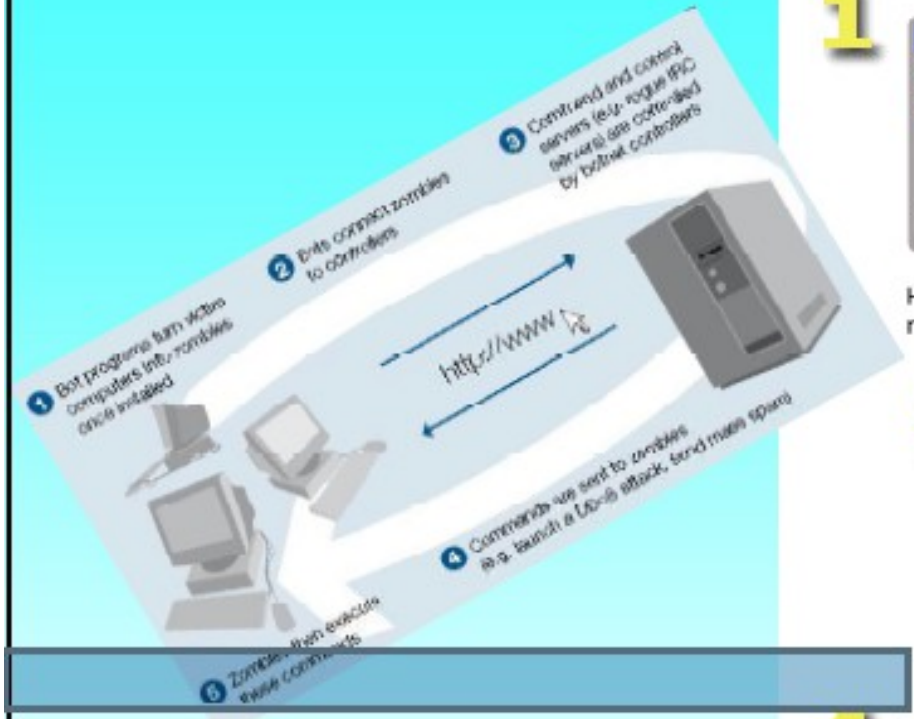
- Alcuni di questi individui sono spesso chiamati "copione kiddie ".

- Script kiddy è un termine negativo usato per descrivere individui immaturi che utilizzano script, programmi software, o le tecniche create da altri, cracker più esperti.

Well Known Exploits

Well Known Exploits

- **Asmodeus (NetIQ security analyzer)** - Network security analyzer and port scanner for Windows that is capable of scanning ranges of hosts for remote security vulnerabilities.
- **SATAN (Security Administrator Tool for Analyzing Networks)** - An outdated network security analyzer for UNIX, similar in function to NetIQ.
- **Saint (The Security Administrator's Integrated Network Tool)** -An updated and enhanced version of SATAN.
- **Strobe (strobe-classb)** - A small but fast scanner, used to scan for open mail relays over class B networks.
- **Ogre** - Service and vulnerability scanner for Windows NT, including NetBIOS shares and some Microsoft Internet Information Services (IIS) vulnerabilities.
- **mscan (Multiscan)** - Scanner used to detect vulnerabilities in commonly used UNIX services, such as DNS, NFS, statd, X and finger.
- **Nmap** - A fast and powerful port scanner for UNIX, capable of scanning ranges of computers via IP address, domain, or randomly for open ports, operating system guess, and other information.
- **ncat (Network Config Audit Tool)** - Utility for scanning Cisco IOS Config files for user defined parameters, such as oversights or errors.
- **BackOffice** - A server that runs in the background of the installed computer, waiting for clientconnections to remotely administer the system, invisible to regular users.
- **NetBus** - Same thing as BackOffice but made by different people. Its not as powerful and is usually attached onto an unrelated executable.
- **SubSeven** - Same as BackOffice and NetBus, but similar to BackOffice in power.
- **trinoo, Stacheldraht, tribe flood network (TFN), mstream, carko, wormkit** - DDoS tools.
- **Ramen** - A collection of tools designed to attack systems by exploiting well-known vulnerabilities in three commonly installed software packages. A successful exploitation of any of the vulnerabilities results in a privileged root compromise of the victim host.



1

HTML_IFRAME.CU is hosted on malicious or hacked Web sites

2

When the said Web sites are visited, the affected system is directed to an IP address, which redirects to another IP address hosting JS_DLOADER.NTJ

3

JS_DLOADER.NTJ exploits browser vulnerabilities to download TROJ_SMALL.HCK

4

TROJ_SMALL.HCK downloads TROJ_PAKES.NC and TROJ_AGENT.UHL

5

TROJ_AGENT.UHL acts as a proxy server while TROJ_PAKES.NC downloads info stealer TSPY_SINOWAL.BJ on the affected system

MPack v0.86 stat

Attacked hosts: (total/uniq)	
IE XP ALL	51966 - 47853
QuickTime	23 - 23
Win2000	3372 - 2988
Firefox	9527 - 9395
Opera7	15 - 15

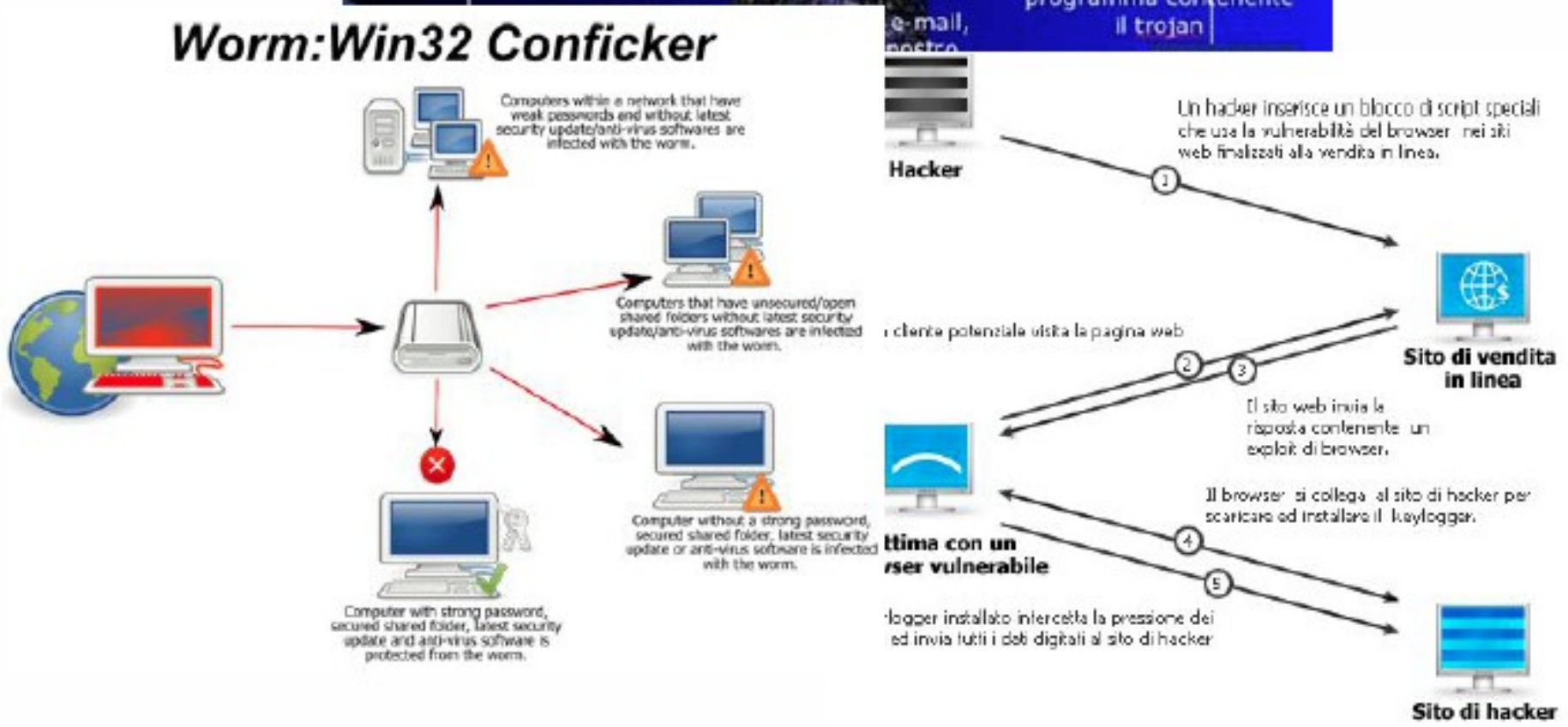
Grave vulnerabilità in Samba

Si consiglia l'aggiornamento alla versione successiva, o di applicare il workaround descritto in questo articolo.

Risale a martedì 10 aprile il bollettino di sicurezza del team di sviluppo di **Samba**, che **denuncia un grave bug** nella nota suite di interoperatibilità.

Le versioni 3.6.3 e precedenti sono tutte afflitte da


Utilizzo di un Trojan RAT
1-L'attaccante Immette il trojan in rete
INTERNET
2-L'utente scarica il trojan dalla rete
Utente
Attaccante
5-L'attaccante prende il controllo del nostro computer
3-L'utente avvia il programma contenente il trojan


Worm:Win32 Conficker
Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.
Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.
Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.
e-mail,
Hacker
Un hacker inserisce un blocco di script speciali che usa la vulnerabilità del browser nei siti web finalizzati alla vendita in linea.
1
Sito di vendita in linea
cliente potenziale visita la pagina web
2
3
Il sito web invia la risposta contenente un exploit di browser.
ttima con un
rser vulnerabile
Il browser si collega al sito di hacker per scaricare ed installare il keylogger.
4
5
logger installato intercetta la pressione dei
ed invia tutti i dati digitati al sito di hacker
Sito di hacker

Inside Threats

- Le minacce alla sicurezza che hanno origine all'interno di una rete possono essere più dannose di quelle minacce esterne.

- Le minacce di alto profilo interne includono comportamenti sleali di dipendenti scontenti che utilizzano il loro accesso per distruggere, rubare, o manomettere i dati.

- Spionaggio industriale è il tipo più sofisticato di minaccia interna alla sicurezza. I dipendenti possono essere avvicinati da aziende concorrenti.

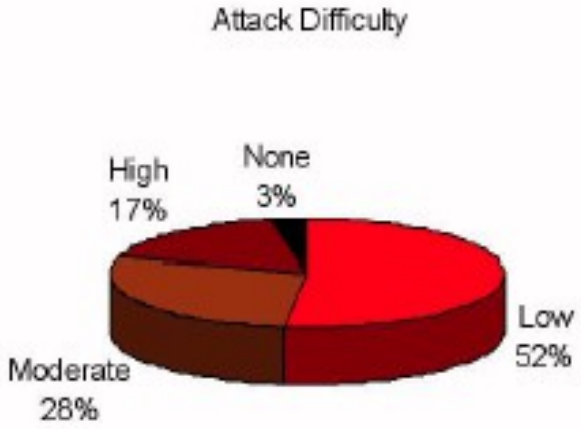
- Violazioni della sicurezza interna può anche essere il risultato di utenti ribelli che sono in disaccordo con le politiche di sicurezza.

- Un problema in crescita per le reti aziendali è la diffusa popolarità della messaggistica istantanea e condivisione di file peer-to-peer. Chat e applicazioni di condivisione possono essere vulnerabili ad altri forme di sfruttamento.

Inside Threats

Oltre ad una politica di sicurezza ben pianificata, le organizzazioni dovrebbe fornire programmi di formazione per tutti i dipendenti che utilizzano la rete. Dal momento che i dipendenti sono spesso presi di mira come un modo per invadere la rete intranet, è importante istruirli su come prevenire i virus, attacchi DoS, furto di dati e così via. Il danno è più probabile che si verifichi per incompetenza

Implementing Security Measures



File Encryption, auditing, and authentication

- La crittografia dei file è un modo di crittografia dei dati memorizzati su un disco in modo da risultare illeggibile a chiunque, tranne che per il creatore della dati.

- 3DES: è un sistema di crittografia in grado di crittografare e decrittografare i dati utilizzando una singola chiave segreta

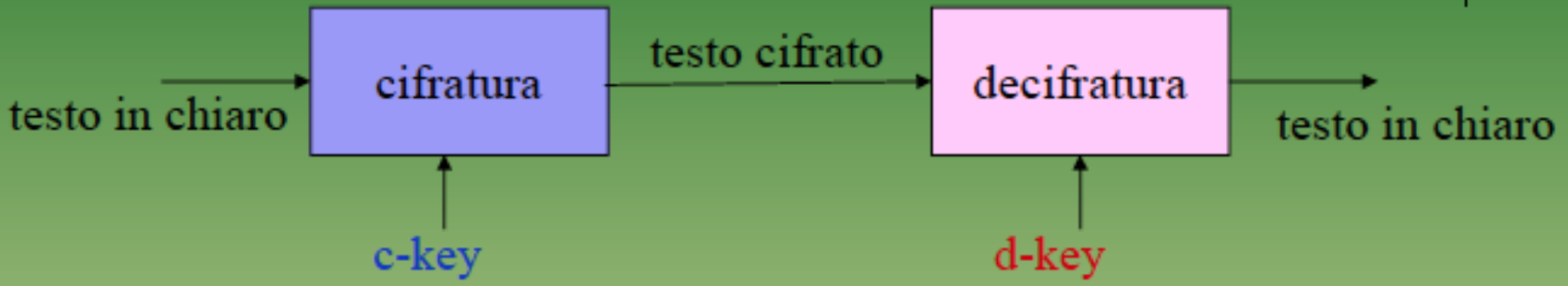
- DES è un cifrario a blocchi, agisce su un blocco di lunghezza fissa di testo in chiaro (64 bit) e lo converte in un blocco di testo cifrato della stessa dimensioni utilizzando la chiave segreta (anche 64 bit, ma 8 bit per la parità).

- La lunghezza della chiave efficace nel DES è a soli 56 bit. In 3DES, 3 fasi di DES con una chiave separata per ogni fase viene applicata. Quindi la lunghezza di chiave 3DES è 168 bit.

- DES è noto come un cifrario a chiave simmetrica perché la stessa chiave viene utilizzata sia nella crittografia e decrittografia.

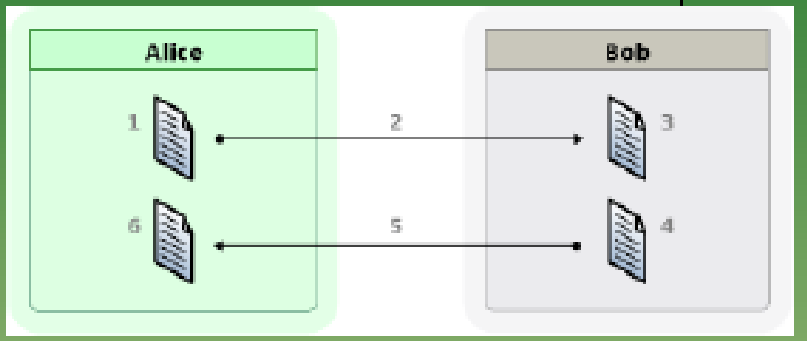
- (DES, 3DES, AES = simmetrico), (RSA, RC4, IDEA = rifl)

Crittografia

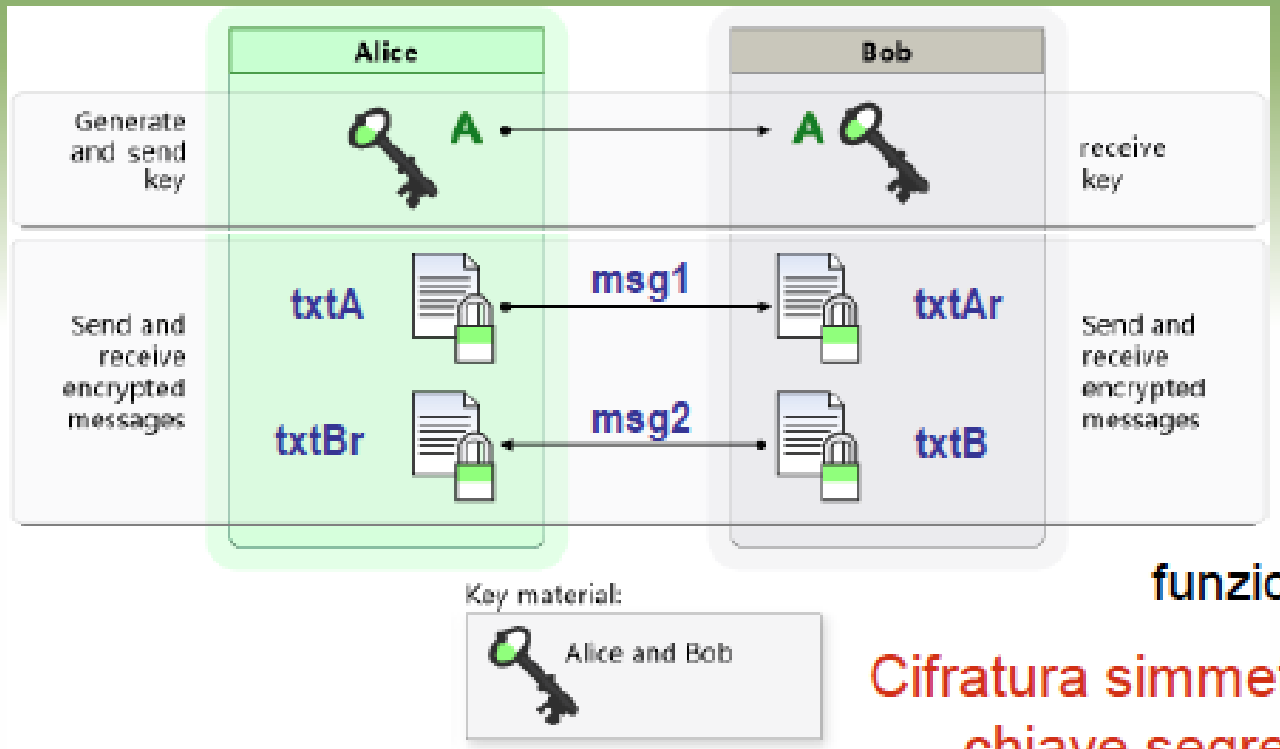


- Gli algoritmi di cifratura/decifratura sono pubblici
- Le chiavi di cifratura/decifratura sono segrete
- Cifratura simmetrica
  - c-key = d-key
  - *problemi di sicurezza nella distribuzione e condivisione*
- Cifratura asimmetrica o a chiave pubblica
  - c-key != d-key
  - *una chiave è pubblica, l'altra è segreta*

Crittografia



Trasmissione in chiaro



msg1 = Cif(txtA, A)
txtAr = Dec(msg1, A) =
= Dec(Cif(txtA,A), A)

msg2 = Cif(txtB, A)
txtBr = Dec(msg2, A) =
= Dec(Cif(txtA,A), A)

funziona se Dec(Cif(txt,k),k) = txt

Cifratura simmetrica (a chiave segreta)

Crittografia

Cifratura simmetrica

Molti sono i possibili schemi di cifratura utilizzati: DES, 3DES, AES, RC4, IDEA, …

In generale, la forza di uno schema di cifratura dipende dalla lunghezza della sua chiave (perchè la ricerca della chiave risulta più complessa)

- DES (data encryption standard, 1975) usa una chiave lunga 56 bit; divenuta vulnerabile per ricerca esaustiva della chiave
- Sostituito nel 2002 da AES (advanced encryption standard, 1998) che usa chiavi lunghe 128, 192, o 256 bit

$$A \rightarrow B : \{ D \}K_{AB} \qquad D = \{ \{ D \}K_{AB} \}K_{AB}$$

Crittografia

Cifratura asimmetrica

- Ciascun utente ha una chiave pubblica K e una chiave privata K^{-1}
- K^{-1} deve essere mantenuta segreta, non va comunicata a nessuno, e non può essere dedotta da K
- K è pubblica e disponibile a tutti
- La cifratura e decifratura con le chiavi K e K^{-1} sono commutative:

$$\{ \{D\}K^{-1} \}K = \{ \{D\}K \}K^{-1} = D$$

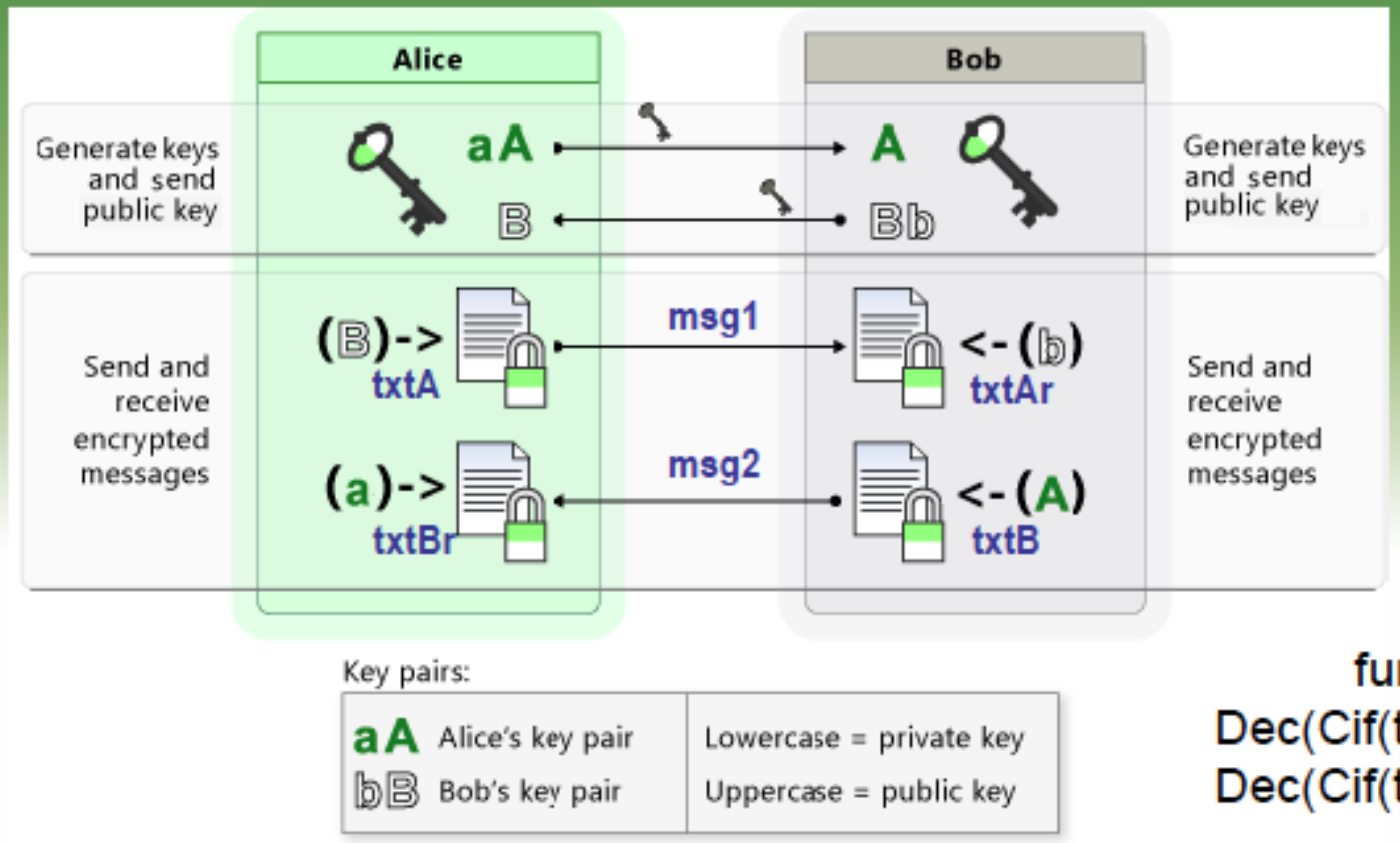
Crittografia

- La cifratura asimmetrica è 3-5 ordini di grandezza più lenta della cifratura simmetrica
- Si utilizza la cifratura asimmetrica per scambiare solo le chiavi simmetriche, mentre i dati vengono scambiati con schemi simmetrici:

$$A \rightarrow B: \{K_{AB}\}K_B, \{D\}K_{AB}$$

- Inoltre la cifratura asimmetrica ha altri importanti utilizzi nel campo dell'autenticazione

Crittografia



msg1 = Cif(txtA, B)
txtAr = Dec(msg1, b) =
= Dec(Cif(txtA,B), b)

msg2 = Cif(txtB, A)
txtBr = Dec(msg2, a) =
= Dec(Cif(txtB,A), a)

funziona se
Dec(Cif(txt,pub),pri) = txt
Dec(Cif(txt,pri),pub) = txt

Cifratura asimmetrica (chiave pubblica e privata) con algoritmo RSA

Crittografia

Come ricavare K e K^{-1}?

Si sfruttano le proprietà dei moduli: come $(x^a)^b = (x^b)^a$, nei moduli se $C=Y^A \pmod P$ e $D=Y^B \pmod P$ allora $C^B \pmod P = D^A \pmod P$.

Inoltre si usano funzioni suriettive con un numero di possibili inversi di complessità esponenziale, come ad esempio l'elevamento a potenza e l'esponenziale con i moduli.

Crittografia

L'algoritmo RSA garantisce l'impossibilità di ricavare la chiave privata da quella pubblica. Le chiavi sono lunghe da 256 a 2048.

Costruzione delle chiavi

- Si prendono due numeri primi, ***p*** e ***q***,
- Si calcolano $n = p \cdot q$ e $z = (p-1) \cdot (q-1)$
- Si sceglie un numero ***d*** che sia primo rispetto a ***z*** (cioè che non abbia divisori comuni con ***z***).
- Si trova ***e*** tale che $(e \cdot d) \pmod z = 1$
- La chiave pubblica è data da ***pri = (e , n)***
- La chiave privata è data da ***pri = (d , n)***

Esempio elementare

p=3 q=11

n = (p)·(q) = 33

z = (p-1)·(q-1) = 20

d = 3

e = 7

Privata = (7, 33)

Pubblica = (3, 33)

Crittografia

Codifica del messaggio

- Suddividere il testo in chiaro in blocchi da **k** bit, con k il più grande intero tale che $2^k<n$,
- Per ogni blocco in chiaro B, il codice cifrato C vale

$$C = B^e \pmod n$$

Decodifica del messaggio

- Per ogni blocco cifrato C, il blocco in chiaro ricevuto R vale

$$R = C^d \pmod n$$

Esempio elementare

messaggio: 1308

k = 5 bit (da 0 a 31)

$B_1 = 13$ $B_2 = 08$

Privata = (7, 33)

Pubblica = (3, 33)

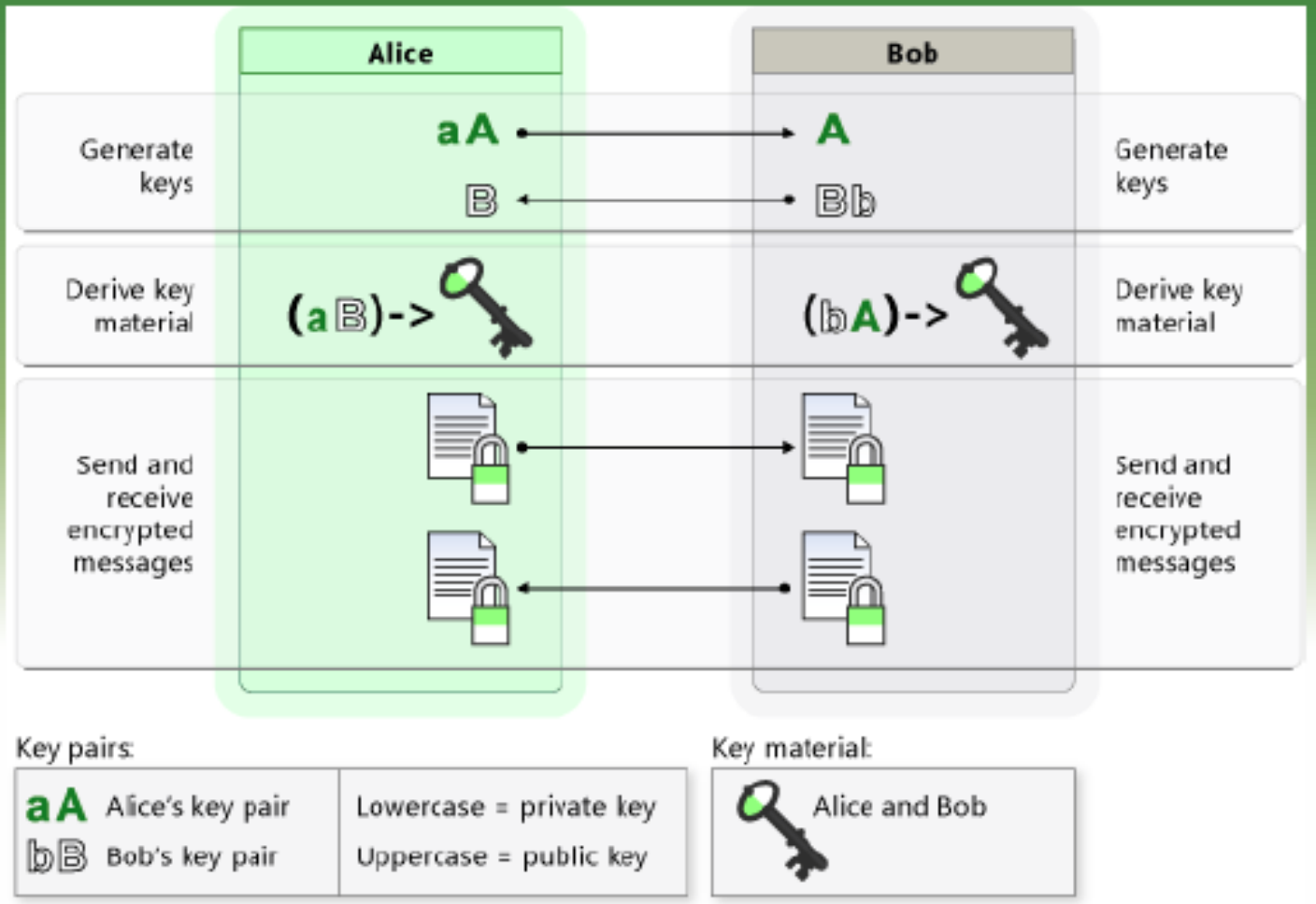
$C_1 = 13^3 \pmod{33} = 19$

$C_2 = 08^3 \pmod{33} = 17$

$R_1 = 19^7 \pmod{33} = 13$

$R_2 = 17^7 \pmod{33} = 8$

Crittografia



Trasmissione a chiave pubblica e privata con algoritmo ECDH
Elliptic Curve Diffie-Hellman

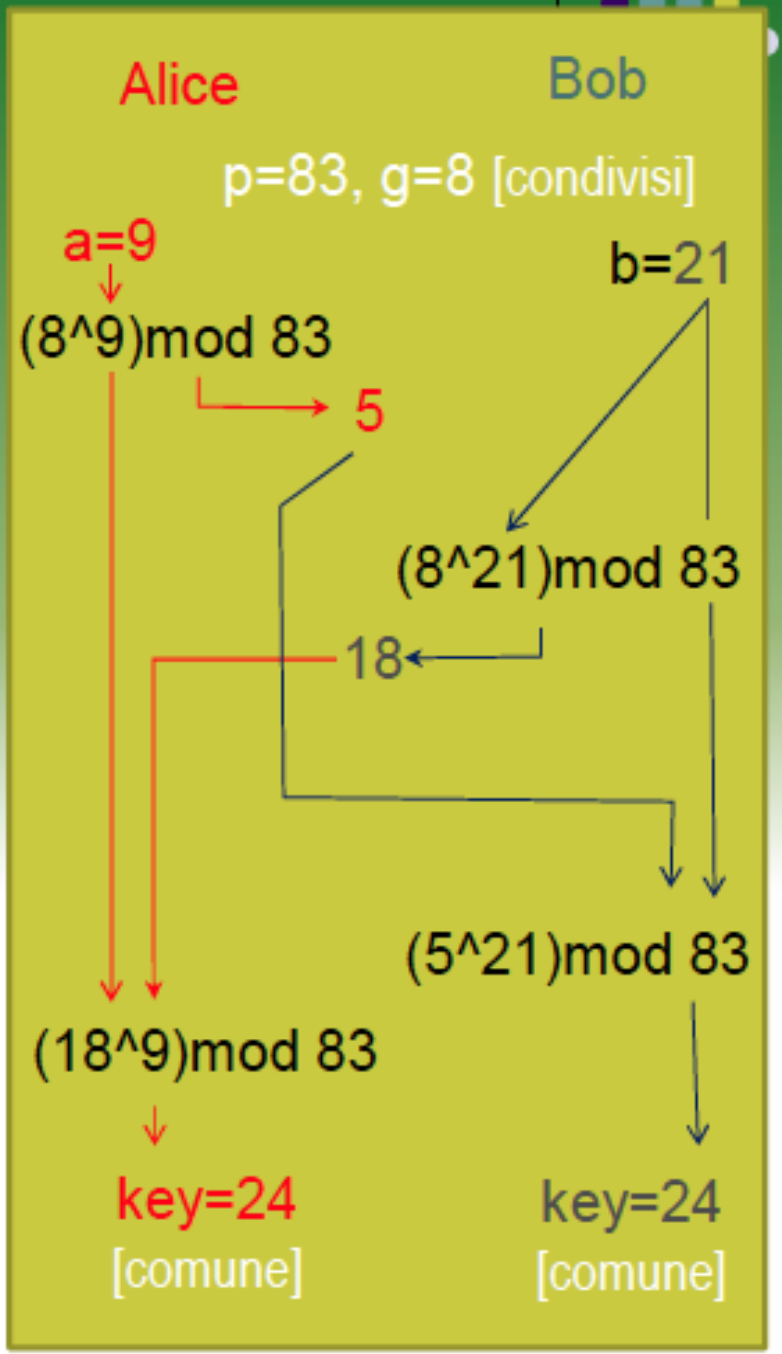
Crittografia

Algoritmo ECDH

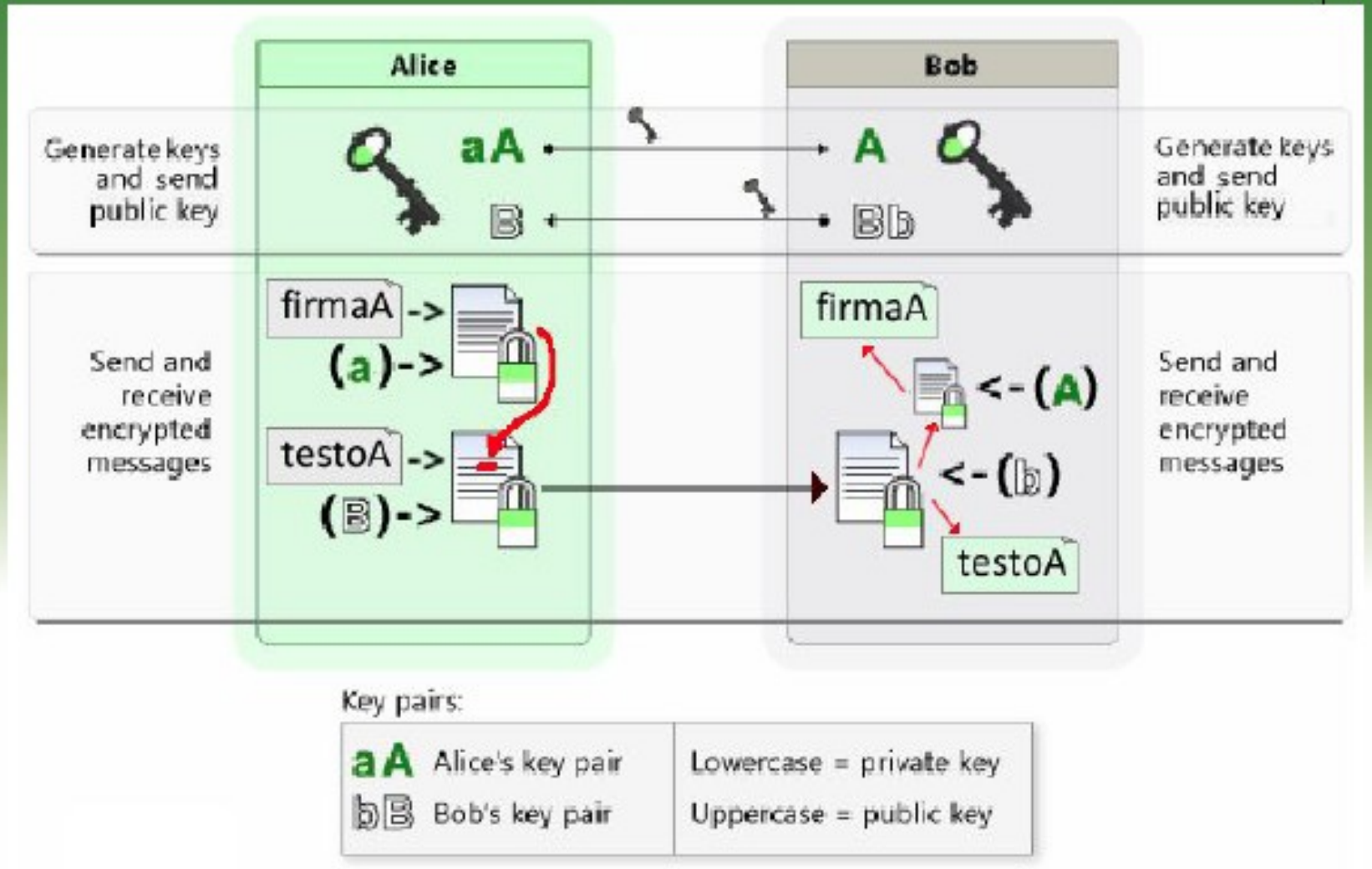
- Alice e Bob concordano di utilizzare un numero primo **p** e un intero di base **g**
- Alice sceglie un intero segreto **a** ed invia a Bob **(g^a) mod p**
- Bob sceglie un intero segreto **b**, ed invia ad Alice **(g^b) mod p**
- Alice calcola la chiave

  (((g^b) mod p)^a) mod p
- Bob calcola la chiave

  (((g^a) mod p)^b) mod p
- Le due chiavi coincidono perché g^(ab) = g^(ba). Questo valore corrisponde alla chiave privata condivisa.



Crittografia



Trasmissione **autenticata** a chiave pubblica e privata con algoritmo RSA

File Encryption, auditing, and authentication

- Windows 2000 include una funzione di crittografia dei file.

- Programmi di crittografia di terze parti sono disponibili per i sistemi operativi:

  -PC Guardian Deltacrypt, Winzap

- Autenticazione fornisce diversi metodi per identificare utenti tra cui le seguenti:

  - Finestra di login e password

  - Sfida e risposta

  - Supporto di messaggistica

- Un server Linux può utilizzare CHAP e l'autenticazione PAP per PPP connessioni.

  - PAP (Password Authentication Protocol)

  - CHAP (Challenge Handshake Authentication Protocol) utilizza chiave segreta già condivisa (in / etc / ppp / chap-secrets) e periodica richieste di sfida

File Encryption, auditing, and authentication

- Auditing - si riferisce al computer e mondo del networking è un software che gira su un server e genera un report mostrando che ha accesso al server e quali operazioni gli utenti hanno eseguito durante un dato periodo di tempo.

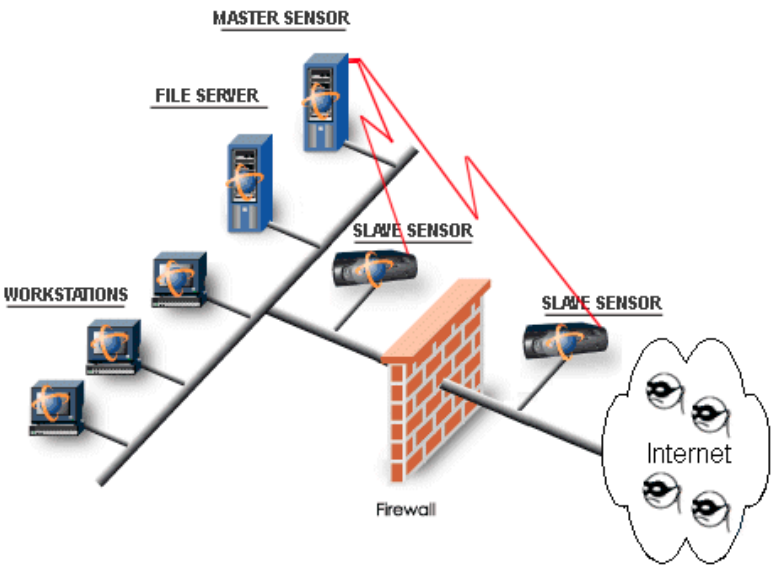
- Un servizio gratuito di software facile da installare auditing è LSAT (Linux Security Auditing Tool). Esso controlla molti sistema configurazioni e le impostazioni di rete locale sul sistema per la sicurezza comune e gli errori di configurazione e per pacchetti che non sono necessari. Si tratta di uno strumento di controllo post-installazione

Intrusion Detection Systems

- Intrusion Detection System (IDS) è un hardware o software che è responsabile del rilevamento di inappropriato, insospettabile, o altri dati che possono essere considerati non autorizzati in una rete.

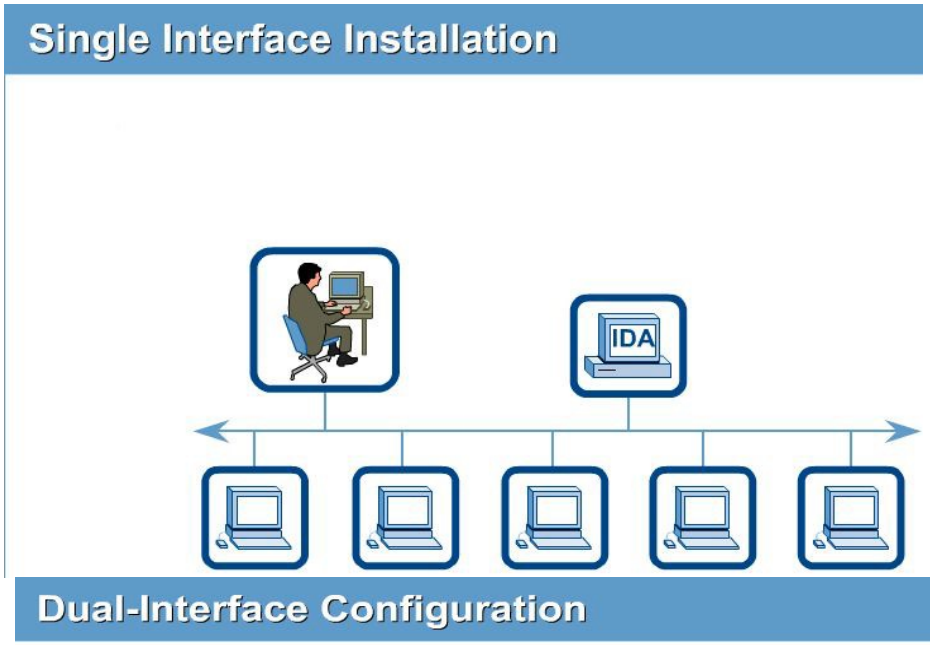
- Un IDS è diverso da un firewall: il firewall limita l'accesso sulla base di un insieme di regole, IDS ispeziona il traffico e valuta una sospetta intrusione, genera un allarme.

- Snort - è un tempo reale basato su software IDS di rete che può essere utilizzato per informare un amministratore di un tentativo di intrusione.



Intrusion Detection Systems

- Snort può essere installato su un server sia una rete singola o doppia interfaccia.
- Su una singola installazione dell'interfaccia la stessa interfaccia ascolto in rete traffico e permette la gestione
- Snort rileva intrusioni secondo un insieme di regole.
- il rules.base file contiene informazioni per la rete INTERNA ed ESTERNA e DNS server dai quali tendono ad innescare la rilevazione portscan di cui avrà bisogno



Intrusion Detection Systems

- PortSentry - è un rilevatore di scansione delle porte che può essere configurato per collegarsi alle porte che si desidera monitorare.

- Dopo la localizzazione può reagire nei seguenti modi:

  - Un registro che indica l'incidente avviene tramite syslog ().

  - L'host di destinazione arriva automaticamente

  / etc / hosts.deny per i wrapper TCP.

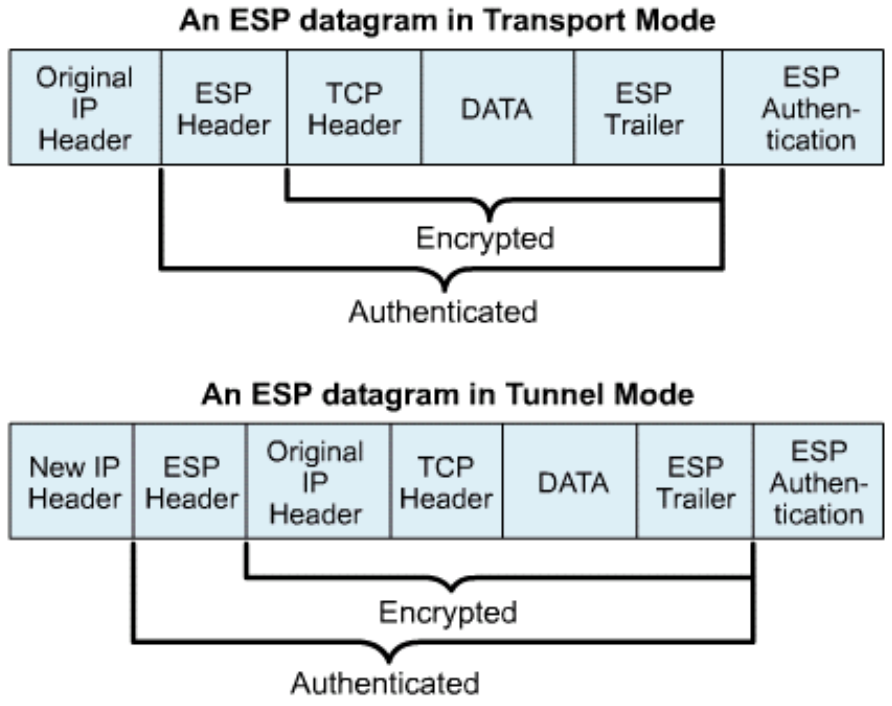
  - L'host locale viene automaticamente ri-configurata per instradare tutto traffico al bersaglio a un host morto per rendere il sistema di destinazione scomparso.

  - L'host locale viene automaticamente riconfigurato per cadere tutti pacchetti dal bersaglio tramite un filtro di pacchetto locale.

- Lo scopo di questo è quello di dire ad un admin che l' ospite è stato rilevato.

IP Security

- IPSec protegge i dati a livello di pacchetto. Esso lavora nella rete bastaa sul modello OSI e le applicazioni non sono a conoscenza di esso.

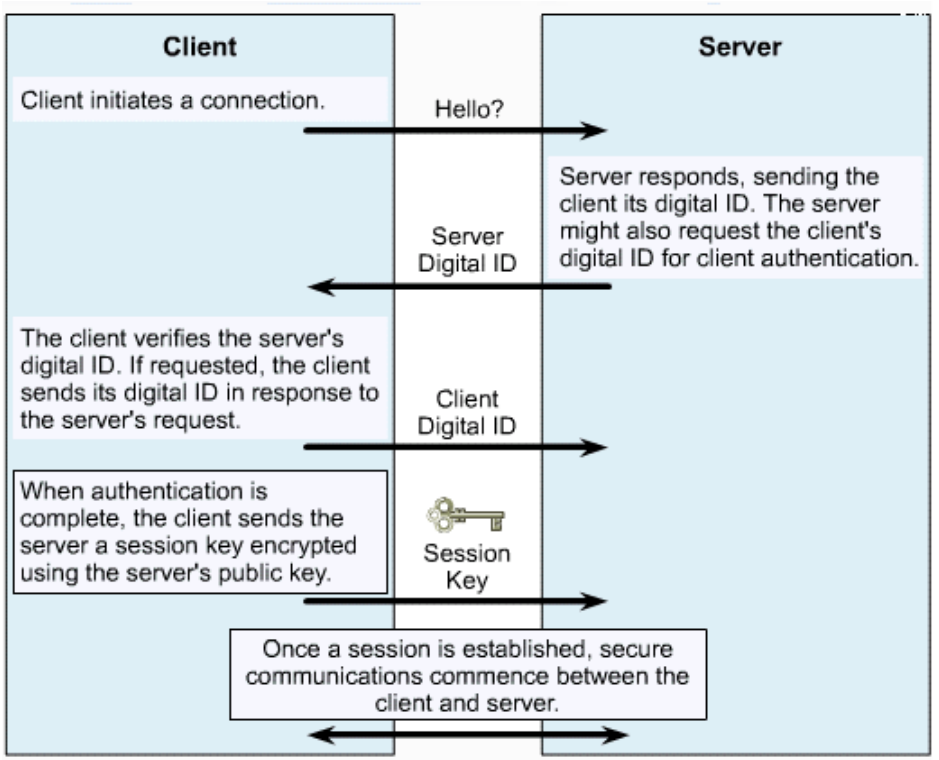


- La suite di IPSec comprende i protocolli AH e ESP. Possono essere utilizzati separatamente o insieme.

- L'Authentication Header (AH) permette la verifica della l'identità del mittente.

- Encapsulating Security Payload (ESP) assicura autenticazione e la riservatezza dei dati stessi.

- IPSec può funzionare in entrambe le modalità : modalità di trasporto (host-tohost) o la modalità tunnel (gateway-to-gateway)



- SSL è stato sviluppato da Netscape per fornire sicurezza per il suo web browser.
- Esso utilizza pubblica e privata chiave crittografia.
- SSL opera con l'applicazione layer e deve essere sostenuto dall' applicazione utente.

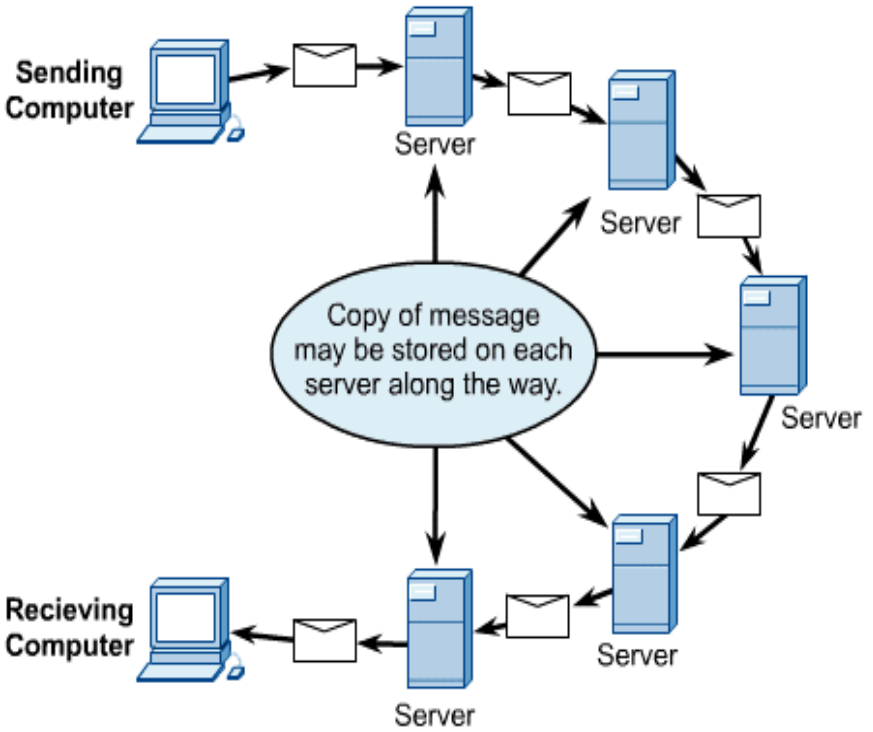
SSL (Secure Socket Layer) ≠ SSH (Secure Shell)

E-mail Security

- Utenti di posta elettronica pensano di avere la stessa aspettativa di privacy durante l'invio di e-mail come fanno quando si invia un lettera attraverso la posta servizio.

- Una previsione più accurata sarebbe assumere che la e-mail è come una cartolina che può essere letto da chiunque durante il su viaggi dal mittente al destinatario.

- Viaggiano spesso attraverso decine di nodi o server dal mittente al destinatario.



- I programmi di protezione di posta elettronica più diffusi sono PGP (Pretty Good Privacy), Kerberos, Fuoco Trust e MailMarshal

Schema of Typical Internet Communication

PGP

by Marián Stach, Slovakia

August 2002

6 Characteristic *message-digest* she cypher with *her private key* by *assymetrical algorithm*. She creates the *digital signature* of this message. She can add the time-stamp or ever her photo, if she wants to.

5 At first, Alice proceed the original unciphered message through *hash CRC algorithm* and gets its unique *message-digest*.

And what will Bill do? S the first he will decrypt *one-time key*: he will pass it by *assymetrical algorithm* with his private key. He will get used *one-time key* and he can decrypt the *message* now. To verify the message, he will pass the message through *hash algorithm* and he will create its *message-digest*. This he will compare with *message-digest* he decrypted from Alice's *digital signature*: all he has to do is decrypt it using *assymetrical algorithm* and Alice *public key*. When they match, the message is authentic and unmodified. As you can see, the whole system is really unbreakable – if the private keys stays really private.

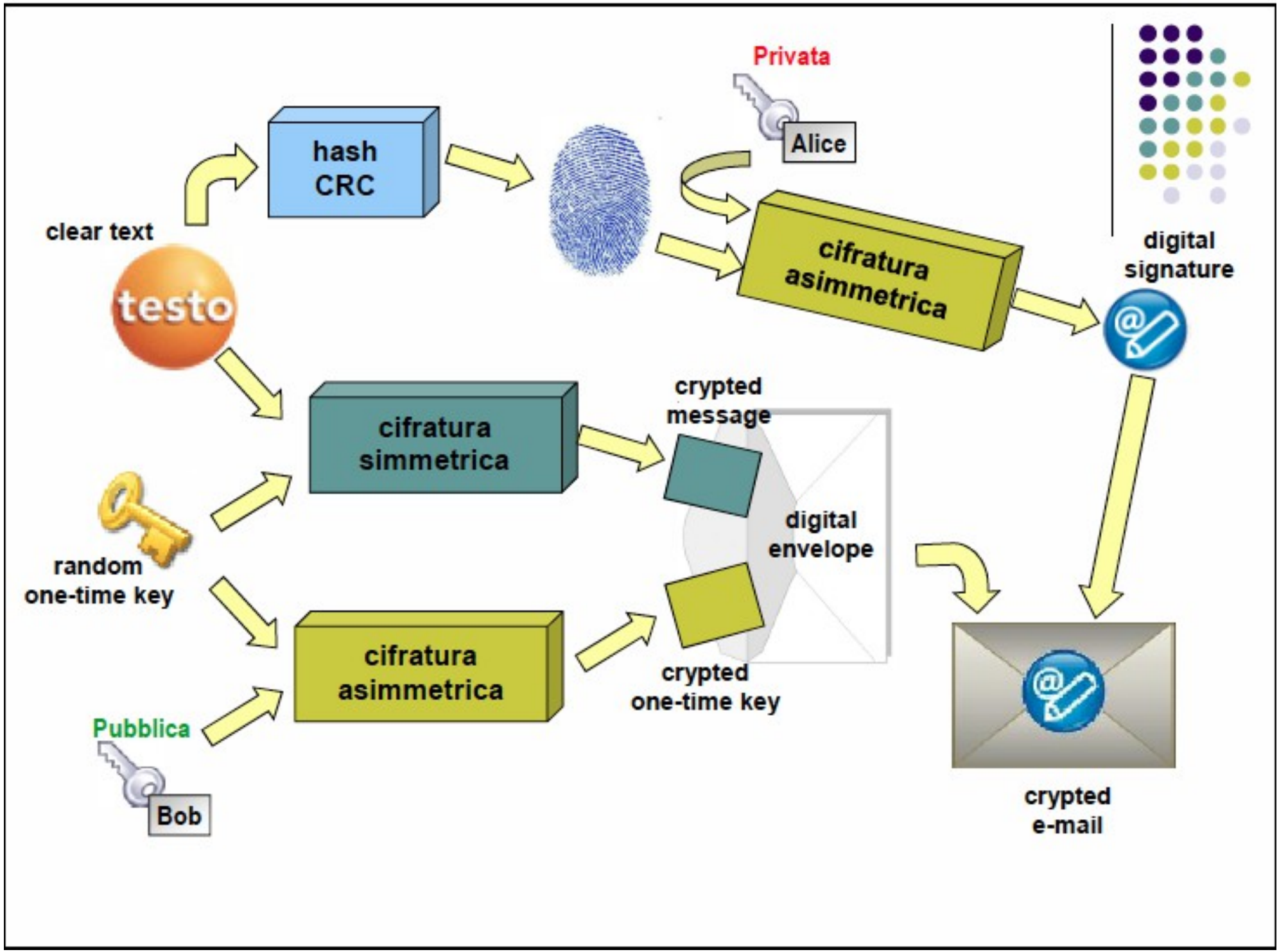
7 *Digital envelope* Alice seals with *digital signature* and finally send it to Bob. He will get everything necessary to decrypt and verify.

2 She crypts the message by *symmetric algorithn* using *the generated one-time key*. The *message* is safely crypted now.

4 *Chaotic babel of characters* (*crypted message*) and *crypted one-time key* she put into envelope. It can be send now, but how can Bob trust that message really comes from Alice? And that the message is unmodified? So she creates its *digital signature*.

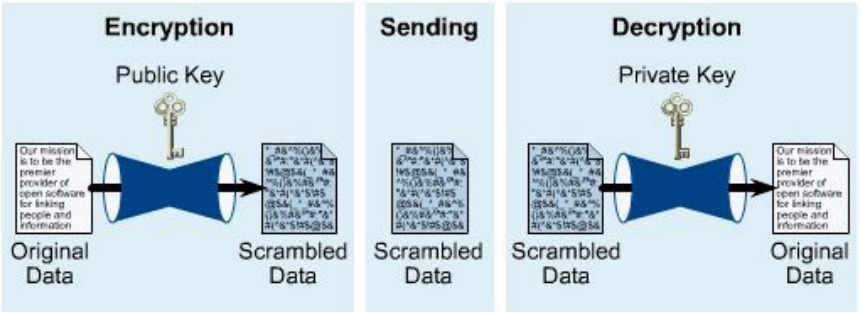
1 Alice writes the message. She will need a key to cipher it. Because they will be sent both, it is safest to generate a *random key for this one-time use only*. Even when catched, it will be useless later.

3 Bob will need the one-time key which Alice used to crypt the *message*. But paranoid Alice will not send it directly, because anywone who catch it can read the message. So she crypt it by *assymetric algorithm* using Bob's public key. This is accessible to everyone. She can be sure that only Bob can decrypt the *one-time key* using his private key.


Privata
Alice
hash
CRC
clear text
testo
cifratura
asimmetrica
digital
signature
cifratura
simmetrica
crypted
message
digital
envelope
random
one-time key
cifratura
asimmetrica
crypted
one-time key
Pubblica
Bob
crypted
e-mail

Public/Private Key Encryption

- Una chiave è pubblicato ed è ampiamente disponibile.
- L'altra chiave è privata e nota solo all'utente.
- Entrambe le chiavi sono tenuti a completare il sicur comunicazione.
- Questo tipo di codifica, è indicato anche come asimmetrica crittografia.
- Con questo tipo di crittografia, ogni utente ha sia una pubblic e una chiave privata, chiamato una coppia di chiavi.



Attacco informatico al sito dell'Aduc

NEWS
10/4/2012

Proposta Ue: sanzioni per chi vende e utilizza strumenti di hacking

La ratifica della proposta di «Direttiva contro gli attacchi informatici» dovrebbe arrivare entro l'estate. Ma c'è chi teme che questo possa avere dan controi- dicazioni, come la limitazione dell'attività di ricerca degli esp sicur

Virus all'attacco di 600mila Apple

E' Flashback l'ultima minaccia ai Mac

Per la McAfee, un gigante della protezione da attacchi informatici, ormai "gli hacker si muovono con rinnovato vigore verso il mondo Mac". L'ultimo trojan, in particolare, è stato portato alla luce lunedì da F-Secure. Il grosso dei Mac attaccati sarebb

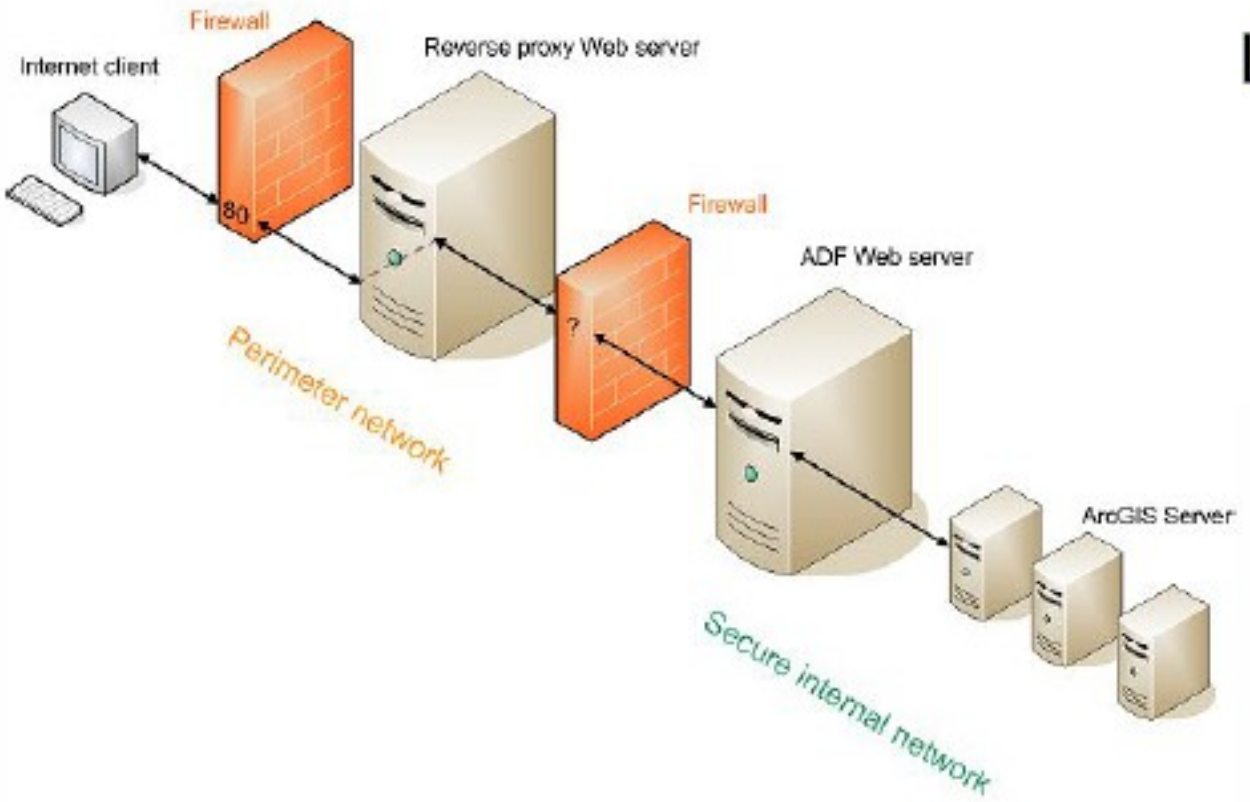
e Canada

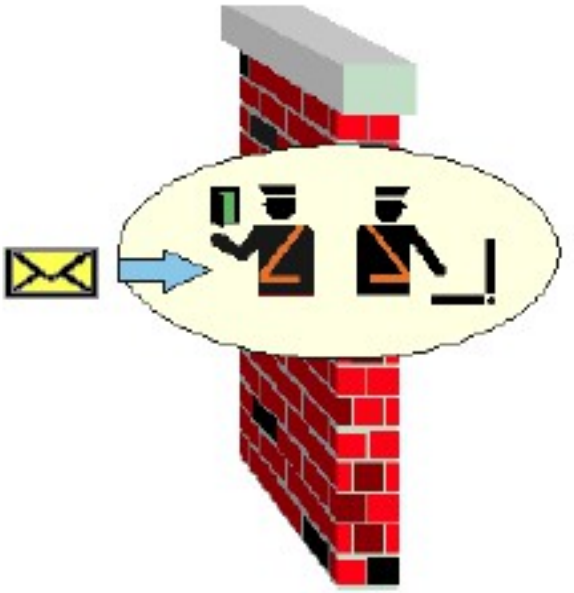
Arriva il CISPA, benvenuti nel regno del Grande Fratello

Cyber Intelligence Sharing and Protection Act of 2011

Full title	To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes. – H.R. 3523
Acronym	CISPA

Firewalls


Firewall
Internet client
Reverse proxy Web server
80
Firewall
ADF Web server
?
Perimeter network
ArcGIS Server
Secure internal network



Introduction to Firewalls and Proxies

- Un firewall è un software specializzato, hardware, o una combinazione dei due, il cui scopo è di prevenire indesiderati o dannosi Pacchetti IP e di raggiungere una rete sicura.

- In genere, un firewall Internet è un software di filtraggio di un host ip packet, accordato ad uno specifico insieme di regole.

- Per esempio, un pacchetto intercetta un particolare indirizzo sorgente che può essere lasciato cadere, inoltrato, o trasformato in qualche modo speciale.

- I primi firewall filtravano i pacchetti sulla base di indirizzamento . Oggi i criteri comuni di corrispondenza sono:

  - Indirizzo IP, l'origine e la destinazione

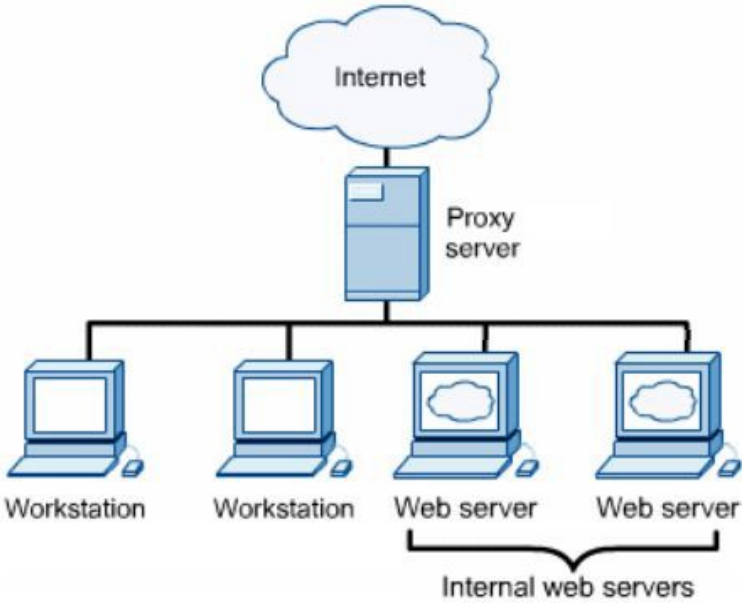
  - Numero porta TCP / UDP, entrambi di origine e di destinazione

  - Protocolli di livello superiore, HTTP, FTP, e così via.

- Questo approccio è indicato anche come l'inoltro basato su regole.

Introduction to Firewalls and Proxies

- Un proxy è un software che interagisce con le reti esterne per conto di un host client.
- Tipicamente, client hosts su una richiesta LAN sicura di una pagina Web da un server che esegue servizi di proxy.
- Il server proxy quindi si adopera su Internet per recuperare la pagina web.
- La pagina Web viene quindi copiato negli server proxy, questo viene indicato come caching.
- Infine, il server proxy trasmette la pagina web al client.



Introduction to Firewalls and Proxies

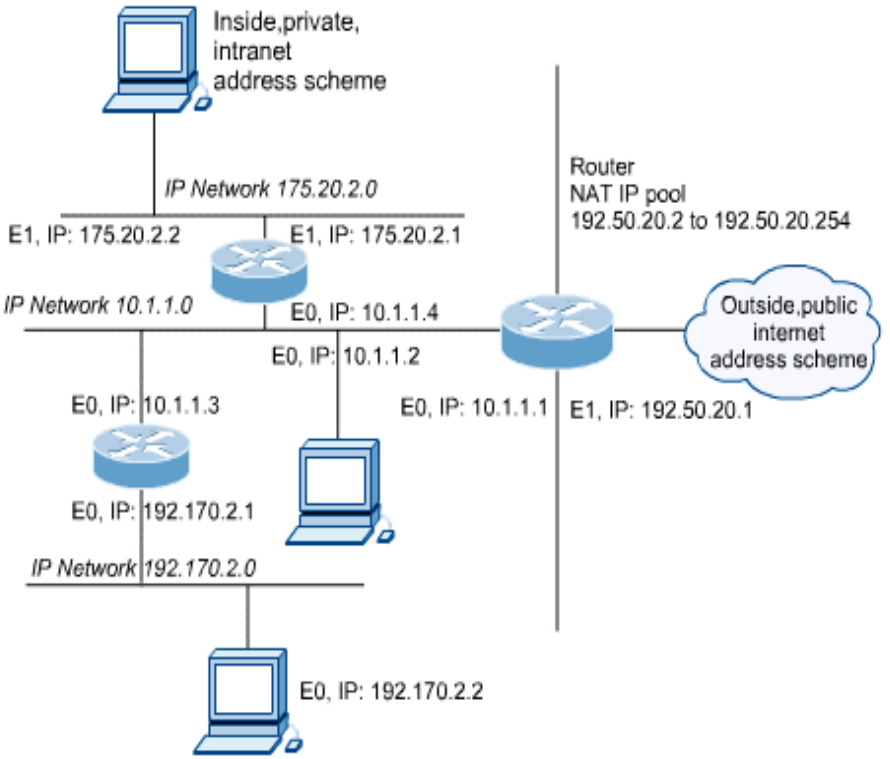
- Gli amministratori utilizzano Network Address Translation (NAT) per alterare indirizzi sorgente dei pacchetti provenienti da una LAN sicura.

- Questo permette rete sicura LAN da affrontare con IP privato.

- Gli indirizzi IP privati non vengono instradati su Internet.

- Un hacker esterno non può raggiungere direttamente un computer con un indirizzo privato.

- Alcuni esperti fanno una distinzione tra NAT e firewall. Altri guardano NAT come incluso il firewall.



- La soluzione firewall di base è un filtro di pacchetto IP.

- Per configurare un filtro di pacchetti, un amministratore di rete deve definire le regole che descrivono come gestire i pacchetti specificati.

- I primi filtri di pacchetti filtrano basandosi su informazioni sull' indirizzamento contenute nell'intestazione del pacchetto (step 3)

- Più tardi, filtri di pacchetti sono stati progettati per basare le decisioni su informazioni contenute nel TCP o UDP intestazione a livello 4.

```
#Clear all rules
/sbin/ipfw -f flush

#Deny Routing Information Protocol on UDP port 520
/sbin/ipfw add deny udp from any 520 to any 520 via xl0

#Send all packets to the NAT Daemon for address translation
/sbin/ipfw add divert and all from any to any via xl0

#Allow specific hosts access
/sbin/ipfw add allow ip from 172.17.4.5 to any
/sbin/ipfw add allow ip from 172.17.87.52 to any

#Allow Web Requests
/sbin/ipfw add allow tcp from any to 192.168.54.198 80

#Deny everything else to 192.168.54.0/24 network
/sbin/ipfw add deny ip from any to 192.168.54.0/24

#Permit the rest
/sbin/ipfw add permit ip from any to any
```

Packet Filtering

- Layer 4 access lists , possono essere configurati per consentire o negare pacchetti.

- Il firewall può anche essere configurato per esaminare il codice TCP bit, analizzando il three-way handshake e mantenendo non invitato fuori traffico (filtraggio del traffico di collegamento).

- Firewall deve indovinare a quale traffico senza connessione (es: IP, ICMP, UTP) è invitato e ciò che il traffico senza connessione non è.

- Ping ICMP non utilizza un livello 4 di intestazione. Non vi è alcun modo per determinare se un datagramma è parte di una connessione stabilita. Questo perché IP e UDP sono entrambi connectionless.

- Firewall intelligenti monitorano il traffico senza connessione notando IP e la sorgente e la destinazione UDP porti in una tabella, e la rilevazione del traffico connectionless che sembra che è invitato (stateful packet filtering). Tali firewall sono dinamici.

Packet Filtering

- La forma più completa di filtraggio dei pacchetti esamina Layer 3 e 4, e il layer 7 di dati delle applicazioni di livello .

- Layer 7 firewall cercare modelli nel payload del pacchetto.

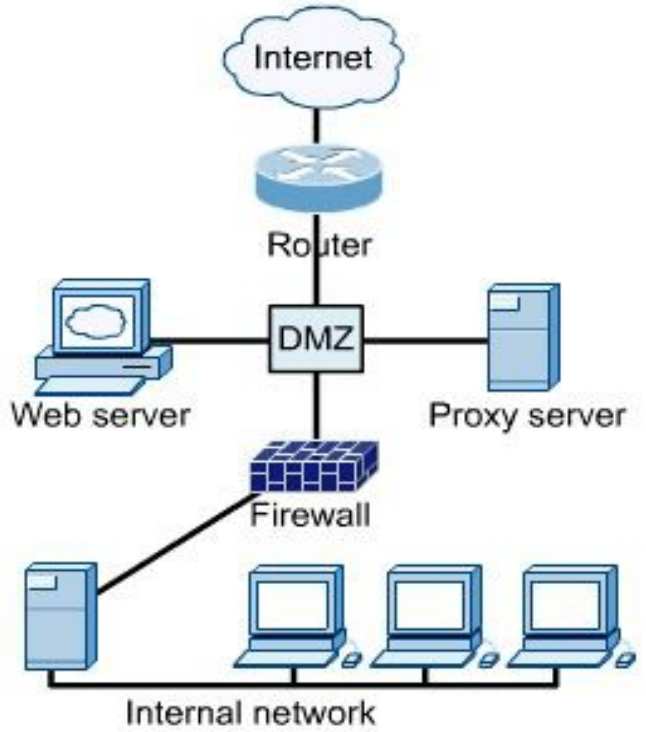
- Questo viene fatto nel tentativo di determinare quale applicazione è in fase di utilizzati, come ad esempio HTTP, FTP, e così via (step 7 packet inspection filtraggio).

- Essi lavorano con il software che è programmato per riconoscere una data applicazione. Pertanto, non tutte le applicazioni saranno supportato.

- Questo tipo di filtraggio pacchetti aggiunge una quantità significativa di ritardo e overhead al processo di routing.

Firewall Placement

- Un router collega il confine LAN aziendale al suo ISP o il Internet.
- Il router di confine solo dovrebbe consentire HTTP, FTP, posta e DNS relativo traffico alla DMZ.
- La DMZ è progettato per mantenere il all'interno della rete pulito.
- I server NAS nella DMZ devono essere accuratamente configurato.



Common Firewall Solutions

- Un appliance è un dispositivo che è autonomo e facile da configurare
- L'appliance firewall più popolari è il Cisco PIX. Esso comprende NAT e stateful packet filtering.

- Il PIX Firewall 515 utilizza TFTP per image scaricare e aggiornare.
- Ha un design a basso profilo, 128.000 sessioni simultanee, e 170 Mbps di throughput.
- Le impostazioni predefinite consentono tutte le connessioni dall'interno accesso all'interfaccia all'esterno interfaccia, e bloccare tutto il collegamento dall'esterno all'interno.

Cisco ASA 5500 Series
§ da 4.000 a 150.000 simultaneous sessions
§ da 150 Mbps a 10 GBbps throughput
§ IPSec VPN capability

Using a NOS as a Firewall

- In ambienti ad alto traffico, filtrando un pacchetto specializzato e la soluzione di NAT è raccomandato.
- Un dispositivo come un apparecchio router o firewall è progettato per passare i pacchetti e manipolare rapidamente.
- A NOS in esecuzione su hardware ordinaria possono essere in grado di fare la stesso lavoro. Tuttavia, non è senza aggiungere latenza e sovraccarico sul server.
- In ambienti a basso traffico, come piccoli uffici e casa reti, una soluzione firewall NOS è una buona scelta.
- Linux può usare ipchains e iptables per agire come un gateway tra una rete privata e Internet, in modo da fornendo funzionalità di firewall.

Using a NOS as a Firewall

- **netfilter** è un componente del kernel di Linux che permette l'intercettazione e la manipolazione dei pacchetti che attraversano il computer (svolge funzioni di firewall).
- **iptables** è il programma che permette di configurare netfilter.
- iptables raggruppa tutti i controlli che può fare sul traffico in entrata nella cosiddetta *INPUT Chain*. I controlli sul traffico in uscita sono invece raggruppati nella *OUTPUT Chain*. La *FORWARD Chain* serve per il traffico non indirizzato a noi ma che comunque passa per il nostro computer.
- Ognuna di queste catene ha una *policy*, cioè un'azione predefinita da eseguire quando tutti gli altri controlli della catena hanno fallito nel riconoscere se il dato era buono o meno.

Using a NOS as a Firewall

- I valori di policy possono essere:

  ACCEPT lascia passare il pacchetto

  DROP scarta il pacchetto

  QUEUE dirotta il pacchetto nello spazio utente per un'analisi succ.

  RETURN viene eseguita la regola di default della catena

- Una catena (che ha la forma di una Access Control List) è composta da una serie di regole suddivise in

  match condizione da verificare

  target azione da intraprendere se il pacchetto soddisfa il match

- La policy, detta anche regola di **default**, viene eseguita quando nessun match precedente è verificato

Using a NOS as a Firewall

```
$ sudo iptables -L                    list the rules in the chains
```

```
Chain INPUT (policy ACCEPT)
target prot opt source          destination
Chain FORWARD (policy ACCEPT)
target prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target prot opt source          destination
```

- Di default, iptables lascia passare tutto, quindi per prima cosa blocchiamo il traffico:

```
$ sudo iptables -P INPUT DROP
$ sudo iptables -P FORWARD DROP      change the policy in a chain
```

```
Chain INPUT (policy DROP)
target prot opt source          destination
Chain FORWARD (policy DROP)
target prot opt source          destination
```

Using a NOS as a Firewall

- consentiamo tutto il traffico interno al nostro computer, che passa per l'interfaccia di loopback (**lo**).

```
$ sudo iptables -A INPUT -i lo -j ACCEPT
```
append a rule to a chain

`-A INPUT` aggiunge una nuova regola alla catena INPUT

`-i lo` il nome dell'interfaccia da cui ricevere i pacchetti

`-j ACCEPT` l'obiettivo della regola

- consentiamo la navigazione e il traffico da noi richiesto

```
$ sudo iptables -m state --state ESTABLISHED,RELATED -j ACCEPT
```

`-m state` aggiunge una nuova regola alla catena INPUT

`--state` x,y se i pacchetti sono nello stato ESTABLISHED (associato ad una connessione) o RELATED (nuova connessione associata ad un'altra)

`-j ACCEPT` l'obiettivo della regola

Using a NOS as a Firewall

- consentiamo il traffico entrante di tipo SSH (porta 22)

```
$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

`-p tcp` il protocollo da controllare

`--dport 22` il port di destinazione da controllare

- consentiamo l'accesso ad un server web interno

```
$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

- scartiamo il traffico ICMP proveniente dall'host 88.11.22.33

```
$ sudo iptables -A INPUT -p icmp -s 88.11.22.33 -j DROP
```

Using a NOS as a Firewall

- vediamo la situazione risultante:

```
$ sudo iptables -vv -L
```

```
Chain INPUT (policy DROP)
target prot opt in  out source   destination
ACCEPT all  --- lo  any anywhere anywhere
ACCEPT all  --  any any anywhere anywhere state RELATED, ESTABLISHED
ACCEPT tcp  --  any any anywhere anywhere tcp dpt:ssh
ACCEPT tcp  --  any any anywhere anywhere tcp dpt:www
DROP   icmp --  any any 88.11.22.33  anywhere

Chain FORWARD (policy DROP)
target prot opt in  out source   destination

Chain OUTPUT (policy ACCEPT)
target prot opt in  out source   destination
```

Using a NOS as a Firewall

- altre opzioni del comando iptables
  - -N crea una nuova catena
  - -X rimuove una catena vuota
  - -P cambia la policy di una catena
  - -L elenca le regole di una catena (o di tutte)
  - -Z azzera i contatori di pacchetti e di byte di tute le regole
  - -A aggiunge una nuova regola in coda alla catena
  - -I aggiunge una nuova regola in un dato posto della catena
  - -R sostituisce la regola posizionata in un dato posto della catena
  - -vv output di tipo verbose

ufw: iptables and Ubuntu

- abilitiamo l'uso di ufw

```
$ sudo ufw enable
```

- per aprire il servizio in una porta (SSH)

```
$ sudo ufw allow 22
```

- per consentire l'accesso ad un server web interno

```
$ sudo ufw allow 80
```

- per scartare il traffico ICMP proveniente da 88.11.22.33

```
$ sudo ufw drop proto icmp from 88.11.22.33 to any port
```