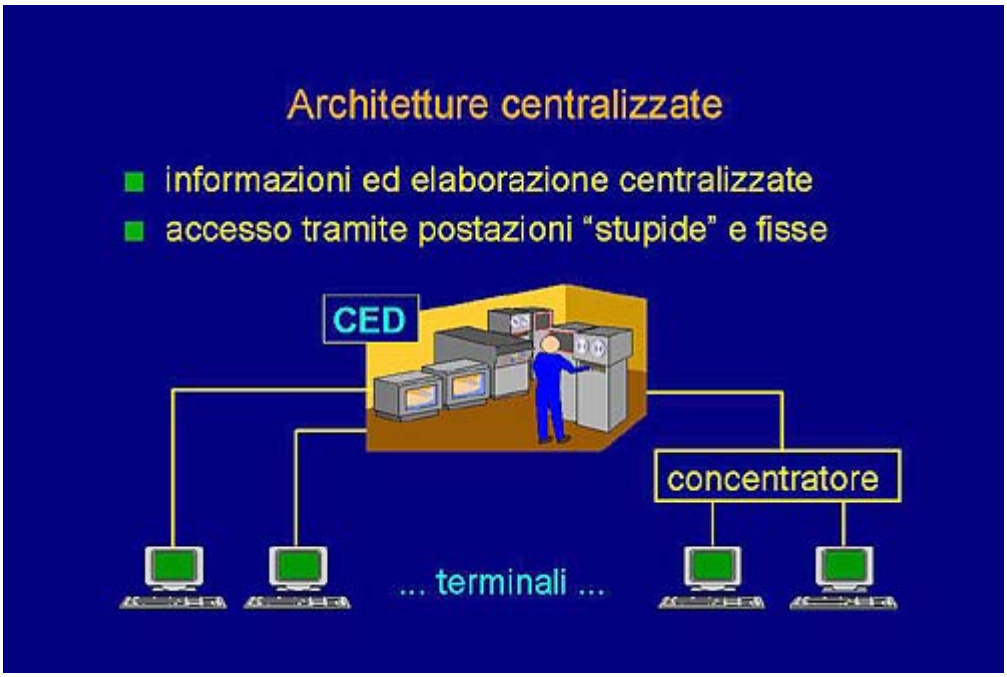
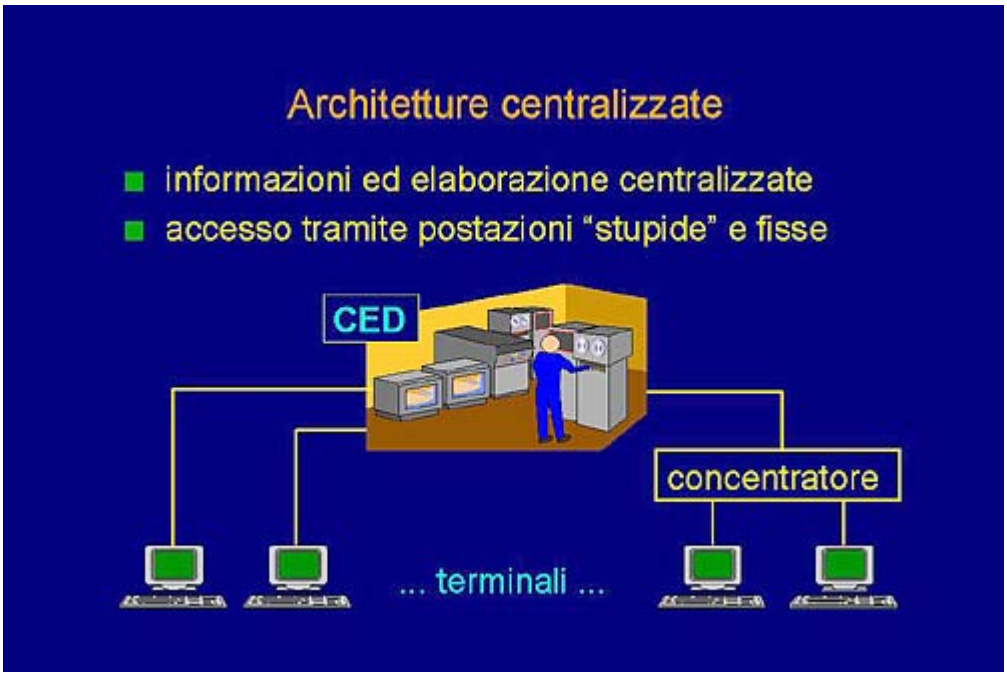
La sicurezza nelle reti
Architetture centralizzate (1)



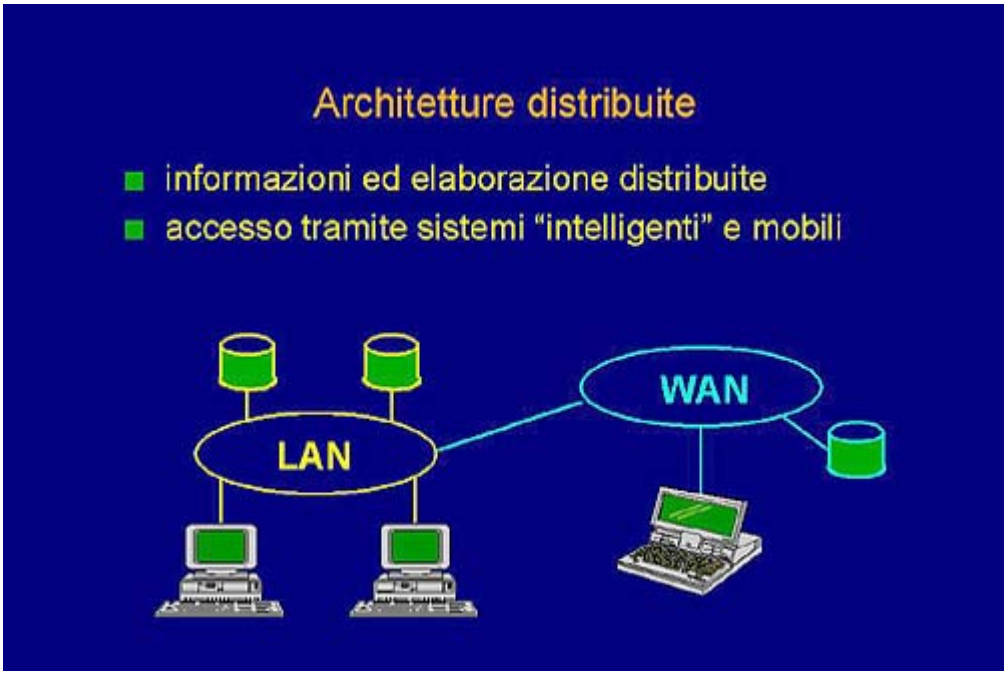
Benvenuti al modulo di sicurezza dei sistemi distribuiti. Io sono il Professor Antonio Lioy del Politecnico di Torino e mi occupo, come tema di ricerca ed anche di insegnamento, di sicurezza delle reti e dei sistemi informativi. In questa prima parte, noi tratteremo specificamente delle problematiche generali di sicurezza negli attuali sistemi informatici. In particolare, ci sono due grandi categorie di sistemi informatici che vengono utilizzati ampiamente da tanti enti e da tante organizzazioni. La prima architettura che andiamo a considerare è l'architettura centralizzata. In questo tipo di architetture tipicamente si ha un Centro di Elaborazione Dati (CED), che normalmente viene mantenuto in un luogo sotterraneo o protetto fisicamente, ad esempio, da porte blindate e accessi controllati, dentro cui sono conservate tutte le unità di elaborazione e tutte le unità di memorizzazione dei dati. Gli utenti accedono e sfruttano queste risorse informatiche tramite dei terminali, cioè dispositivi di input e output nei confronti del sistema di elaborazione; quindi una tastiera ed un video, non un vero e proprio Personal Computer o una work-station.

Architetture centralizzate (2)



La sicurezza di un sistema di questo genere è in gran parte affidata alla sicurezza fisica del sistema complessivo; infatti l'accesso alle strutture di calcolo e di memorizzazione dei dati è protetto fisicamente dal locale dentro cui si trovano e gli utenti non possono in alcun modo svolgere degli attacchi attivi. Anche il tipo di collegamento che viene fatto tra la postazione di lavoro dell'utente e il sistema di elaborazione è, bene o male, fisicamente protetto, perché si tratta di un cavo che corre dalla postazione di lavoro fino al sotterraneo dove sono testati i sistemi di elaborazione. Anche nel caso in cui ci sia una sede remota, quindi non sia possibile far correre direttamente un cavo dal terminale al sistema di elaborazione, anche questa architettura è protetta fisicamente, perché tutti i terminali vengono portati, con un collegamento, su un concentratore e da questo c'è poi una linea dedicata che va al sistema di elaborazione. Riassumendo, nelle architetture di tipo centralizzato la sicurezza è di tipo fisico o, al massimo, del sistema operativo del sistema di elaborazione e gli utenti hanno a disposizione dei meri dispositivi di input/output.

Architetture distribuite



Molto diversa è la situazione nel caso delle architetture più recenti, le cosiddette architetture distribuite. In queste architetture gran parte dei presupposti che abbiamo appena enunciato non sono più validi. Innanzitutto non è più vero che tutti i sistemi di elaborazione e di memorizzazione sono conservati in un unico locale, anzi tipicamente, come si vede qui illustrato, i sistemi sono sparsi, sia all'interno di una rete locale (LAN) ma anche su una rete geografica (WAN), diventa quindi difficile controllare fisicamente tutti quanti i sistemi. Inoltre, le postazioni di lavoro dell'utente non sono più delle semplici postazioni di input/output, ma sono delle postazioni di lavoro complesse, sono tipicamente dei Personal Computer, ossia hanno una capacità di elaborazione autonoma ed indipendente dai sistemi cui ci si collega. Questo vuol dire che l'utente del nostro sistema di elaborazione non può soltanto svolgere operazioni di input/output, ma ha anche la possibilità di attivare localmente, presso la sua stazione di lavoro, dei programmi. Questi potrebbero essere dei programmi di attacco, cioè che inficiano la sicurezza del sistema complessivo. La protezione fisica di tutti questi elementi di elaborazione non è, ovviamente, possibile ed inoltre c'è il problema dei computer mobili: i computer portatili si stanno diffondendo sempre di più e quindi diventa molto difficile riuscire ad offrire una protezione fisica, dato che questi sistemi si collegano e si scollegano alla rete in vari punti, sia all'interno della nostra rete locale, sia, nel caso di personale che stia viaggiando, da vari punti dell'Italia, se non addirittura dell'intero pianeta, tramite Internet. È quindi chiaro che, per architetture di tipo distribuito, bisogna ripensare completamente alla sicurezza, in modo tale che sia indipendente dalla locazione fisica dei sistemi di elaborazione e sia indipendente anche dalle reti a cui ci colleghiamo. È quindi sempre meno ipotizzabile il fatto che un certo nodo di elaborazione sia sempre collegato al medesimo tipo di rete.

Sicurezza: dove è il nemico? (1)

Se dobbiamo mettere in piedi un sistema di sicurezza, una delle cose più importanti è identificare dove si trova il nemico da cui vogliamo difenderci. In generale possiamo fare tre ipotesi: possiamo supporre che noi siamo i buoni ed i cattivi stiano fuori dalla nostra organizzazione. In questa ipotesi ciò che bisogna fare è cercare di proteggere la nostra rete dalle intrusioni che potrebbero provenire dall'esterno. È questo il caso tipico in cui trovano applicazione i cosiddetti firewall, letteralmente muri taglia-fuoco, porte antincendio, cioè evitano che l'incendio, la pericolosità insita nella rete esterna, si propaghi anche nella nostra rete interna. Purtroppo questa ipotesi, che i cattivi stiano fuori dalla nostra organizzazione, trova sempre meno corrispondenza nella realtà: le conoscenze informatiche si stanno diffondendo a tutti i livelli, ma soprattutto si stanno diffondendo sempre di più dei semplicissimi programmini di attacco che possono essere utilizzati anche da persone non

esperte. Bisogna quindi considerare, almeno a livello teorico, ma molto spesso anche pratico, l'ipotesi che all'interno della nostra organizzazione ci sia qualcuno che, per vari motivi che si possono facilmente immaginare, possa volere attaccare il sistema dall'interno. Quindi, la messa in opera di un sistema di tipo firewall non è più sufficiente, bisogna riuscire a fare protezione della rete locale o della Intranet.

Sicurezza: dove è il nemico? (2)

Questo ci causa un problema, perché sia la rete locale sia la Intranet tipicamente sono costruite con dei sistemi che sono stati ideati per facilitare la collaborazione fra le persone ed invece la sicurezza tende ad impedire, o quantomeno a limitare, la collaborazione. Inoltre, nel caso che il nostro personale sia in viaggio, in trasferta, all'esterno della nostra rete, non si riesce più a farlo interoperare correttamente con tutti i sistemi. Da queste considerazioni deriva la conseguenza che l'unica soluzione applicabile, in generale, in maniera completamente indipendente dalla rete a cui il nostro personale è collegato, è la protezione delle applicazioni: siccome le applicazioni sono a livello più elevato dello stack di rete, sono le uniche ad essere completamente indipendenti dalla rete sottostante. Se noi riusciamo a proteggere le nostre applicazioni, abbiamo reso il sistema sicuro, indipendentemente dalle reti che attraversiamo e dalle postazioni di lavoro dove operiamo.

Autenticazione semplice

Introduciamo la terminologia di base della sicurezza informatica, il cosiddetto gergo di sicurezza, che useremo esplicitamente in questa lezione e nelle prossime. Si parla di autenticazione, ed in particolare di autenticazione semplice, ogniqualvolta un utente desidera accedere ad un sistema di elaborazione. In questo caso, noi abbiamo questa persona che, nonostante rivesta l'identità di Barbara, pretende di essere una persona diversa, pretende di essere Alice. È chiaro che un corretto sistema di autenticazione non deve credere ciecamente a quello che l'utente dice di essere, ma deve chiedere una prova formale. Per ottenere questa prova formale si useranno dei sistemi di autenticazione precisi, esatti e soprattutto non falsificabili facilmente. Questo è il tipico modo di autenticazione a cui siamo abituati: normalmente infatti quando ci presentiamo ad un sistema di elaborazione ci viene chiesto Username e Password; vedremo in seguito che questo tipico modo di autenticazione è fortemente sconsigliato, perché altamente insicuro.

Mutua autenticazione

Si parla anche di mutua-autenticazione, che corrisponde alla situazione mostrata in questa slide: non soltanto l'utente deve presentarsi nei confronti del sistema, ma l'utente potrebbe avere un ragionevole dubbio che il sistema cui lui sta facendo il collegamento, non sia quello a cui desidererebbe collegarsi. Questo perché è possibile, abbastanza facilmente, mettere in piedi una rete di calcolatori, i cosiddetti server-ombra, o anche server-fantasmi, shadow-server, i quali con tecniche opportune, che illustreremo in seguito, mostrano un'interfaccia simile a quella del sistema originale e quindi sarebbero in grado di fornirci dei dati sbagliati, mentre noi in assoluta buona fede crediamo di esserci collegati al sistema giusto. Questa è una caratteristica che manca normalmente nei correnti sistemi, sia di tipo centralizzato sia di tipo distribuito.

Autorizzazione

Una volta che abbiamo fatto l'autenticazione degli utenti e dei sistemi a cui si stanno collegando, bisogna decidere se questi utenti, o questi sistemi, hanno diritto a svolgere certe operazioni. In gergo informatico si parla quindi di autorizzazione per decidere se, in base ai dati di autenticazione che sono stati forniti, è lecito ottenere il controllo di un certo oggetto o attivare una certa procedura di elaborazione. In questo caso la signorina chiede di poter aprire il box elettronico, controllato dal computer, per prelevare questa bella automobile; il computer ha il ragionevole dubbio che non basta la sua identità o la sua parola per far prendere questa bella auto e farsi un giro.

Riservatezza

Un'altra proprietà di sicurezza rilevante nei sistemi informativi è la riservatezza. Con la riservatezza si intende il fatto che una comunicazione, o comunque dei dati memorizzati all'interno di un sistema di elaborazione, non possano essere visualizzati, catturati, da persone che non hanno diritto di accedere a questi dati. In questa slide noi abbiamo una comunicazione tra due persone che intendevano mantenerla riservata soltanto tra loro due, ma come spesso capita, una terza persona che sia in mezzo fisicamente, o dal punto di vista logico, di questa comunicazione, è sicuramente in grado di intercettarla, se questa non è stata protetta con opportuni codici di riservatezza.

Integrità (1)

Un'altra proprietà che noi desideriamo avere all'interno di un sistema sicuro è la cosiddetta integrità dei dati. Intuitivamente è abbastanza facile da capire che cos'è l'integrità: evitare delle modifiche, ma in realtà non è questa l'unica accezione. Supponiamo di aver ricevuto un ordine di pagamento di 1.000 Euro. Questo ordine di pagamento, mentre transita in rete, potrebbe essere modificato in vario

modo: ad esempio se è un assegno che sta arrivando a me, io potrei avere interesse ad aggiungerci un semplicissimo zero per trasformare la cifra da 1.000 a 10.000 Euro. Ma, nel caso in cui il pagamento sia destinato ad una persona, che mi sta cordialmente antipatica, quello che io posso fare è cancellare uno o più zeri, ad esempio trasformando l'ordine da 1.000 Euro a soltanto 100 Euro. Ovviamente ci vogliono dei codici che prevengano questo genere di modifiche; fortunatamente tale compito risulta essere in genere abbastanza facile: è più difficile, ad esempio, rilevare degli attacchi all'integrità che comportino la cancellazione del messaggio, perché se il sistema ricevente non si aspettava di ricevere questo ordine di pagamento di 1.000 Euro, il fatto che qualcuno, durante il transito in rete di questo ordine, lo cancelli, non comporta nessun allarme automatico da parte del sistema ricevente. Bisogna quindi avere dei sistemi che siano in grado di rilevare se dei messaggi sono stati cancellati. Questo tipicamente viene fatto a livello applicativo, nel senso che quando ad esempio si manda un ordine di pagamento, si aspetta una conferma che il pagamento sia stato effettivamente ricevuto, ma a livello basso, a livello di pacchetti di rete, la cancellazione di pacchetti è una cosa che può anche essere dovuta a guasti di rete e quindi i sistemi non sanno bene distinguere un attacco da un semplice guasto.

Integrità (2)

Infine, anche nel caso che noi siamo riusciti a proteggere i nostri pacchetti da attacchi che tendano a modificarli o a cancellarli, esiste una terza categoria di attacchi all'integrità del sistema che è abbastanza pericolosa: sono gli attacchi di tipo replay. Anche se noi abbiamo protetto molto bene il nostro ordine di pagamento da 1.000 Euro, una persona che lavori all'interno della rete di elaborazione potrebbe semplicemente catturare quei bit e, in tempo successivo, rimetterli in circolo in rete. È una sorta di metodo sperimentale: io ho fatto un'osservazione, ho visto che quando passano quei bit in rete, di cui magari non capisco pienamente la sintassi e il significato, il mio conto corrente cresce di 1.000 Euro, allora se ho la possibilità di rimettere in gioco questi stessi bit, potrò far crescere nuovamente, per un numero di volte a piacere, il mio conto di altri 1.000 Euro. Quindi un altro tipo di attacco molto difficile da parare.

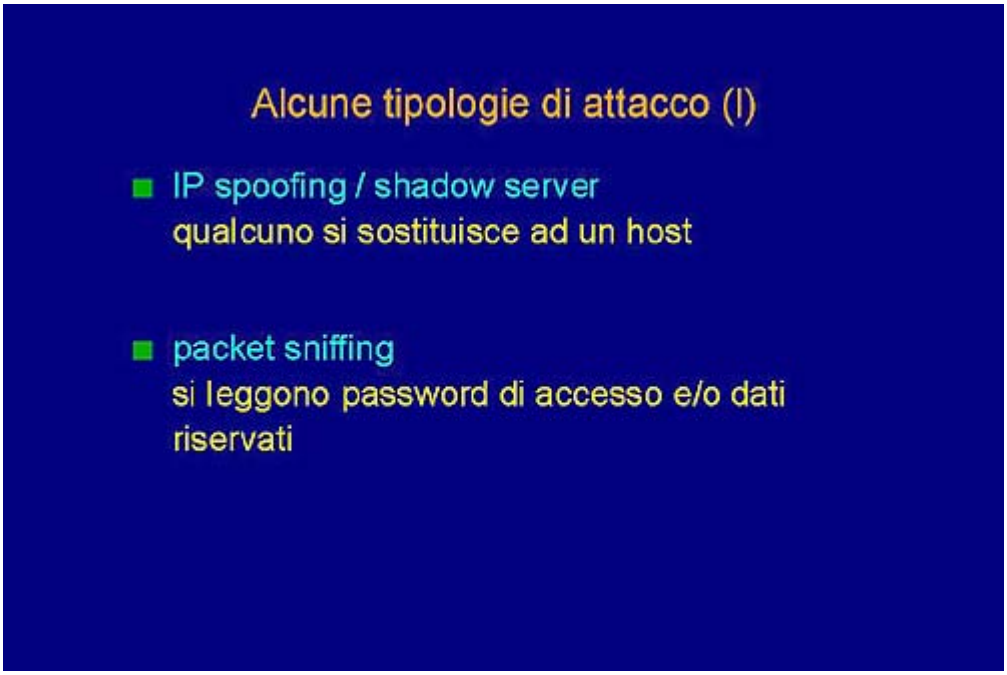
Tracciabilità e non ripudio

Altre proprietà di sicurezza desiderata all'interno di un sistema informativo sono: la tracciabilità e il non ripudio. Per tracciabilità si intende il fatto che quando una persona compie delle operazioni all'interno di un sistema di elaborazione, noi vorremmo poter essere in grado di seguire le sue orme, le sue tracce. Vorremmo poter essere in grado di evidenziare quali operazioni sono state compiute e da quali persone, all'interno del nostro sistema di elaborazione. Noi possiamo volerlo dimostrare sia in maniera informale, soltanto per dei nostri controlli interni, oppure vogliamo poter dimostrare le azioni che sono state compiute in modo inoppugnabile, ad esempio in modo che possa essere utilizzato anche come prova a carico o a discarico di un certo elemento, in tribunale. Quando le prove che noi adduciamo sono delle prove che sosterrebbero la verifica di un tribunale, normalmente si parla di non ripudio: ossia la persona in questione non può negare di aver svolto effettivamente un certo lavoro o una certa operazione.

Disponibilità

Una cosa spesso trascurata quando si parla di sicurezza, è il fatto che fa parte dell'ambito e della competenza del sistema di sicurezza anche garantire la disponibilità del sistema. Per disponibilità si intende che se c'è un certo sistema di elaborazione che deve svolgere un certo compito, che può anche essere molto delicato (in questo esempio vedete illustrata la situazione in cui questo sistema di elaborazione è preposto al controllo del traffico aereo, del traffico ferroviario, all'erogazione di denaro, al controllo di un impianto chimico) sicuramente il fatto che un sistema di questo genere non sia più in grado di svolgere le proprie funzioni potrebbe causare un danno anche molto rilevante.

Alcune tipologie di attacco (1)

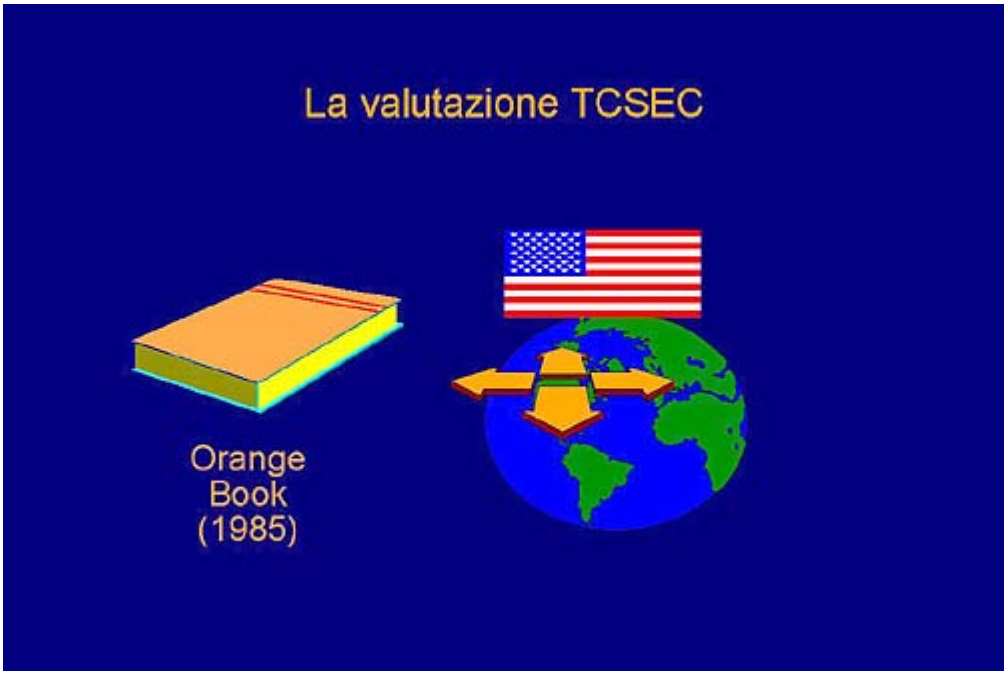


Parlando di sicurezza informatica si sentono molto spesso citare anche una serie di termini che riguardano degli attacchi specifici, che possono essere condotti contro i sistemi. In particolare, si parla di attacchi di tipo IP spoofing quando il nodo di elaborazione che sta conducendo l'attacco falsifica il proprio indirizzo IP, cioè il proprio indirizzo di rete, per far finta di essere un'altra macchina, tipicamente uno shadow-server o server-ombra. Si parla invece di packet sniffing, letteralmente annusamento dei pacchetti e quindi cattura dei pacchetti, quando un qualunque nodo di elaborazione collegato ad una rete di tipo broadcast, come sono in realtà gran parte delle reti locali, svolge delle operazioni di cattura dei pacchetti e quindi dei dati in essi contenuti, durante il loro transito davanti alla sua postazione di lavoro.

Alcune tipologie di attacco (2)

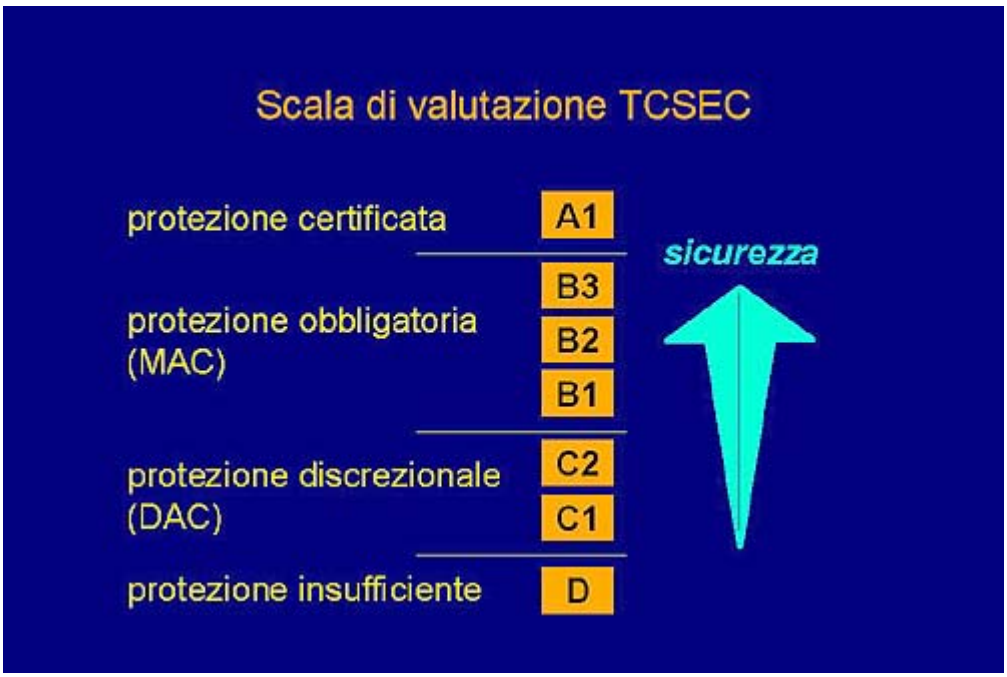
Ci sono poi degli attacchi ancora più raffinati: si parla di connection hijacking o di data spoofing quando un nodo di elaborazione non soltanto svolge un'operazione di cattura dei pacchetti che stanno transitando, ma addirittura emette dei pacchetti falsi all'interno di un collegamento già stabilito. Si parla invece di attacchi denial-of-service per quegli attacchi che sono mirati a togliere la disponibilità di un certo sistema informatico, tipicamente degli attacchi che portano al crash o al blocco di un sistema di elaborazione. Statisticamente si vede che la maggior parte degli attacchi informatici più banali vengono condotti semplicemente sfruttando bachi del software. Questo è un grosso problema: i normali sistemi informativi tendono ad essere sviluppati con sempre minor cura nella parte di sviluppo del software, questo perché c'è sempre maggior pressione per arrivare più in fretta alla nuova release del prodotto e i codici divengono sempre più grossi. Bisogna però ricordarsi che ogni baco software che è rimasto all'interno di un programma può essere sfruttato da un attaccante per conquistare o mettere in ginocchio il nostro sistema.

La valutazione TCSEC



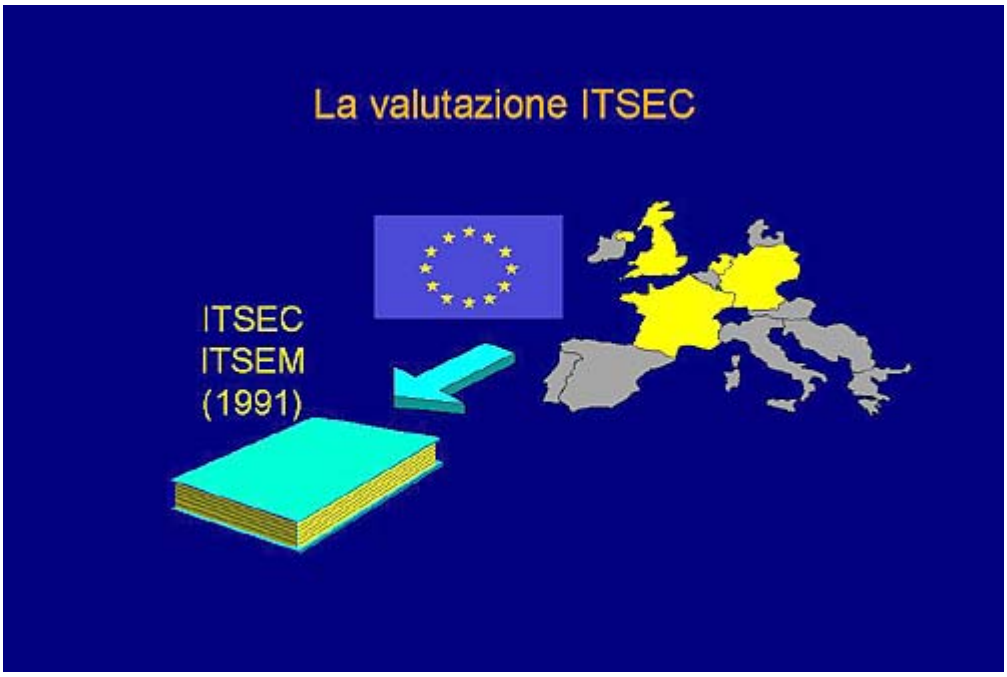
In generale, non è semplice riuscire a valutare la sicurezza di un sistema informativo: come ausilio per tale valutazione sono stati messi a punto dei criteri nazionali ed internazionali. Lo standard TCSEC è uno standard molto vecchio, del 1985, sviluppato dagli USA, per valutare la sicurezza dei sistemi che venivano venduti alla pubblica amministrazione americana non solo agli enti militari, ma anche agli enti civili statunitensi. Siccome questi criteri con cui valutare un sistema informatico sono stati pubblicati in un libro dalla copertina arancione, sono anche noti come Orange Book. Questo è stato appunto il primo tentativo di sistematicizzare la valutazione e la certificazione di sicurezza informatica e quindi dagli USA questa tecnologia si è rapidamente diffusa in tutto il mondo.

Scala di valutazione TCSEC



Il risultato di una valutazione di tipo TCSEC consiste in una classe, ossia il sistema che è stato valutato viene definito con uno dei seguenti tipi : D; C1, C2; B1, B2, B3; A1, a seconda del livello di sicurezza che il valutatore ha riscontrato nel sistema in esame. Come si vede dalla figura, la classe D non si nega a nessuno, è la classe in cui i sistemi hanno una protezione insufficiente. Le classi C, invece, vengono date ai sistemi dotati di protezione discrezionale o DAC (Discretionary Access Control), cioè il grado di protezione effettivo di questi sistemi dipende fortemente dalla loro configurazione, dalla loro manutenzione, quindi dalla operatività che il system-manager svolge su di essi. I sistemi nella classe B sono invece a protezione obbligatoria, vuol dire che il sistema operativo ha una serie di controlli intrinseci che non possono essere aggirati neanche dal system-manager; in questo senso la protezione è già cablata, insita dentro al sistema. Bisogna però prestare attenzione al fatto che più un sistema ha questi meccanismi di autodifesa, tanto più tende a limitare la normale operatività degli utenti. Quindi i sistemi di classe B sono dei sistemi che tendono ad essere di sempre più difficile utilizzo per un utente normale o medio. Infine nella classe A1 troviamo i sistemi detti a protezione certificata, ossia sistemi che sono stati progettati con tecniche formali, matematiche, informatiche, che dimostrano che il sistema è assolutamente sicuro. Come è facile intuire non esiste ad oggi nessun sistema informatico al mondo che sia mai stato certificato in classe A1, perché sembra essere un compito improponibile.

La valutazione ITSEC



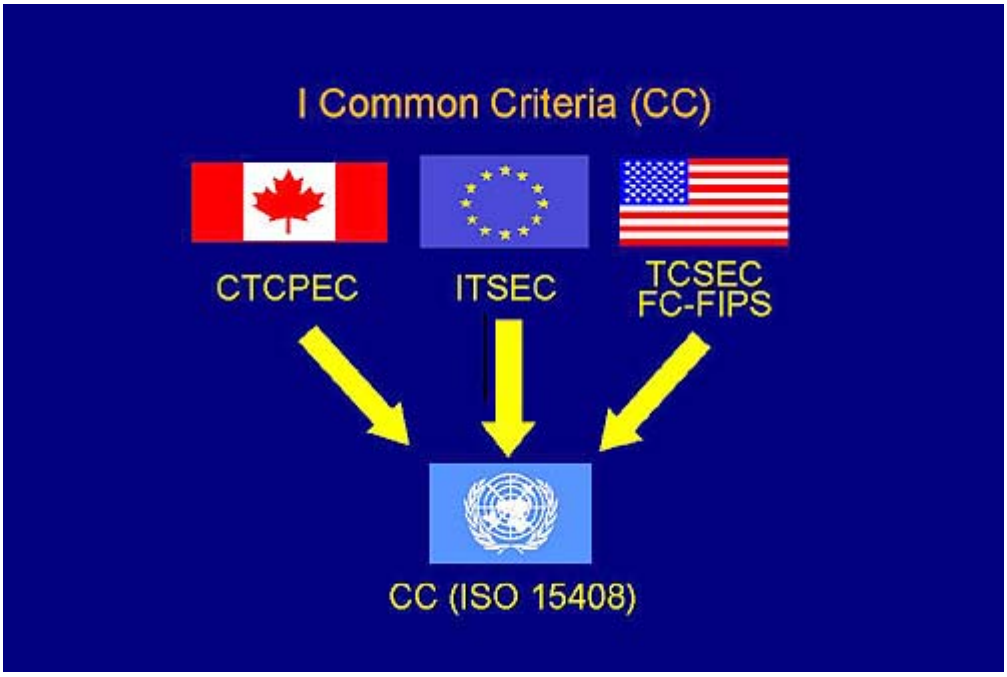
Successivamente ai criteri TCSEC, sono stati sviluppati i cosiddetti criteri di valutazione ITSEC, ideati da un gruppo di lavoro misto tra esperti tedeschi, olandesi, francesi ed inglesi, ed è poi stato adottato in gran parte da molti altri paesi appartenenti all'Unione Europea. Sono stati sviluppati nel 1991 ed in particolare uno dei loro principali vantaggi è quello di descrivere non soltanto la procedura di certificazione, ma anche la procedura con cui viene sviluppata la valutazione dei sistemi.

Scala di valutazione ITSEC

Il risultato di una valutazione ITSEC è dato da una coppia di parametri: la forza dei meccanismi di difesa (strength), che può essere BASIC, MEDIUM o HIGH, e il livello di correttezza dell'implementazione. Questa può essere E0, che equivale ad una correttezza bassissima o non verificata, oppure può essere un numero crescente da E1 a E6. Per comodità d'uso, a volte si fanno delle equivalenze con le classi di TCSEC, ad esempio si dice che una classe TCSEC C2 equivale ad

una classe ITSEC con funzionalità equivalenti alla C2 (F-C2) e con grado di correttezza E2. Invece, ad esempio, una classe A1 corrisponderebbe ad una funzionalità B3, ma con un livello di correttezza assoluto, ossia E6.

I Common Criteria (CC)



Per comporre questa diatriba tra Europa e USA per quale sia il corretto sistema di valutazione di un sistema informatico è entrata in campo ISO, l'organizzazione internazionale degli standard, il quale ha sviluppato i cosiddetti Common Criteria, che sono una armonizzazione dei criteri di sicurezza canadesi, europei (ITSEC) e americani, che nel frattempo, dopo aver pubblicato TCSEC, avevano sviluppato anche altri nuovi criteri, detti FC-FIPS. Questi criteri sono quelli che attualmente, in prospettiva, dovrebbero armonizzare tutte le valutazioni di sicurezza e sono già uno standard ISO con il numero 15408.

Validità di una valutazione (1)

Infine due parole circa la validità di una valutazione. Bisogna prestare molta attenzione al fatto che se un sistema è stato valutato con un certo livello di sicurezza, questo non significa assolutamente che il suo utilizzo sarà certamente sicuro, perché l'utilizzo del sistema informativo in questione dipenderà moltissimo da eventuali bachi ancora presenti nella sua implementazione, da procedure di manutenzione non appropriate e dall'uso non corretto da parte degli utenti o da parte del system-manager.

Validità di una valutazione (2)

Un altro errore che si commette solitamente quando si parla di valutazione dei sistemi informatici, è dimenticarsi che la valutazione si riferisce ad una ben precisa combinazione di hardware e software, è quindi scorretto in ogni modo trasferire questa valutazione su sistemi simili ma non identici. Se, ad esempio, si cambia l'hardware sul quale un sistema informativo è stato implementato, non è detto che la valutazione sia ancora valida, in generale occorre una nuova valutazione ogni volta che si

cambia anche la più piccola parte dell'hardware o del software rispetto alla configurazione che è stata valutata.