UNIVERSITÀ DEGLI STUDI ROMA TRE
FACOLTÀ DI SCIENZE MATEMATICHE FISICHE E NATURALI

Tesi di Laurea in Matematica

di

Francesco Corsi

Livelli di Sicurezza nei Sistemi Virtualizzati

Relatore
Roberto Di Pietro, PhD

Il Relatore

Il Candidato

ANNO ACCADEMICO 2006 - 2007
LUGLIO 2007

Classificazione AMS: 60J10, 91B30, 68N25.
Parole Chiave: Privacy, Sicurezza, Hidden Markov Model, Sistemi Virtualizzati.

Indice

Introduzione

Contesto

Negli ultimi anni le aziende si sono viste costrette a porre sotto stretta osservazione i budget ed i livelli dei servizi informatici allo scopo di ottenere un maggiore ritorno sugli investimenti IT. Molte organizzazioni si sono rese conto che, nonostante gli sforzi compiuti, l'infrastruttura informatica non sempre riesce a fornire un servizio efficiente e flessibile, in grado di adattarsi rapidamente al mutare delle esigenze del proprio business. La gestione IT, per garantire un supporto adeguato alle aziende, caratterizzate da elevato dinamismo, deve superare le attuali architetture infrastrutturali statiche e fortemente legate alle applicazioni. La tematica del computing on-demand, mediante strumenti tecnologici innovativi come la Server Virtualization, consente alla funzione IT di utilizzare le risorse elaborative come se fossero un servizio di pubblica utilità, alla stessa stregua dell'energia elettrica. La virtualizzazione deve consentire di utilizzare e condividere le risorse in maniera sicura per permettere di astrarre una risorsa d'elaborazione dalla struttura fisica per supportare contemporaneamente differenti applicazioni o sistemi operativi. Ne consegue che il concetto di virtualizzazione è strettamente legato e condizionato dalla necessità di soddisfare i principi della sicurezza che le aziende devono e vogliono rispettare.

Contributi

Questa tesi vuole offrire un escursus sull'evoluzione del concetto di Privacy, delle leggi che la tutelano e degli Stadard internazionali per valutare la sicurezza delle informazioni gestite dalle Aziende, sicurezza che si raggiunge adottando determinate metodologie quali il Risk Management. Si vuole offrire un supporto per la valutazione del livello della sicurezza delle soluzioni IT emergenti basate sulle potenzialità offerte dalla virtualizzazione ed evidenziare i vantaggi che apportano e le problematiche che introducono in termini di attacchi al sistema. Tali attacchi possono essere segnalati tramite l'anomaly detection che si basa sull'Hidden Markov Model, di cui sarà riportata una descrizione dettagliata. Inoltre poichè le Aziende hanno la necessità sia di essere aggiornate sui principali trend tecnologici che possono avere impatto

sulle scelte strategiche, sia di garantire la sicurezza in linea con gli Standard internazionali, è stato effettuato uno scouting sui livelli di sicurezza garantiti dalle soluzioni di virtualizzazione offerti dai maggiori Vendor.

Capitolo 1

La privacy

Legislazione in materia di Privacy

La privacy è il diritto alla riservatezza delle informazioni personali e della propria vita privata: *the right to be let alone*, secondo la formulazione del giurista statunitense Louis Brandeis che fu probabilmente il primo al mondo a formulare una legge sulla riservatezza, insieme a Samuel Warren (si veda il loro articolo *The Right to Privacy*, in Harvard Law Review, 1890). Brandeis in questo fu ispirato dalla lettura dell'opera di Ralph Waldo Emerson, il grande filosofo americano, che proponeva la solitudine come criterio e fonte di libertà.
La privacy si traduce spesso nella capacità di una persona (o di un gruppo di persone), di impedire che le informazioni che la riguardano diventino note ad altri, inclusi organizzazioni ed enti, qualora il soggetto non abbia volutamente scelto di fornirle.

Fonti comunitarie

Le fonti comunitarie rilevanti sono contenute nella **Direttiva del Parlamento europeo e del Consiglio** del 24 Ottobre 1995, contrassegnata dalla sigla 95/46/CE, [1], pubblicata nella **GUCE** L. 281 del 23.11.1995. Tale direttiva costituisce il testo di riferimento, a livello europeo, in materia di protezione dei dati personali, l'oggetto è:
Gli Stati membri garantiscono la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.
I principi relativi alla legittimazione del trattamento dei dati sono:

- il trattamento dei dati personali può essere effettuato solo con il consenso esplicito della persona interessata;
- la persona interessata ha il diritto di opporsi al trattamento di dati che la riguardano;
- la riservatezza e la sicurezza dei trattamenti.

Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali.

Fonti in Italia

La normativa vigente va desunta dal **D. lgs. N. 196/2003**, [2], intitolato **Codice in materia di protezione dei dati personali** entrato in vigore il 1 gennaio 2004.
Le finalità del **D. lgs. 196/03** consistono nel riconoscimento del diritto del singolo sui propri dati personali e, conseguentemente, nella disciplina delle diverse operazioni di gestione o tecnicamente trattamento dei dati, riguardanti la raccolta, l'elaborazione, il raffronto, la cancellazione, la modificazione, la comunicazione o la diffusione degli stessi.

Proprietà del Decreto legislativo 30 giugno 2003, n. 196

Sanzioni previste

L'art. 15 del **D. lgs. 196/03** (Danni cagionati per effetto del trattamento di dati personali) dice che: *Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile.*

Obblighi dell'Azienda (Documento programmatico sulla sicurezza)

Il **Decreto legislativo 30 giugno 2003, n. 196** obbliga l'adozione, per tutti i titolari che trattano i dati con strumenti elettronici, di un **documento programmatico sulla sicurezza (DPS)**, che deve essere predisposto annualmente.
I contenuti del documento sono elencati al punto 19 del **Disciplinare tecnico in materia di misure minime di sicurezza**.

Capitolo 2

Sicurezza metodologica

La sicurezza dell'informazione

L'attenzione verso la sicurezza delle informazioni ha portato alla definizione di Standard internazionali per valutare la Sicurezza dei prodotti e dei sistemi IT e per l'intero sistema di governo della sicurezza dell'informazione. Le Aziende che vogliono soddisfare tali Standard possono, tramite la certificazione, garantire ai clienti un livello di sicurezza riconosciuto in ambito internazionale. Per ottenere questa certificazione le Aziende sono tenute ad adottare un programma per stimare e governare il rischio che le informazioni possano venir danneggiate.
La sicurezza dell'informazione è caratterizzata da: *Riservatezza, Integrità, Disponibilità.*

Obiettivi degli Standard

Dal momento che l'informazione è un bene che aggiunge valore all'impresa, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. L'obiettivo del nuovo standard **ISO/IEC 27001** è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (**ISMS**) finalizzato ad una corretta gestione dei dati sensibili dell'azienda.

2.1 Standard per i sistemi di valutazione della sicurezza dei prodotti e dei sistemi IT

I primi tentativi ufficiali di definire il concetto di valutazione e di elaborare i criteri e le tecniche su cui basare tale operazione risalgono all'inizio degli anni ottanta quando il Dipartimento della Difesa degli Stati Uniti creò a questo fine un centro che prese il nome di *Department of Defense Computer Security Center* (oggi denominato *National Computer Security Center*). Nel 1983 il centro pubblicò la versione preliminare di una raccolta di criteri di valutazione intitolata Trusted Computer Systems Evaluation Criteria (**TCSEC**), [5], principalmente orientata alla valutazione dei sistemi operativi multiutente.

Alla fine degli anni ottanta anche in Europa si cominciò a sentire l'esigenza di sviluppare criteri di valutazione della sicurezza dei sistemi di trattamento automatico dell'informazione. Ciò portò nel 1989 alla pubblicazione di criteri nazionali in Germania, in Gran Bretagna e in Francia. A queste iniziative nazionali ne seguì una congiunta di Francia, Germania, Olanda e Gran Bretagna che mirava all'armonizzazione dei vari criteri nazionali. Il risultato di questa iniziativa fu una raccolta di criteri denominata Information Technology Security Evaluation Criteria - **ITSEC**, [6], la cui prima versione fu pubblicata nel maggio del 1990.

Parallelamente alle iniziative in Europa, anche in Canada e negli USA sono state avviate importanti attività che hanno portato alla produzione di nuove raccolte di criteri di valutazione. La prima versione dei criteri canadesi *Canadian Trusted Computer Product Evaluation Criteria* (**CTCPEC**) è stata pubblicata nel 1989. Nel 1991 il NIST (*National Institute for Standard and Technology*) e lNSA (*National Security Agency*) hanno avviato un progetto congiunto, denominato *Federal Criteria Project*, che ha portato, nel dicembre del 1992, alla definizione dei nuovi criteri federali per la valutazione della sicurezza dei prodotti per il trattamento automatico dell'informazione (**FC**), [7].

Common Criteria

Per armonizzare gli approcci USA ed europei e per di superare i limiti mostrati, dal 1993, le attività del WG3 risultano notevolmente condizionate da quelle di un altro gruppo, denominato CCEB (*Common Criteria Editorial Board*), nato per iniziativa della Comunità Europea e costituito da esperti

europei, statunitensi e canadesi. L'obiettivo del CCEB è quello di armonizzare i criteri europei ITSEC, i nuovi criteri federali statunitensi (FC) e i criteri canadesi CTCPEC attraverso la definizione di una nuova raccolta di criteri denominata **Common Criteria - CC**.

Le valutazioni CC sono realizzate nel rispetto di un insieme di livelli di garanzia predefiniti, indicati come *Evaluation Assurance Level* (EAL), in una scala crescente dal livello EAL1 al livello EAL7 precisando, per ogni livello di tale scala i requisiti specifici, detti requisiti di *assurance*, che devono essere soddisfatti dal TOE - Target Of Evaluation, dallo sviluppatore e dal valutatore: *il livello* **EAL1** - *Functionally Tested*; *il livello* **EAL2** - *Structurally Tested*; *il livello* **EAL3** - *Methodically Tested and Checked*; *il livello* **EAL4** - *Methodically Designed, Tested and Reviewed*; *il livello* **EAL5** - *Semiformally Designed and Tested*; *il livello* **EAL6** - *Semiformally Verified Designed and Tested*; *il livello* **EAL7** - *Formally Verified Designed and Tested.*

Protection Profile

Un Protection Profile definisce un insieme di requisiti di sicurezza, opzionali ed aggiuntivi ai CC, indipendenti dalla specifica implementazione della soluzione IT, in particolare si evidenziano: *Controlled Access Protection Profile - CAPP, Role Based Access Control Protection Profile - RBAC PP e Labeled Security Protection Profile - LSPP.*

2.2 Standard per il sistema di governo della sicurezza dell'informazione

Vista la scarsa adattabilità dei **Common Criteria, ITSEC** e **TCSEC**, data l'analicità ed il formalismo accentuato dei loro schemi, alla certificazione di sicurezza informatica delle orgnanizzazioni nel 1993 il **BSI** - British Standard Institute decise di sviluppare lo standard **BS7799** un documento di riferimento contenente una serie di *best practices* nell'area della sicurezza informatica per certificare il sistema di governo della sicurezza dell'informazione aziendale. Lo standard **BS7799** è diviso in tre parti: **BS7799-1** *standard code of practice* pubblicato nel 1995; **BS7799-2** *Information Security Management System - Specification with guidance for use* pubblicato nel 1999; **BS7799-3** *Guidelines for information security risk management* pubblicato nel 2005.

Lo Standard ISO/IEC 17799

La linea guida ISO 17799, [3], nasce dall'esperienza del mondo industriale/bancario inglese, e raggruppa in se gli elementi di best practice sulla sicurezza. L'ISO 17799 include le prime due parti dello standard BS 7799. La normativa prevede 10 diverse categorie di controlli, identificando per ciascuna gli obiettivi dei controlli ed i controlli stessi da implementare: *politica di sicurezza, organizzazione della sicurezza, classificazione e controllo degli asset, gestione del personale, sicurezza fisica ed ambientale, gestione dei sistemi, controllo accessi, sviluppo e manutenzione dei sistemi, continuità del business e conformità.*

Lo Standard ISO/IEC 27001

Lo standard ISO/IEC 27001, [4], è stato creato e pubblicato nell'ottobre 2005 a fini certificativi, in modo da costituire, assieme alla sua linea guida **ISO/IEC 17799**, un sistema completo per garantire la Gestione della Sicurezza nella Tecnologia dell'Informazione (Information Security Management System - **ISMS**). I requisiti definiti all'interno del Information Security Management System mirano ad ottenere i seguenti obiettivi: *identificare gli asset da proteggere, definire un approccio organizzativo al risk management, definire ed identificare i controlli da attuare, definire il livello di sicurezza richiesto.*

Gli standard elencati forniscono elementi per realizzare il ISMS sotto diversi aspetti, in tutti i casi il ISMS, per essere realizzato, deve comportare i seguenti passi: *definizione delle politiche di sicurezza aziendali e dell'ambito di applicazione del ISMS, analisi e gestione del rischio, selezione degli strumenti di gestione e stesura della dichiarazione di applicabilità.*

2.3 La certificazione degli Standard

La certificazione del ISMS attualmente è possibile attraverso la BS 7799 (o ISO 17799) che riporta requisiti obbligatori, anche se l'organizzazione puó escludere alcuni aspetti perché ritenuti non applicabili (la non applicabilitá dovrà però essere dimostrata). Lo schema di certificazione prevede, dopo una valutazione iniziale, il rilascio di un certificato di conformità alla norma di riferimento valido 3 anni, verifiche periodiche di convalida durante il triennio e verifiche alla sua scadenza ai fini del rinnovo.

2.4 Risk Management

Il Risk Management, [8], letteralmente Gestione del Rischio, è l'insieme degli strumenti, dei metodi e delle azioni con cui si misura o si stima il rischio e con cui, successivamente, si sviluppano le strategie per governarlo. L'introduzione di una metodologia logica e sistematica consente, attraverso fasi successive, di identificare, valutare, comunicare, eliminare e monitorare i rischi associati a qualsiasi attività lavorativa. Nel caso di garantire la sicurezza del patrimonio informativo di un'Azienda occorre quindi individuare, classificare e valutare i dati, i sistemi e le applicazioni rilevanti. Un sistema di sicurezza deve essere congruente con le leggi, le politiche e gli standard di sicurezza, occorre quindi effettuare un'accurata analisi dei sistemi in esercizio e definire il rischio che si può correre al presentarsi di una minaccia e individuare il sistema di contromisure e le regole generali da seguire per la protezione dei dati e dei sistemi. Occorre descrivere in modo esaustivo e dettagliato le caratteristiche principali del sistema in esame, l'architettura logica e fisica, i servizi che esso realizza e le interazioni con l'ambiente circostante indicando i flussi di input e di output, il colloquio con gli altri sistemi, le diverse tipologie di utenti, le modalità di accesso e di autenticazione, quali privilegi e quali funzionalità sono consentite all'interno del sistema.

In funzione delle politiche di sicurezza di un'Azienda le possibili azioni da intraprendere per gestire il rischio possono essere: *l'accettazione del rischio, l'assicurazione dei sistemi e la riduzione del rischio ad un livello accettabile.*

Il processo di Risk Management, [9], prevede due fasi: *il Risk Assessment* per la fase di analisi e di determinazione del rischio; *il Risk Treatment* per la definizione delle procedure di gestione e riduzione del rischio.
A fronte dei risultati ottenuti dal Risk Assessment viene attivato il processo di Risk Treatment che stabilisce la strategia più opportuna per il trattamento del rischio e rappresenta le azioni da intraprendere per ridurre i livelli di rischio.

2.4.1 Risk Assesement

L'analisi del rischio prevede che su tutti i sistemi ICT sia preliminarmente eseguita un'analisi di alto livello che permette di stimare il rischio in relazione al business aziendale.

Valutazione dei rischi

La criticità dei dati è legata alle eventuali minacce a cui il dato può essere esposto e quindi è strettamente legata ai livelli di sicurezza. Le tre caratteristiche universalmente accettate per definire il livello di sicurezza di un servizio, applicazione o sistema sono: Riservatezza, Integrità e Disponibilità (RID), questi requisiti possono essere compromessi da una serie di eventi di carattere accidentale o intenzionale: *la Perdita di Riservatezza, la Perdita di Integrità e la Perdita di Disponibilità*

Identificazione dei rischi

Per identificare i rischi occorre correlare gli eventi potenzialmente configurabili come minacce al contesto architetturale e applicativo che si sta analizzando. Gli eventi potenzialmente dannosi da considerare devono comprendere minacce derivanti da circostanze o errori accidentali, minacce derivanti da interventi umani di tipo volontario ed involontario.
In particolare devono essere considerate le seguenti categorie di eventi: *eventi di natura fisica, eventi di natura logica ed eventi di natura organizzativa.*

Modellazione dello scenario

Per modellare lo scenario occorre evidenziare la relazione tra i dati trattati da un processo, gli applicativi, i sistemi e i dispositivi di rete che permettono l'elaborazione e la trasmissione dei dati stessi appartenenti al perimetro di intervento. Il componente è l'elemento su cui viene eseguita l'analisi del rischio ed a cui compete l'onere di opporre le necessarie difese alle minacce cui è soggetto. I Macrodati sono categorie di informazioni che condividono gli stessi requisiti di sicurezza, e sono tra loro omogenei per severità dell'impatto, affinità semantica, finalità di trattamento, esigenze tecnologiche di elaborazione.

Classe di Criticità dei Macrodati

La fase di valutazione dei Macrodati si pone l'obiettivo di valutare gli impatti sui processi di business aziendali derivanti dalla perdita di Riservatezza, Integrità e Disponibilità (RID) di tali dati. Le aree di impatto sono: *perdite finanziarie, impatto sul business, perdita di competitività, perdita di immagine e sanzioni.*

Rischio Intrinseco

Il rischio intrinseco di un componente è determinato dal valore del rischio del componente stesso nell'ipotesi che tutti gli attacchi tentati contro di esso vadano a buon fine per assoluta mancanza di protezione.

2.4.2 Risk Treatment

Il Risk Treatment descrive le azioni necessarie al fine di trattare il rischio non accettabile rilevato attraverso la fase di Risk Assessment.

Il primo passo nella fase di trattamento del rischio è verificare lo stato di attuazione delle contromisure. È quindi necessario individuare le policy in essere, le contromisure di sicurezza tecnologiche operative e le procedure organizzative. Il secondo passo consiste nel verificare se le contromisure per un componente sono soddisfatte dalle misure di sicurezza attuali. I possibili stati sono: *la contromisura è stata attuata con una graduazione pari o superiore a quella indicata, la contromisura è stata attuata con una graduazione inferiore a quella indicata, la funzione di protezione non è stata attuata.*

Rischio Residuo

Il livello di rischio residuo può essere stimato a livello di componente, di sistema o di intero perimetro di intervento. Il rischio residuo corrisponde al livello di rischio calcolato tenendo conto delle contromisure presenti. Sulla base del livello di rischio residuo, si verifica se le contromisure già in atto o pianificate sono sufficienti o addirittura sovradimensionate o si può determinare la necessità di adottare ulteriori protezioni.
Una valutazione del rischio residuo di un componente è data dal rapporto tra il valore del rischio residuo del componente RRc e la somma dei valori delle graduazioni delle contromisure proposte ottimali GCottimale e rappresenta la percentuale di misure di sicurezza non implementate rispetto a quelle ottimali proposte: PMSI = RRc / Somma GCottimale

Efficacia delle Contromisure - EC

In funzione della Classe di Criticità Finale - CCF di appartenenza e dei requisiti di Legge, deve essere proposto un insieme di contromisure di sicurezza, con un grado di efficacia (EC) determinato, da combinare con quelle even-

tualmente presenti nel servizio, applicazione o sistema, poter contrastare le minacce alla sicurezza e ridurre di conseguenza i rischi.

Le contromisure sono dei meccanismi implementabili per rendere più sicuro un sistema informatico.

Contromisure per le Applicazioni

Per una funzione applicativa ad ogni categoria di meccanismi è assegnato un grado di efficacia che esprime, in modo qualitativo, quanto il meccanismo in questione consente di contrastare e di ridurre gli effetti negativi della minaccia su di un macrodato.

Contromisure di Hardening

Con il termine hardening si intende la procedura utilizzata per rendere i sistemi il più resistenti ai vari tentativi di attacco. Le attività di hardening sono finalizzate all'eliminazione e/o mitigazione di eventuali vulnerabilità insiste nelle configurazioni di default proposte dal costruttore e indotte dall'ambiente in cui l'applicazione opera.

Livello Sicurezza Rete - LSR

Il Livello di Sicurezza richiesto per la Rete - LSR dipende dalla Classe di Criticità Finale a cui appartengono i servizi/applicazioni/sistemi attestati su di essa. La valutazione va espressa sulla base dei soli livelli di sensibilità rispetto alla riservatezza (R) ed all'integrità (I) assegnati ai dati.

Le contromisure applicabili a livello network possono variare molto in funzione dei diversi parametri che caratterizzano la rete e i singoli sistemi che la compongono.

Modalità di interconnessione

Determinato il grado di criticità dei sistemi, da attestare o attestati in rete, e di conseguenza della rete stessa, occorre definire la modalità di interconnessione e/o attestazione. I livelli di sicurezza individuati dovranno essere omogenei; ciò significa che sistemi classificati con uno stesso grado di criticità dovranno risiedere su reti di pari livello di sicurezza.

Capitolo 3

La sicurezza nei sistemi informatici

3.1 Minacce e Vulnerabilità

Per Minaccia si intende un evento la cui manifestazione può arrecare danno al servizio e/o ai dati da questo trattati, provocando almeno una violazione di uno dei requisiti di sicurezza. È necessario stimare l'esposizione alle Minacce ed Attacchi.

Livello di Esposizione alla Minaccia

Per determinare il Livello di Esposizione alla Minaccia si possono combinare informazioni di tipo oggettivo ad es. statistiche che indichino in media quanto una data minaccia abbia dato esito ad un attacco sfruttando una determinata vulnerabilità, oppure statistiche effettuate da terze parti su problematiche di sicurezza, con valutazioni di tipo soggettivo come ad es. valutazioni sul livello di competenza tecnica necessaria per porre in essere una data minaccia e, eventualmente, confrontandole con la competenza delle persone che operano sul sistema.

Livello di Vulnerabilità

Si devono identificare, rispetto a ciascuna minaccia ritenuta applicabile, le vulnerabilità che la minaccia può sfruttare.

Il Livello di Vulnerabilità può assumere i valori: Base, Medio, Alto.

Livello di Esposizione all'Attacco

L'attacco è la modalità con cui si attua una minaccia che sfrutta una specifica vulnerabilità. Ad ogni vulnerabilità corrisponde quindi un possibile attacco, ci possono essere più attacchi per la stessa minaccia. Il Livello di Esposizione all'attacco viene stimato combinando il Livello di Esposizione alla Minaccia ed il Livello di Vulnerabilità.

Ci sono tre principali metodologie per proteggere le risorse dalle intrusioni e vengono implementate utilizzando diverse tecnologie.

- Threat Prevention Management: permette di filtrare il traffico di rete con l'obiettivo di bloccare i tentativi di attacco in real-time e di far continuare le attività legittime;
- Threat Deception Management: permette di ingannare l'intrusore, fornendogli delle informazioni false, così da rende i tentativi di hacking frustranti e di rilevare immediatamente l'attacco;
- Threat Detection Management: abilita il monitoraggio del traffico per rilevare le intrusioni e solleva diversi tipi di warning o alert. I sistemi risultano protetti solo se all'alert viene fornita velocemente un risposta adeguata, ad esempio l'Intrusion Detection Systems (IDS) esamina il traffico di rete per trovare comportamenti o pattern che indicano un'intrusione.

3.2 Intrusion Detection System (IDS) e Intrusion Prevention System (IPS)

Un Intrusion Detection System (IDS) è un sistema di rilevamento delle intrusioni che consente di individuare attacchi e minacce ad un sistema informatico che possono provenire sia dall'interno sia dall'esterno. Il sistema IDS deve identificare e analizzare in tempo reale gli eventi connessi alla sicurezza di un sistema informatico che richiedono un intervento immediato con lo scopo di rilevare e segnalare usi non autorizzati, utilizzi impropri e abusi da parte sia

di utenti autorizzati che di utenti esterni, inoltre deve riconoscere e limitare: *i falsi positivi e i falsi negativi.*

Mentre le funzionalità IDS permettono di rilevare le possibili intrusioni, le funzionalità IPS (Intrusion Prevention System) permettono anche di bloccare e reagire automaticamente alle minacce di attacchi sconosciuti ad esempio modificando le policy di sicurezza. Un sistema IPS è un sistema che è in grado di bloccare i tentativi di intrusione prima che questi compromettano il sistema.

Anomaly Detection

Un sistema di anomaly detection parte da due presupposti fondamentali: il traffico di rete ha connotazioni tipiche e tutti gli attacchi presentano similitudini osservabili rilevando la presenza di traffico insolito. A questo viene abbinata unanalisi di consistenza del traffico e di correlazione di eventi.

Modelli utilizzabili

Data una metrica per una variabile casuale x e n osservazioni $x_1, ..., x_n$, occorre stabilire se una nuova osservazione x_{n+1} è anomala rispetto le precedenti osservazioni.

Ciò è possibile utilizzando i seguenti modelli: il modello della soglia che stabilisce valori minimi e massimi per il valore della variabile x per cui si è in presenza di un comportamento anomalo, il modello della media e della deviazione standard dove si conoscono la media e la deviazione standard della variabile x, sulla base delle osservazioni precedenti se il valore della nuova osservazione non cade all'interno dell'intervallo si è in presenza di un comportamento anomalo, infine il modello di Markov nascosto (HMM) esposto nel capitolo successivo.

3.3 Hidden Markov Model - HMM

Gli Hidden Markov Models o modelli di Markov nascosti HMM si possono definire come dei modelli di sistemi dinamici stocastici parzialmente osservabili.

HMM è un'estensione delle catene di Markov, [51], ed è costituito da un insieme finito di stati, ciascuno è associato ad una distribuzione di probabilità (generalmente multidimensionale). Le transizioni fra gli stati sono governate

da un insieme di probabilità denominate probabilità di transizione. In un modello di Markov nascosto soltanto il risultato è visibile ad un osservatore esterno, mentre gli stati rimangono nascosti. Lo scopo dell'Anomaly Detection tramite un HMM è di distinguere se il comportamento corrente del sistema è normale o meno:

Definizione - Hidden Markov Model (HMM)

Un Hidden Markov Model, [52], [53], [54], [55], è caratterizzato da:

- N, ovvero il numero di stati del modello: $S = \{S_1, S_2, ..., S_N\}$;
- M, ovvero il numero di simboli osservabili per ogni stato: $V = \{v_1, ..., v_M\}$;
- A, ovvero la matrice N x N di probabilità di transizione di stato; indicando con q_t lo stato del modello all'istante t abbiamo che $a_{ij} = P(q_{t+1} = S_j | q_t = S_i)$ con $1 \leq i, j \leq N$;
- B, insieme di distribuzioni di probabilità dei simboli per ciascuno stato: $B = \{b_j(k), 1 \leq j \leq N, 1 \leq k \leq M\}$, dove $b_j(k)$ rappresenta la probabilità di osservare il simbolo v_k ad un certo istante t quando lo stato del modello nel medesimo istante è S_j, $b_j(k) = P\{v_k$ al tempo $t | q_t = S_j\}$, $1 \leq j \leq N$, $1 \leq k \leq M$;
- π, distribuzione iniziale $\pi = \{\pi_i, 1 \leq i \leq N\}$ dove π_i rappresenta la probabilità che lo stato iniziale del modello sia lo stato S_i, $\pi_i = P\{q_1 = S_i\}$, $1 \leq i \leq N$.
- O, la sequenza delle osservazioni $O = O_1, O_2, ..., O_T$, dove ogni osservazione O_i è uno dei simboli di V e T è il numero di osservazioni nella sequenza.

Indicheremo un modello HMM tramite la notazione compatta $\lambda = (A, B, \pi)$.

L'Hidden Markov Model è caratterizzato da tre principali tematiche: *la valutazione, la ricerca della sequenza più probabile e l'addestramento del modello.*

La valutazione

La valutazione per una determinata sequenza di osservazioni di lunghezza t $O = O_1, O_2, ..., O_t$ con un dato HMM $\lambda = (A, B, \pi)$ è data dalla probabilità: $P_\lambda(O)$

Questo valore può essere calcolato enumerando ogni possibile sequenza di stati di lunghezza t:

si fissa una sequenza di stati $Q = q_1, q_2, ..., q_t$, dove q_1 rappresenta lo stato iniziale. La probabilità di ottenere la sequenza di osservazioni $O = O_1, O_2, ..., O_t$, supponendo che siano indipendenti, tramite la sequenza di stati $Q = q_1, q_2, ..., q_t$ è data da: $P_\lambda(O|Q) = \prod_{k=1}^{t} P_\lambda(O_k|q_k) = b_{q_1}(O_1)b_{q_2}(O_2)...b_{q_t}(O_t)$.

Calcoliamo la probabilità di ottenere la sequenza di stati $Q = q_1, q_2, ..., q_t$: $P_\lambda(Q) = P_\lambda(q_1, q_2, ..., q_t) = \pi_{q_1} a_{q_1 q_2} a_{q_2 q_3} ... a_{q_{t-1} q_t}$.

Calcoliamo la probabilità di ottenere un'occorrenza simultanea di O e Q, che si ottiene moltiplicando le due probabilità calcolate precedentemente: $P_\lambda(O, Q) = P_\lambda(O|Q)P_\lambda(Q)$.

Infine la probabilità di ottenere la sequenza di osservazioni O si ottiene sommando la formula precedente su ogni possibile sequenza di stati Q: $P_\lambda(O) = \sum_Q P_\lambda(O|Q)P_\lambda(Q) = \sum_{q_1, q_2, ..., q_t} \pi_{q_1} b_{q_1}(O_1) a_{q_1 q_2} b_{q_2}(O_2) ... a_{q_{t-1} q_t} b_{q_t}(O_t)$

Il processo continua in questo modo fino ad ottenere la lista di transizione al tempo finale t dallo stato q_{t-1} allo stato q_t con probabilità $a_{q_{t-1} q_t}$ e si genera il simbolo O_t con probabilità $b_{q_t}(O_t)$.

Il problema di questo metodo è che per calcolare $P_\lambda(O)$ si devono fare $2t \cdot N^t$ operazioni, questo risultato non è accettabile.

Utilizzando invece un procedimento induttivo, detto forward procedure, si può calcolare $P_\lambda(O)$ con un ordine inferiore di operazioni.

Si definisce $\alpha_k(i)$ la probabilità di ottenere la sequenza parziale di osservazioni $O = O_1, O_2, ..., O_k$, $k \in [1, ..., t-1]$ e che al tempo k ci si trovi nello stato S_i, quindi: $\alpha_k(i) = P_\lambda(O, q_k = S_i) = P_\lambda(O_1, O_2, ..., O_k, q_k = S_i)$

Il procedimento induttivo è definito nel modo seguente:

1. Passo iniziale: $P_\lambda(O_1, q_1 = S_i) = P_\lambda(O_1|q_1 = S_i)P_\lambda(q_1 = S_i) = \pi_i b_i(O_1)$, $1 \leq i \leq N$

2. Passo induttivo: $\alpha_{k+1}(j) = P_\lambda(O_1, O_2, ..., O_{k+1}, q_{k+1} = S_j) =$
$P_\lambda(O_{k+1}|q_{k+1} = S_j)P_\lambda(O_1, O_2, ..., O_k, q_k = S_i) =$
$b_j(O_{k+1})P_\lambda(O_1, O_2, ..., O_k, q_k = S_i) = b_j(O_{k+1}) \sum_{i=1}^{N} \alpha_k(i)a_{ij}$
$1 \leq k \leq t-1$, $1 \leq j \leq N$

3. Passo finale: Permette di calcolare $P_\lambda(O)$, cioè la somma delle probabilità di ottenere la sequenza O su un qualsiasi stato finale: $P_\lambda(O) = \sum_{i=1}^{N} \alpha_t(i)$

Per calcolare $\alpha_k(j)$, $1 \leq k \leq t, 1 \leq j \leq N$, le operazioni necessarie sono dell'ordine di N^2t, rispetto al metodo analizzato in precedenza, con N=2 e t=78 sono necessarie circa 600 operazioni invece di 2^{80}.

Anche utilizzando un altro procedimento induttivo, detto backward procedure, si può calcolare $P_\lambda(O)$.

Si definisce $\beta_k(i)$ la probabilità di ottenere la sequenza parziale di osservazioni da k+1 fino a t, $O = O_{k+1}, O_{k+2}, ..., O_t$, e che al tempo k ci si trovi nello stato S_i quindi: $\beta_k(i) = P_\lambda(O, q_k = S_i) = P_\lambda(O_{k+1}, O_{k+2}, ..., O_t, q_k = S_i)$

Il procedimento induttivo è definito nel modo seguente:

1. Passo iniziale: si definisce in modo arbitrario $\beta_t(i)$ per ogni i è uguale a 1: $\beta_t(i) = 1, 1 \leq i \leq N$

2. Passo induttivo: $\beta_k(i) = P_\lambda(O_{k+1}, O_{k+2}, ..., O_t, q_k = S_i) =$
$\sum_{j=1}^{N} a_{ij}P_\lambda(O_{k+1}|q_{k+1} = S_j)P_\lambda(O_{k+2}, O_{k+3}, ..., O_t, q_{k+1} = S_j) =$
$\sum_{j=1}^{N} a_{ij}b_j(O_{k+1})\beta_{k+1}(j)$, $k = t-1, t-2, ..., 1$, $1 \leq j \leq N$.

Quindi andando a ritroso si ottiene il valore di $P_\lambda(O)$.

Per calcolare $\beta_k(i)$, $1 \leq k \leq t$, $1 \leq i \leq N$, sono necessarie N^2t operazioni, lo stesso risultato ottenuto con la forward procedure.

Ricerca della sequenza di stati più probabile

La ricerca della sequenza di stati più probabile del HMM $\lambda = (A, B, \pi)$ che generi una determinata sequenza di osservazioni $O = O_1, O_2, ..., O_t$ equivale al cercare la sequenza di stati del HMM che massimizzi il valore della seguente probabilità: $P_\lambda(Q|O)$ ossia trovare il cammino più probabile nell'HMM che ha portato alla generazione di O.

Per la proprietà della probabilità congiunta si ottiene: $P_\lambda(Q|O) = \frac{P_\lambda(Q,O)}{P_\lambda(O)}$ quindi basta massimizzare $P_\lambda(Q,O)$.
Dalla proprietà di Markov si ottiene:
$P_\lambda(q_1, q_2, ..., q_t) = P_\lambda(q_1)P_\lambda(q_2|q_1)P_\lambda(q_3|q_2)...P_\lambda(q_t|q_{t-1})$
inolre per definizione del modello:
$P_\lambda(O_1, O_2, ..., O_t) = P_\lambda(O_1|q_1)P_\lambda(O_2|q_2)P_\lambda(O_3|q_3)...P_\lambda(O_t|q_t)$
quindi bisogna effettuare la massimizzazione sulle possibili scelte degli stati $q_1, ..., q_t$ di:
$P_\lambda(Q,O) = P_\lambda(q_1)P_\lambda(O_1|q_1)P_\lambda(q_2|q_1)P_\lambda(O_2|q_2)...P_\lambda(q_t|q_{t-1})P_\lambda(O_t|q_t)$.

Si indica con $\gamma_k(i)$ la più alta probabilità lungo un singolo cammino al tempo $k \in [1, ..., t]$, che comprende le prime k osservazioni e termina allo stato S_i:
$\gamma_k(i) = \max_{q_1,q_2,...,q_{k-1}} P_\lambda(q_1, q_2, ..., q_k = S_i, O_1, O_2, ..., O_k)$
tale probabilità può anche essere scritta in forma ricorsiva nel modo seguente:
$\gamma_{k+1}(j) = P_\lambda(O_{k+1}|q_{k+1} = S_j) \max_i P_\lambda(q_{k+1} = S_j|q_k = S_i)\gamma_k(i) =$
$b_j(O_{k+1})(\max_i a_{ij}\gamma_k(i))$

Per individuare la sequenza di stati più pobabile è necessario tenere traccia degli argomenti che massimizzano l'equazione precedente per ogni i e j, si indica con $\phi_k(j)$ l'array che traccia tali argomenti.

Utilizzando l'algoritmo di Viterbi:

- passo iniziale: $\gamma_1(i) = P_\lambda(O_1, q_1 = S_i) = P_\lambda(O_1|q_1 = S_i)P_\lambda(q_1 = S_i) = \pi_i b_i(O_1), 1 \leq i \leq N$, $\phi_1(i) = 0$
- passo induttivo:
  $\gamma_k(j) = P_\lambda(O_k|q_k = S_j) \max_{1\leq i\leq N} P_\lambda(q_k = S_j|q_{k-1} = S_i)\gamma_{k-1}(i) =$
  $b_j(O_k) \max_{1\leq i\leq N}(a_{ij}\gamma_{k-1}(i))$, $2 \leq k \leq t$, $1 \leq j \leq N$
  $\phi_k(i) = \arg\max_{1\leq i\leq N} P_\lambda(q_k = S_j|q_{k-1} = S_i)\gamma_{k-1}(i)$,$2 \leq k \leq t$,$1 \leq j \leq N$
- passo finale: $p^* = \max_{1\leq i\leq N}(\gamma_t(i))$, $q_t^* = \arg\max_{1\leq i\leq N}(\gamma_t(i))$
- traceback: $q_k^* = \phi_{k+1}(q_{k+1}^*)$, $k = t-1, t-2, ..., 1$.

Si individua, tramite la successione dei traceback, la sequenza di stati più probabile che porta alla generazione dell'osservazione O.

L'addestramento del modello

Data una sequenza finita di osservazioni O, si addestra il modello $\lambda = (A, B, \pi)$ massimizzando la probabilità $P_\lambda(O)$ cercando il modello $\lambda^* = (A', B', \pi')$ tale che: $\lambda^* = \max_\lambda P_\lambda(O)$

Per trovare i nuovi valori A', B', π' del modello λ^* si può utilizzare l'algoritmo di Baum-Welch:

1. si imposta il modello $\lambda = (A, B, \pi)$ con dei valori iniziali random;
2. si definiscono:
   - $\xi_k(i,t)$ rappresenta la probabilità, conoscendo la sequenza di osservazioni O, di trovarsi nello stato S_i al tempo k e allo stato S_j al tempo k+1: $\xi_k(i,j) = P_\lambda(q_k = S_i, q_{k+1} = S_j|O) = \frac{P_\lambda(q_k=S_i, q_{k+1}=S_j, O)}{P_\lambda(O)} = \frac{\alpha_k(i)a_{ij}b_j(O_{k+1})\beta_{k+1}(j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_k(i)a_{ij}b_j(O_{k+1})\beta_{k+1}(j)}$ quindi $\sum_{k=1}^{t-1}\xi_k(i,j)$ rappresenta il numero medio di transizioni dallo stato S_i allo stato S_j,
   - $\delta_k(i)$ rappresenta la probabilità, conoscendo la sequenza di osservazioni O, di trovarsi nello stato S_i all'istante k: $\delta_k(i) = P_\lambda(q_k = S_i|O) = \frac{P_\lambda(O, q_k=S_i)}{P_\lambda(O)} = \frac{\alpha_k(i)\beta_k(i)}{\sum_{j=1}^{N}\alpha_k(j)\beta_k(j)}$ quindi $\sum_{k=1}^{t-1}\delta_k(i)$ esprime il numero medio di visite allo stato S_i.
3. si aggiornano i paramentri A, B, π del modello λ nel seguente modo:
   - sia $\bar{\pi}_i$ il numero di volte che ci si trova allo stato S_i al tempo k=1: $\bar{\pi}_i = \delta_1(i)$, si aggiorna π con: $\pi' = \bar{\pi}_i$, $1 \leq i \leq N$,
   - sia $\bar{a}_{ij}$ il numero medio di transizioni dallo stato S_i allo stato S_j sul il numero medio di visite allo stato S_i: $\bar{a}_{ij} = \frac{\sum_{k=1}^{t-1}\xi_k(i,j)}{\sum_{k=1}^{t-1}\delta_k(i)}$, si aggiorna A con: $A' = \bar{a}_{ij}$, $1 \leq i, j \leq N$,
   - sia $\bar{b}_i(k)$ il numero medio di visite allo stato S_i e che l'osservazione O_k fornisca il simbolo v_z sul numero medio di visite allo stato S_i: $\bar{b}_i(k) = \frac{\sum_{k=1 \wedge O_k=v_z}^{t}\delta_k(j)}{\sum_{k=1}^{t}\delta_k(j)}$, si aggiorna B con:$B' = \bar{b}_i(k)$, $1 \leq i \leq N$, $1 \leq k \leq t$

   con questi nuovi parametri si ottiene il modello aggiornato $\lambda^* = (A', B', \pi')$.

Capitolo 4

La Virtualizzazione

4.1 Virtual Machine

In origine, il termine **Virtual Machine** veniva usato per indicare la creazione di una molteplicità di ambienti di esecuzione identici in un unico computer, ciascuno con il proprio sistema operativo, per cui più utenti condividevano l'uso di un singolo computer avendo l'impressione di esserne l'unico utilizzatore. Il software che realizza questa condivisione è detto **Virtual Machine Monitor** o **Hypervisor**. Le principali tecniche per realizzare la virtualizzazione, [14], sono: *l'emulazione, la virtualizzazione nativa e la paravirtualizzazione.*

L'**Hypervisor** opera in modo trasparente senza pesare con la propria attività sul funzionamento e sulle prestazioni dei sistemi operativi, svolge attività di controllo al di sopra di ogni sistema ed essendo in grado di segnalare ed eventualmente interrompere attività pericolose viene impiegato come monitor e debugger delle attività sia dei sistemi operativi che delle applicazioni.

L'adozione di tecniche e strumenti integrati al sistema virtualizzato per la sicurezza del sistema stesso porta alla realizzazione di un **Secure Hypervisor**, [10], [11], [12]. Le partizioni dei sistemi operativi guest sono isolate e mediate dallo strato di virtualizzazione. Attraverso speciali partizioni virtuali (Security Partions), è possibile eseguire dei servizi di sicurezza (Secure Services). Questi servizi hanno il compito di effettuare il controllo sul flusso d'informazioni tra le partizioni, monitorando l'integrità del contenuto delle VM e dell'intera piattaforma. Inoltre, questa architettura permette di effettuare il controllo ed il metering delle risorse condivise al fine di prevenire attacchi

di tipo Denial of Service. L'Hypervisor è un possibile obiettivo di attacchi perchè una volta compromesso, l'intero server su cui è in esecuzione sarà a rischio. Un hypervisor compromesso è impossibile da rilevare con le normali tecniche di sicurezza da nessuno dei sistemi operativi host, perchè invisibile alle partizioni che gestisce.

La sicurezza tramite una soluzione di virtualizzazione

La virtualizzazione dei server viene adottata principalmente per ridurre i costi di manutenzione, la quantità di hardware, il software da acquistare ed i costi energetici. La virtualizzazione ha anche un enorme potenziale per migliorare la sicurezza dei sistemi informatici nell'ambito della Threat Prevention, Deception e Detection:

- Virtualization per il disaster recovery e l'high availability (Threat Prevention): la virtualizzazione permette di creare un nodo secondario virtuale, ovvero il nodo primario viene installato su dell'hw fisico ma il nodo secondario è disponibile su una macchina virtuale, pronta a partire in caso di guasto. Dato che il nodo in standby non consuma risorse, una singola macchina fisica può memorizzare più nodi secondari e dinamicamente riservare le risorse fisiche necessarie al nodo virtuale durante il guasto.

- Virtualization per la forensic analysis (Threat Detection): la forensic analysis è l'applicazione delle tecniche di analisi e investigazione informatica per raccogliere prove che possano essere presentate in un tribunale.

- Virtualization per il sandboxing (Threat Deception): spostare una o più applicazioni in una macchina virtuale aiuta i manager IT a controllare due tipi di problemi: l'instabilità applicativa che può portare ad un significante spreco di risorse o, nel peggiore dei casi, ad un crash dell'intero sistema e la compromissione dell'applicazione che può portare ad un'escalation locale dei privilegi ed un controllo non autorizzato del sistema.

- Virtualization per l'honey potting (Threat Deception): Un honeypot è un sistema che si presenta e si comporta come se fosse un ambiente di produzione. Il sistema è posizionato in punti specifici della rete con

dati sufficientemente interessanti da attrarre un hacker, ma il sistema viene riempito di sensori per il logging. Lo scopo è quello di scoprire più informazioni possibili sui nuovi tool e le nuove tecniche di hacking e di confondere l'hacker il più a lungo possibile così che i security manager possano applicare una patch ai sistemi reali contro i nuovi tipi di attacchi scoperti.

Le principali caratteristiche di sicurezza che offre una soluzione di virtualizzazione sono: *isolation, attack mitigation, policy enforcement, defense-in-depth, encapsulation.*

La virtualizzazione può essere realizzata a livello di Storage e Server.

4.2 Storage Virtualization

La Storage Virtualization è un insieme di tecniche con cui è possibile separare la vista logica dello storage da quella fisica, in modo da disaccoppiare le applicazioni dai dischi. L'idea è di rendere fruibile, come un unico serbatoio, la totale capacità disponibile anche su macchine eterogenee e multi-vendor.

La Storage Virtualization si può applicare a tre diverse tipologie d'architettura storage, che si differenziano per complessità e livello prestazionale. I tre modelli sono: *Directed Attached Storage (DAS),Network Attached Storage (NAS) e Storage Area Network (SAN).*

Esistono diverse tipologie di virtualizzazione dello storage che si caratterizzano per la diversa collocazione dell'hardware che la realizza: *Array Based Virtualization, Host Based Virtualization, In-Band Virtualization, Out-Of-Band Virtualization, Switch Based Virtualization e Controller Based Virtualization*

4.3 Server Virtualization

La Server Virtualization è nata dal concetto di partizionamento del server che permette di superare alcuni limiti intrinsici nella gestione tradizionale delle risorse infatti utilizzare un server per ogni applicazione significa dimensionarlo secondo i picchi che l'applicazione può richiedere, con la conseguenza di avere un utilizzo medio della risorsa pari al 20% - 30% delle sue potenzialità. Il partizionamento consiste nel dividere un sistema SMP (Symmetric MultiProcessing) in sistemi più piccoli ognuno con la sua istanza di sistema

operativo e le sue risorse di sistema (cpu, memoria e I/O), il partizionamento può essere realizzato in modo fisico o virtuale.

I principali ambiti in cui impattano le soluzioni di Server Virtualization sono:

- Server Unix: le soluzioni di virtualizzazione sono guidate dalla tecnologia proprietaria legata al Sistema Operativo sviluppato per l'hardware che commericilizzano. I fornitori di Server Unix hanno il proprio Sistema Operativo e quindi la propria tecnologia di virtualizzazione;

- Server Wintel e Open Source: le soluzioni di virtualizzazione sono trasversali ai fornitori di hardware.

Server Unix

Le tecnologie di virtualizzazione in ambito Server Unix sono apparse sul mercato negli ultimi anni ed hanno attualmente raggiunto un livello sufficiente di maturità. I principali prodotti presenti sul mercato odierno possono essere racchiusi in HP, IBM, SUN e FSC:

HP

Il sistema operativo HP-UX11i, [15], [16], [17], [18], [19], [20], [21], fornisce diversi modi per isolare o combinare le risorse di un sistema: *Virtual Partition (vPars), Integrity Virtual Machines e Secure Resource Partitions.*

Il pacchetto certificato rispetto ai Common Criteria, [22], [23], è il sistema operativo HP-UX 11i v2 con il livello EAL4+: EAL4 augmented by ALC_FLR.3 (Systematic flaw remediation). I protection profile aggiuntivi sono: Controlled Access Protection Profile CAPP, Role Based Access Control Protection Profile RBAC PP.
È da notare che nella configurazione certificata non risultano incluse le partizioni fisiche (nPar) e virtuali (vPar).

IBM

Il partizionamento virtuale di IBM, [24], [25], [26], [27], [28], [29], si basa sull'utilizzo di un firmware (indicato come Hypervisor) e comprende diverse soluzioni: *LPAR, DLPAR e Micropartizionamento.*

La soluzione proposta da IBM per la virtualizzazione è Advanced POWER Virtualization, che utilizza la tecnica del micropartizionamento ed i suoi componenti principali sono: *il Virtual I/O Server - VIOS, l'Hardware Management Console - HMC e l'Integrated Virtualization Manager - IVM.*
Il pacchetto certificato rispetto ai Common Criteria, [30], [31], è Advanced POWER Virtualization for IBM AIX 5L V5.3 with optional IBM Virtual I/O Server V1.3 con il livello EAL4+: EAL4 augmented by ALC_FLR.3 (Systematic flaw remediation). Il protection profile aggiuntivo è Controlled Access Protection Profile CAPP.

SUN

La virtualizzazione dei server SUN, [32], è stata introdotta con Solaris 10 grazie a funzionalità di partizionamento software:*Solaris Container e Logical Domain.*
Il pacchetto certificato rispetto ai Common Criteria, [33], [34], è il sistema operativo Solaris 10 Release 03/05 con il livello EAL4+: EAL4 augmented by ALC_FLR.3 (Systematic flaw remediation). I protection profile aggiuntivi sono: Controlled Access Protection Profile CAPP, Role Based Access Control Protection Profile RBAC PP e Labeled Security Protection Profile LSPP.

FSC (Fujitsu Siemens Computers)

La linea dei server PRIMEPOWER XA di FSC, [35], è basata sui processori SPARC64V ed è certificata per il sistema operativo Solaris. Quindi è applicabile la tecnologia di virtualizzazione fornita con il sistema sperativo Solaris10.

Considerazioni tecnologiche Server Unix

Tutti i principali fornitori hardware hanno una soluzione di virtualizzazione proprietaria; La soluzione attualmente più matura ed avanzata è il micropartizionamento di IBM che consente la virtualizzazione di cpu e I/O; la stessa caratteristica è disponibile su Solaris 10 (Sun/Fujitsu) ma è di più recente introduzione. Solo i Container di SUN e la SRP di HP consentono la condivisione della RAM; mentre il Micropartizionamento di IBM consente comunque di associare la RAM di qualsiasi board a qualsiasi partizione logica, ciò non è consentito per le vPars e la IVM di HP che sono limitate all'interno della

singola partizione fisica. La soluzione HP più consolidata è la vPar che ha granularità limitata.

Server Wintel e Open Source

Le tecnologie di virtualizzazione in ambito Wintel e Open Source presenti sul mercato odierno sono di due tipologie: *basata su Hypervisor (Non Hosted Architecture) e basata su Sistema Operativo (Hosted Architecture).*

I principali prodotti presenti sul mercato odierno possono essere racchiusi in VMware, Microsoft e Xen:

VMware

Offre due diverse soluzioni, **GSX Server** basata su Sistema Operativo realizzata mediante uno strato software che si integra con il sistema operativo attraverso il quale gestisce le risorse hardware. **ESX Server**, [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], basata su Hypervisor uno strato software che si sostituisce al sistema operativo e gestisce direttamente le risorse hardware mediante driver in genere specializzati. VMware ESX Server è composto da quattro componenti principali: *il Virtualization layer, o VMkernel, le Virtual Machines, il Service Console e il Virtual networking layer.*

Il pacchetto certificato rispetto ai Common Criteria, [47], [48], è VMware ESX Server 2.5.0 & VirtualCenter 1.2.0 con il livello EAL2. È prevista una nuova certificazione per ESX Server 3 & VirtualCenter 2.0 con il livello EAL4+.

Microsoft Virtual Server

Soluzione basata su sistema operativo, [49], e realizzata mediante uno strato software che si integra con il sistema operativo attraverso il quale gestisce le risorse hardware, Microsoft dichiara che avrà una soluzione di virtualizzazione basata su Hypervisor per il 2008-2009.

Xen

Soluzione di virtualizzazione, [50], basata su hypervisor che si sostituisce al sistema operativo e gestisce direttamente le risorse hardware mediante driver in genere specializzati di virtualizzazione per ambienti open source.

Considerazioni tecnologiche Server Wintel

Le soluzioni basate su Hypervisor sono meglio adatte a livello Enterprise rispetto a quelle basate su sistema operativo in quanto, interfacciandosi direttamente con l'hardware, sono meno complesse, hanno prestazioni maggiori (overhead di circa il 5% contro il 25% delle soluzioni basate su OS) e sono meno vulnerabili dal punto di vista della sicurezza e della stabilità.
Le soluzioni basate su Hypervisor hanno lo svantaggio di richiedere drivers specializzati per la gestione delle periferiche.

Conclusioni

Si è visto come dal concetto di privacy come riferimento alla sfera della vita privata si è arrivati ad un concetto tutelato dalla legislatura e poichè le Aziende hanno nel loro patrimonio informativo dati sensibili rispetto alla privacy queste sono state obbligate a introdurre nei loro sistemi informativi procedure di sicurezza per il trattamento di tali dati.
L'insieme di procedure di sicurezza sono governate da Standard riconosciuti a livello internazionale che permettono alle Aziende, tramite la certificazione, di garantire ai clienti il raggiungimento di un determinato livello di sicurezza. Tali Standard forniscono una metodologia per definire l'Information Security Management System - ISMS che mira a definire un approccio organizzativo al Risk Management.

D'altro canto le nuove tecnologie si stanno orientando verso la virtualizzazione dei Sistemi che offrono la possibilità controllare l'instabilità e la compromissione di un'applicazione (Threat Deception), creare un sistema honeypot per confondere gli attaccanti (Threat Deception), tecniche di analisi e investigazione informatica (Threat Detection) ed essere di supporto per il disaster recovery e l'high availability (Threat Prevention).

La virtualizzazione offre anche delle caratteristiche di sicurezza per isolare i dati, la memoria fisica e la rete (Isolation), mettere velocemente in quarantena un sistema compromesso sostituendolo con un nuovo sistema di produzione a partire dalle copie di backup (Attack Mitigation), realizzare una virtual machine con specifiche Policy (Policy Enfocement), creare macchine virtuali con dei componenti di sicurezza specifici (Defense-In-Depth), proteggere i dati contenuti all'interno di virtual machine attraverso meccanismi di crittografia (Encapsulation).

La virtualizzazione è realizzata attraverso un nuovo soggetto software, l'hypervisor, che a sua volta deve essere protetto per non inficiare i benefici di cui sopra diventando esso stesso il cavallo di Troia per tutto il sistema, in quanto è impossibile rilevare la sua compromissione con le normali tec-

niche di sicurezza da nessuno dei sistemi operativi host, perchè invisibile alle partizioni che gestisce.

Si ha quindi la necessità di garantire i livelli di sicurezza definiti nel Risk Management utilizzando protezioni ad hoc.

Per far fronte a queste esigenze, la teoria matematica fornisce uno strumento adatto: l'Hidden Markov Model.
Il modello permette, una volta definiti i valori di un comportamento corretto, di segnalare gli attacchi al sistema rilevando i comportamenti anomali. Grazie all'HMM sono stati realizzati prodotti come l'IDS e l'IPS per l'anomaly detection, che ben possono essere utilizzati per il monitoraggio di una soluzione di virtualizzazione.

Comunque, secondo Gartner Group, le soluzioni di virtualizzazione non sono ancora mature in tutti i loro aspetti, quindi le Aziende che le stanno adottando devono introdurre nei loro sistemi IT quelle soluzioni offerte dai Vendor che rispettano i criteri di sicurezza necessari.

A tale proposito è stato condotto uno scouting sui principali Vendor i cui risultati possono essere riassunti come segue:

- L'IBM ha presentato un sistema di virtualizzazione che raggiunge il livello di sicurezza, secondo i Common Criteria, EAL4+ con l'aggiunta del Protection Profile: Controlled Access Protection Profile - CAPP;

- VMware ha presentato una nuova versione del ESX Server che attualmente non è stato certificato, ma dovrebbe raggiungere il livello di sicurezza, secondo i Common Criteria, EAL4+, la versione precedente raggiunge solo il livello di sicurezza EAL2;

- SUN ha presentato un prodotto che raggiunge il livello di sicurezza, secondo i Common Criteria, EAL4+ con l'aggiunta dei Protection Profile: Controlled Access Protection Profile - CAPP, Role Based Access Control Protection Profile - RBAC PP e Labeled Security Protection Profile LSPP;

- HP ha presentato una soluzione per la virtualizzazione all'interno del proprio sistema operativo HP-UX11i che raggiunge il livello, secondo i Common Criteria, EAL4+ ma nella configurazione certificata non risultano incluse le partizioni fisiche nPar e virtuali vPar.

Bibliografia

[1] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio (24 ottobre 1995),

[2] Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali,

[3] Standard ISO/IEC 17799,

[4] Standard ISO/IEC 27001,

[5] TCSEC - Trusted Computer Systems Evaluation Criteria,

[6] ITSEC - Information Technology Security Evaluation Criteria,

[7] FC - Federal Criteria for Information Technology Security,

[8] A Risk Management Standard, *Published by AIRMIC, ALARM, IRM: 2002*,

[9] National Institute of Standards and Technology - NIST, *Risk Management Guide for Information Technology Systems*,

[10] Gartner Gorup, *Secure Hypervisor Hype: Myths, Realities and Recommendations*,

[11] Gartner Gorup, *Hype Cycle for Information Security, 2006*,

[12] Gartner Gorup, *Security Considerations and Best Practices for Securing Virtual Machines*,

[13] Gartner Gorup, *PC & ServerVirtualization: From Anomaly to Default, 2005*,

[14] Giuseppe Paternò, *Virtualizzazione e Sicurezza*, Marzo 2007.

[15] HP White Paper, *Introducing HP-UX 11i Virtual Partitions*,

[16] HP Virtual Server Environment for HP Integrity and HP 9000 servers Optimize server utilization in real time,

[17] HP Partitioning Continuum for HP-UX11i on HP 9000 and HP Integrity servers,

[18] HP, *Introduction to Integrity Virtual Machines*,

[19] HP, *Best Practices for Using Integrity Virtual Machines*,

[20] HP, *Designing High Availability Solutions with Serviceguard and Integrity VM*,

[21] HP, *HP-UX Virtual Partitions Administrators Guide*,

[22] Common Criteria Security Target, *HP-UX 11i v2 Security Target*,

[23] Common Criteria Certification Report No. P225, *Hewlett-Packard HP-UX Version 11.23 (11i Version 2)*,

[24] IBM Redbooks, *Advanced POWER Virtualization on IBM System p5: Introduction and Configuration*,

[25] IBM, *Partitioning for AIX*,

[26] IBM Redpaper, *IBM System p Advanced POWER Virtualization Best Practices*,

[27] IBM Redpaper, *Integrated Virtualization Manager on IBM System p5*,

[28] IBM Redbooks, *Partitioning Implementations for IBM E-server p5 Servers*,

[29] IBM Redbooks, *Virtualization and Clustering Best Practices Using IBM System p Servers*,

[30] Common Criteria Security Target, *AIX 5L Version 5.3 Technology level 53000502 with optional Virtual I/O Server Security Target*,

[31] Common Criteria Certification Report BSI-DSZ-CC-0385-2006, *IBM AIX 5L for POWER V5.3 Technology Level 5300-05-02 with optional Virtual I/O Server (VIOS), Version 1.3*,

[32] SUN Technical White Paper, *Solaris Containers: Server Virtualization and Manageability*,

[33] Common Criteria Security Target, *Solaris 10 03/05 Security Target*,

[34] Common Criteria Certification Report, *EAL 4+ Evaluation of Sun Microsystems Inc. Solaris 10 Release 03/05*,

[35] Fujitsu Siemens Computers, *www.fujitsu-siemens.com*,

[36] VMware White Paper, *Virtualization Overview*,

[37] VMware Book, *Introduction to VMware Infrastructure: ESX Server 3.0.1 and VirtualCenter 2.0.1*,

[38] VMware Book, *Quick Start Guide: ESX Server 3.0.1 and VirtualCenter 2.0.1*,

[39] VMware Book, *Installation and Upgrade Guide: ESX Server 3.0.1 and VirtualCenter 2.0.1*,

[40] VMware Book, *Basic System Administration: ESX Server 3.0.1 and VirtualCenter 2.0.1*,

[41] VMware Book, *Virtual Infrastructure Web Access Administrators Guide: ESX Server 3.0.1 and VirtualCenter 2.0.1*,

[42] VMware Book, *Server Configuration Guide: ESX Server 3.0.1 and VirtualCenter 2.0.1*,

[43] VMware Book, *Resource Management Guide: ESX Server 3.0.1 and VirtualCenter 2.0.1*,

[44] VMware White Paper, *Security Design of the VMware Infrastructure 3 Architecture*,

[45] VMware Best Practices, *Security Hardening of the VMware Infrastructure 3*,

[46] VMware White Paper, *Building the Virtualized Enterprise with VMware Infrastructure*,

[47] Common Criteria Security Target, *VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Security Target*,

[48] Common Criteria Certification Report, *VMware ESX Server 2.5.0 and VirtualCenter 1.2.0*,

[49] Microsoft, *www.microsoft.com*,

[50] Xen, *www.xensource.com*,

[51] P. Baldi, *Calcolo delle probabilità e statistica*, McGraw-Hill, Milano, 1998.

[52] L. R. Rabiner, *A tutorial on hidden Markov models and selected applications in speech recognition*, Proceedings of the IEEE (1989).

[53] Ye Du, Huiqiang Wang and Yonggang Pang, *A Hidden Markov Models-Based Anomaly Intrusion Detection Method*

[54] Shrijit S. Joshi and Vir V. Phoha, *Investigating Hidden Markov Models Capabilities in Anomaly Detection*

[55] Rahul Khanna and Huaping Liu, *System Approach to Intrusion Detection Using Hidden Markov Model*