Rete Dati di un polo Universitario: Strumenti e metodologie per la raccolta di prove in supporto alle indagini dell'Autorità Giudiziaria.

Implicazioni in ambito Privacy

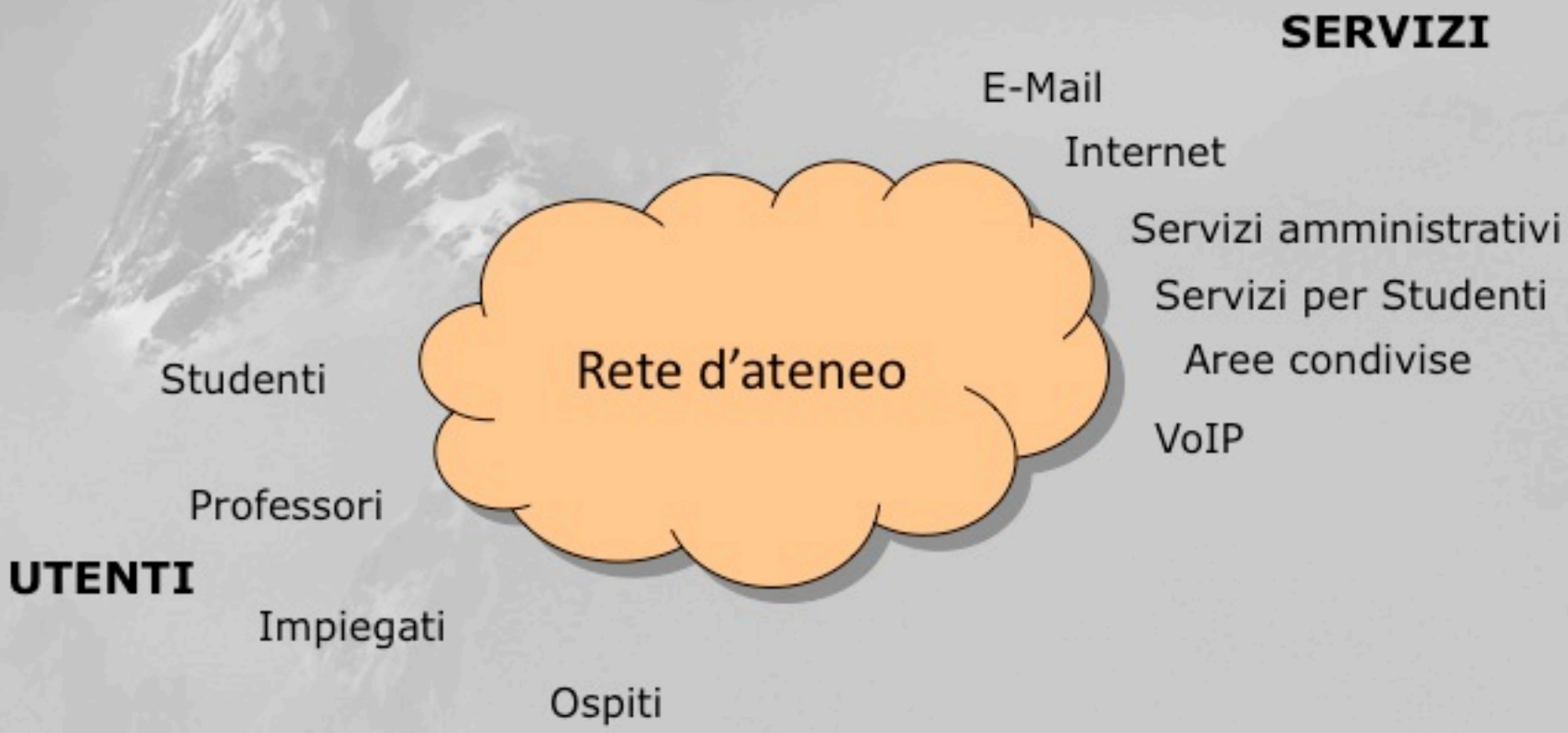
(Università degli Studi di Milano, Facoltà di Giurisprudenza, 21 giugno 2012)

Il livello di Privacy cui noi aspiriamo è alto
come la vetta di una montagna ...
ma sul percorso, nuvole s'adombrano...

Nicla Diomede Donato La Muscatella Marco Carlo Spada

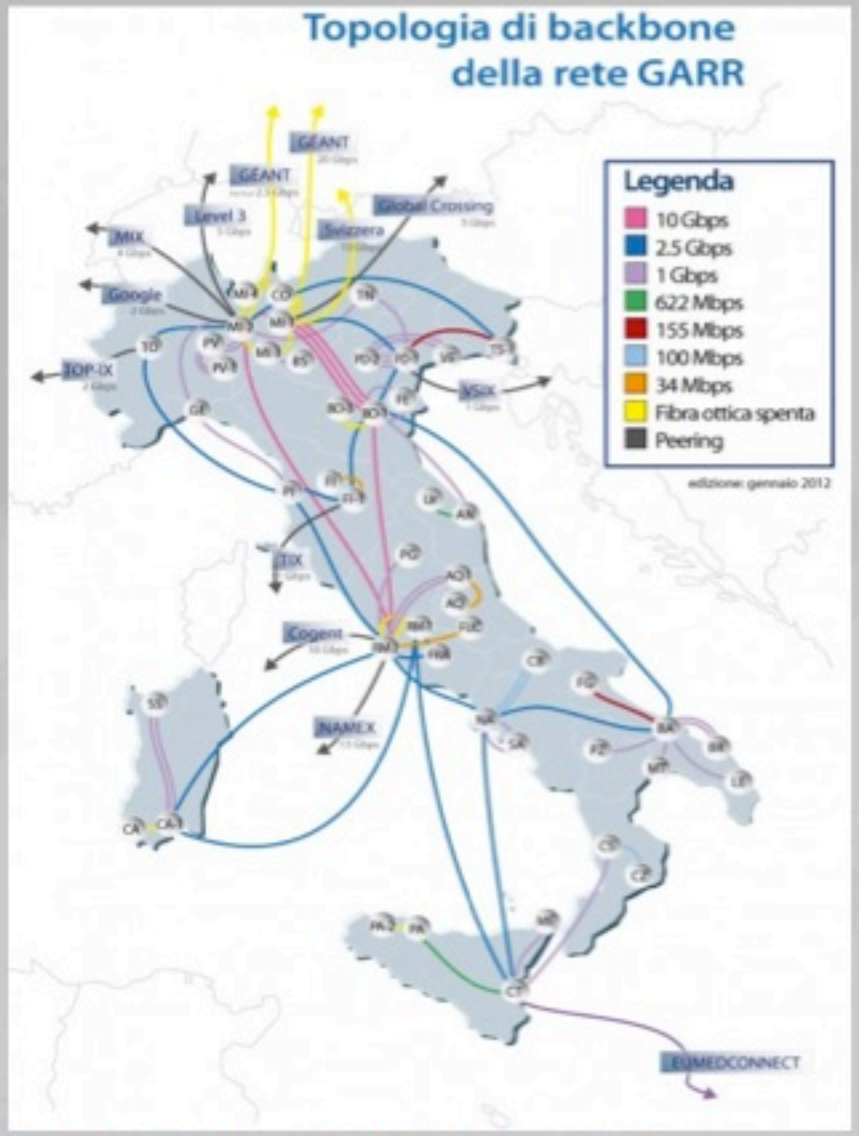
Le Reti Universitarie

Ambiente Universitario



Caratteristiche della rete Universitaria

- Lo scenario considerato è di una rete complessa, estesa ed eterogenea:
  - Unica per Ricerca, Didattica, Amministrazione
  - Elevato (>70) numero di sedi distribuite sul territorio
  - ambienti misti: presenza negli Ospedali
  - 65000 utenti
  - 40.000 punti cablati di cui circa 10.000 attivi
  - Cablata e wireless
  - Presenza promiscua nella stessa zona di varie tipologie di utenti appartenenti a strutture diverse
- Caratterizzato da:
  - Alta velocità
  - Affidabilità (ridondanza logica e fisica)
  - Supporto di servizi evoluti
- Interconnessa a Global Internet attraverso la Rete nazionale **GARR**



Consortium GARR

- gli Enti fondatori (CNR, ENEA, INFN e la Fondazione CRUI);
- gli organismi di ricerca vigilati dal MIUR, tra cui ASI, INAF, INGV e altri;
- i Consorzi Interuniversitari per il Calcolo (CASPUR, CILEA, CINECA);
- Organismi culturali e di ricerca afferenti ad altri Ministeri, quali MiBAC e Salute;

- Rete ad altissima velocità collegata a:
  - rete della ricerca Europea
  - Global Internet

- Regolamentata da policy

I beni universitari

- L'università acquisisce, usa e memorizza informazioni relative ai suo utenti: impiegati, docenti, pazienti, studenti, società con cui collabora.
- E' necessario che questi dati siano gestiti in modo appopriato per prevenire la perdita, il danneggiamento, l'accesso o il furto delle informazioni.
- Il cattivo utilizzo, la perdita o compromissione comportano un costo economico, un danno d'immagine e possibili ripercussioni legali/penali.
- DATI UNIVERSITA':
  - Proprietà intellettuale → ricerca, brevetti
  - Dati sensibili: dati medici
  - Dati amministrativi: dati del personale, stipendi, etc..
  - Dati legati al core business: dati carriera scolastica
  - Dati di studio per attività conto terzi
- La rete stessa è un bene

Criticità della sicurezza nelle Università

La sicurezza informatica è un problema

- complesso (coinvolge la rete, gli hosts e le persone),
- multilivello (tecnico, organizzativo, legale e sociale),
- in divenire (non è uno status, va costantemente mantenuta).

La sicurezza = protezione dei propri beni

≠ controllo o censura

L'Università NON è un azienda

Sicurezza Facilità d'uso

LE POLICY UNIVERSITARIE (AUP)

- Forniscono un insieme di regole per la tutela della rete, degli host e dei servizi informatici.
- Sensibilizzare e responsabilizzare l'utenza: costituisce una sorta di carta dei diritti e dei doveri dell'utente dell'Università.
- Impedire che la rete universitaria possa essere fonte di attacchi verso l'esterno.

Immagine tratta da:

http://www.thetis.it/projects/transportation-management/urban-mobility-delhi.html

Acceptable Use Policy

- Tutti gli utenti devono essere riconosciuti ed identificabili;
- Uso per sole attività istituzionali

E' VIETATO

- fornire accesso a soggetti non autorizzati;
- Compiere attività (diffusione di virus, etc.) che danneggino, molestino o limitino le attività altrui o i servizi;
- creare o trasmettere materiale che attenti alla dignità umana, se non per motivi di ricerca
- Danneggiare o cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti,
- Pubblicizzare attività proprie per fini di lucro
- Attività vietata da leggi dello Stato
- ------

Il regolamento di Sicurezza

DEFINISCE

- Chi può accedere alla rete
- Come e dove accedervi:
  - LAN cablate
  - HOTSPOT, Wireless LAN, Eduroam
  - Biblioteche
  - Via vpn
  - Aule informatiche
- Protocolli consentiti
- Attività ammesse e non
- Identificazione degli utenti
- Responsabilità personali dei contenuti diffusi
- Sanzioni per trasgressori
- Misure minime per server centrali, locali e postazioni utente
- Ruoli nella gestione della sicurezza

LA REALTA' E' MOLTO COMPLESSA

Immagine Tratta da "Minority Report"

Gestione tecnica dell'infrastruttura simile a quella del provider:

- Estensione e complessità della rete
- Presenza promiscua e contemporanea di diversi tipologie di utenti appartenenti a strutture diverse
- Controllo e gestione totale dell'infrastruttura di rete
- Nessun controllo dei singoli pc/server locali gestiti in autonomia dalle singole strutture
- No controllo sull'accesso fisico alle sedi universitarie

Dal punto di vista giuridico il modello è quello privato:

- Rete riservata ai soli aventi diritto

Difficoltà di adottare policy stringenti di sicurezza:

- Eterogeneità utenti, vastità e molteplicità di utilizzo, libertà di ricerca
- Facilità di uso (autenticazione centralizzata per accesso alla rete solo in zone ad accesso pubblico)

Incidenti Informatici : > 500 all'anno

- Rete molto veloce, soggetta a continui tentativi di intrusione
- 10.000 host in rete
- Macchine con alte performance ma non sempre ben gestite

di cui alcuni con risvolti penali/legali (richiesta A.G.)

RICERCA DEL COMPROMESSO TRA:

- Necessità di proteggere beni universitari
- Garantire livelli di servizio
- Tutelare l'ente da responsabilità (D. Lgs 231/2001)
- Tutelare la privacy degli utenti
- Garantire la conformità allo Statuto dei lavoratori

I Profili Giuridici

L'amministrazione delle Reti di questa complessità presenta, per lo studioso di *ICT law*, plurimi aspetti di interesse.

Cos'è l'ente amministratore della Rete?

Si tratta, sulla base di :

- copertura territoriale della rete;
- finalità di concessione dell'utilizzo della rete;
- logica dell'infrastruttura di rete interna;
- identificazione dei terminali utilizzati sulla Rete *web*

di un soggetto (nel caso dell'Università degli Studi di Milano un'**Amministrazione Pubblica**) che offre e gestisce (in ispecie gratuitamente) una **rete privata di comunicazioni elettroniche** con **funzioni istituzionali**, sulla quale operano **utenti identificati di diversa natura**.

Nel caso preso ad esempio, infatti, la Rete dell'Università degli Studi di Milano, è collegata alla rete *GARR* , della quale accetta (e fa accettare all'utente) le *policies*.

... tuttavia...

Non sono utilizzati applicativi di controllo dell'attività degli utenti che impediscono la consultazione di siti *web* "*non edu*" (per garantire la ricerca ad ampio raggio).

... ergo ...

La Rete può essere utilizzata, potenzialmente, per *navigazioni private*, con scopi estranei a quelli per i quali il servizio di comunicazione elettronica viene predisposto e concesso in utilizzo all'utenza (ed eventualmente illeciti).

A ciò s'aggiunga il rischio proveniente da attacchi esterni all'infrastruttura, a tutt'oggi molto frequenti.

Pur non trattandosi di un ente assimilabile agli ISPs, trovano applicazione alcune modalità di regolamentazione dell'infrastruttura telematica ad essi riferiti.

Il monitoraggio della Rete, tuttavia, avverrà essenzialmente come attività di prevenzione rispetto a lesioni dei "beni aziendali".

Pur non trattandosi di un ente assimilabile agli ISPs, trovano applicazione alcune modalità di regolamentazione dell'infrastruttura telematica ad essi riferiti.

Il monitoraggio della Rete, tuttavia, avverrà essenzialmente come attività di prevenzione rispetto a lesioni dei "beni aziendali".

RESPONSABILITÀ

CONTROLLO

REGOLAMENTAZIONE IBRIDA

Questo tipo di qualificazione, come si vedrà, non è priva di effetti, tanto e gli **obblighi** dell'Istituzione universitaria, devono essere modulati anche in ordine ai **diritti** vantati dalle diverse categorie di utenti.

Che tipo di dati transitano sulla Rete?

Si tratta di dati *personali* e, in alcuni casi, *sensibili* degli utenti.

Peraltro, anche i *dati tecnici* relativi alla trasmissione delle informazioni rientrano, secondo un orientamento che si sta diffondendo a livello comunitario, nella categoria dei dati sensibili.

Tra questi l'Avvocato Generale Jaaskinen che così si è espresso in relazione al caso *Bonner Audio* discusso dinanzi alla Corte di Giustizia dell'Unione Europea.

(vd. conclusioni del 19.11.2011, CGUE C-451/10)

Che tipo di utenti utilizzano la Rete?

Utenti Generici (studenti)

Questa tipologia di utenti, è tutelata dalle norme generali in materia di protezione dei dati personali.

Utenti Generici (studenti)

- *informativa* sul trattamento dei dati

✓ cosa

✓ come

✓ chi

✓ per quanto tempo

che assicuri un'adeguata "*informazione e consapevolezza*"

- non è necessario il *consenso* al trattamento

***Utenti Qualificati* (lavoratori)**

Questa classe di utenti, si giova di un ampliamento di protezione legato alla disciplina giuslavoristica.

In particolare, l'attività del lavoratore **non può essere monitorata in tempo reale** per verificarne l'operato, anche sulla Rete.

Utenti Qualificati (lavoratori)

Sul punto, la Corte di Cassazione ha ritenuto legittimo, anche in assenza di accordo o autorizzazione preventiva *"il monitoraggio delle strutture informatiche aziendali che prescinde dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa, ma è diretto ad accertare* ***ex post*** *la perpetrazione di eventuali comportamenti illeciti"*

(cfr. Cass.Civ., Sez.Lav., 13.12.2011 (23.02.2012), n. 2722)

Utenti Qualificati (lavoratori)

- *informativa* sul trattamento dei dati formulata in modo specifico;
- non è necessario il consenso al trattamento
- *disciplinare interno* redatto in modo chiaro e senza formule generiche;
- rispetto dei *divieti assoluti* di utilizzo (es. *keyloggers*, analisi occulta dei *laptops*, etc.)

(Delibera n. 13 del 01.03.2007 del Garante per la Protezione dei Dati Personali)

Utenti Qualificati (lavoratori)

Peraltro i datori di lavoro, anche pubblici, hanno l'onere di adottare *"tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi"* (cc.dd. *PETs*)

... ma...come?

Come *monitorare* l'attività della Rete?

Con il termine si intende :

- ✓ analisi dei dati relativi alle operazioni di comunicazione elettronica in senso stretto;
- ✓ analisi delle attività di navigazione *web*;
- ✓ analisi della corrispondenza telematica degli utenti assegnatari di un indirizzo *e-mail*

… che ne è della Privacy?

Alla luce di quanto detto, peraltro, i protocolli operativi dovranno tener conto del **massimo livello di tutela** possibile in rapporto alla categoria di utenti alla quale spettino maggiori garanzie.

Il trattamento dei dati, dovrà avvenire, in primo luogo, conformemente ai *principi* di

- *necessità*
- *pertinenza*
- *non eccedenza*

L'eventuale analisi dei dati, dovrà avvenire solo ed esclusivamente **a posteriori**, da **personale autorizzato** e per **fini legalmente autorizzati**.

inoltre

I *files di log* dovranno essere:

- leciti (in relazione alla disciplina in materia di dati personali e tutela dei lavoratori);
- conservati in forma aggregata ed in formato grezzo;
- conservati per un periodo massimo di dodici mesi;
- identificabili solo dopo disaggregazione e correlazione delle informazioni;
- sovrascritti automaticamente allo scadere del periodo di *data retention*

mentre

Più opinabili sono:

- ✓ adozione di misure tecniche e organizzative adeguate al rischio esistente;
- ✓ comunicazione al Garante ed agli interessati "*senza indebiti ritardi*" di eventuali violazioni di dati personali (salvo i*nintellegibilità* dei dati);
- ✓ adozione ed aggiornamento dell'*inventario delle violazioni di dati personali*

(cfr. D.Lgs. n. 69 del 28 maggio 2012, in vigore la 01.06.2012)

Come collaborare alle indagini?

Due le ipotesi in campo:

I. richiesta proveniente dall'Autorità Giudiziaria (artt.247, I *bis*, 253, 254 *bis* c.p.p.)

II. richiesta proveniente dal difensore (art. 391 *quater* c.p.p.)

In entrambi i casi bisognerà operare sul sistema se il soggetto presenti **idoneo provvedimento o documentazione** (decreto A.G. o atti di polizia giudiziaria relativi ai mezzi di ricerca della prova in ipotesi d'urgenza; richiesta di documentazione motivata del difensore).

- consegnando i soli dati rilevanti in copia conforme all'originale, in forma aggregata ed in formato grezzo, riferiti al periodo oggetto di investigazione;
- mantenendo integro e disponibile l'originale delle informazioni digitali consegnate sul sistema di amministrazione, evitandone la sovrascrittura;
- sollecitando accertamenti tecnici urgenti, compiuti dalle Autorità competenti con ogni garanzia necessaria, qualora il sistema presenti rischi di instabilità

Esempio di Infrastruttura

Infrastruttura di monitoraggio e raccolta di Dati relativi alla sicurezza provenienti da diverse fonti

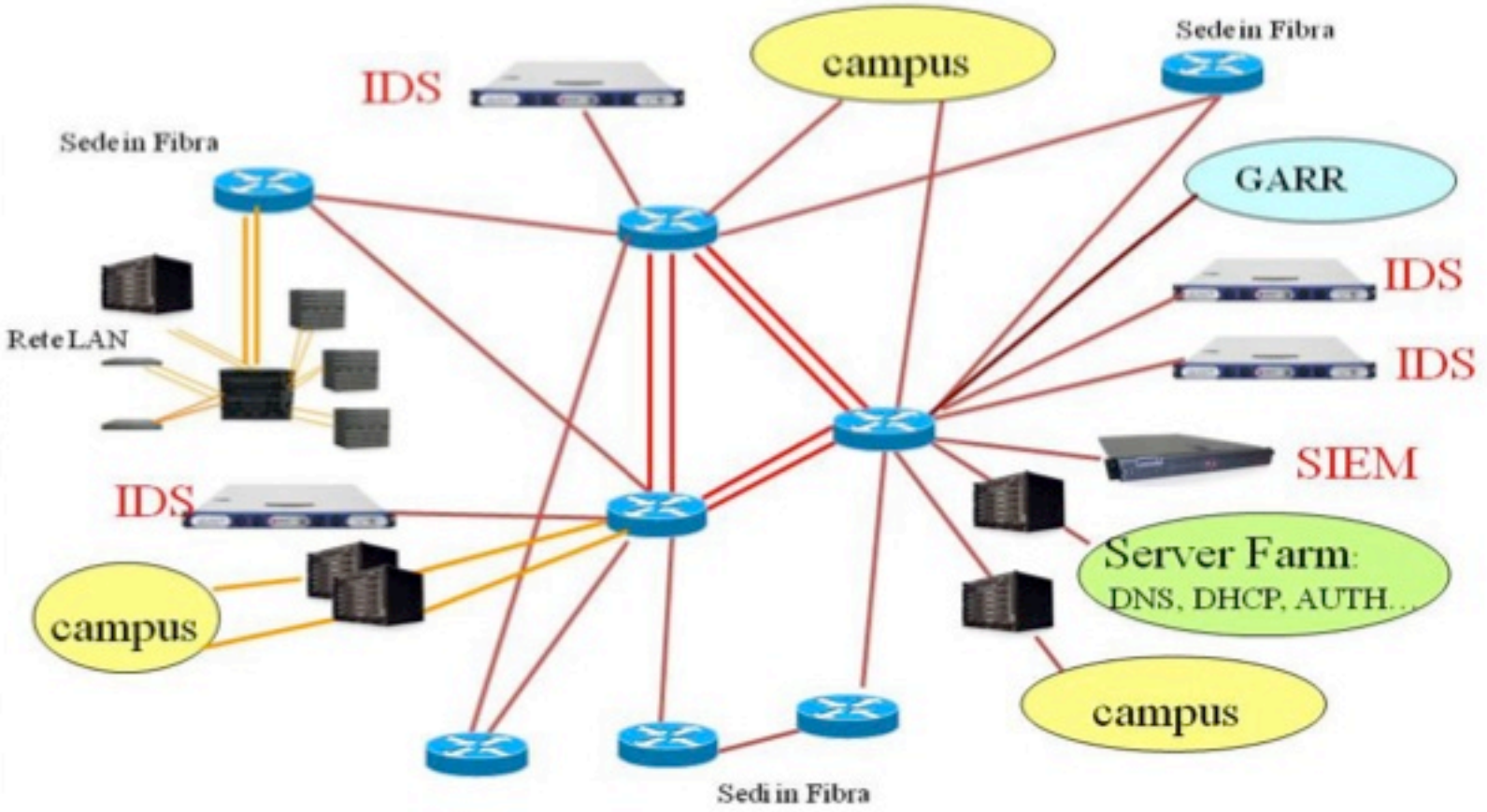
Ha lo scopo di:

- individuare tempestivamente gli incidenti informatici attraverso sofisticate metodologie di detection e blocco automatico per alcuni di essi (limitare l'impatto all'esterno)
- Eventuali indagini interne
- Fornire le opportune risposte in caso di richiesta dell'AG

Correla, normalizza e prioritizza le informazioni provenienti da più punti di osservazione
al fine di ricostruire la dinamica dell'incidente/illecito

- Eventi di sicurezza IDS distribuiti in rete (analizzano tutto il traffico su rete geografica)
- Log server (DHCP, DNS, ..), log dei firewall e router,
- Analisi comportamentale degli host attraverso l'analisi traffico
  - Traffico backbone rete e server farm (Netflow v. 5)
  - Traffico IN/OUT verso la rete esterna GARR (netflow v.9)

SCHEMA ESEMPLIFICATIVO DELL'ARCHITETTURA



INFRASTRUTTURA DI RACCOLTA DEI DATI

Segnalazione Incidente 1/2

Esempio di notifica di incidente:

Offense 359

Magnitude	[redacted]		Relevance	4	Severity	5	Credibility	3
Description	Multiple Login Failures for the Same User preceded by Multiple Login Failures from the Same Source	Offense Type	Source IP				
		Event/Flow count	439 events and 5073 flows in 4 categories				
Source IP(s)	187.141.[redacted]	Start	2012-03-13 15:11:08				
Destination IP(s)	Local (2132)	Duration	38m 49s				
Network(s)	Multiple (102)	Assigned to	Not assigned				

Offense Source Summary

IP	187.141.231.140	Location	Mexico
Magnitude		Vulnerabilities	0
User	root	MAC	Unknown
Host Name	customer-187-141-231-140-sta.uninet-ide.com.mx.		
Asset Name	Unknown	Asset Weight	0
Offenses	2	Events/Flows	5520

Last 5 Notes

Notes	User Name	Create Date

No results were returned.

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
187.14[redacted]		Mexico	Unknown	root	Unknown	0	2	2132	2d 36m 19s	5520

Top 5 Destination IPs

Destination IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows
159.[redacted]		ScienzeDellaInformazione[redacted]	Unknown	No	Unknown	Unknown	0	8	8	1h 53m 11s	16
159.[redacted]		[redacted]	Unknown	No	Unknown	c6:c0:36:6c	0	9	31	15m 25s	68
159.[redacted]		[redacted]ospedale[redacted]	Unknown	No	Unknown	4d:a1:d8:b9	0	8	8	2h 28m 53s	15
159.[redacted]		[redacted]	Unknown	No	Unknown	7e:f0:fc:2b	0	11	29	1h 54m 21s	37
159.[redacted]		[redacted]MedicinaLavoro	Unknown	No	Unknown	a3:38:8e:d6	0	10	10	11h 45m 57s	91

Segnalazione Incidente 2/2

Top 5 Log Sources

Name	Description	Group	Events/Flows	Offenses	Total Events/Flows
IOS @ 159.	IOS device		332	5	3681
IOS @ 159.	IOS device		99	5	3254
Custom Rule Engine-8 :: dsco-unimi	Custom Rule Engine		8	524	5409

Top 5 Users

Name	Events/Flows	Offenses	Total Events/Flows
root	316	4	5800
bin	7	3	205
www	6	2	55
oracle	6	3	105
mircle	4	2	53

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
Misc Login Failed		2	4	03-13 15:14:45	03-13 15:47:52		
User Login Failure		2	4	03-13 15:14:43	03-13 15:37:19		
SSH Login Failed		2	431	03-13 15:14:33	03-13 15:49:52		
Remote Access		2132	5073	03-13 15:11:45	03-13 15:40:17		

Top 10 Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:27
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:13
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:20
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:47:59
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:52
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:47
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:28
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:38
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:11
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:57

Top 10 Flows

Application	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Last Packet Time
RemoteAccess.SSH_TCP_Allot	187.141.	40281	159.	22	2	2012-03-13 15:40:45
RemoteAccess.SSH_TCP_Allot	187.141.	35964	159.	22	2	2012-03-13 15:40:17
RemoteAccess.SSH_TCP_Allot	187.141.	39447	159.	22	2	2012-03-13 15:40:17
RemoteAccess.SSH_TCP_Allot	187.141.	36115	159.	22	2	2012-03-13 15:40:17

Dettaglio Flusso

Esempio dettaglio flusso sospetto connesso all'incidente con annesso l'elenco delle regole che si son verificate e che hanno partecipato allo scatenarsi della segnalazione dell'incidente


Esempio di flusso sospetto, correlato all'incidente

Flow Information

Protocol:	tcp_ip	Application:	RemoteAccess:SSH_TCP_Alot				
Magnitude:	(8)	Relevance:	10	Severity:	5	Credibility:	10
First Packet Time:	2012-01-23 23:36:45	Last Packet Time:	2012-01-24 00:36:15	Storage Time:	2012-03-13 15:40:45		
Event Name:	Terminals:___SSH_TCP						
Low Level Category:	Remote Access						
Event Description:	Application detected with Signature						
allot_group (custom):	Terminals						
allot_application (custom):	SSH						

Source and Destination Information

Source IP:	8.[redacted]167.14	Destination IP:	[redacted]158
Source Asset Name:	N/A	Destination Asset Name:	N/A
IPv6 Source:	0:0:0:0:0:0:0:0	IPv6 Destination:	0:0:0:0:0:0:0:0
Source Port:	40281	Destination Port:	22
Source Flags:	S,Illegal9	Destination Flags:	P,U,Illegal9
Source QoS:	Best Effort	Destination QoS:	Best Effort
Source ASN:	0	Destination ASN:	0
Source If Index:	0	Destination If Index:	0
Source Payload:	0 packets, 1 bytes	Destination Payload:	0 packets, 1 bytes

Source Payload
Destination Payload

ascii	hex	base64	ascii	hex	base64
Wrap Text			Wrap Text		
FLOWS=1;IP_PROTOCOL_VERSION=4;Vendor65=608,Terminals;					

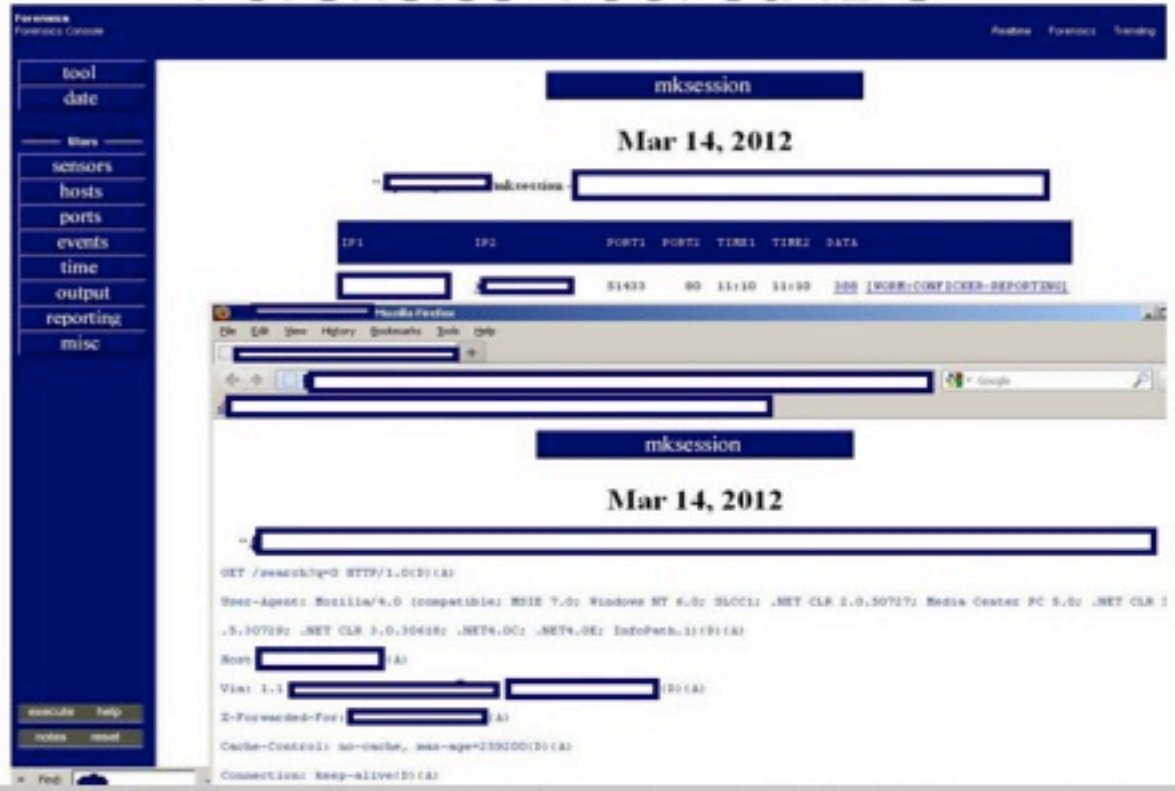
Additional Information

Flow Type:	Standard Flow	Flow Source/Interface:	
Flow Direction:	R2L		
Custom Rules:	BB:PortDefinition: SSH Ports BB:CategoryDefinition: Any Flow Magnitude Adjustment: Destination Network Weight is Low Recon: Remote SSH Server Scanner Users Magnitude Adjustment: Destination Asset Exists Magnitude Adjustment: Source Network Weight is Low Magnitude Adjustment: Context is Remote to Local BB:NetworkDefinition: Client Networks BB:PortDefinition: Authorized L2E Ports BB:NetworkDefinition: Inbound Communication from Internet to Local Host BB:NetworkDefinition: Untrusted Network Segment		
Custom Rules Partial Matched :	System: Flow Source Stopped Sending Flows		
Annotations:	Relevance has been decreased by 2 because the destination network weight is low. Relevance has been increased by 8 because the destination asset exists. Relevance has been decreased by 2 because the source network weight is low. Relevance has been increased by 2 because the context is Remote to Local.		

Eventi catturati da IDS

Per gli eventi IDS è possibile consultarne i dettagli attraverso la console di visualizzazione del sistema IDS

Forensics Tool su IDS



Premessa

La sicurezza implementata sull'infrastruttura di raccolta e conservazione dati è il

COMPROMESSO TRA

- complessità dello scenario,
- costi economici
- risorse umane

E

- probabilità di riuscita di un attacco verso una delle componenti della infrastruttura
- scopi della raccolta stessa.

Attività intraprese per PRESERVARE la fonte di prova e la protezione ai fini PRIVACY

I dati raccolti possano essere "prove" in ambito giudiziario se vi son garanzie di

- Disponibilità
- Autenticità
- Integrità

La messa in sicurezza di tutte le componenti dell'infrastruttura di raccolta e conservazione dei dati contribuiscono a dare le opportune garanzie in termini di normativa privacy.

Disponibilità dei dati

Server, firewall e router -> log a syslog server (syslog-ng) soggetto a backup
LOG disponibili su:

- syslog server per un anno (conservato in modo compresso) e ruotati giornalmente)
- server in locale (>= 1 mese)
- SIEM

Uso timestamping e firma digitale sui log archiviati a garanzia integrità e autenticità.
Eventi IDS:

- DB locale eventi ultimi 6 mesi;
- backup giornaliero su appliance dedicata: DB dell'ultimo anno in formato compresso e con garanzia di integrità

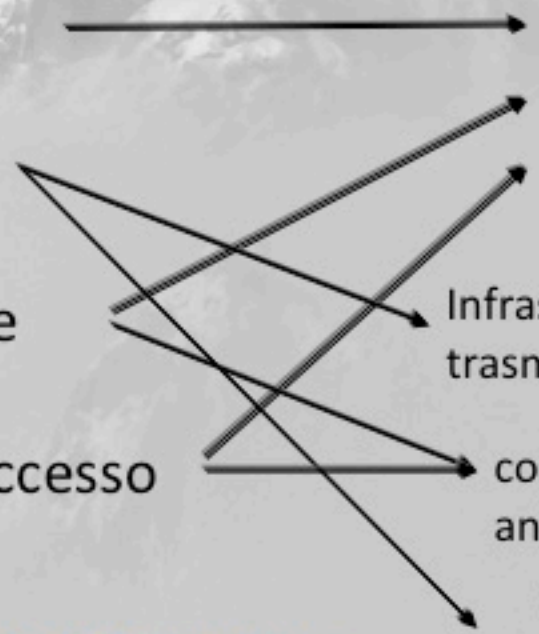
- SIEM
  - Meccanismi di hash su DB eventi e DB flussi
  - Retention personalizzabile su eventi, flussi e offese
- Infrastruttura di rete ridondata

Integrità e autenticità

In che modo garantirle?

Rendendo sicuri i dati memorizzati in fase di

- Generazione
- Trasmissione
- Conservazione
- Controllo di accesso



Messa in sicurezza di ciascuna componente infrastruttura (server, router, IDS, firewall, SIEM)

Infrastruttura totalmente gestita anche a livello trasmissivo internamente,

controlli di integrità e crittografia dati, sistemi antintrusione e auditing

Uso crittografia in comunicazioni tra IDS-SIEM e IDS-gestore IDS

Misure di sicurezza minime comune intraprese

Ciascun server erogante servizi di rete (DNS, DHCP, Auth,…) o appliance:

- Ridondato (solo server)
- Sincronizzato a NTP di Ateneo
- posizionati in Server Farm ad accesso controllato
- Soggetto a Backup
- Configurata in DMZ dedicata (netmask /29 o /30)
- installato e configurato seguendo le linee guida della NSA USA (server)
- adozione di controlli di integrità sui file, di meccanismi antintrusione e auditing
- Controllo accessi (compliance normativa AdS)
- S.O. linux o appliance con S.O. proprietario (derivato da linux)

Infrastruttura di rete a livello fisico, trasmissivo, logico gestita in modo autonomo (improbabile attacchi MiD)

Comunicazione crittografata:

Sonde IDS -> gestore IDS;

Gestore IDS → SIEM

Integrità e autenticità: su IDS

- IDS e gestore IDS su sottorete dedicata (netmask /30)
- IDS e gestore IDS connessi fisicamente ai router di backbone posti in locali protetti
- Password per il DB eventi
- S. O. proprietario
- ACL sui router coinvolti (accesso solo da sottoreti autorizzate) + iptables
- Host IDS sul gestore IDS (ad es. controlli integrità file)
- Sincronizzazione con il server NTP dell'Università (orario ufficiale).
- Comunicazione crittata:
  - IDS e gestore IDS
  - gestore IDS e suo backup
  - gestore IDS - SIEM (snmpv3 in modalità crittata).
- Accesso al gestore IDS tramite:
  - connessioni ssh2 da IP e utenti autorizzati.
  - applicativo proprietario basato su crittografia e autenticazione.
  - Visualizzazione DB degli eventi via SSL.

Integrità e autenticità: SIEM

- Configurazione su una sottorete dedicata (netmask /30)
- SIEM connessa fisicamente a router di backbone in locale protetto
- password per la scrittura nei DB
- S.O. proprietario hardened
- ACL sui router coinvolti (accesso solo da sottorete autorizzata) + iptables
- sincronizzazione NTP ateneo.
- Logging
- Comunicazione crittata:
  - Gestore IDS – SIEM
  - Accesso alla SIEM via ssh2 (ai soli ip e sistemisti responsabili del servizio);
  - Accesso alla console di SIEM via SSL.
- Hashing per i DB eventi e DB flussi

Integrità e autenticità: SERVER

- Configurazione su una sottorete dedicata (netmask /30-29)
- Server in DMZ d'Ateneo e fisicamente in Server Farm protetta
- Configurato secondo le linee guida della NSA-USA (National Security Agency)
- Iptables e ACL router
- Logging e invio al syslog server
- Hardening S.O.(attivazione anche SELinux)
- Disattivazione Mount dinamico/ supporto USB
- Permessi RWX personalizzati su file/directory.
- Update automatico del SW
- Attivazione di sistemi anti intrusione, SW di controllo di integrità, audit, antiDOS
- Accesso:
  - Via SSH solo da apposita sottorete e sistemisti autorizzati.
  - Disabilitazione root
  - modalità privilegiata via 2° livello autenticazione
  - Controllo accessi al sistema e ai suoi file/directory (partizioni per ogni user).
  - Protezione dell'accesso fisico alla console
- Crittografia dei filesystem

Integrità e autenticità: router

- Infrastruttura gestita , anche a livello trasmissivo, e manutenuta in totale autonomia
- Router in locali tecnici chiusi di proprietà universitaria
- Accesso solo da IP/tecnici autorizzati:
  - 1° Livello (RO): protocollo SSH2 con autenticazione via server AAA
  - 2° Livello (RW): tramite password locale dedicata
- Sincronizzazione NTP centralizzata
- Logging accessi
- Accesso fisico via console autenticato con server AAA
- ACL servizi locali (SSH, snmp, time etc.)
- ACL IN/OUT antispoofing
- ACL ulteriori sul router di bordo

CONCLUSIONI:

La piattaforma in oggetto può fornire utile supporto probatorio grazie a:

- adozione di opportune misure di sicurezza su ciascuna componente
- Rete totalmente gestita e mantenuta dall'Università
- bassa probabilità di buona riuscita di un attacco volto a eludere le misure
- Alto livello di competenza tecnica (expertise) richiesto

NETWORK FORENSICS

- ✓ che atteggiamento tengo come CTP a fronte del materiale informatico acquisito presso una rete di questo tipo?
- ✓ la terzietà del gestore della rete mi garantisce sempre e comunque?
- ✓ e un'analisi delle caratteristiche dei sistemi di raccolta e trasmissione delle tracce di rete ci può portare alla definizione di un insieme di "Best Practices" in tal senso?

- ✓ Cosa sono i Log ?
- ✓ Quale è la loro principale funzione ?
- ✓ Dove si trovano ?

I Log: da dove vengono, come vengono trasferiti, come si presentano

Apparati:

- Switch
- Router/Firewall
- IDS
- Proxy Server
- Application Server

Protocolli:

- Syslog
- NetFlow

Formati:

- ASCII
- Binari
- pcap dump
- DB

È in linea teorica possibile:

- ✓ l'alterazione dei log attraverso la compromissione degli apparati
- ✓ l'alterazione dei log attraverso attività malevoli sulla rete

Lavori teorici sui log:

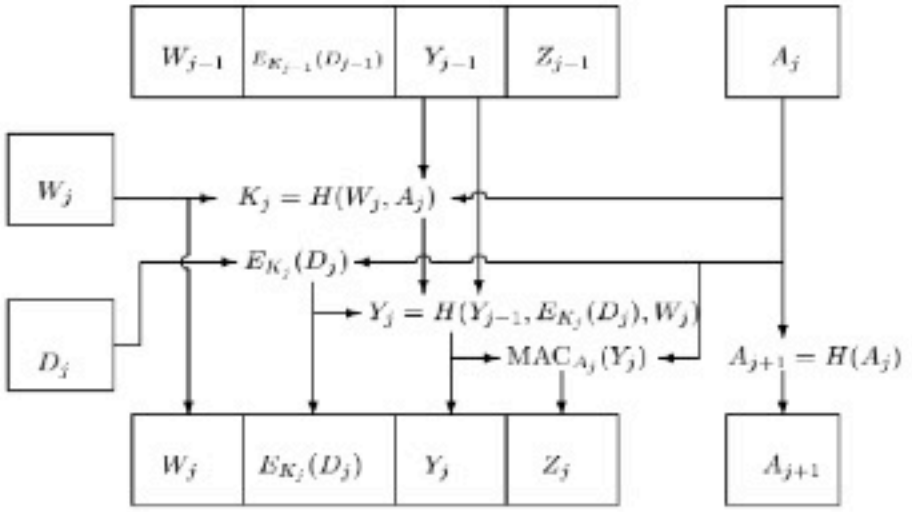


Figure 1: Adding an entry to the log.

- ✓ Bruce Schneier, John Kelsey - Secure Audit Logs to Support Compter Forensics - 1999
- ✓ Steena Dominica Steven Monteiro, Robert F. Erbacher - An Authentication and Validation Mechanism for Analyzing Syslogs Forensically

Trasmissione dei log sulla rete:

IEEE 802.__	VLAN – MAC ACLs
IPv4	VPN – IPsec – Tunnelling – IP filtering
UDP	
IPv6	AH – ESP

Vantaggi con IPv6

(Bruce J. Nikkel - An introduction to investigating IPv6 networks - 2007)

- ✓ Migliore identificabilità degli apparati in forza dell'ampio spazio di indirizzi
- ✓ Scansioni più complesse per gli attaccanti
- ✓ AH ed ESP incorporati

Concludendo, un draft di proposta per best practices

- ✓ "Logs chaining and hashing"
- ✓ Adozione di modalità di trasmissione sicure e controllate
- ✓ Descrizione "a priori" del sistema di raccolta dei log

Q & A

Grazie per l'attenzione

Nicla Diomede Donato La Muscatella Marco Carlo Spada

Nicla Diomede
nicla.diomede@unimi.it

Donato La Muscatella
donato.lamuscatella@hotmail.it

Marco Carlo Spada
m.c.spada@opimaint.it