ICT security awareness programme

SecureLog Appliance™

SECURE EDGE
your safety net

Sandro Fontana, CISSP, CISA, CISM, L.A. BS7799
CTO Secure Edge
sfontana@secure-edge.com

di cosa si parla

di quanto i log siano necessari
per implementare ed aumentare
la sicurezza ed affidabilità dei vostri sistemi.

di come implementare una infrastruttura che,
basandosisu tecniche crittografiche,
permetta la loro corretta e *certificata*
acquisizione e conservazione.

perchè è importante

- La mancanza di meccanismi di raccolta dati indebolisce o annulla la capacità di scoprire comportamenti sospetti e tentativi di intrusione;
- Inoltre rende impossibile determinare se queste aggressioni hanno avuto successo o meno;
- L'errata configurazione e gestione sicura dei dati di log, metterà questi ultimi a rischio di compromissione, rendendo i successivi esami ed analisi più difficili, se non impossibili;

Log importance /1

Avere un sistema sicuro presuppone
la generazione di dati di log utili,
la loro acquisizione e conservazione centralizzata
la garanzia di avere i log disponibili, completi ed integri (*)

(*) e di effettuarne una corretta e tempestiva analisi

Log importance /2

L'esistenza di un log sicuro, permette:

- di effettuare una estensiva analisi di guasti ed errori del sistema e delle applicazioni presenti su di esso
- di evidenziare i segni di anomalie o di abuso del sistema
- di supportare le fasi successive ad un incidente
- di fornire dati critici in caso di computer forensic analysis

The FBI rate 6th highest priority
on their list of top 20 vulnerabilities:
"Non-existent or Incomplete logging"

Norme e standards

ISO 9001:2000

ISO/IEC 17799:2005

ISO/IEC 27001:2005

Common Criteria

Common Criteria

(Security functional requirements)

Class FAU: Security Audit

- **FAU_ARP: Security audit automatic response**
- **FAU_GEN: Security audit data generation**
- **FAU_SAA: Security audit analysis**
- **FAU_SAR: Security audit review**
- **FAU_SEL: Security audit event selection**
- **FAU_STG: Security audit event storage**

Information Security Policies

(by Charles Cresson Wood - May 2005)

27 policies che descrivono:

- cosa deve e non deve essere registrato nei log
- la gestione dei log
- come assicurare ai log integrità e protezione
- le norme di accesso ed uso
- requirements per l'infrastruttura IT di supporto

Richiami alla gestione dei log

- *10.1.1 Documented operating procedures*
- *10.1.2 Change management*
- *10.10.2 Monitoring system use*
- *10.10.3 Protection of log information*
- *12.2.1 Input data validation*
- *12.2.2 Control of internal processing*
- *12.2.4 Output data validation*
- *12.4.1 Control of operational software*
- *12.4.3 Access control to program source code*
- *12.6.1 Control of technical vulnerabilities*
- *13.2.3 Collection of evidence*
- *15.1 Compliance with legal requirements*

Decreto Pisanu

si inserisce in un contesto normativo preesistente sulle intercettazioni

- Decreto Legislativo 196 del 30/06/2003
  (Codice in materia di protezione dei dati personali")
- Decreto Legge 144 del 24/07/2005
  convertito nella Legge 155 del 31/07/2005 (Legge Pisanu)
- Legge 547/93 sui crimini informatici
- Capo IV (artt.266 e ss.) del Codice di procedura penale
  "Intercettazioni di conversazioni o comunicazioni"
- Art.617 bis del Codice Penale
  " Installazione di apparecchiature atte ad intercettare
  o ad impedire comunicazioni o conversazioni telegrafiche
  o telefoniche"

Norme antiterrorismo /1

Europa:

Al lavoro il Consiglio dei Ministri Europei di Giustizia

Ipotesi

- periodo minimo per data retention:
  obbligo per operatori telecomunicazioni e Internet Provider:
  12 mesi per dati telefonia mobile
  6 mesi per dati traffico internet
- NO contenuto comunicazioni *ma*
  identificazione interlocutori della conversazione,
  data e ora della stessa, mittente e destinatario e-mail;
- Indicazioni su eventuali compensazioni per
  i costi sostenuti dagli operatori per la data retention

Norme antiterrorismo /2

Italia:

- "Pacchetto Pisanu"

(Decreto Legge 144 del 24/07/2005 convertito nella Legge 155 del 31/07/2005)

Con esclusione dei contenuti delle comunicazioni, si stabilisce che i dati relativi al traffico telefonico e telematico non possano essere cancellati fino al 31 Dicembre 2007 (art.6)

- Decreto del Ministero dell'Interno del 16/08/2005

(specificato dalla Circolare Ministero dell'Interno n° 557 del 2005)

condiziona l'apertura degli Internet Point al rilascio di una licenza del Ministero stesso e impone agli Internet Point l'obbligo di identificazione "..dei soggetti che utilizzano postazioni pubbliche non vigilate.."


what ?

Management

- Controllo accessi:
  - l'accesso ai dati è riservato;
  - l'accesso ai dati deve essere tracciato;

- Prevenzione da
  - Alterazioni
  - Disattivazione
  - Cancellazione

I log devono:
- risiedere su un sistema fisicamente e logicamente protetto;
- poter dimostrare la propria integrità

- Log Rotation and Archive Process:
  - Log generato senza soluzione di conti
  - BackUp conservato in luogo sicuro
  - Definizione di un retention period

how ?

SecureLog Appliance

un sistema centrale[1]
dedicato alla raccolta dei log
comprensivo di una suite di software tools open source

garantisce l'esistenza
di una copia dei log integra
tramite firma digitale e *forward integrity MAC*

agevola la generazione di log/msg dalle applicazioni
agevola il backup e l'analisi real-time

[1] Tipicamente un sistema Linux (hardened) ad accesso controllato

Componenti sw

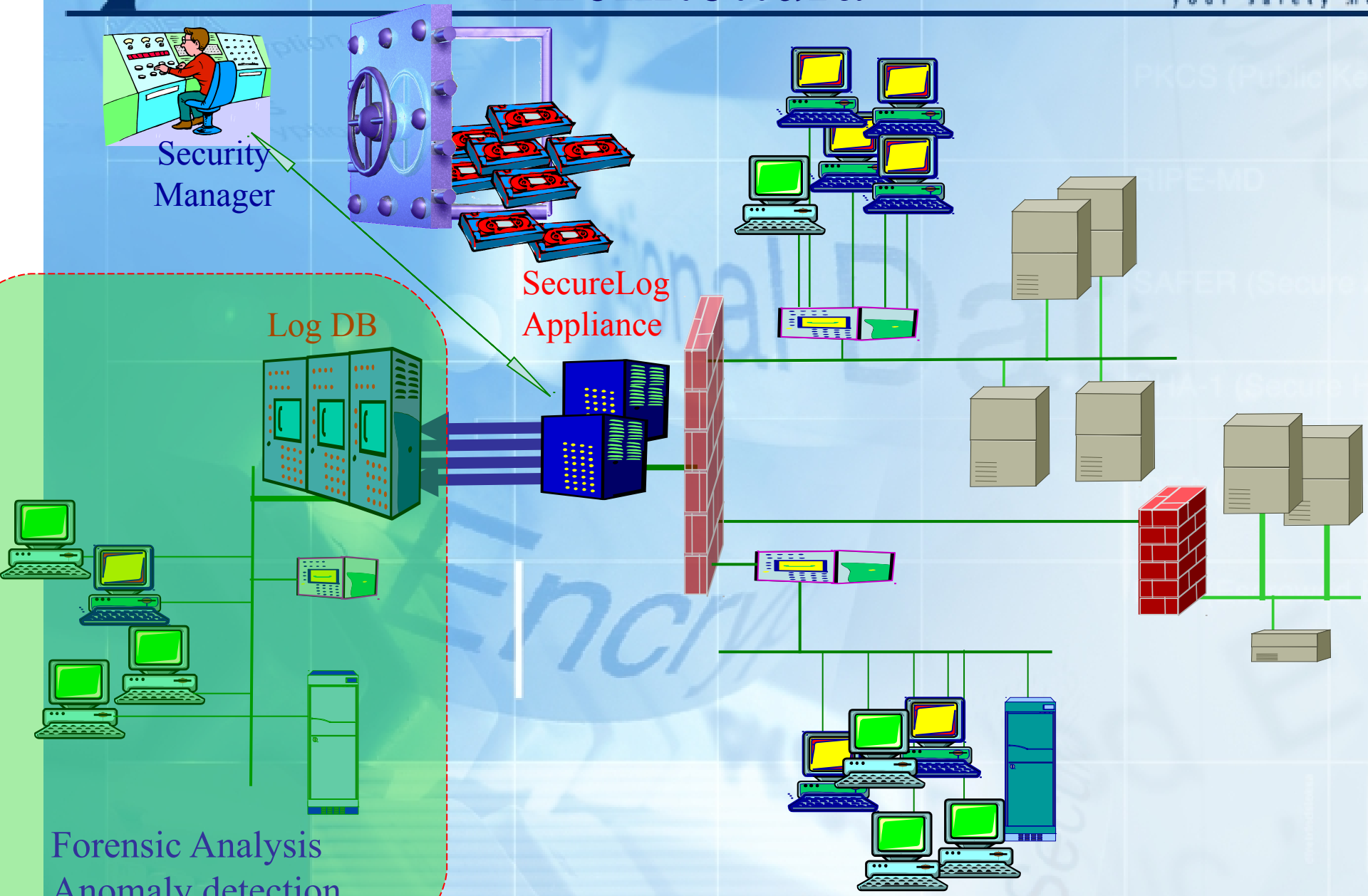
Source

- Unix / Linux
  - ☞Syslog-ng
  - ☞Stunnel
  - ☞SecurLog_Wrapper
- Windows
  - ☞NT Syslog, Kiwi
  - ☞Stunnel
  - ☞SecurLog_Wrapper

Receiver

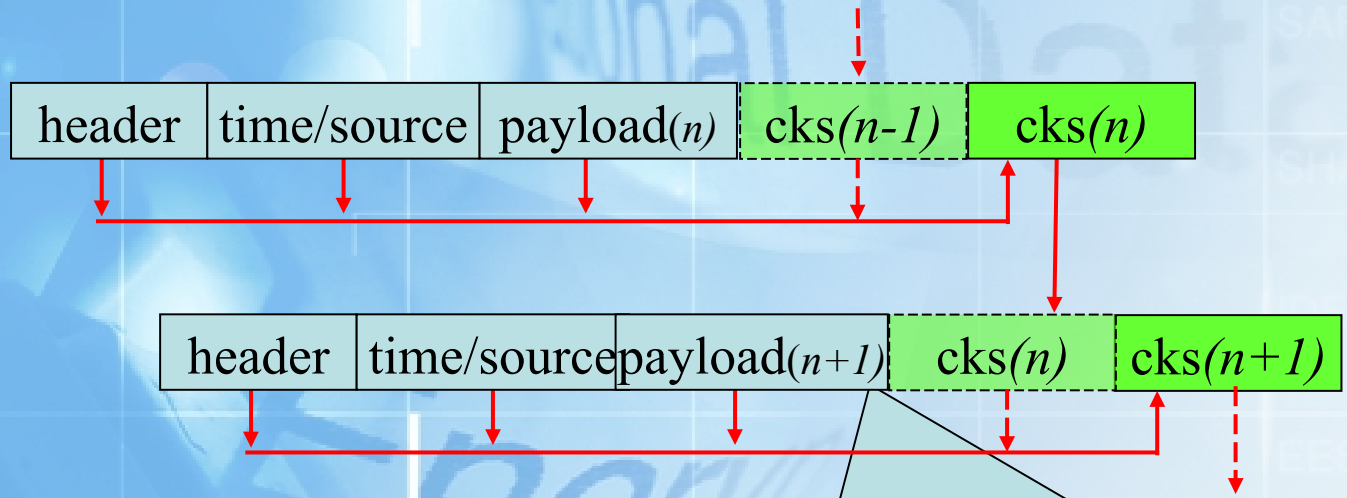
- SecureLogD
- S-Tunnel

Architettura



SecurLog Wrapper

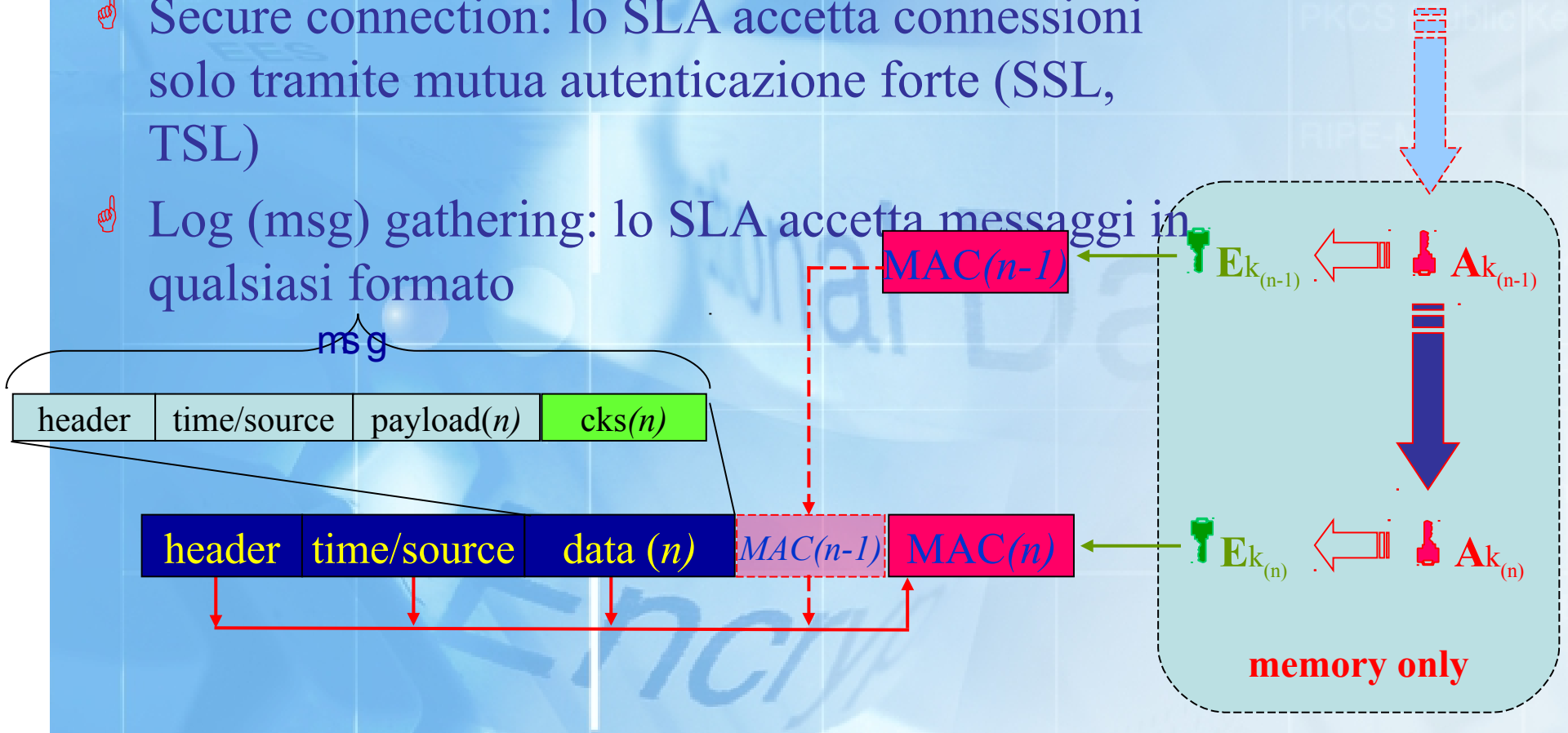
- Chained message:
  il sistema sorgente inserisce in ogni messaggio un checksum sul quale ha effetto il checksum precedente; invia quindi il messaggio al SecureLog Appliance




```
31MAR2005 11:03:20 ---------- INFORMATION DISPLAY ----------------------
COMMAND ===> SCROLL ===> PAGE     CURR WIN ===> 1 ALT WIN ===>   W1
=SYSDUMP==========EYUPLX01=EYUPLX01=31MAR2005==11:03:20====CPSM==== 1
CMDDump  CICS          Dump     Curr      Max      Total     Dumps   Shutdown
 --- Code---- System--      Option---- Dumps-- Dumps-- Dumps-- Suprsd-  Option----
   MT0001   SE-TEST1A   YES          1       999        1         0       NO
```

SecureLogD

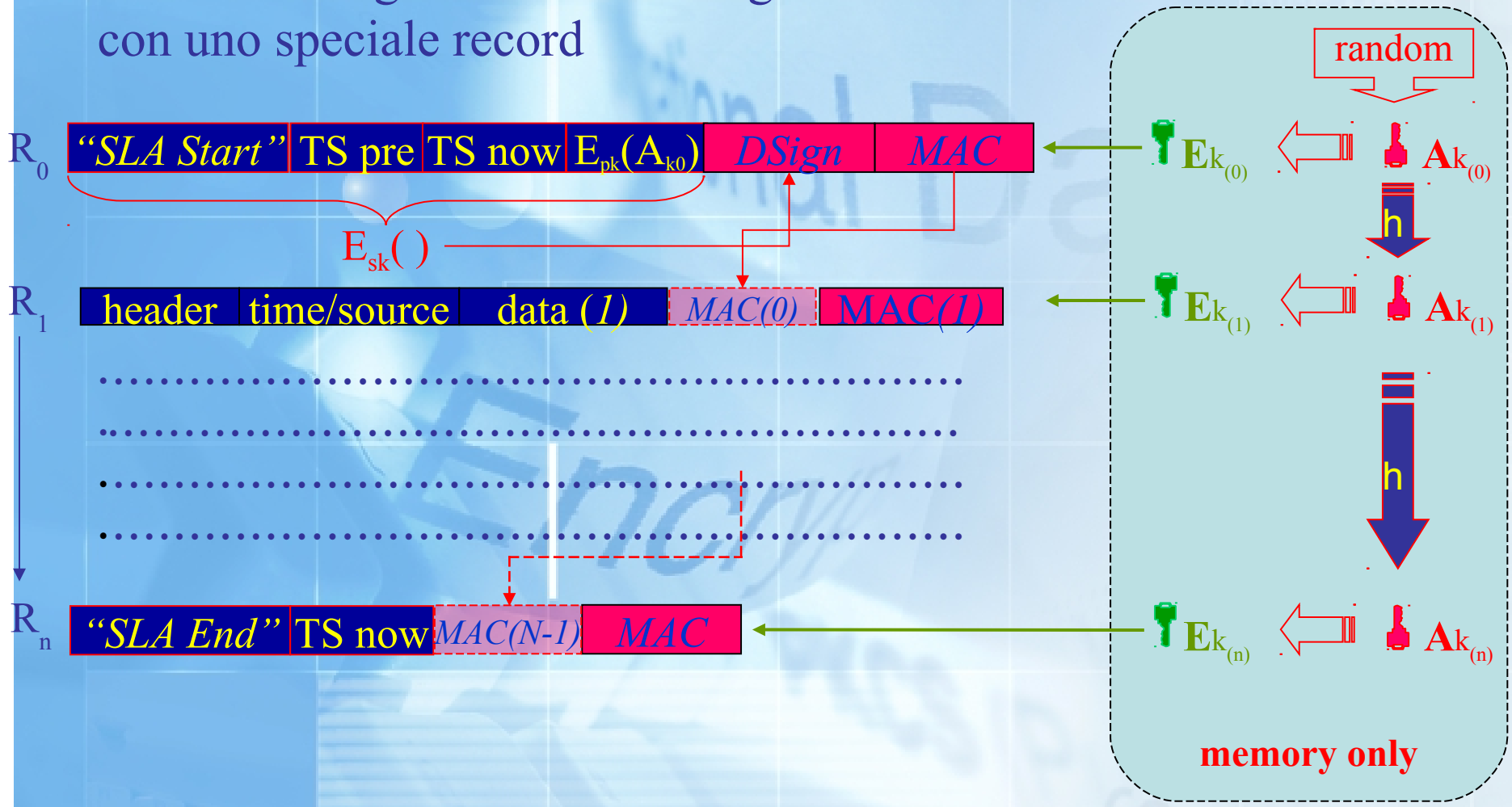
- Secure connection: lo SLA accetta connessioni solo tramite mutua autenticazione forte (SSL, TSL)
- Log (msg) gathering: lo SLA accetta messaggi in qualsiasi formato



- Forward Integrity MAC: lo SLA imbusta ogni msg utilizzando un chained MAC creando in questo modo il record del log sicuro

Forward Integrity MAC

- **Digital Signature & Timestamp**: ogni file di sessione di registrazione dei msg inizia e termina con uno speciale record



Security

- **Rotation & Archiving**: almeno ogni giorno viene aperto un nuovo file di sessione; deve essere effettuato il backup del precedente file; il file viene quindi rimosso.

- **Clock Syncronization**: il clock dello SLA viene sincronizzato al bootstrap tramite fonte ufficiale(*); semplifica la correlazione degli eventi.

(*) http://www.ien.it/tf/time/index.html

Source

- Operating Systems:
  - Windows: 2003Server, XP, ...
  - Unix: Linux, BSD, Solaris, AIX,...
  - OS/390, GCOS, VMS, ...
  - Appliance: Router & Switches, NAS, RAS

Crash, hardware failure, resource exhaustion, reboot/restart, patches, log-in/log-out, su, login/su failure, printer use/errors, mail/http transaction, security software exceptions, accounting, security related events, ...

- System Applications:
  - Daemons process: TCPWrappers, http, FTP, Telnet, SSH, SMTP, POP3, DNS, LDAP, DHCP, Radius, Kerberos, ...
  - Application process: RDBMS, firewall (FW1), IDS, system&network management, cron, ...

- User Applications:
  - SAP, WebMail, BackUp, ...

Policy Based

References /1

- **Information Security Policies Made Easy Version 10**
  Charles Cresson Wood
  Information Shild Inc. 2005
- **Cryptographic Support for Secure Logs on Untrusted Machines**
  Bruce Schneier, John Kelsey
  Counterpane Systems
- **Secure Audit Logs with Forward Integrity Message Authentication Code**
  Iiang Tao, Liu Ji-qiang, Han Zhen
  2004 7th International Conference on Signal Processing, Proceedings. ICSP '04
  IEEE Publications
- **The Importance of Logging and Traffic Monitoring for Information Security**
  Seham Mohamed GadAllah
  SANS Institure 2004
- **Secure Audit Logs Server to support Computer Forensic in Criminal Investigations**
  Liu Ji-qiang, Han Zhen, Lan Zengwei
  2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering, Proceedings. TENCON '02
  IEEE Publications
- **Building a Logging Infrastructure**
  Abe Singer, Tina Bird
  Sage Publication http://www.sage.org/pubs/12_logging/
- **Building an Encrypted and Searchable Audit Log**
  Brent R. Waters, Dirk Balfanz, Glenn Durfee, and D. K. Smetters
  Paolo Alto Research Center January 9, 2004

References /2

- **IRITALY** (http://iritaly.org) Progetto nato in collaborazione con il Dipartimento di Tecnologie dell'Informazione dell'Università Statale di Milano, Polo Didattico e di Ricerca di Crema. Lo scopo principale è informare e sensibilizzare la comunità scientifica italiana, le aziende piccole e grandi, gli attori privati e pubblici sui temi dell'Incident Response

  [http://www.honeynet.it]

- **SIKUREZZA.ORG** (http:// Sikurezza.org) è un portale non commerciale finalizzato alla diffusione ed alla discussione di informazioni e tecnologie legate alla sicurezza informatica. Sikurezza.org gestisce numerose mailing list "security-related" in italiano. Ospita progetti, software ed e-zine "security-related" della "scena italiana".

ICT security awareness

SecureLog Appliance™

SECURE EDGE
your safety net

Sandro Fontana, CISSP, CISA, CISM, L.A. BS7799
CTO Secure Edge
sfontana@secure-edge.com