Safekeeping Digital Evidence with Secure Logging Protocols

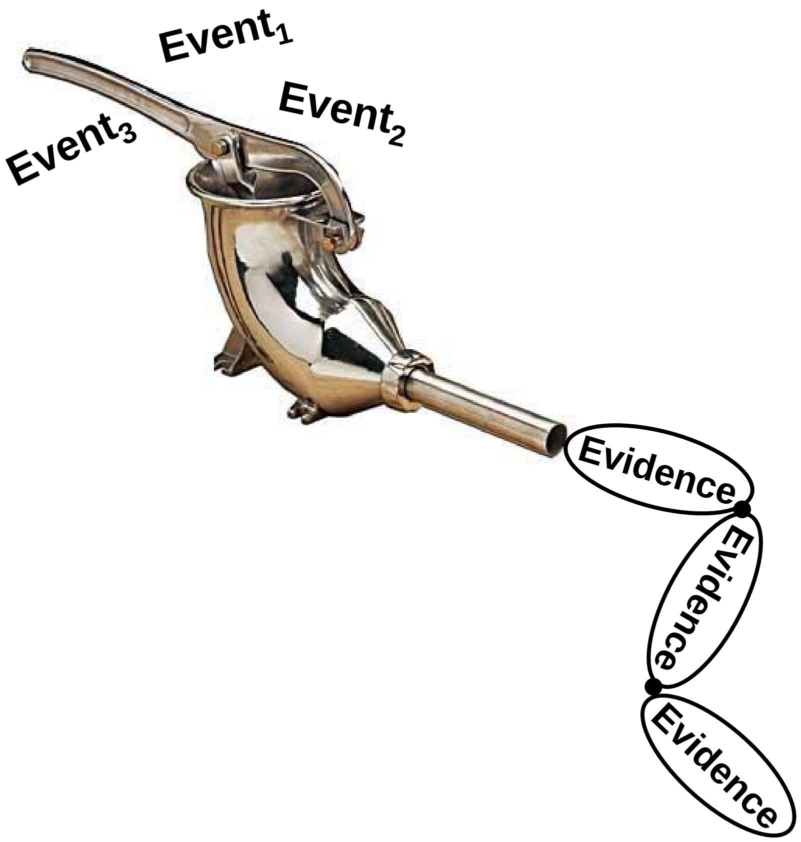
State of the Art and Challenges

Rafael Accorsi
University of Freiburg, Germany
accorsi@iig.uni-freiburg.de

IMF, September 2009

Logs = System activity

- System logs are omnipresent.
- Events record system activity i.e. “state transitions.”
- Valuable source of evidence!
- But very tricky to bring to court.



Agenda

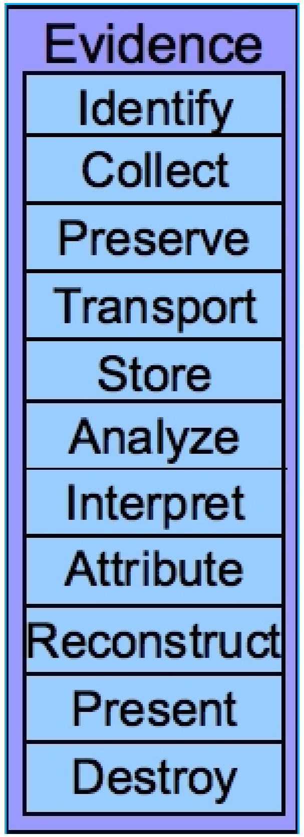
- On digital evidence.
- Admissibility and protection goals.
- Secure logging protocols:
  State of the art.
- Challenges.

Digital evidence

- Transmitted, stored and analyzed digital information that may be relied upon in court.

- Some criteria:
  - admissible.
  - relevant.
  - complete.
  - believable.

- Admissibility issue: missing consensus.



Evidence

Identify

Collect

Preserve

Transport

Store

Analyze

Interpret

Attribute

Reconstruct

Present

Destroy

Cohen'09

Admissibility and protection goals

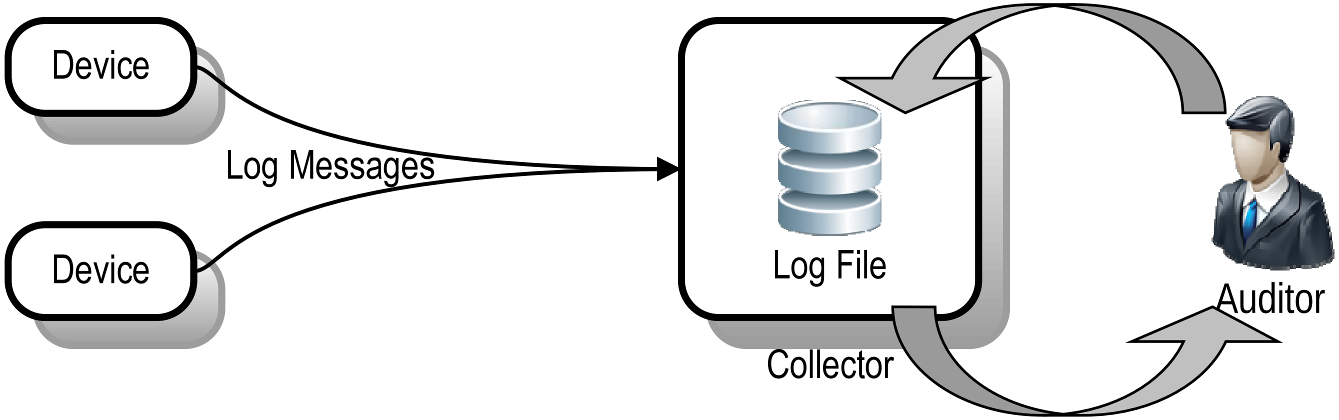
- Admissibility's bottom line: log data must be authentic.

- Transmission phase:
  - event provenance.
  - message confidentiality.
  - message uniqueness.
  - reliable delivery.

- Storage phase:
  - entry integrity, i.e.
    - accuracy.
    - completeness.
    - compactness.
  - entry confidentiality.

- Analysis phase:
  - restrain information flow.

Architecture and Protocols



Device

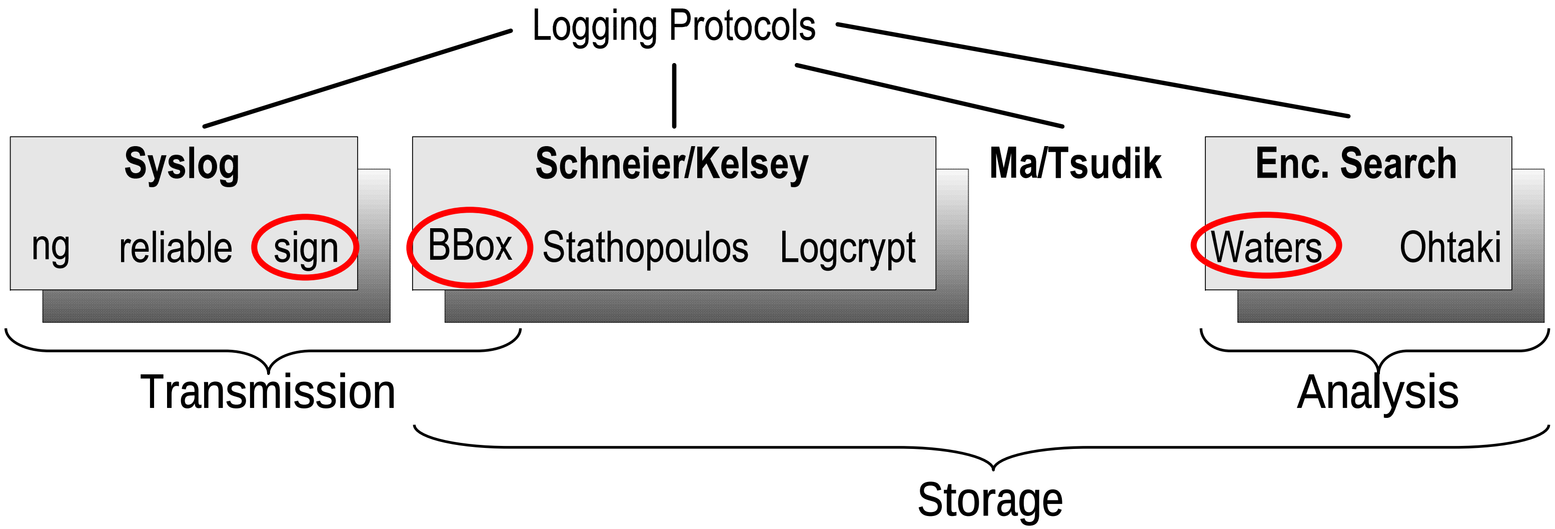
Device

Log Messages

Log File

Collector

Auditor



Logging Protocols

Syslog

ng reliable sign

Schneier/Kelsey

BBox Stathopoulos Logcrypt

Ma/Tsudik

Enc. Search

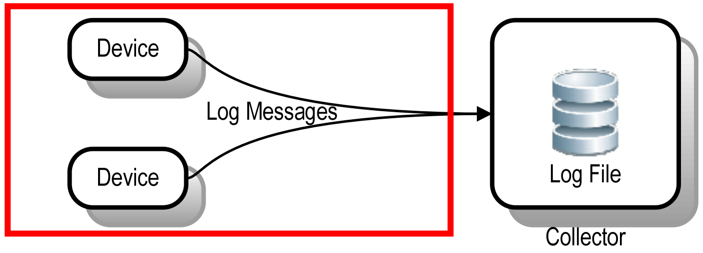
Waters Ohtaki

Transmission

Analysis

Storage

Syslog-Sign: Message transmission

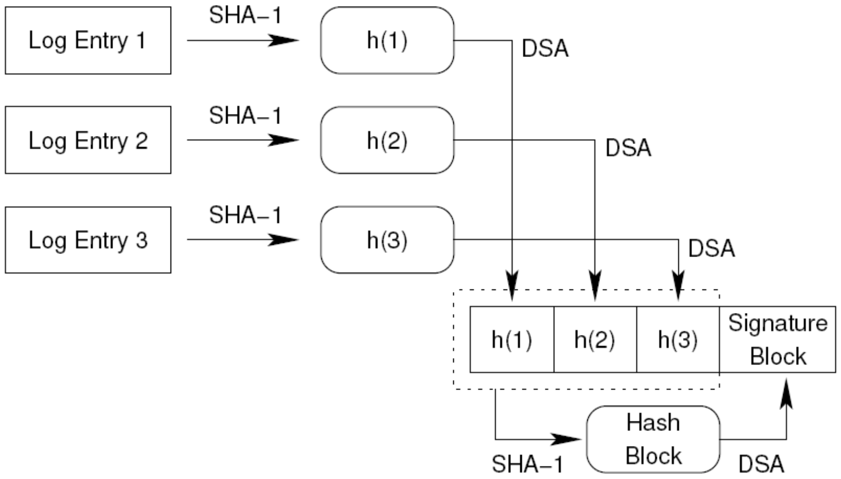


Assumptions:

- underlying PKI.
- powerful devices.

Message authentication:

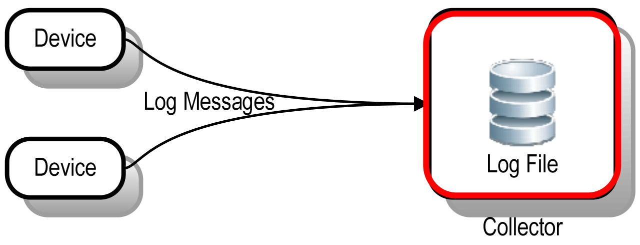
- “batch” operation.
- hashes of each event are signed (DSA).
- Signature block: signed “sum” of all previous hashes of the batch.



Issues:

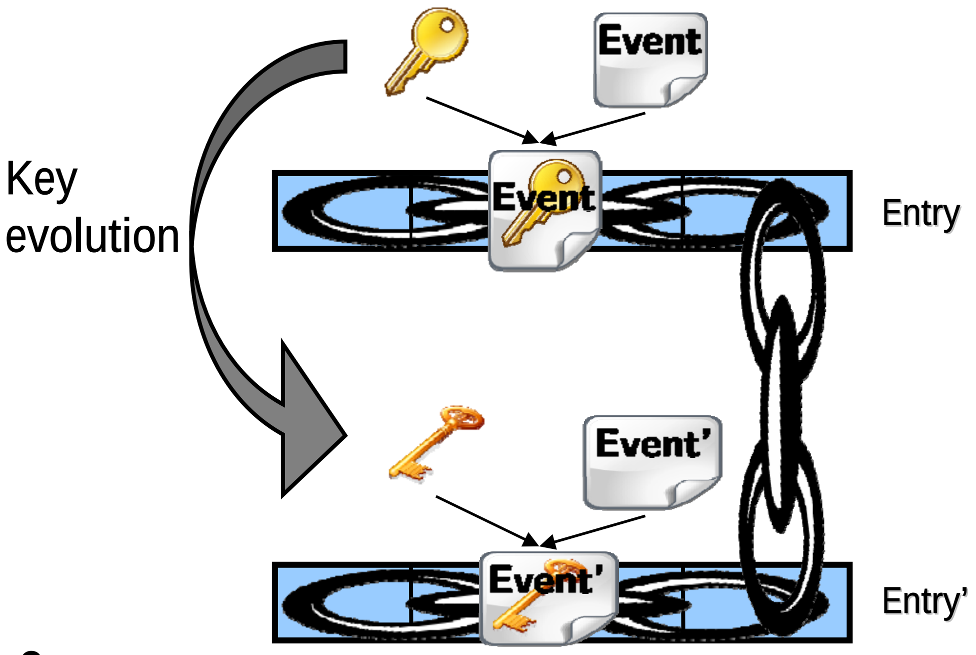
- no payload encryption.
- deletion signature blocks after receipt.

BBox:
Storage and tamper evidence



Crypto building blocks:

- symmetric encryption.
- checksums.
- evolving cryptographic keys.
- hash chain links signed
  with BBox' certificate.



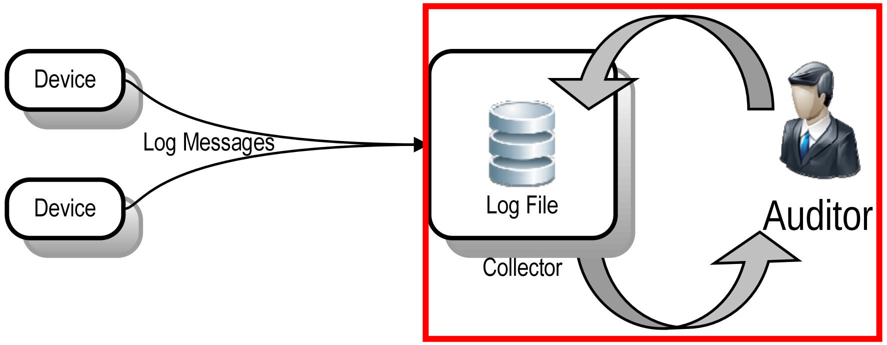
Tamper detection

- checks the integrity of the chain.

Issues:

- what if one breaks the root of the chain?
- confidentiality of root key.
- difficult extraction of payloads.

Waters et al.: IBE encrypted search (I)



IBE: takes any string as public key.

Scheme:

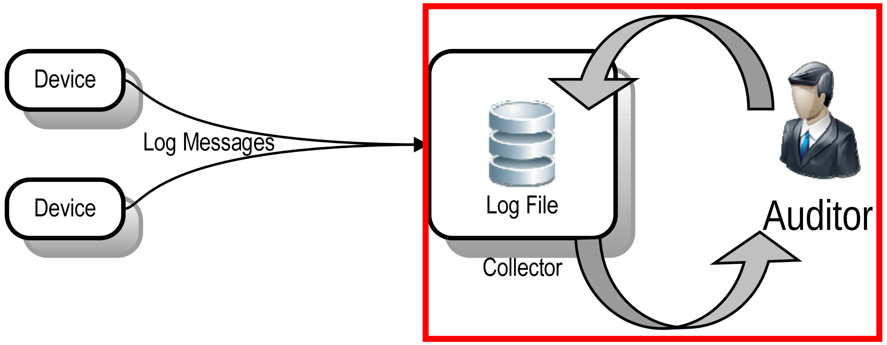
- phases: storage and retrieval of entries.
- principals: key escrow *T* and investigators *V*.

Phase 1: Storage

- given an event *m*, extract the keywords *w*.
- generate private *K* based on keywords *w*.
- generate for each *w* the index c_w.

$$R_i := \begin{array}{|c|c|c|}\hline E_{K_i}(m_i) & H(R_{i-1}) & c_{w_a}, c_{w_b}, c_{w_c} \\ \hline\end{array}$$

Waters et al.: IBE encrypted search (II)



$$R_i := \begin{array}{|c|c|c|}\hline E_{K_i}(m_i) & H(R_{i-1}) & c_{w_a}, c_{w_b}, c_{w_c} \\ \hline \end{array}$$

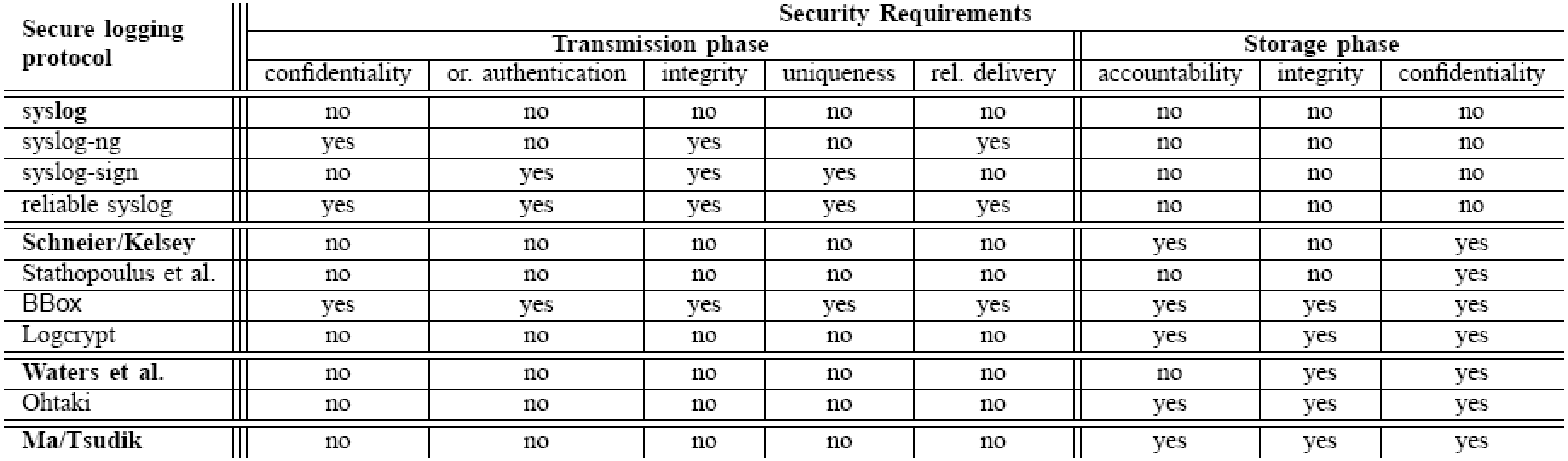
Phase 2: Retrieval and decryption

- upon a query from *V* for the keyword *w*, generate “capability” d_w.
- *V* tests d_w against the indexes *c* of each entry.
  - *V* either obtains the key *K* or void information.

Issues:

- derivation of keywords not deterministic.
- operators (and/or/not) still not possible.
- no revocation of capabilities.

Protocols and protection goals



Secure logging protocol	**Security Requirements**							
	Transmission phase					**Storage phase**		
	confidentiality	or. authentication	integrity	uniqueness	rel. delivery	accountability	integrity	confidentiality
syslog	no	no	no	no	no	no	no	no
syslog-ng	yes	no	yes	no	yes	no	no	no
syslog-sign	no	yes	yes	yes	no	no	no	no
reliable syslog	yes	yes	yes	yes	yes	no	no	no
Schneier/Kelsey	no	no	no	no	no	yes	no	yes
Stathopoulus et al.	no	no	no	no	no	no	no	yes
BBox	yes	yes	yes	yes	yes	yes	yes	yes
Logcrypt	no	no	no	no	no	yes	yes	yes
Waters et al.	no	no	no	no	no	no	yes	yes
Ohtaki	no	no	no	no	no	yes	yes	yes
Ma/Tsudik	no	no	no	no	no	yes	yes	yes

- Despite protection, missing full authenticity.

- Subtle vulnerabilities ⇒ (undetectable) attacks ⇒ wrong Evidence.

- Assumptions are sometimes too strong or implicit.

⇝ Rigorous reasoning about protocols needed!

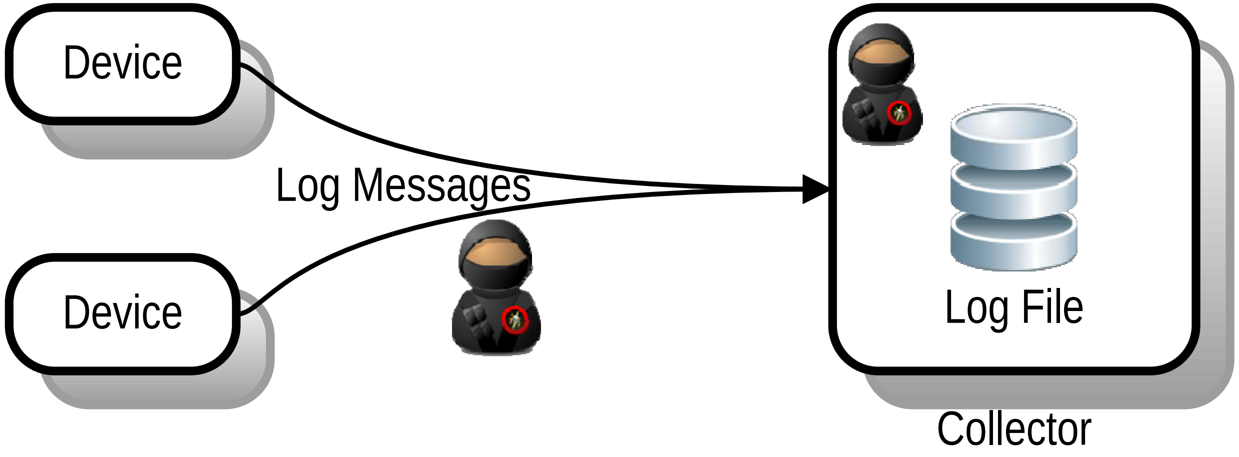
Open issues

- Obtaining reliable signals.
- Advanced adversarial models.
- Formal verification of logging protocols.
- Standard evidence formats.

- Consolidation of log data.
- Evidence mining.

Backup Slides

What’s the threat model?



- Outsider can
  - read
  - compose
  - modify
  - block

  log data in transit.

- Insider can
  - read
  - compose
  - modify
  - delete

  log data at rest.