A Privacy-Preserving Infrastructure to Monitor Encrypted DNS Logs

Adam Oumar Abdel-rahman, Olivier Levillain, Eric Totel

SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, France

December 7, 2023
Introduction and Motivation

- Forensics analysis in cybersecurity
Introduction and Motivation

- Forensics analysis in cybersecurity
- Outsourcing log storage to cloud providers
Introduction and Motivation

- Forensics analysis in cybersecurity
- Outsourcing log storage to cloud providers
- Look for indicators of compromise (IoCs)
Introduction and Motivation

- Forensics analysis in cybersecurity
- Outsourcing log storage to cloud providers
- Look for indicators of compromise (IoCs)
- Logs may contain sensitive information
Introduction and Motivation

- Forensics analysis in cybersecurity
- Outsourcing log storage to cloud providers
- Look for indicators of compromise (IoCs)
- Logs may contain sensitive information
- Encryption as a solution?
Monitoring Encrypted Logs

- Data privacy in the cloud providers
Monitoring Encrypted Logs

- Data privacy in the cloud providers
- Dilemma between security and privacy
Monitoring Encrypted Logs

- Data privacy in the cloud providers
- Dilemma between security and privacy
- Reconcile outsourced search with data privacy concerns
Monitoring Encrypted Logs

- Data privacy in the cloud providers
- Dilemma between security and privacy
- Reconcile outsourced search with data privacy concerns
- Searchable Encryption as a solution
Outsource *storage* and *queries* on the encrypted logs to an external Cloud Provider.
Outsource *storage* and *queries* on the encrypted logs to an external Cloud Provider.
Outsource *storage* and *queries* on the encrypted logs to an external Cloud Provider.

User 1 | User 2 | User 3
---|---|---

Server → Cloud Provider

Authority
Outsource *storage* and *queries* on the encrypted logs to an external Cloud Provider.
Proposed Framework

Server

Encryption

Key Store

Cloud Provider

Database

Search

Authority

TrapdoorGen

FinalDecryption

Setup

secret key

security parameters

Monitoring Encrypted DNS Logs – CRiSIS 2023
December 7, 2023
Proposed Framework

Server

- Encryption
- Key Store

Cloud Provider

- Database
- Search

Authority

- TrapdoorGen
- FinalDecryption
- Setup

request → Encryption

Encrypted log → Database

secret key → TrapdoorGen

security parameters → Setup

Relevent Logs (Plaintext)
Proposed Framework

Server

- Encryption
- Key Store

Cloud Provider

- Database
- Search

Authority

- TrapdoorGen
- FinalDecryption
- Setup

request

Encrypted log

IoC

secret key

security parameters

Trapdoor $T(IoC)$

Relevant Logs (Plaintext)
Proposed Framework

Server

- Encryption
- Key Store

Cloud Provider

- Database
- Search

Authority

- TrapdoorGen
- FinalDecryption
- Setup

request

Encrypted log

IoC

Trapdoor $T(\text{IoC})$

Relevant Logs (Plaintext)

secret key

security parameters

Adam Oumar Abdel-rahman (Télécom SudParis)  Monitoring Encrypted DNS Logs – CRiSIS 2023  December 7, 2023
Proposed Framework

Server

- Encryption
- Key Store

Cloud Provider

- Database
- Search
- Trapdoor $T(IoC)$

Authority

- TrapdoorGen
- FinalDecryption
- Setup

encrypted log

request

secret key

Relevant Logs (Plaintext)

Search Results

 sécurité paramaters
Use Case Application
Domain Name System (DNS)

Why DNS?
- DNS as a security keystone
- Cybersecurity implications of DNS monitoring

DNS Logs
\[ \log = \{ \text{Timestamp}; \text{IP client}; \text{domain name}; \text{qtype}; \text{rcode}; \text{IP results} \} \]

KW
\[ \text{KW} = \{ \text{domain name}, \text{IP results} \} \]
\[ \text{IP results} = \{ \text{kw}_1, \ldots, \text{kw}_t \} \]

Goal: Finding IoCs in encrypted DNS logs
- IoC may be domain name or IP address of C&C server
- Query on encrypted logs:
  - The DNS request for a given domain name
  - The DNS response producing a given IP address
Use Case Application
Domain Name System (DNS)

Why DNS?
- DNS as a security keystone
- Cybersecurity implications of DNS monitoring

DNS Logs
- $\text{log} = \{\text{Timestamp}; \text{IP\_client}; \text{domain\_name}; \text{qtype}; \text{rcode}; \text{IP\_results}\}$
- $\text{KW} = \{\text{domain\_name}, \text{IP\_results}\} = \{k\text{w}_1, \ldots, k\text{w}_t\}$

Goal: Finding IoCs in encrypted DNS logs
- IoC may be domain name or IP address of C&C server
- Query on encrypted logs:
  - The DNS request for a given domain name
  - The DNS response producing a given IP address
Use Case Application
Domain Name System (DNS)

Why DNS?
- DNS as a security keystone
- Cybersecurity implications of DNS monitoring

DNS Logs
- \[ \text{log} = \{\text{Timestamp}; \text{IP\_client}; \text{domain\_name}; \text{qtype}; \text{rcode}; \text{IP\_results}\} \]
- \[ \text{KW} = \{\text{domain\_name}, \text{IP\_results}\} = \{\text{kw}_1, \ldots, \text{kw}_t\} \]

Goal: Finding IoCs in encrypted DNS logs
- IoC may be domain name or IP address of C&C server
- Query on encrypted logs:
  - The DNS request for a given domain name
  - The DNS response producing a given IP address
Privacy Requirements

- Confidentiality of the logs
Privacy Requirements

- Confidentiality of the logs
- Log Unforgettability
Privacy Requirements

- Confidentiality of the logs
- Log Unforgettability
- Predicate Privacy
Privacy Requirements

- Confidentiality of the logs
- Log Unforgettability
- Predicate Privacy
- Correlation Privacy
Proposed Solutions

- Asymmetric Searchable Encryption (ASE)
  - using Identity-Based Encryption (IBE)

- Symmetric Searchable Encryption (SSE)
  - using Pseudo-Random Function (PRF)
Cryptographic Primitives – Recall

Identity-Based Encryption (IBE)

Authority

\((mpk, msk)\)

Alice

Bob

\(M \rightarrow\)

\[C = IBE.\text{Enc}(M, mpk, ID_{bob})\]

\[IBE.\text{Dec}(C, sk_{ID_{bob}}) = M\]
Cryptographic Primitives – Recall

Identity-Based Encryption (IBE)

authority

\((mpk, msk)\)

public params

\(mpk\)

\(M\rightarrow C = IBE.\text{Enc}(M, mpk, ID_{bob})\)

\(\rightarrow\) Bob

\(\rightarrow\) Alice

\(C\rightarrow\)
Cryptographic Primitives – Recall
Identity-Based Encryption (IBE)

Alice

Authority

Bob

public params

$mpk$

$(mpk, msk)$

upon successful authentication

$sk_{ID_{bob}}$

$M \rightarrow C = IBE.Enc(M, mpk, ID_{bob}) \rightarrow IBE.Dec(C, sk_{ID_{bob}}) = M$

$C = IBE.Enc(M, mpk, ID_{bob})$

$IBE.Dec(C, sk_{ID_{bob}}) = M$
Cryptographic Primitives – Recall

Pseudo-Random Function (PRF)

$F_K(x) = y$
Proposed Solutions – ASE
Log Encryption

DNS Logs (Reminder)

- \(\text{log} = \{\text{Timestamp}; \text{IP\_client}; \text{domain\_name}; \text{qtype}; \text{rcode}; \text{IP\_results}\}\)
- \(KW = \{\text{domain\_name}, \text{IP\_results}\} = \{kw_1, \ldots, kw_t\}\)
DNS Logs (Reminder)

- $\log = \{\text{Timestamp}; \text{IP\_client}; \text{domain\_name}; \text{qtype}; \text{rcode}; \text{IP\_results}\}$
- $KW = \{\text{domain\_name}, \text{IP\_results}\} = \{kw_1, \ldots, kw_t\}$

DNS Server

Cloud Provider

User → request

$K \xleftarrow{\$} \{0, 1\}^n, K' = F_{KR}(K)$

$C_i \leftarrow IBE.E\text{nc}(K, kw_i), \forall kw_i \in KW$

$\text{enc\_log} \leftarrow \text{Sym.E\text{nc}(log, K')}$
Proposed Solutions – ASE

Log Encryption

DNS Logs (Reminder)

- \( \log = \{\text{Timestamp}; \text{IP\_client}; \text{domain\_name}; \text{qtype}; \text{rcode}; \text{IP\_results}\} \)
- \( KW = \{\text{domain\_name}, \text{IP\_results}\} = \{kw_1, \ldots, kw_t\} \)

Diagram:

User \rightarrow request \rightarrow DNS Server

\( K \xleftarrow{\$} \{0, 1\}^n, K' = F_{KR}(K) \)

\( C_i \leftarrow IBE.Enc(K, kw_i), \forall kw_i \in KW \)

\( \text{enc\_log} \leftarrow \text{Sym.Enc}(\log, K') \)

\( \{\text{enc\_log}, C_1, \ldots, C_t\} \rightarrow \text{Cloud Provider} \)

store \( \{\text{enc\_log}, C_1, \ldots, C_t\} \)
Proposed Solutions – ASE
Search on Encrypted Logs

Cloud Provider

Authority

query search \{sk_{IoC}\}

\(sk_{IoC} = \text{TrapdoorGen}(msk, IoC)\)
Proposed Solutions – ASE
Search on Encrypted Logs

\[ \text{Cloud Provider} \]

\[ \text{Authority} \]

\[ \text{query search} \{ sk_{IoC} \} \]

\[ \text{Encrypted Search Results (ESR)} \]

\[ ESR \leftarrow \{ \} \]

For each \{enc\_log, C_1, \ldots, C_t\}

if \( \exists i, \text{s.t.} \ IBE.Dec(C_i, sk_{IoC}) =: \text{success} \)

Add \{enc\_log, K\} to ESR

\[ sk_{IoC} = \text{TrapdoorGen}(msk, IoC) \]
Proposed Solutions – ASE
Search on Encrypted Logs

\[ ESR \leftarrow \{\} \]

For each \( \{\text{enc \_log}, C_1, \ldots, C_t\} \)

- if \( \exists i, \text{s.t. } \text{IBE. Dec}(C_i, sk_{\text{IoC}}) =: K \text{ success} \)
- Add \( \{\text{enc \_log}, K\} \) to \( ESR \)

\[ sk_{\text{IoC}} = \text{TrapdoorGen}(msk, IoC) \]

For each \( \{\text{enc \_log}, K\} \) in \( ESR \)

- \( K' = F_{K_R}(K) \)
- \( log = \text{Sym. Dec}(\text{enc \_log}, K') \)
- Add \( log \) to Plaintext Logs
Proposed Solutions – SSE
Log Encryption

Core idea

\[ \text{enc\_rec} = \{\text{Sym.Enc}(\log, K'), C_1, \ldots, C_t\}, \quad K' = F_{KR}(K) \text{ and } C_i = IBE.Enc(K, kw_i) \]

Build secure index on encrypted logs
Core idea

\[ \text{enc.rec} = \{\text{Sym.Enc}(\text{log}, K'), C_1, \ldots, C_t\}, \quad K' = \mathcal{F}_{KR}(K) \text{ and } C_i = \text{IBE.Enc}(K, kw_i) \]

Build secure index on encrypted logs
Proposed Solutions – SSE

Log Encryption

Core idea

\[ \text{enc}_\text{rec} = \{ \text{Sym.Enc}(\text{log}, K'), C_1, \ldots, C_t \}, \quad K' = \mathcal{F}_{KR}(K) \text{ and } C_i = \text{IBE.Enc}(K, kw_i) \]

Build secure index on encrypted logs

DNS Server

User

TK_i \leftarrow \mathcal{F}_{KR}(kw_i || TS), \forall kw_i

K \leftarrow \text{Hash}(TK_1 || \cdots || TK_t)

K' \leftarrow \mathcal{F}_{KR}(K)

\text{enc.log} \leftarrow \text{Sym.Enc}(\text{log}, K')

Cloud Provider
Proposed Solutions – SSE
Log Encryption

Core idea

\[ \text{enc}_\text{rec} = \{\text{Sym.Enc}(\text{log}, K'), C_1, \ldots, C_t\}, \quad K' = \mathcal{F}_{KR}(K) \text{ and } C_i = \text{IBE.Enc}(K, kw_i) \]

Build secure index on encrypted logs

DNS Server

User

request

DNS Server

\{\text{enc_log}, K, TK_1, \ldots, TK_t\}

Cloud Provider

\text{store}

\{\text{enc_log}, K, TK_1, \ldots, TK_t\}

\begin{align*}
TK_i & \leftarrow \mathcal{F}_{KR}(kw_i || TS), \forall kw_i \\
K & \leftarrow \text{Hash}(TK_1 || \cdots || TK_t) \\
K' & \leftarrow \mathcal{F}_{KR}(K) \\
\text{enc_log} & \leftarrow \text{Sym.Enc}(\text{log}, K')
\end{align*}
Proposed Solutions – SSE
Search on Encrypted Logs

Cloud Provider

query search \{tk_1, \ldots, tk_l\}

Authority

\{tk_i\}_{1 \leq i \leq l} = \text{TrapdoorGen}(K_R, IoC, [T_A, T_B])
Proposed Solutions – SSE

Search on Encrypted Logs

Cloud Provider

\[
\text{query search } \{tk_1, \ldots, tk_l\}
\]

Authority

\[
\{tk_i\}_{1 \leq i \leq l} = \text{ TrapdoorGen}(K_R, IoC, [T_A, T_B])
\]

\[
ESR \leftarrow \{\}
\]

For each \{enc\_log, K, TK_1, \ldots, TK_t\}

if \exists i, j \text{ s.t. } TK_i = tk_j \text{ (success)}

Add \{enc\_log, K\} to \text{ESR}
Proposed Solutions – SSE
Search on Encrypted Logs

\[ ESR \leftarrow \{ \} \]
For each \( \{ \text{enc}_\log, K, TK_1, \ldots, TK_t \} \)
if \( \exists i, j \text{ s.t. } TK_i = tk_j \) (success)
Add \( \{ \text{enc}_\log, K \} \) to \( ESR \)

\[ \{ tk_i \}_{1 \leq i \leq l} = \text{TrapdoorGen}(K_R,IoC,[T_A,T_B]) \]
For each \( \{ \text{enc}_\log, K \} \)
\[ K' = \mathcal{F}_{K_R}(K) \]
\[ \log = \text{Sym} \cdot \text{Dec}(\text{enc}_\log, K') \]
Add \( \log \) to Plaintext Logs
Implementation and Evaluation

Implemented schemes

- Plaintext & Plaintext + DB, DB for Database
- WBDS–SSE : SSE scheme of Waters et al.
- our SSE scheme
- SSE + DB : our SSE scheme with a database
- our ASE scheme using IBE
Implementation and Evaluation

Implementation details

- Symmetric primitives: AES, HMAC
- Asymmetric setting: elliptic curve BLS12-381 & RELIC library
- Dataset: TI-2016 DNS dataset, 2019 → 21 million logs

---

1. The Search Time corresponds to the processing time of one IoC in 705,524 encrypted logs.
2. DB for Database
### Implementation and Evaluation

#### Implementation details
- **Symmetric primitives**: AES, HMAC
- **Asymmetric setting**: elliptic curve BLS12-381 & RELIC library
- **Dataset**: TI-2016 DNS dataset, 2019 → 21 million logs

<table>
<thead>
<tr>
<th></th>
<th>Encryption Time (µs/log)</th>
<th>Ciphertext size</th>
<th>Search Time&lt;sup&gt;1&lt;/sup&gt; (s/IoC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext</td>
<td>2.7</td>
<td>1.0</td>
<td>0.4</td>
</tr>
<tr>
<td>Plaintext + DB&lt;sup&gt;2&lt;/sup&gt;</td>
<td>2.7</td>
<td>2.4</td>
<td>&lt; 0.01</td>
</tr>
<tr>
<td>WBDS–SSE</td>
<td>22.4</td>
<td>2.3</td>
<td>2.2</td>
</tr>
<tr>
<td>Our SSE</td>
<td>28.9</td>
<td>1.3</td>
<td>9.97</td>
</tr>
<tr>
<td>Our SSE + DB</td>
<td>28.9</td>
<td>3.3</td>
<td>0.02</td>
</tr>
<tr>
<td>Our ASE</td>
<td>5569.0</td>
<td>4.7</td>
<td>2189.28</td>
</tr>
</tbody>
</table>

<sup>1</sup>The Search Time corresponds to the processing time of one IoC in 705,524 encrypted logs.

<sup>2</sup>DB for Database
Discussion and Limitations

Privacy Requirements (Recall)

- Log Unforgettability
- Predicate Privacy
- Correlation Privacy
Discussion and Limitations

Privacy Requirements (Recall)

- Log Unforgettability
- Predicate Privacy
- Correlation Privacy

<table>
<thead>
<tr>
<th></th>
<th>Log Unforgeability</th>
<th>Predicate Privacy</th>
<th>Correlation Privacy</th>
<th>Token Collisions</th>
<th>Search Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>WBDS–SSE</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>if $</td>
<td>r</td>
</tr>
<tr>
<td>Our SSE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Within the truncation window</td>
<td>++</td>
</tr>
<tr>
<td>Our ASE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
<td>– –</td>
</tr>
</tbody>
</table>
Conclusion

Contributions

- Monitoring encrypted DNS logs
- A privacy-preserving infrastructure
- Two new solutions: ASE and SSE
Conclusion

Contributions
- Monitoring encrypted DNS logs
- A privacy-preserving infrastructure
- Two new solutions: ASE and SSE

Perspectives
- Extension to other log types
- Improve query expressiveness
- Build an efficient SSE with no token collisions?
Questions?

Thank you!

adam_oumar.abdel_rahman@telecom-sudparis.eu