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

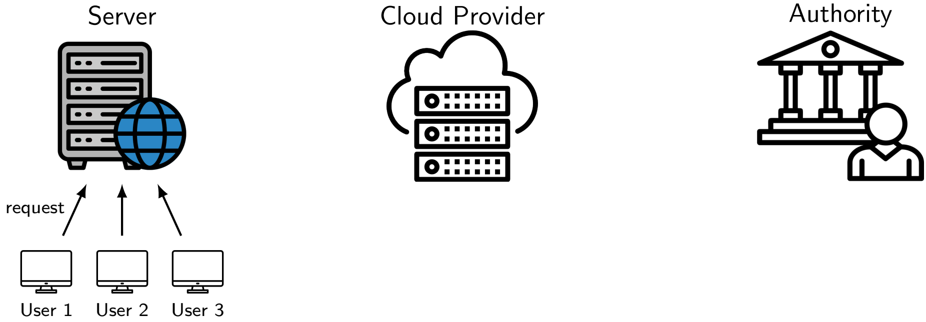
- Data privacy in the cloud providers
- Dilemma between security and privacy
- Reconcile outsourced search with data privacy concerns
- Searchable Encryption as a solution

Monitoring Encrypted Logs

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

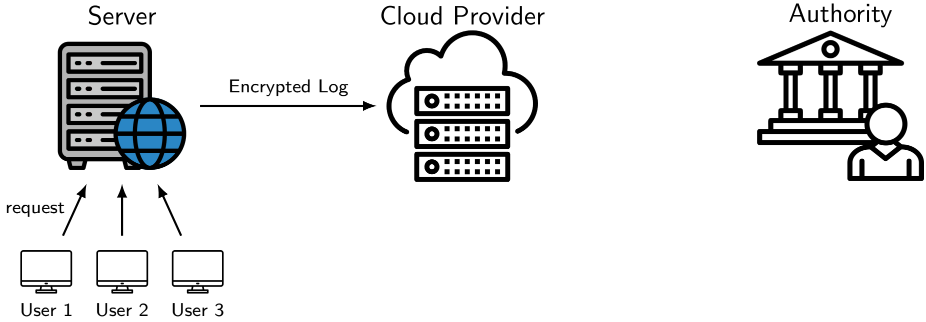
Monitoring Encrypted Logs

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



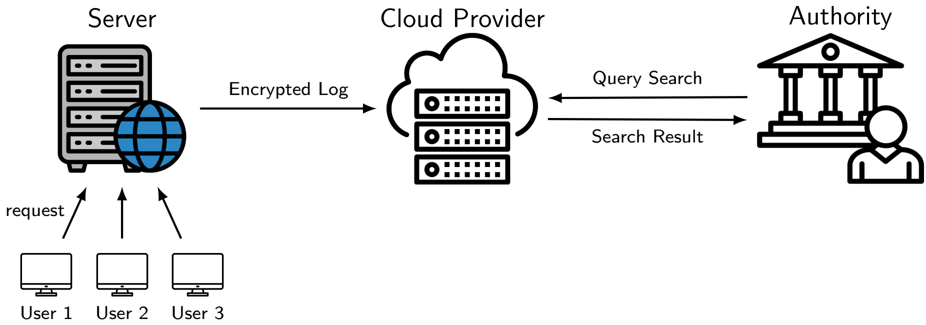
Monitoring Encrypted Logs

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

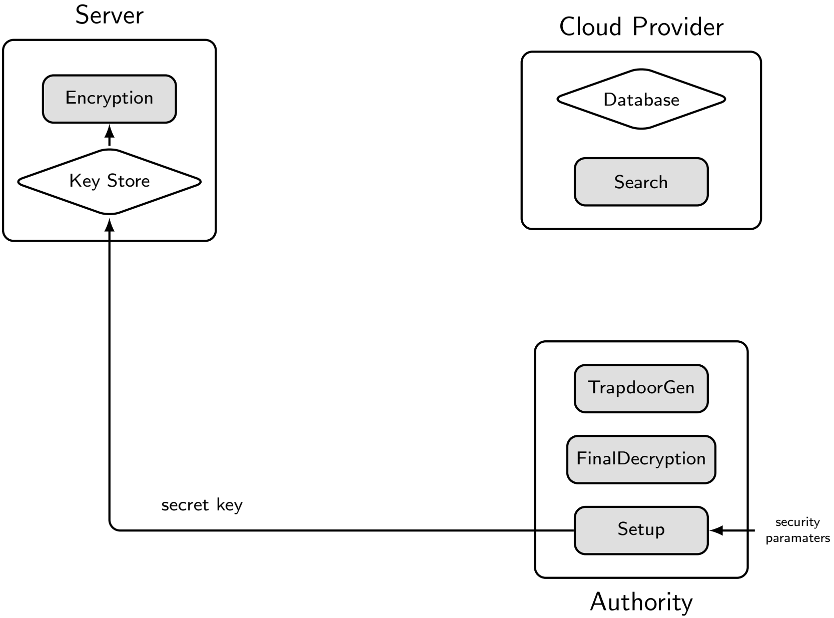


Monitoring Encrypted Logs

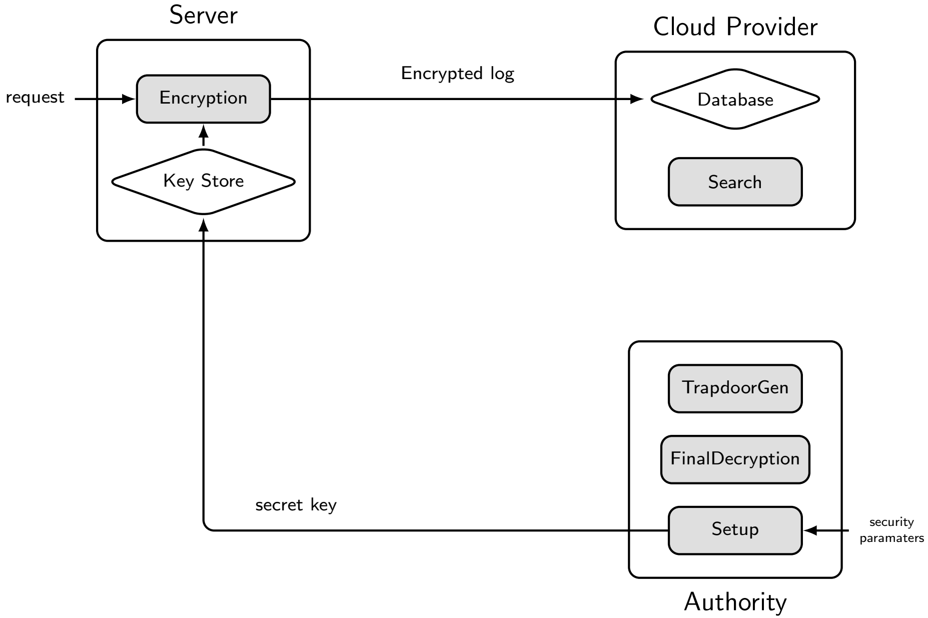
Outsource *storage* and *queries* on the encrypted logs to an external Cloud Provider.



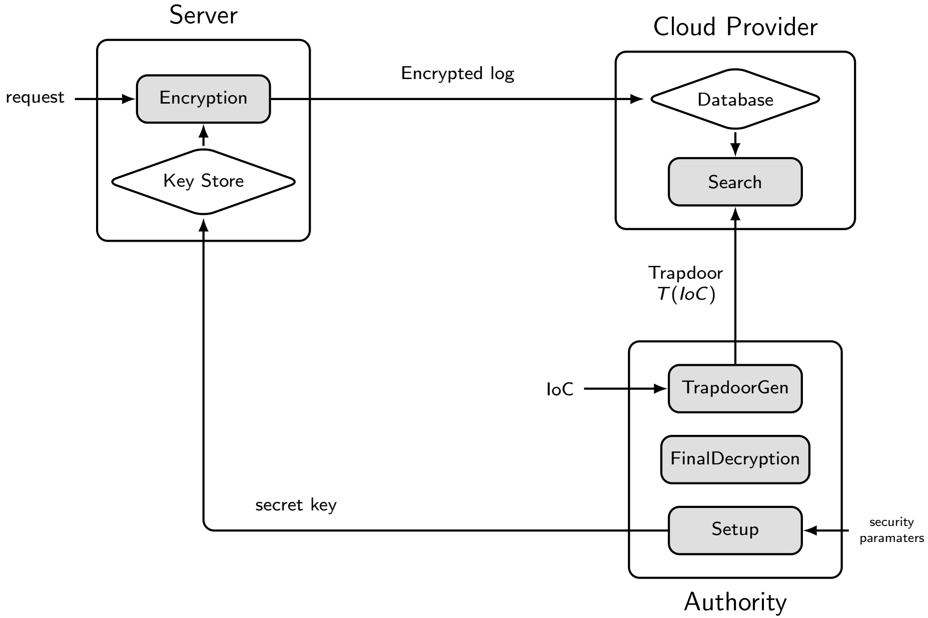
Proposed Framework



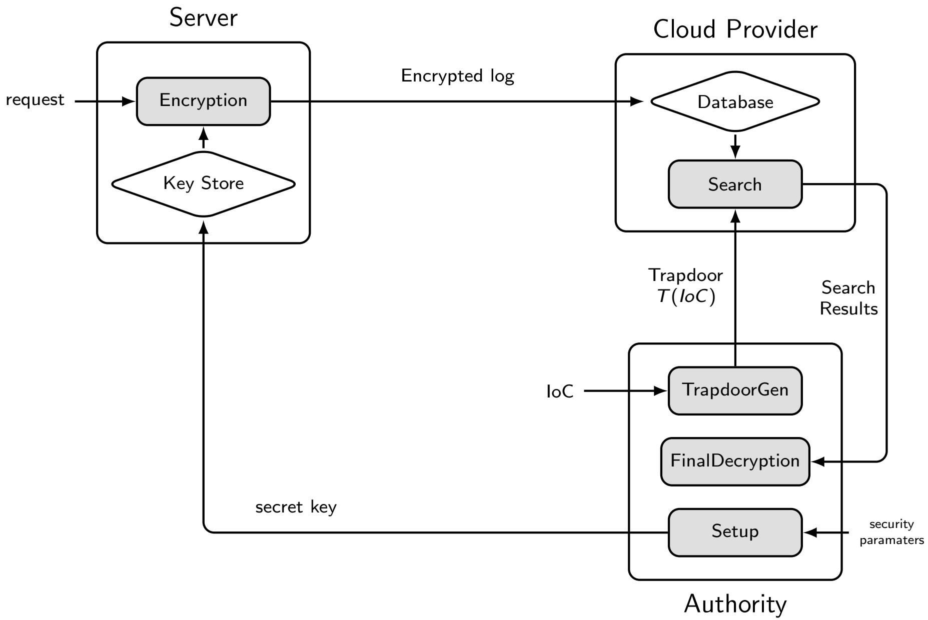
Proposed Framework



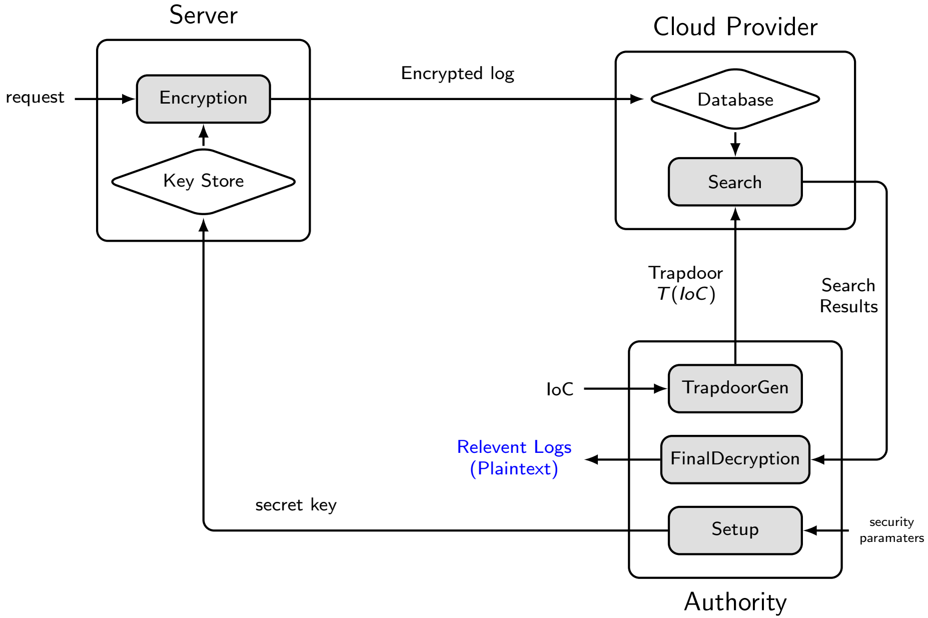
Proposed Framework



Proposed Framework



Proposed Framework



Use Case Application

Domain Name System (DNS)

Why DNS ?

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

Use Case Application

Domain Name System (DNS)

Why DNS ?

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

DNS Logs

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

Use Case Application

Domain Name System (DNS)

Why DNS ?

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

DNS Logs

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

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

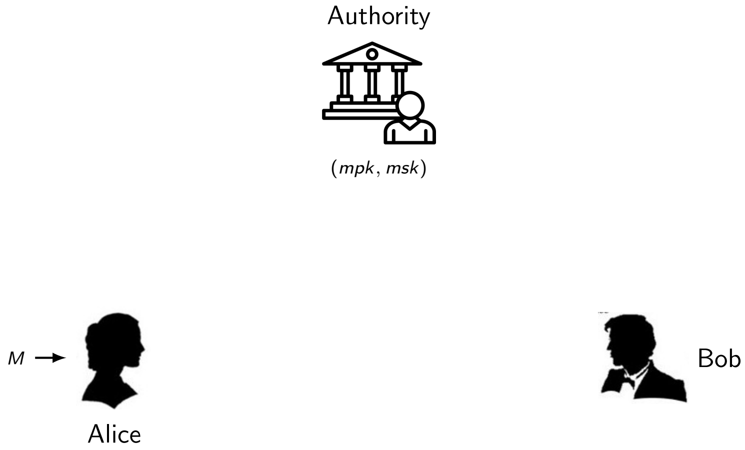
- Confidentiality of the logs
- Log Unforgettability
- Predicate Privacy
- Correlation Privacy

Proposed Solutions

- Asymmetric Searchable Encryption (ASE)
  - using Identity-Based Encryption (IBE)
- Symmetric Searchable Encryption (SSE)
  - using Pseudo-Random Function (PRF)

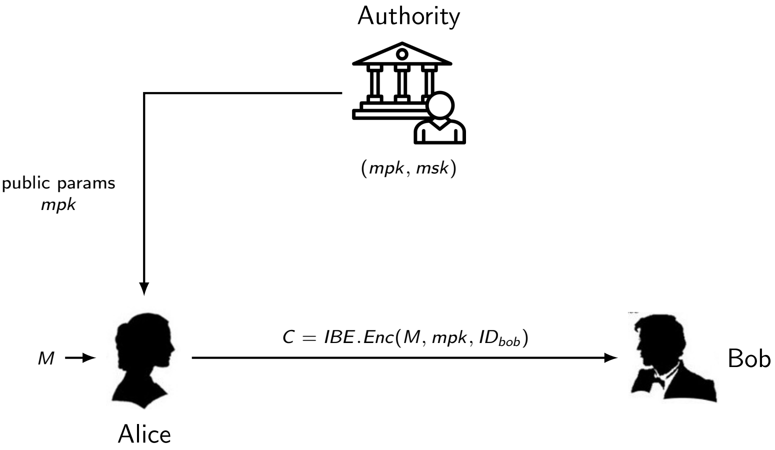
Cryptographic Primitives – Recall

Identity-Based Encryption (IBE)



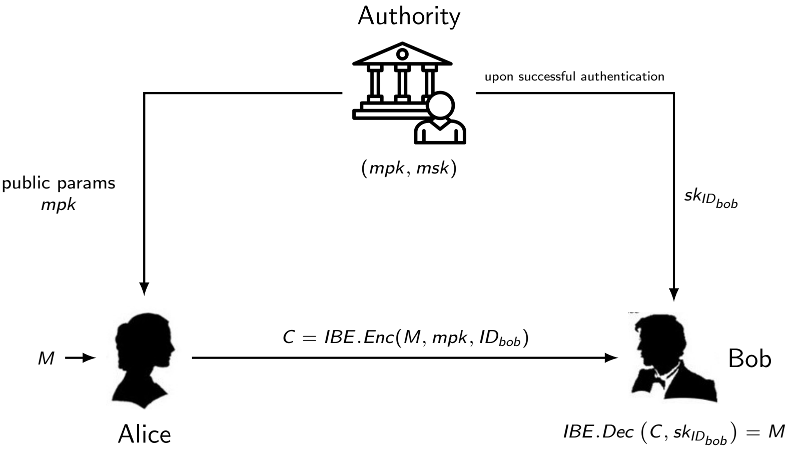
Cryptographic Primitives – Recall

Identity-Based Encryption (IBE)



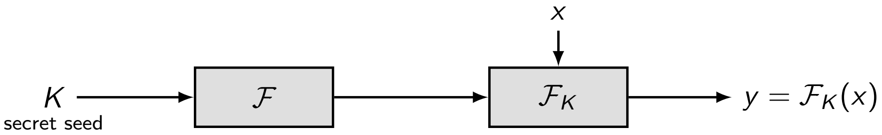
Cryptographic Primitives – Recall

Identity-Based Encryption (IBE)



Cryptographic Primitives – Recall

Pseudo-Random Function (PRF)



Proposed Solutions – ASE

Log Encryption

DNS Logs (Reminder)

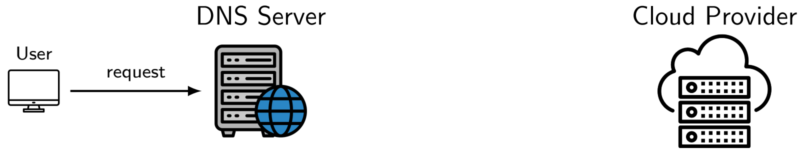
- $\texttt{log} = \{\texttt{Timestamp}; \texttt{IP\_client}; \texttt{domain\_name}; \texttt{qtype}; \texttt{rcode}; \texttt{IP\_results}\}$
- $KW = \{\texttt{domain\_name}, \texttt{IP\_results}\} = \{kw_1, \ldots, kw_t\}$

Proposed Solutions – ASE

Log Encryption

DNS Logs (Reminder)

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



$$K \xleftarrow{\$} \{0,1\}^n, K' = \mathcal{F}_{K_R}(K)$$

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

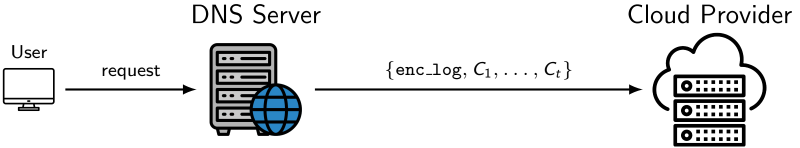
$$\texttt{enc\_log} \leftarrow Sym.Enc(log, K')$$

Proposed Solutions – ASE

Log Encryption

DNS Logs (Reminder)

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



$$K \xleftarrow{\$} \{0,1\}^n, K' = \mathcal{F}_{K_R}(K)$$

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

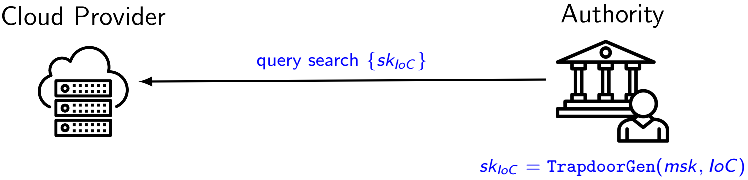
$$\texttt{enc\_log} \leftarrow Sym.Enc(log, K')$$

store

$\{\texttt{enc\_log}, C_1, \ldots, C_t\}$

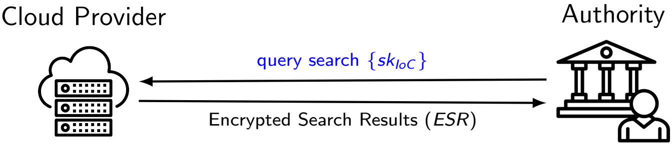
Proposed Solutions – ASE

Search on Encrypted Logs



Proposed Solutions – ASE

Search on Encrypted Logs



$sk_{IoC} = \texttt{TrapdoorGen}(msk, IoC)$

$ESR \leftarrow \{\}$

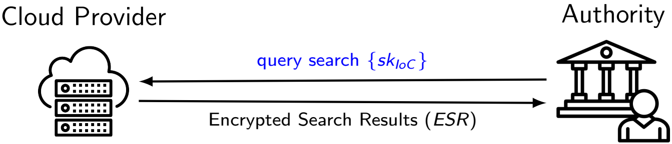
For each $\{\texttt{enc\_log}, C_1, \ldots, C_t\}$

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

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

Proposed Solutions – ASE

Search on Encrypted Logs



$ESR \leftarrow \{\}$

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

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

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

$sk_{IoC} = \texttt{TrapdoorGen}(msk, IoC)$

For each $\{\texttt{enc\_log}, K\}$ in ESR

    $K' = \mathcal{F}_{K_R}(K)$

    $log = Sym.Dec(\texttt{enc\_log}, K')$

    Add log to Plaintext Logs

Proposed Solutions – SSE

Log Encryption

Core idea

$\texttt{enc\_rec} = \{Sym.Enc(log, K'), C_1, \ldots, C_t\}, \quad K' = \mathcal{F}_{K_R}(K)$ and $C_i = IBE.Enc(K, kw_i)$

Build secure index on encrypted logs

Proposed Solutions – SSE

Log Encryption

Core idea

$\texttt{enc\_rec} = \{Sym.Enc(log, K'), C_1, \ldots, C_t\}, \quad K' = \mathcal{F}_{K_R}(K)$ and $C_i = IBE.Enc(K, kw_i)$

Build secure index on encrypted logs

Proposed Solutions – SSE

Log Encryption

Core idea

$\texttt{enc\_rec} = \{Sym.Enc(log, K'), C_1, \ldots, C_t\}, \quad K' = \mathcal{F}_{K_R}(K)$ and $C_i = IBE.Enc(K, kw_i)$

Build secure index on encrypted logs

$$
\begin{aligned}
TK_i &\leftarrow \mathcal{F}_{K_R}(kw_i \,\|\, TS), \forall kw_i \\
K &\leftarrow Hash(TK_1 \| \cdots \| TK_t) \\
K' &\leftarrow \mathcal{F}_{K_R}(K) \\
\texttt{enc\_log} &\leftarrow Sym.Enc(log, K')
\end{aligned}
$$

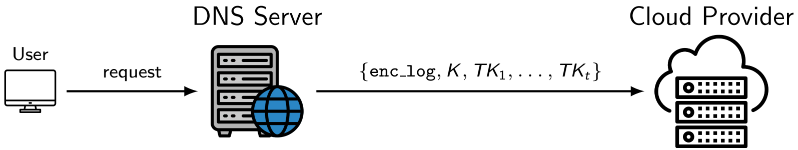
Proposed Solutions – SSE

Log Encryption

Core idea

$\texttt{enc\_rec} = \{Sym.Enc(log, K'), C_1, \ldots, C_t\}, \quad K' = \mathcal{F}_{K_R}(K)$ and $C_i = IBE.Enc(K, kw_i)$

Build secure index on encrypted logs



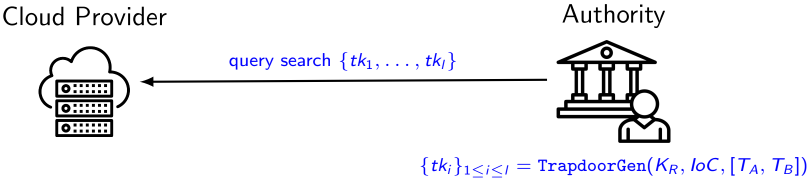
$$
\begin{aligned}
TK_i &\leftarrow \mathcal{F}_{K_R}(kw_i \,\|\, TS), \forall kw_i \\
K &\leftarrow Hash(TK_1 \| \cdots \| TK_t) \\
K' &\leftarrow \mathcal{F}_{K_R}(K) \\
\texttt{enc\_log} &\leftarrow Sym.Enc(log, K')
\end{aligned}
$$

store

$\{\texttt{enc\_log}, K, TK_1, \ldots, TK_t\}$

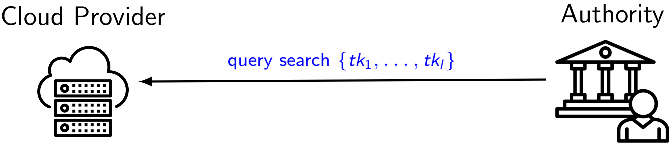
Proposed Solutions – SSE

Search on Encrypted Logs



Proposed Solutions – SSE

Search on Encrypted Logs



$\{tk_i\}_{1 \le i \le l} = \texttt{TrapdoorGen}(K_R, IoC, [T_A, T_B])$

$ESR \leftarrow \{\}$

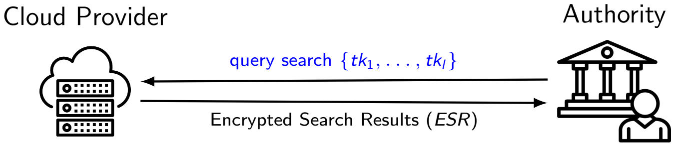
For each $\{\texttt{enc\_log}, K, TK_1, \ldots, TK_t\}$

if $\exists i, j \ s.t. \ TK_i = tk_j$ (success)

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

Proposed Solutions – SSE

Search on Encrypted Logs



$ESR \leftarrow \{\}$

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

if $\exists i, j$ $s.t.$ $TK_i = tk_j$ (success)

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

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

For each $\{\texttt{enc\_log}, K\}$

$K' = \mathcal{F}_{K_R}(K)$

$\texttt{log} = Sym.Dec(\texttt{enc\_log}, K')$

Add $\texttt{log}$ 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 $\longrightarrow$ 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 $\longrightarrow$ 21 million logs

	Encryption Time (μs/log)	Ciphertext size	Search Time[1] (s/IoC)
Plaintext	2.7	1.0	0.4
Plaintext + DB[2]	2.7	2.4	< 0.01
WBDS–SSE	22.4	2.3	2.2
Our SSE	28.9	1.3	9.97
Our SSE + DB	28.9	3.3	0.02
Our ASE	5569.0	4.7	2189.28

[1] The Search Time corresponds to the processing time of one IoC in 705,524 encrypted logs.
[2] 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

	Log Unforgeability	Predicate Privacy	Correlation Privacy	Token Collisions	Search Efficiency
WBDS–SSE	✗	✓	✗	if $\|r\| \ll l$	$+$
Our SSE	✓	✓	✓	Within the truncation window	$++$
Our ASE	✓	✓	✓	No	$--$

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