A Secure and Privacy-Friendly Logging Scheme

Cloud Cyber Security and Privacy: Readiness for the Next Decade

Andreas Aßmuth\textsuperscript{1}, Robert Duncan\textsuperscript{3}, Simon Liebl\textsuperscript{1,2}, and Matthias Söllner\textsuperscript{1}

\textsuperscript{1} Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany
\textsuperscript{2} PhD Student at Abertay University, Dundee, UK
\textsuperscript{3} University of Aberdeen, Aberdeen, UK

April 18, 2021 to April 22, 2021
About me

Professor of Computer Networks and Mathematics

Dean of Studies (Department of Electrical Engineering, Media and Computer Science)

Teaching:
  Mathematics, Computer Networks, Cryptography, Coding Theory, Information Security

Research:
  Applied Cryptography, Information Security, Ethical Hacking

IARIA Fellow
1. Introduction

2. Logging Strategies

3. Proposed Logging System

4. Conclusion and Future Work
Authentication ensures that only authorised persons may use computers or machines.
Features and services that are used to track individual actions to single employees can violate their privacy.

Microsoft productivity score feature criticised as workplace surveillance

Tool allows managers to use Microsoft 365 to track their employees' activity


PRESS RELEASE

The Hamburg Commissioner for Data Protection and Freedom of Information

October 1st, 2020

35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center

Goal: Find a solution to this problem, to be capable of tracking down individuals without violating their privacy.
Logging Strategies

- Logging is carried out to provide an audit trail of all activities involved in running the system. In the event of a disaster, the audit trail may be used to restore the records.

- Logging system is a high-value target for attackers.

- Ensure that logging data cannot be manipulated or deleted!
Immutable Storage

- Basic idea is to ensure that we can only ever add new records to the database.

- Database entries are permanent records which store any information related to the authentication of employees.

- Goal: retain permanency of all such transactions and audit trail of all transactions

- Data is encrypted to fulfil the demanded privacy constraints.
SageMath Demo!
Proposed Logging System

Logging System

- public key (encryption)
- private key (decryption)

Group 1

Secret Sharing: split the shared secret

Group 2

Secret Sharing: split the shared secret

Group 3

Secret Sharing: split the shared secret

© A. Aßmuth, R. Duncan, S. Liebl, and M. Söllner: “A Secure and Privacy-Friendly Logging Scheme”
Proposed Logging System  

Adaptability (1)

Logging System

public key (encryption)

private key (decryption)

Secret Sharing: split the private key \((j;m)\)

Group 1

Secret Sharing: split the shared secret \((k_1; n_1)\)

Group 2

Secret Sharing: split the shared secret \((k_2; n_2)\)

Group 3

Secret Sharing: split the shared secret \((k_3; n_3)\)

© A. Aßmuth, R. Duncan, S. Liebl, and M. Söllner: “A Secure and Privacy-Friendly Logging Scheme”
Proposed Logging System

Adaptability (2)

Logging System

- public key (encryption)
- private key (decryption)

Secret Sharing:
- split the private key ($j; m - 1$)
- split the shared secret ($k; n$)

Necessary Group 1

Group 2

Group 3

© A. Aßmuth, R. Duncan, S. Liebl, and M. Söllner: “A Secure and Privacy-Friendly Logging Scheme”
Conclusion and Future Work

- Proposed logging approach is highly secure and provides privacy.
- Works for companies with only one, but also for those with multiple facilities.
- Cloud-ready solution
- Next step: proof-of-concept implementation as a collaboration between the two universities
- Performance? Immutable database? Secret Sharing Scheme?
- Key-related issues: distribution, revocation, etc.
Prof. Dr. Andreas Assmuth
OTH Amberg-Weiden, Amberg, Germany
a.assmuth@oth-aw.de

Dr. Robert Duncan
University of Aberdeen, Aberdeen, UK
robert.duncan@abdn.ac.uk

Simon Liebl, PhD candidate
OTH Amberg-Weiden, Amberg, Germany
s.liebl@oth-aw.de

Prof. Matthias Söllner
OTH Amberg-Weiden, Amberg, Germany
m.soellner@oth-aw.de