

Database Forensics

Edgar Weippl
eweippl@securityresearch.at

Presented by Johannes Heurix
jheurix@securityresearch.at

Secure Business Austria

ISSI2009, NII

Introduction

- Importance of database forensics
 - Critical/sensitive information stored in databases, e.g. bank account data, health data
 - Loss caused by security incidents, corporate governance
- Aims of database forensics
 - To find out what happened when
 - To revert any unauthorized data manipulation operations
- Things to consider
 - How to gain access to the system
 - Live vs. dead system
 - Integrity
 - Images
 - Data encryption
 - Goal

- Files
 - MAC - (last) Modified time, Access time, Change/Create time (file attributes)
 - Timeline analysis
- Internal structures
 - SQL Server artifacts: data cache, plan cache, VLF, error logs,
 - Forensic tools (e.g. Windows Forensic Toolchest), automated scripts
 - Volatility, file locks
- Logical structures (index)
 - B-trees
 - Different trees for different node entry sequences

System breach suspected. What now?

- Find out if system was actually breached

- Error logs – failed logins

```
2007-03-02 07:39:10.20 Logon      Error: 18456, Severity: 14, State: 8.  
2007-03-02 07:39:10.20 Logon      Login failed for user 'sa'. [CLIENT: 192.168.1.20]  
2007-03-02 07:39:10.40 Logon      Error: 18456, Severity: 14, State: 8.  
2007-03-02 07:39:10.40 Logon      Login failed for user 'sa'. [CLIENT: 192.168.1.20]  
2007-03-02 07:39:10.60 Logon      Error: 18456, Severity: 14, State: 8.  
2007-03-02 07:39:10.60 Logon      Login failed for user 'sa'. [CLIENT: 192.168.1.20]  
2007-03-02 07:39:10.80 Logon      Error: 18456, Severity: 14, State: 8.  
2007-03-02 07:39:10.80 Logon      Login failed for user 'sa'. [CLIENT: 192.168.1.20]  
2007-03-02 07:39:11.00 Logon      Error: 18456, Severity: 14, State: 8.  
2007-03-02 07:39:11.00 Logon      Login failed for user 'sa'. [CLIENT: 192.168.1.20]  
2007-03-02 07:39:11.20 Logon      Error: 18456, Severity: 14, State: 8.  
2007-03-02 07:39:11.20 Logon      Login failed for user 'sa'. [CLIENT: 192.168.1.20]  
2007-03-02 07:53:07.39 Logon      Login succeeded for user 'sa'. Connection: non-trusted. [CLIENT: 192.168.1.20]
```

- Plan cache – UNION, single quotes ('), double dashes (--)

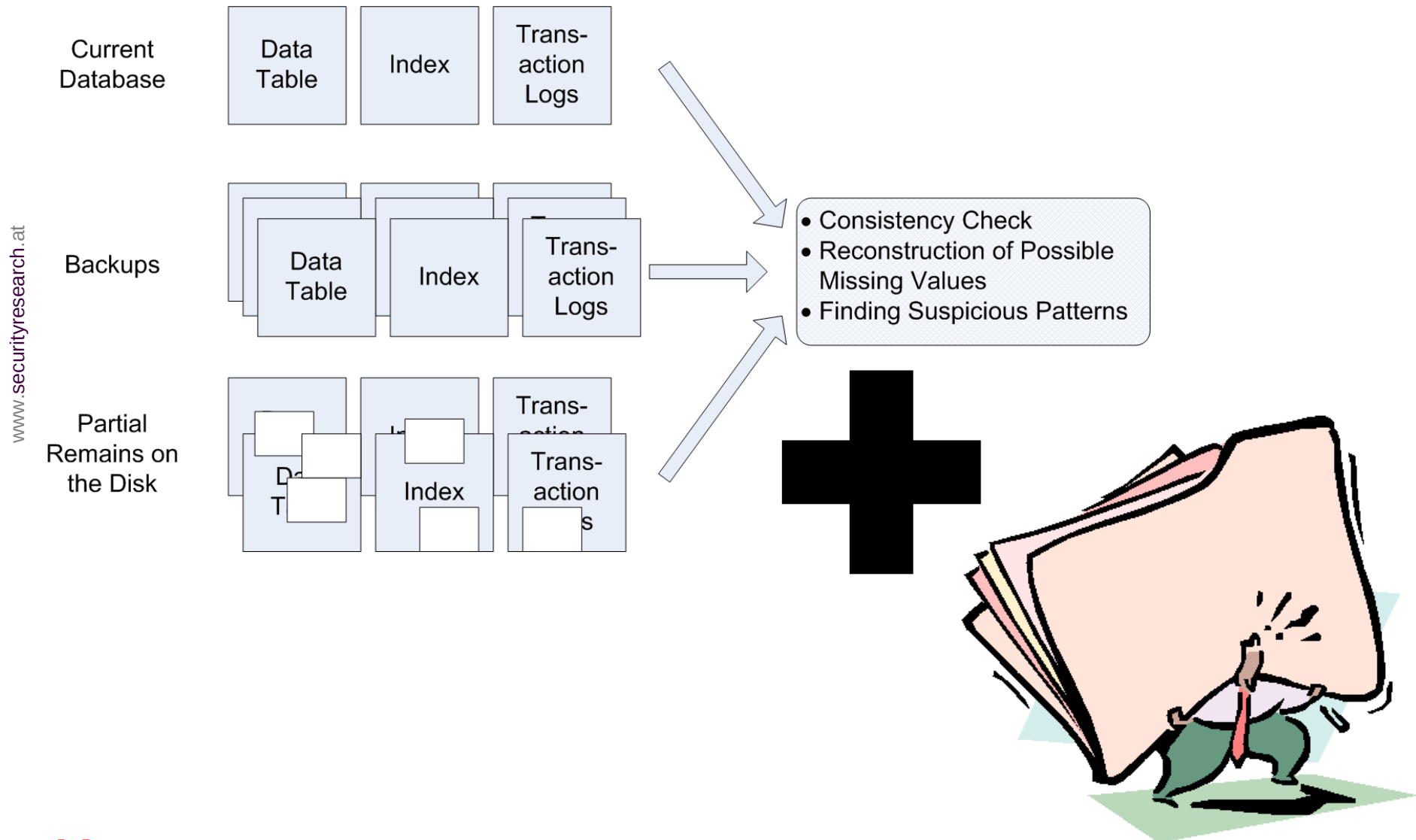
```
SELECT * FROM ORDERS WHERE FirstName = '' UNION ALL SELECT 6666, name, 'text', 'text',  
'text', 'text', 'text', 'text', 'text', 'text', 'text', 'text', 'text' from sys.sysobjects  
WHERE xtype = 'U'
```

- Find out which data records were retrieved

- Data cache – recently accessed data pages
 - Plan cache – cached database statements
 - Server state – most recently executed statement by session

Source: Kevvie Fowler – SQL Server Forensic Analysis, Addison-Wesley

Ongoing Research



Pseudonymization of Health Data

Thomas Neubauer
tneubauer@securityresearch.at

Johannes Heurix
jheurix@securityresearch.at

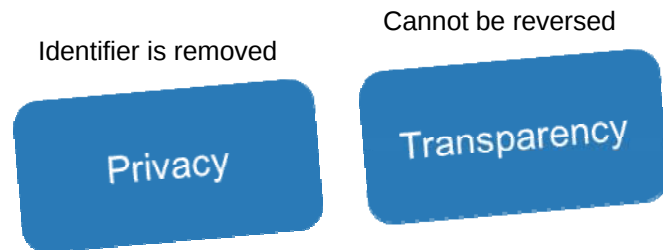
Secure Business Austria

ISSI2009, NII

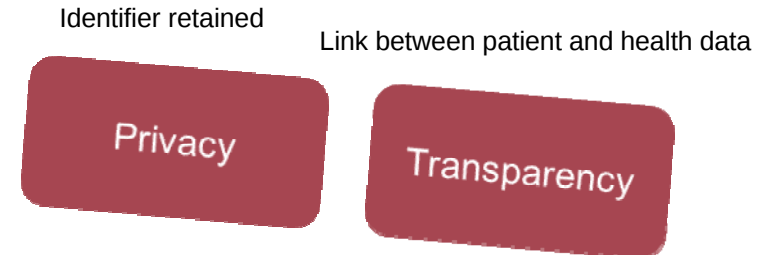
Motivation

- Privacy is one of the fundamental issues in health care today, especially when digitizing medical data
 - Electronic health records (EHR) improve communication between health care providers
- With interconnected systems comes highly sensitive and personal information whose disclosure may cause serious problems for the individual
 - Insurance companies denying health coverage
 - Employers denying employment
- Laws for the protection of privacy
 - Health Insurance Portability and Accountability Act (HIPAA)
 - European Directive 95/46/EC
- Secondary use of medical data in clinical studies

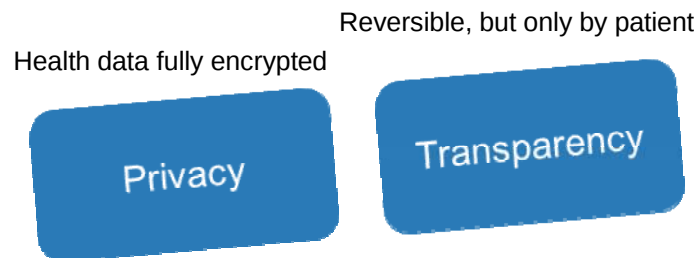
Trade Off – Secondary Use



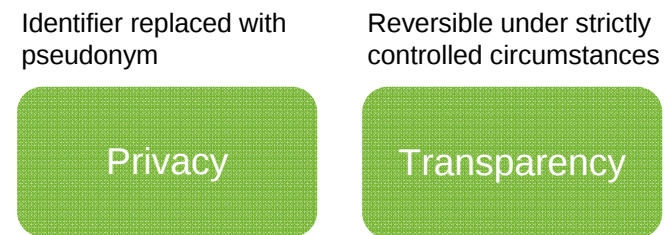
Anonymization



Normal Secondary Use

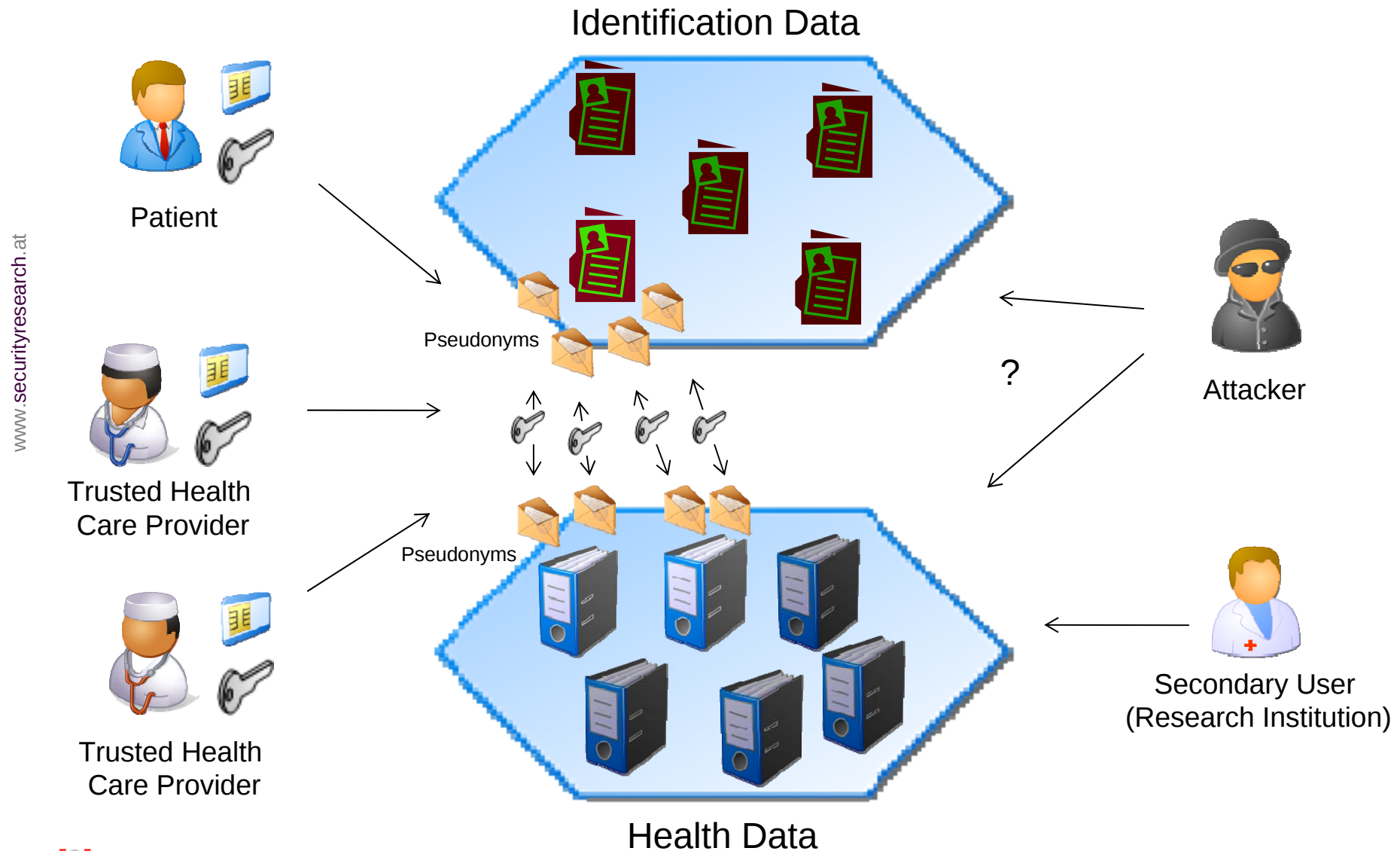


Encryption



Pseudonymization

PIPE - Pseudonymization of Information for Privacy in e-Health



PIPE Benefits and Ongoing Research

- Hull-based security architecture
 - Combination of symmetric and asymmetric cryptography
 - Multiple roles supported
- Patient as data owner
 - Grants data access authorizations to trusted relatives and health care providers
- Secondary use supported
 - Secondary users gain access to health data without the ability to reconnect the pseudonymized data to the corresponding patients
- Ongoing research
 - Extension with advanced privacy-preserving query and retrieval techniques
 - Development of configurable pseudonymization workflows for different domains
 - Service-based centralized design