To be published at IFIP/SEC'97

Pseudonymous Audit for Privacy Enhanced Intrusion Detection

Michael Sobirey[1], *Simone Fischer-Hübner*[2], *and Kai Rannenberg*[3]

[1]*Brandenburg University of Technology at Cottbus, Computer Science Institute, PO 10 13 44, D-03013 Cottbus, Germany, Phone: +49-355-69-2101, Fax: +49-355-69-2236, E-Mail: sobirey@informatik.tu-cottbus.de*

[2]*University of Hamburg, Faculty for Informatics, Vogt-Kölln-Str. 30, D-22527 Hamburg, Germany, Phone: +49-40-5494-2225, Fax: +49-40-5494-2226 E-Mail: fischer@rz.informatik.uni-hamburg.d400.de*

[3]*University of Freiburg, Institute for Informatics and Society, Telematics Department, Friedrichstraße 50, D-79098 Freiburg, Germany, Phone: +49-761-203-4926, Fax: +49-761-203-4929 E-Mail: kara@iig.uni-freiburg.de*

Abstract

Intrusion detection systems can serve as powerful security audit analysis tools. But by analysing the user activities, they are affecting the privacy of the users at the same time. Pseudonymous audit can be the basis for privacy enhanced intrusion detection. In this paper, the concept of pseudonymous audit for privacy enhanced intrusion detection and its prototype realisations are presented. Furthermore it is discussed whether IT security evaluation criteria cover pseudonymous audit and the respective changes are suggested.*

Keywords

Pseudonymous audit, privacy enhancing technologies, intrusion detection systems, IT security evaluation criteria

1 INTRODUCTION

IT security mechanisms can be technical data protection measures and are therefore required by most western data protection acts. On the other hand, they require the collection and use of specific personal data of users and usees† especially for access control and audit. This results in the conflict where security mechanisms can both help to protect the privacy of the data subjects and can be used to invade the privacy of the users and usees [De+87, Schae91, Fi+92, Fi94].

Audit provides the recording, analysis and review of data related to security relevant events. It shall deter and detect penetration of computer systems and forms a last line of defence against many kinds of security violations which cannot be prevented by authentication and access control. But audit generates personal data about the activities and behaviour of users. These data provide detailed information about: *Who* has accessed *when*, *where* and *how*, *what* and *whose* resource?

Up to now, the large amounts of audit data have caused no true privacy problems due to the lack of powerful analysis tools. The increasing use of intrusion detection systems is chanching this. Recent systems are capable of detecting intrusive behaviour by monitoring the system usage for subversive, suspicious or anomalous, possibly security violating activities.

Pseudonymous audit can help to balance the conflict between accountability and privacy. It is a privacy enhancing security audit technique where user identifying audit data are pseudonymized. Intrusion detection systems which operate with pseudonymized audit data offer a more socially and legally acceptable approach.

In this paper, we first briefly discuss criteria for privacy enhancing technologies. Then we present the concept and the first realisations of pseudonymous audit and privacy enhanced intrusion detection. Finally, we discuss whether IT security evaluation criteria cover pseudonymous audit and privacy enhanced intrusion detection and we recommend the respective changes.

2 IT SECURITY TECHNOLOGIES AND PRIVACY

2.1 Privacy and Privacy Enhancing Technologies

Privacy can be defined (as it has been done by the German Constitutional Court in its Census Decision of 1983) by the term right of informational self-determination, meaning the right of individuals to determine the disclosure and use of their personal data on principle at their discretion. In order to protect this right, the Council of Europe's Convention 108, the EU directive on data protection [EU95] as well as privacy laws of many western states require basic privacy principles to be guaranteed when personal data are collected or processed, such as:

- Purpose binding (personal data obtained for one purpose should not be used for another purpose without informed consent);
- Necessity of data collection and processing (the collection and processing of personal data shall only be allowed, if it is necessary for the tasks falling within the responsibility of the data processing agency);
- Requirement of adequate technical and organisational safeguards to guarantee the confidentiality, integrity and availability of personal data.

*Parts of this work are funded by the Gottlieb Daimler and Karl Benz Foundation (Ladenburg, Germany) as part of its Kolleg "Security in Communication Technology".

†Usees are personally affected by the collection and processing of data about them, but lack control over these activities.

In a fully networked society privacy is seriously endangered. Data protection commissioners are therefore demanding that privacy requirements should be technically enforced and that privacy should be a design criteria for information systems.

For example, recently the Dutch Data Protection Authority (the Registratiekamer) and the Information and Privacy Commissioner for the Province of Ontario, Canada, have collaborated in the production of a report [ReIPC95] exploring privacy enhancing technologies that are providing anonymity or pseudonymity for the users.

Extended security criteria for systems with high privacy requirements should cover a diversity of privacy enhancing security aspects, such as:

- Anonymity, pseudonymity, unlinkability, unobservability of users;
- Anonymity and pseudonymity of data subjects;
- Purpose binding and necessity of data processing of personal data of users and data subjects.

The privacy principle of necessity of data collecting means that personal data should not be collected or used for identification purposes when not truly necessary. Consequently, information systems should guarantee that, if possible, users can act anonymously. Examples for anonymous communication systems can be found in [Chau85, Pfi+91]. If storage is needed, personal data of data subjects should be anonymized or pseudonymized as soon as possible. Security mechanisms, such as inference control for statistical databases, can help to guarantee that personal data are usable for statistical purposes without revealing the data subject's identities. Furthermore, the privacy principles of purpose binding and necessity of data processing can be technically supported through an appropriate security policy and access control mechanisms (see e.g. [Fi94] for a formal privacy-enforcing access control model).

2.2 Intrusion Detection and Privacy Requirements

Security mechanisms, such as identification and authentication mechanisms, access control, audit or encryption, are necessary to protect the confidentiality and integrity of personal data. But, as mentioned above, audit and intrusion detection can conflict with privacy requirements for collecting and using as few user identifying data as possible.

Especially in Germany and in other Western European countries, data protection and labour legislation can restrict or prevent the use of intrusion detection systems in organisations, if the privacy of the users is not protected sufficiently. The privacy principle of necessity of data collection requires that personal data should not be collected or used for identification purposes when not truly necessary. Furthermore, according to Art. 6 of the EU directive on data protection, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Consequently, according to these provisions, user identifying data shall not be used in audit data, if not truly necessary, and should be pseudonymized, as far as possible.

Furthermore, according to German labour legislation, the works council in a company has the right of co-determination, if a system shall be introduced, that can be used or misused for monitoring the employees performance. As intrusion detection systems could be easily used for monitoring the users' activities and performance, works councils are normally not willing to accept them. This is probably also one reason, why in Germany there are hardly any powerful intrusion detection systems in use so far. Pseudonymous audit for privacy enhanced intrusion detection can be a socially and legally acceptable solution.

3 PSEUDONYMOUS AUDIT AND INTRUSION DETECTION

3.1 Functionality of Pseudonymous Audit

Pseudonymous audit is a special security audit technique, where subject identifiers and further user identifying data in audit records are pseudonymized right after creation and analysed in this representation, e.g. by an intrusion detection system (see Figure 1). When analysing the audit data, the security administrator does not have to know the real user identities of the monitored users. It is sufficient, that the real identity of a user can be determined, when suspicious or obviously intrusive behaviour was detected. Ideally, the security administrator should unmask an intruder only in cooperation with a data protection officer.

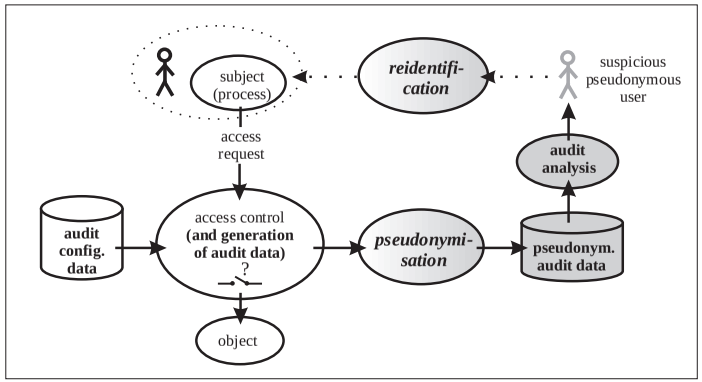

Figure 1 Functionality of pseudonymous operating system audit

By this way pseudonymous audit provides user accountability as well as pseudonymity. Regardless of the focus on operating system audit in this chapter pseudonymous audit is in principle also applicable to other kinds of audit, e.g. application audit [SoFi96].

3.2 The Raising Need for Pseudonymous Audit

Motivating the need for pseudonymous audit requires a short review of the developments in intrusion detection. Until recently the large amounts of audit data have caused no real privacy problems due to the lack of powerful analysis tools for a sophisticated, possibly abusing monitoring. With the gradually increasing usage of intrusion detection systems this situation is changing.

Many developments in this area were funded by government, military and intelligence agencies of the USA. Examples are the intrusion detection systems *Haystack* [Sma88] and *IDES* [Lu+92]. These systems monitored among others US Air Force mainframes and the in-house database system FOIMS (Field Office Information Management System) of the FBI headquarter in Washington D.C. Some research prototyps originated at universities and enterprises [BauKo88, Sna+91, Mo91, HaMa92]. With the beginning of the 90es first commercial intrusion detection systems became available, e.g. AT&T's *Computer Watch* [DoRa90], *Stalker* [SmaWi94] from the Haystack Laboratories and *CMDS* [Pro94] from SAIC.

Privacy problems were discussed occasionally [De+87, DSL90], but they received nearly no technological consideration. The following statement in a product description [HLI95] demonstrates how some developers handle privacy: *"Stalker does not examine user's keystrokes, files, or electronic mail, so it does not violate user privacy."* However, the Haystack Labs recommend to inform the users with each login that they *"are subject to security monitoring and testing."*

The availability of commercial intrusion detection systems makes an efficient automatic network monitoring for "data intensive" enterprises, such as banks or insurance companies, possible. Large amounts of audit data, that have to be collected for intrusion detection, are getting more and more technically manageable and are at the same time sharpening privacy concerns.

Global networking, increasing numbers of incidents in enterprises and public institutions, and the previous unability to detect and ward off security violations seem to result in a gradual change in thinking of the people affected and the decision makers. For instance in Europe military and enterprises begin to build up own intrusion detection capacities. To deal with the increasing privacy risks, technical solutions for privacy enhanced intrusion detection have to be developed. Besides, IT security evaluation criteria have to be extended to cover this concept.

3.3 User Identifying Data in Audit Records

To support the understanding of structure and content of the audit data the following example of a Solaris 2.4 audit record is given. This record consists of several tokens (data lines) beginning with a token identifier. The *header* token contains general information, as the size of this record, the audit event and the time stamp among others. The *path* and the *attribute* tokens provide object related information, e.g. the object name, the corresponding access rights, owner and owner group.

The following *subject* token contains detailed information about the initiator of the recorded action, especially the audit ID[‡], the effective user ID, the effective group ID, the real user ID, the real group ID and finally after some other data the host name. The last token contains the status of the audit event and a return value.

[‡]With each login a user gets a unique audit identifier that is unchangeable during his sessions regardless of temporary changes to other user identities, e.g. with the system command *su*. Each process runs under the audit ID of the user who initiated its start.

```
header,113,2,open(2) - read,,Mon Jan 22 09:34:32 1996, + 650002 msec
path,/usr/lib/libintl.so.1
attribute,100755,bin,bin,8388638,29586,0
subject,richter,richter,rnks,richter,rnks,854,639,0 0 romeo
return,success,0
```

In a simplified way the record can be interpreted as follows: On *22nd January 1996, 9.34:32,650002* user *"richter"* (see the audit ID) acted on his own account (audit ID and the real user ID are identical) and opened the file *libintl.so.1* successfully *(success, 0)* for reading *(open(2) - read)*. Owners of the program are user and group *"bin"*.

We distinguish concrete and conditionally user identifying data and data that can only be occasionally with additional knowledge used for reidentification. Concrete user identifying data are contained in the previously detailed interpreted subject and attribute token. Conditionally user identifying data are in the path token if a subject accesses own files or files owned by other users unlike system standard users *(e.g. daemon, bin or sys)*. In these cases the name of the *home directory*, often identical with the user name, is part of the complete recorded access path. Often the naming and the structure of subdirectories and the names of files/programs that are owned by regular users are user identifying in such cases. Similar path problems are caused by the recording of user account specific environment data (in certain audit records between the attribute and the subject token).

```
exec_args,2,
/usr/bin/sh,/home/fischer/my_special_subdir/xyz
exec_env,28,
DISPLAY=:0.0,GROUP=sec,HELPPATH=/usr/openwin/lib/locale:/usr/openwin/
lib/help,HOME=/home/schmal,HOST=hawk,HOSTTYPE=sun4,HZ=100, ...
```

Under certain conditions, especially if data on running processes of other users are available, the following data can be used for unwanted reidentification:

- Action in combination with date/time and the final action status;
- Action under consideration of the access rights, in combination with date/time and the final action status;
- Host identifier or name and host type.

For instance, if a file is writeable only for the object owner this action can only be successfully initiated by the object owner, the system administrator *root* or a masquerader who successfully hacked one of these accounts.

3.4 Pseudonymous Representations

The problem of the pseudonymisation is to find representations that provide optimal privacy for the audit based monitored users and that ensure on the other

hand significant analysis results. Very extensively pseudonymized audit records provide no significant analysis results. Analysis problems will especially be caused if action, date/time (, access rights) and action status are pseudonymised. That is shown with the following example interpretation of a pseudonymous audit record.

A *certain user* acted on his *own account* (pseudonyms for audit ID and real user ID are identical) and refered *somewhere* (host), *sometime* (date, time), *somehow* (action, status) *an own file* (subject ID's and object owner ID are identical).

Our examinations have shown, that an effective pseudonymisation of audit records should cover:

- All concrete user ID's;
- Location ID's;
- Conditionally subdirectories and objects.

3.5 Technological Requirements

The analysis of pseudonymous audit data requires the *ability to link* the pseudonyms (to each other) that represent identical user identifying data. This is necessary to trace the actions back to the initiating user. Possible technologies for the pseudonymisation are pseudonym databases, secret key or public key encryption.

To minimize performance losses and especially to support real time intrusion detection and audit analysis, a fast technology for pseudonymisation is required.

3.6 First Example Realisations

The IDA Approach

The IDA (Intrusion Detection and Avoidance) system concept couples a reference monitor with a kernel integrated intrusion detection component. Before the reference monitor is performing a kernel request, it sends the corresponding audit record, which is pseudonymized by encryption of the subject fields[§], to the intrusion detection component for further analysis (see Figure 2).

If a subject acting under a certain pseudonym has initiated a suspicious action, the decision module sends a negative response to the reference monitor. Only kernel requests that pass the reference monitor and the intrusion detection component, will be performed by the reference monitor. The IDA prototype was realised as model implementation. The analysis module was tested for known DOS viruses using audit data that were generated on an MSDOS machine, see [Bru+91].

IDA can react in real time without *manual* interactions and reidentification of a suspicious subject by the security administrator. In the prototype implementation, only the subject ID of the audit records are replaced by pseudonyms. For the IDA concept it was also planned to pseudonymize also subject identifying data in the object fields as well as parameters that are unique for certain users (e.g. terminal ID's). To approach the problem of unwanted reidentification it was planned that pseudonyms for subjects should at least be replaced in certain time intervals.

[§] To realise the 4-eyes principle, the key for decryption could be split into two halves, which are given to the security administrator and to the data protection officer.

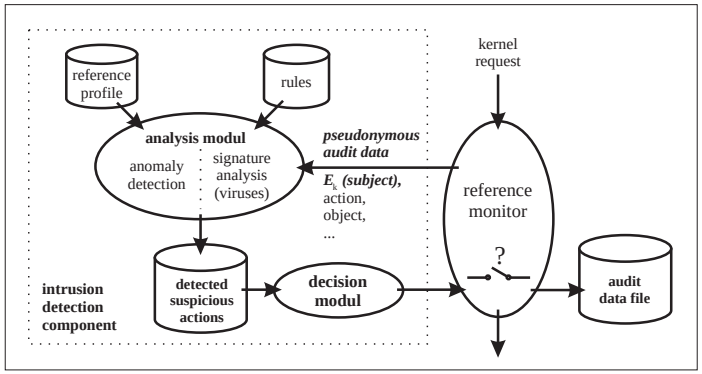

Figure 2 Architecture of the IDA system

The AID Approach

AID (Adaptive Intrusion Detection system) is a distributed intrusion detection system that monitors a local area network in real time. The system is based on a client-server architecture consisting of a central monitoring station and several *agents* on the monitored hosts. The central station hosts a *manager* and an *expert system* (see Figure 3).

The agents take the audit data that were collected by the local audit functions and convert them into an operating system independent data format. Then the data are transferred to the central monitoring station using secure RPC and analysed by an RTworks based real time expert system. The security officer can access the monitoring capabilities via a graphical user interface. In addition security reports are created. AID has been successfully tested in a Solaris 2.x network environment [So+96].

To provide a privacy enhanced audit based monitoring the audit data from the underlaying operating system are kernel internal pseudonymized before they are stored in the local audit data files. The pseudonyms are created by a *secret key* encryption. The audit functions of all monitored hosts use the same key that is changed from time to time. Only if security violations are detected, e.g. if an audit record and relevant context consitions match with (a part of) a certain attack signature, the user identifiers and other user identifying data (cf. 3.4) of the corresponding pseudonymized audit records are automatically reidentified respectively depseudonymized to enable countermeasures in time. That is required to support *real time* monitoring. In addition all depseudonymisations of audit records are logged. The implementation of this functionality in Solaris 2.4 and in AID is under way. The usage of *public key* encryption for pseudonymization is also examined.

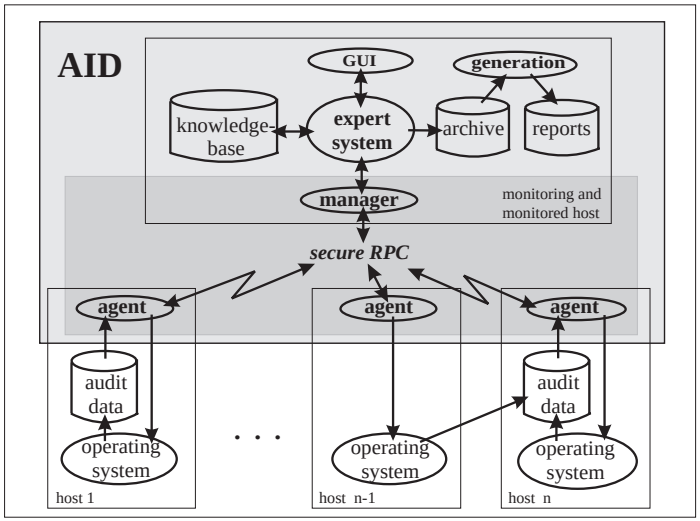

Figure 3 Architecture of the AID system

4 PSEUDONYMOUS AUDIT AND IT SECURITY EVALUATION

For over a decade now independent ("3rd Party") evaluation of the security properties of IT products and systems is considered as a relevant instrument to raise the level of IT security. The main idea behind this evaluation is, that users and procurs can place more trust into evaluation results or certificates of independent evaluators than into declarations just stated by producers or vendors.

A basic element for the evaluation results and the evaluation process is the criteria used. Therefore this chapter gives a short analysis whether the rather innovative security concept of pseudonymous audit is covered by the criteria in a way leading to meaningful evaluation results.

4.1 Evaluation Criteria and Privacy Enhancing Security

Most criteria differentiate the security properties of a *Target of Evaluation* (TOE; i.e. the IT product or system under evaluation) into *functionality* and *assurance* aspects. *Functionality* aspects describe what a TOE can do regarding IT security, e.g. audit, privacy protection or information flow control. *Assurance* aspects focus on how and to which extent the TOE has been evaluated, e.g whether just black box testing or a real code verification have been done. Consequently pseudonymous audit should be covered by the functionality part of criteria.

Early criteria are the US "Trusted Computer System Evaluation Criteria" [US_DOD85], the European "Information Technology Security Evaluation Criteria" [CEC91] and "The Canadian Trusted Computer Product Evaluation Criteria" (CTCPEC) [CDN_SSC93]. A former analysis [Ra94] showed, that none of these criteria really covers user and privacy friendly functionality, as their focus is biased on the protection of system owners instead of users or usees.

Despite its shortcomings the CTCPEC's structure of functional criteria was extendable to cover user and privacy friendly functionality. This was one reason, why it formed the basis for the functionality part of the "Evaluation Criteria for IT Security" currently drafted by Working Group 3 "Security Evaluation Criteria" of ISO/IEC JTC1/SC27. The last version of this approach can be found in the winter 1995/96 draft of the ISO-ECITS part 2 [ISO/IEC95]. Its coverage of pseudonymous audit is discussed in 4.3.

In parallel to the work in ISO/IEC, seven government IT security organisations (eg. the US National Security Agency and the German Information Security Agency) from six transatlantic countries (CDN, D, F, NL, UK, USA) started to develop an own set of criteria, the so-called "Common Criteria" (CC), whose draft version 1.0 [CCEB96] has been published in January 1996. The CC aimed to cover all the previous national and regional criteria. In April 1996 the CC replaced the previous working drafts in ISO/IEC JTC1/SC27/WG3, although they had caught hard criticism for their size, their structure and the fact, that they did not cover all the functionality from the previous drafts.

4.2 The Common Criteria and Pseudonymous Audit

According to the CC, the TOE IT security functional requirements (and consequently the evaluation results) are to be structured on the basis of *Security Functional Components*. These ca. 180 functional components are grouped into 76 *Families*, which are further grouped into 9 classes. *Dependencies* between functional components are listed in the components definitions.

Pseudonymity (FPR_PSE) is a family in the the class *Privacy* (FPR). Its component *Reversible Pseudonymity* (FPR_PSE.2) has a linkage to pseudonymous audit: it specifies, that aliases for user identities are provided and that only under certain conditions (to be defined before the evaluation) an authorised administrator can determine the user identity from the alias. So there is a partial coverage for pseudonymous audit, but the protection of user identifying data besides the user identities (cf. 3.3) is not covered.

The class *Security Audit* (FAU) consists of twelve families. Pseudonymous audit should be covered by those families, which specify requirements for the the generation and analysis of audit data:

- Security Audit Data Generation (FAU_GEN);
- Profile-Based Anomaly Detection (FAU_PAD);
- Penetration Identification Tools (FAU_PIT);
- Security Audit Analysis (FAU_SAA);
- Security Audit Review (FAU_SAR).

No component of these families considers pseudonymous audit or contains any declaration of dependencies to the Pseudonymity components. Only audit based

on "classical" user identities (as described in component *Basic User Identification* (FIA_UID.1) is covered. Although the term "Identity" is not defined in the CC, the way in which it is used leaves no room for the interpretation, that pseudonyms are covered. To achieve this coverage via redefinition of "Identity" probably requires greater restructuring of the CC. An alternative [SoRa96] would be to modify the families listed above by:

1. Extension of the functionality to cover the use of reversible pseudonyms: This applies especially to FAU_GEN and its component FAU_GEN.2 (User Identity Generation);
2. Integration of a dependency statement to FPR_PSE.2 (Reversible Pseudonymity) into all components of the families FAU_PAD, FAU_PIT, FAU_SAA, FAU_SAR.

4.3 The ISO-ECITS Draft and Pseudonymous Audit

The basis for structuring the TOE IT security functional requirements are *Functionality Levels* (roughly comparable to the CC's functional components) of 29 *Security Services* (roughly comparable to the CC's families). *Dependencies* between functionality levels are declared in their definitions. Generally the description of the functionality levels as well as that of the security services is much broader and less detailed than that of the corresponding elements in the CC.

The *Pseudonymity Services* come in two functionality levels: "Pseudonymity for Partner Authentication" and "Pseudonymity for Third Party Authentication". They describe that users "may use a resource or service without disclosing their identity but can still be held accountable for that use". Depending on whether the audit analysis is done by the same party as the audit generation, the first or the second level can be used to specify the requirements. The rather general service specifications also cover the protection of user identifying data besides the user identities.

Five functionality levels are given for the *Audit Services*. The range of audit functionality described in this paper is covered by the highest level "Advanced Detection". As well as in the CC the declaration of dependencies to Pseudonymity Services is missing and should be added. Different from the CC the "Identity" management issue is handled in a way that makes it much easier to cover pseudonymous audit. This is achieved by a reasonable general specification, especially concerning the identity recoverage process.

All in all, the functionality descriptions of the ISO-ECITS Draft, though being much shorter than those of the CC, provide a more comprehensive basis for specifying the requirements for a pseudonymous audit TOE.

5 OUTLOOK

The concept of pseudonymous audit for privacy enhanced intrusion detection can help to approach the conflict between classical IT security and privacy by providing both accountability and pseudonymity. So far, privacy enhanced intrusion detection has been only implemented in two research prototypes. But it will probably become more relevant in future, because it can be a more privacy friendly and thereby socially and legally acceptable solution. In a networked society witzh increasing privacy risks it will be neccesary to develop and apply more privacy enhancing technologies as well as criteria for their assessment and comparison.

REFERENCES

[BauKo88] Bauer, D. S.; Koblentz, M. E.: NIDX - An expert system for real-time network intrusion detection, Proc. of the IEEE Computer Networking Symp., New York, NY, April 1988, 98-106

[Bru+91] Brunnstein, K.; Fischer-Hübner, S.; Swimmer, M.: Concepts of an expert system for virus detection, Lindsay, D.; Price, W. (eds.): Information Security, Proc. of the IFIP/Sec'91-Conference, Brighton, UK, May 1991, North Holland, Elsevier, 391-402

[CCEB96] Common Criteria Editorial Board: Common Criteria for Information Technology Security Evaluation, version 1.0, Jan. 1996, 4 of 5 parts

[CDN_SSC93] Canadian System Security Center: The Canadian Trusted Security Evaluation Criteria, version 3.0e, Jan. 1993, Communications Security Establishment, Government of Canada

[CEC91] Commission of the European Communities: IT Security Evaluation Criteria, V. 1.2, Office for Official Publications of the European Communities, Luxembourg, June 1991

[Chau85] Chaum, D.: Security without Identification: Transaction systems to make a Big Brother obsolete, CACM 28(1985)10, 1030-1044

[De+87] Denning, D. E.; Neumann, P. G.; Parker, D.: Social aspects of computer security, Proc. of the 10th National Computer Security Conference (NCSC), Baltimore, MD, 1987, 320-325

[DoRa90] Dowell, C.; Ramstedt, P.: The ComputerWatch data reduction tool, Proc. of the 13th NCSC, Washington, D.C., Oct. 1990, 99-108

[DSL90] Intrusion Detection: The State of the Art, Data Security Letter no. 22, Nov. 1990, 4-7

[EU95] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[Fi92] Fischer-Hübner, S.: IDA - An Intrusion Detection and Avoidance System (in German), dissertation, Aachen, Shaker, 1992

[Fi94] Fischer-Hübner, S.: Towards a privacy-friendly design and use of IT-security mechanisms, Proc. of the 17th NCSC, Baltimore, MD, Oct. 1994, 142-152

[Fi+92] Fischer-Hübner, S.; Yngström, L.; Holvast, J.: Addressing vulnerability and privacy problems generated by the use of IT-security mechanisms, in Aiken, R. (ed.): Proc. of the IFIP 12th World Computer Congress, vol. II, Education and Society, Madrid, Sept. 1992, 245-257

[HaMa92] Habra, N.; Mathieu, I.: ASAX: Software architecture and rule-based language for universal audit trail analysis, Deswarte, Y.; Eizenberg, G. (eds.): Proc. of the 2nd European Symposium on Research in Computer Security (ESORICS' 92), Toulouse, Nov. 1992, 435-450

[HLI95] Haystack Laboratories, Inc.: Stalker version 2, product description, 1995

[ISO/IEC95] International Organization for Standardization /International Electrotechnical Commission, Joint Technical Committee 1, Subcommittee 27: Evaluation Criteria for IT Security, Part 1-3, Working Drafts Winter 1995/96; Documents ISO/IEC JTC1/SC27/N1269, ISO/IEC JTC1/SC27/N1270, ISO/IEC JTC1/SC27/N1271

[Lu+92] Lunt, T. et al.: A real time Intrusion Detection Expert System (IDES) - Final Report, SRI International, Menlo Park, CA, Feb. 1992

[Mo91] Moitra, A.: Audit Log Viewer and Analyzer, Proc. of the 7th Intrusion Detection Workshop, May 1991, SRI International, Menlo Park, CA

[Pfi+91] Pfitzmann, A.; Pfitzmann, B.; Waidner, M.: ISDN-MIXes: Untraceable communication with very small bandwidth overhead, Proc. of the IFIP-TC11 Sec'91 Conference, Brighton, UK, May 1991, 245-257

[Pro94] Proctor, P.: Audit reduction and misuse detection in heterogeneous environments: Framework and application, Proc. of the 10th Annual Computer Security Applications Conference, Orlando, FL, Dec. 1994, 117-125

[Ra94] Rannenberg, K.: Recent Development in IT Security Evaluation - The Need for Evaluation Criteria for multilateral Security; in Sizer, R. et al.: Security and Control of Information Technology in Society - Proc. of the IFIP TC9/WG 9.6 Working Conference, August 12-17, 1993, St. Petersburg, Russia; North-Holland, Amsterdam, 1994, 113-128

[ReIPC95] Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada: Privacy-enhancing Technologies: The path to anonymity, vol. I, Aug. 1995

[Schae91] Schaefer, L. J.: Employee privacy and intrusion detection systems: Monitoring on the job, Proc. of the 14th NCSC, Washington, D. C., Oct. 1991, 188-194

[Sma88] Smaha, S. E.: Haystack: An intrusion detection system, Proc. of the 11th NCSC, Baltimore, MD, Oct. 1988, 37-44

[SmaWi94] Smaha, S. E.; Winslow, J.: Misuse detection tools, Computer Security Journal 10(1994)1, Spring, 39-49

[Sna+91] Snapp, S. R. et al.: DIDS (Distributed Intrusion Detection System) - Motivation, architecture and an early prototype, Proc. of the 14th NCSC, Washington, Oct. 1991, 167-176

[So+96] Sobirey, M.; Richter, B.; König, H.: The Intrusion Detection System AID. Architecture, and experiences in automated audit analysis, in Horster, P. (ed.): Communications and Multimedia Security II, Proc. of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security, Essen, Germany, Sept. 1996, Chapman & Hall, London, 278-290

[SoFi96] Sobirey, M.; Fischer-Hübner, S.: Privacy oriented audit, Draft Proc. of the 13th Annual CSR (Centre for Software Reliability) Workshop "Design for Protecting the User", Bürgenstock, Switzerland, Sept. 1996, section 13

[SoRa96] Sobirey, M.; Rannenberg, K.: Remarks on the Coverage of Pseudonymous Auditing in the Evaluation Criteria for IT Security; Att. 2 to the German NB Reasons for disapproval of ISO/IEC CD 15408-2 (ISO/IEC JTC 1/SC 27 N 1402); Summary of Voting, ISO/IEC JTC 1/SC27 N1476

[US_DOD85] US DoD Standard: Department of Defense Trusted Computer System Evaluation Criteria, Dec. 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug. 83

BIOGRAPHIES

Michael Sobirey completed his diploma in computer science at the University of Technology "Otto v. Guericke" Magdeburg. Since April 1993 he has been scientific assistent at the Brandenburg University of Technology at Cottbus, Computer Science Institute. His research interests are real-time monitoring of heterogeneous networks and privacy-oriented security functions. He is member of the DIN working group NI 27c "Evaluation criteria for IT security" and of the National Expert Working Group "IT Security Criteria". He is leader of the research project AID.

Simone Fischer-Hübner studied Computer Science with a minor in Law at Hamburg University. She obtained her doctoral degree (Ph.D.) in July 1992. She is currently an Assistant Professor at the University of Hamburg, Faculty for Informatics. From Sept. 1994 - March 1995 she was a Guest Professor at the Copenhagen Business School, Institute for Computer and System Sciences. Her teaching and reseach has been focused on IT security and privacy. She is a founding member and secretary of IFIP WG 9.6, member of IFIP WG 11.8 and member of the National Expert Working Group on IT Security Evaluation Criteria.

Kai Rannenberg, Dipl.-Inform., TU Berlin 1989. 1989-1993 TU Berlin; 1990 Berlin Privacy Commissioner; 1993- University of Freiburg, Coordinator of the "Security in Communication Technology" Kolleg sponsored by Gottlieb Daimler and Karl Benz Foundation. Member of IFIP WG 9.6, IFIP WG 11.4, ISO/IEC JTC1/SC27/WG3 "Security Evaluation Criteria" and its German shadow group, GI "Privacy and IT Security Task Force", National Expert Working Group "IT Security Criteria"; Secretary of the CEPIS Special Interest Network Legal and Security Issues. Research focus: IT Security and Privacy for public and open communication systems, especially in standards and evaluation criteria.