Economical Benefits of Standardized Intrusion Detection Parametrization

Björn-C. Bösch

Abstract— Intrusion Detection Systems (IDS) are very important to protect important services against malicious actions. Detailed knowledge of information processing and protocols are necessary to protect the services and systems sufficient against attacks. IDS are currently independent and coexisting solutions. Each single IDS requires its individual administration access, administration handling and management infrastructure. Possible savings of a standardized parameterization infrastructure over all IDS will be analyzed. In every part of the solution life cycle process, design, infrastructure and additional expenses were analyzed. Based on the Return-on-Security-Investments model the benefit of a standardized parameterization was pointed out.

Index Terms— IDPEF, IDXP, Intrusion Detection, Network Management, Standardization, System Management.

1 Introduction

Today, company assets have changed from hardware (like machines and buildings) to information. It is very important to protect these company assets sufficiently. One way is to make a risk analysis to find out the information's importance by identifying the financial and reputation impact. The corresponding counter measurements have to be selected, that an attacker has to invest more than the value of the gathered information. Attackers automate their work and write supporting tools to make their work more effective. As result complexity of attacks increases when at the same time the knowledge to exploit these vulnerability decreases [1]. Attack trees [4] or a treatment of costs on site of the attacker [5] could be used to assess the concerted time and efforts for dedicate attack ways to gain or disclose information. Based on these characteristics, security safeguards could be planned more economically. The remaining paper is organized as follows: A brief business management analysis and return-on-security-investments are described in section 2. Section 3 describes the architectural solution approach and the standardized parameterization. Subsequent the economic impact along the product life cycle of standardized parameterization of IDS is described. Based on the technical approach the economic benefit will be pointed out. Section 4 concludes this work.

2 Business management Analysis

Based on the point of view, that "a wall has to be so high, that an attacker is not able to overcome it", all security measures have to be so planned, that they are economically. To have a practical benchmarking procedure the Return-on-Invest (RoI) model will be used. The greatest challenge in security investments is to argue the invest and benefits of a solution

2.1 Return-on-Security-Investments

A common and accepted model to calculate security investments is the Return-on-Security-Invests (RoSI) model, which is an evolution of the RoI model. The expected return is defined as product of risk exposure (RE) and percentaged mitigated risk (%mR). With the solution costs (SC) the RoSI could be calculated as:

$$RoSI = \frac{(\%mR \cdot RE) - SC}{SC}$$

Based on this formula the solution costs include all expenses of the solution - expenses for planning and conception, solution investments and operating costs. The costs are detailed within the section 3.2 "Solution Live Cycle Benefits". The RoSI model based on single risk management and risk mitigation. Complex and comprehensive risk mitigations have some limitations but it is still a good choice for investment decisions including security investments [6].

3 Approach

This section describes current IDS architectures and the architectural approach to separate the IDS manager. The economic impact along the product life cycle of standardized parameterization of IDS is subsequent described. This section closes with the economic benefit of standardized parameterization of IDS.

3.1 Current IDS Architectures

Intrusion Detection Systems (IDS) protect critical infrastructures and services of companies against malicious actions. IDS are highly specialized and have detailed knowledge of application and communication to protect services adequate. Therefore IDS are scoped on a single application (special kind of Host based IDS), a single operating system (Host based IDS) or communication protocols (Network IDS). To detect intrusions in an IT

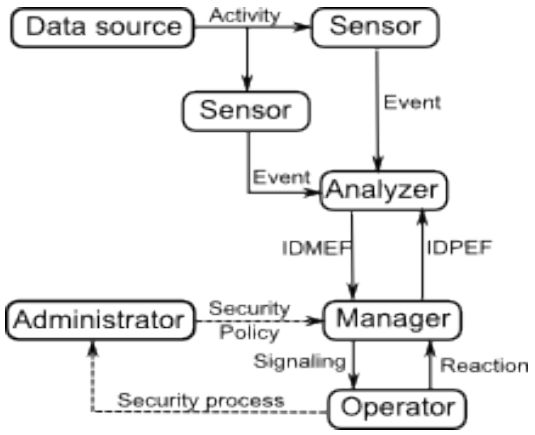

Fig. 1. IDS model with standardized communication to and from the manager.

• **Björn-C. Bösch**, System Software and Distributed Systems Group, Faculty II - Department of Computing Science, Carl - von – Ossietzky - University Oldenburg, Oldenburg, Germany.
e-mail: bjoern.carsten.boesch@uni-oldenburg.de

composite, different IDS are required to protect and monitor computer systems at all levels, top to bottom. Security safeguards (e.g. IDS) are currently isolated solutions and will be administrated separately. Application-based IDS become more and more specialized and focusing to one single application. So, vendors provide own specialized IDS-functionalities for their products. Current multi-vendor IDS architectures do not interact with each other. Every additional IDS requires a full independent coexisting IDS solution. A full functional integration with a consistent security policy for an existing IDS landscape is currently not available. Based on the Intrusion Detection Message Exchange Format (IDMEF) [9] it is possible to integrate an additional general monitoring system as notification umbrella. This article is focused on the economical benefit of standardized parameterization for IDS with one central IDS Manager. This work set up on the IDS model of the IETF and their definitions [12]. The entities Analyzer and Sensor are vendor-specific entities. In the IETF IDS model, the Manager is the only entity that could be shared with other IDS. The communication between a general Manager and vendor-specific Analyzers has to be standardized to manage a multi-vendor IDS architecture with one Manager. Today, IDMEF standardizes notifications to a monitoring application. As transport protocol the Intrusion Detection eXchange Protocol (IDXP) [10] is already created on top of the Blocks Extensible Exchange Protocol (BEEP) [11]. The BEEP framework provides confidentiality, integrity and authentication for the communication. IDXP provides a streamtype option and the value "alert" is already used by IDMEF. This work uses IDXP with the streamtype value "config" as communication framework. The Manager was separated from the rest of the IDS with a standardized communication between Analyzer and Manager. The communication between Sensor and Analyzer is continuously vendor-specific. The communication in the IETF IDS model [12] was modified. As visualized in fig. 1, the security policy will be applied to the Manager and distributed to the Analyzers and forwarded to the Sensors instead of directly from the Administrator to all IDS entities. Operators and Administrators use the Manager as single point of human interface to operate the entire IDS. Based on this architectural approach, requirements for a standardized format are defined [13], [14]. Based on this, the format was created [15] and implemented in a proof-of-concept environment [16], [17] in three open source IDS. The independence of the IDS Manager is pointed out for different scopes in [18] and [19].

3.2 Solution Life Cycle Benefits

A standardized parameterization format has various impacts along the solution life cycle. It starts within the planning and conception phase and continues via the purchasing to the implementation. Subsequent operations and disposal proceed the solution life cycle. Parallel to the operations a contingency planning for the IDS has to be in place.

Planning and Conception: The planning and conception phase defines coverage and scope of the IDS. In-scope systems and services will be documented. Requirements for the IDS have to be defined. Based on the standardized parameterization and parameter exchange between Manager and Analyzer, the requirements could be split in two independent parts. On one side is the Manager with its usability comfort and reporting requirements. On the other side are various Analyzer-Sensor-combinations in context to each single in-scope service with their analyzing techniques and quality. This makes the planning and conception of an IDS more easier and reduces the complexity. The needed time and the efforts to maintain the modular IDS concept and the requirements will be reduced. The resulting savings based on time and external consulting support depends on the prior complexity and coverage of the IDS. As next step available IDS will be evaluated. It starts with a theoretical analysis of IDS features against the set out requirements. A free combination of Analyzers and Manager enables a wider choice of possible IDS and more components have to be evaluated. The evaluations are more specialized and focused on a single Analyzer for a service or system instead of an analysis of every single requirement of complete IDS. As result a more focused solution in all parts of the IDS will be found. Based on the best fitting IDS components the proposed solution will be described and the added technical value will be pointed out in detail. In case of an expansion of the IDS, the Manager still exists and has not to be evaluated again. At the end of this phase the IDS architecture is theoretical planned and the IDS components are defined. Now the procurement department is able to order the material of the IDS.

Purchasing: Based on a free combination of Analyzers under one administration front-end (Manager), the selection process for IDS will become simpler. New in-scope systems and services are able to be integrated in an existing IDS with individual Analyzers. The purchasing could be focused to the actual solution and could be freely expanded. Within the purchasing phase there are no savings directly possible, but multi vendor strategies are possible to earn better buying conditions.

Implementations: Within the implementation phase savings base on the design of the planning and conception phase. Instead of one Manager for every single IDS only one Manager for all IDS is required. In this central Manager all Analyzers of the different services will be integrated in this entity. This includes also Analyzers that will be integrated later in this IDS-landscape. This enables a small first integration spot with an expansion on other systems and services where an IDS is reasonable and economically. Later efforts to expand the IDS conception and evaluate additional Analyzers for new in-scope services are not necessary. This architecture is primary focused on evaluation of the IDS Manager with its features and usability comfort and secondary on the Analyzers which depend strong on the corresponding systems and services. The IDS-landscape could be build up step by step in accordance to the needs of systems and services and could be implemented together with upcoming system refreshes. The roll out could be organized modular and simple by integration in central change management processes. The implementation phase includes also the integration of the IDS in incident handling and response processes. This will be done at one single central point. Only the one central IDS Manager has to be provide an interface for integration in the existing incident handling applications and processes. There is no need for the incident handling applications to integrate more than this one central IDS Manager. This will be reducing relevant system integration expenses. The results of the planning and conception phase and the implementation phase raise up here also savings of recurred expenses within the use

period of the systems. For example the interface for incident handling reduces the complexity for maintenance and the expenses will be reduced by minimizing complexity and quantity. This phase is the determining factor of onetime and recurred savings.

Operations: All infrastructure elements and their savings are part of the implementation phase. The savings in operations are focused on system management processes and personnel expenses. To efficiency of interaction with the IDS could be improved in three ways [7]:

- Reduction of poorly configured components
- Improvement of configuration management: i.e. training of operators to understand underlying system processes and configurations correctly
- Automation of processes

As result, the "interface design [...] must be flexible [...] to the ever changing landscape of the cybersecurity operational environment" [7]. A separation of the IDS Manager with a standardized format and consistent front end design for operators achieve this finding. Each single IDS Manager front end could have a good usability based on ISO EN 9241 [8]. An analysis over all IDS Manager shows that syntax and front ends to maintain the different Analyzers of an IDS are individual. There is currently no common configuration procedure, structure or syntax to maintain IDS. A change over several Analyzers results that parameters have to be changed with different management access, administration front ends, administration syntax and administration files. Each Analyzer has to be changed individual. Affected by a prevalent use of the consistent front end, operational staff will have routine in usage. A consistent parameterization format and front end design supports the operator in administrations. Integrated consistency checks for activated service monitors and aggregated thresholds could be established and supports Operators in calibration of single Analyzers over the complete IDS network to a consistent security policy. No different syntax and front ends are necessary to maintain different Analyzers of an IDS. The use of one parameterization interface only reduces the training expenses. Usability savings i.e. less handling errors, efficient work processing or stress of operational personal, are very individual and depends on their setup and IDS combinations. Therefore it is not possible to analyze the usability of different IDS integration in general. So the improvement of usability is beyond the scope of this paper. Updates of the IDS software (i.e. signatures and software patches) as well as backup and restore mechanisms could be automated by the standardized format with a central IDS Manager. The standardized format is able to support cascaded and multi-user IDS management structures. This supports interfaces for various applications to adapt the IDS services to a changed landscape in virtual or cloud environments. The support of the IT planning and development based on an expansion of the existing IDS. New IDS Analyzers will be integrated in the existing IDS Manager and could be evaluated with focus to the special needs of the protected systems and services. No additional IDS has to be operated in later operations. The evaluation tests are reduced to the Analyzer features only.

Disposal: The disposal is focused on the run down of systems and services with a secure discard of hardware including containing data. In this analysis the disposal phase includes the efforts to migrate the systems from one hardware platform or vendor to a second one. Within the migration parameters have to be evaluated, adjust and set again. This could be all prepared parallel to the current installation and switched within a maintenance window. A smooth migration of single systems could be realized. There is no need to operate more than one IDS front end (Manager). In case of a change of the IDS Manager, the applications could be operated parallel and the operation handling could be switched from the prior system to the new system step by step. Both Managers could be operated parallel during the migration. There is no need to make a hard cut. The base information like sensor addresses have to be integrated in the new Manager. All other information, e.g. build up the backup database could be generated automatically or are provided by the Analyzers within the parameterization session. Parameterization changes could be automated by the prior Manager.

Contingency Planning: The contingency planning is a part of operations. It documents the procedure and power to act of different people including roles in case of a disaster. It will be less complex to maintain the IDS part of the contingency planning handbook, because the IDS will become more modular and has one central entity for all IDS components. A standardized format has no direct impact to complexity or savings of the contingency planning.

3.3 Economic Benefits

The described technical benefits raise economical savings along the product life cycle. The analysis base on identical implementations and roll out strategies for comparable and suitable results. Therefore the listed points have no direct (but secondary) impact of the expenses for an IDS in combination with a standardized format:

- Hard- and software
- Integration expenses and times
- Operations of the analyzers
- Change management
- Evaluation of IDS components (Analyzers and Managers)
- Maintenance fees for the Analyzers
- Incident response handling

So these facts are not a part of this analysis. A standardized format has direct impact on onetime expenses for:

- Integration of the Manager
- Evaluation of the Manager
- Systems integration for incident response handling

Based on this a theoretical analysis of one time savings will be determined. The used times and expenses [21] are used as guidance values. The effective expenses depend highly on organization and integration within the company and have to be determined individual. The one time savings (S_{OT}) add all single savings in total. The first summand are the integration saving of the IDS Manager. For installation and initial configuration of each IDS Manager are 3 man-days (MD)

($I_{D_{HW}}$) needed. Hard- and software will be calculated with 5.000 US-$ for each IDS Manager ($I_{C_{HW}}$). Without a standardized parameterization format a dedicate IDS Manager would be needed for each in-scope-service (iss). With a standardized format only one central IDS Manager will be needed ($\sum iss - 1$). The difference between available IDS Managers (aIDM) and the IDS Manager of the in-scope service (iss) will affect the evaluation scale of possible IDS Manager. This could be more as without a standardized format. For each single evaluation 2 man-days are planned ($I_{D_{Eval}}$). The integration of the IDS Manager in existing incident response handling applications and processes will be simplified from a dedicate IDS Manager for each in-scope service to one central IDS Manager ($\sum iss - 1$). For the systems integration five man-days ($I_{D_{IR}}$) and 5.000 US-$ are calculated ($I_{C_{IR}}$). Based on this frame conditions, the one time savings could be expressed mathematically as:

$$S_{OT} = \sum iss - 1 \cdot ((I_{D_{HW}} + I_{C_{HW}}) + I_{D_{Eval}} \cdot \sum aIDM - iss + (I_{D_{IR}} + I_{C_{IR}}))$$

Direct impacts on recurrent expenses have:

- Savings of hardware operations (power, climate, rack space, etc.)
- Training expenses for the Manager
- Maintenance expenses for the IDS Management
- Patch-Management of the IDS Landscape
- Documentation of configuration actions
- Consistent policy planning and checks

Expenses for additional hardware operations for individual IDS Manager of all in-scope services are not necessary ($\sum iss - 1$). There is only one hardware platform required, 1.000 US-$ are saved for each substituted server ($I_{C_{HW}}$). The training expenses depends on the courses expenses and the involved staff for IDS operations. The trainings reduces from all in-scope services to one central management application ($\sum iss - 1$). As average two man-days per month and 2.000 US-$ per year (I_{C_S}) and in-scope service could be planned as training expenses. The maintenance of IDS Managers are reduced to one remaining IDS Manager for all in-scope services ($\sum iss - 1$). The maintenance (including patch-management, calibrations and documentation of configuration actions) for the IDS-landscape will be reduced. The expenses for vendor-maintenance of the IDS-Manager will be reduced to one remaining IDS Manager ($\sum iss - 1$). 20 % of invest for hard- and software (I_{C_M}) will be calculated per year for maintenance fees. The maintenance operations will be calculated with five days per in-scope service IDS per month. It is expected that the efforts for every additional in-scope service ($I_{D_{Ops}}$) will be reduced by the central IDS Manager to one day per month. A new upcoming operations element is a consistent IDS policy over all distributed Analyzers. This lifts the security level and preserves the performance of the Analyzers. Each Analyzer (A) has to be adjust to the traffic, which could be passed. In wide or complex environments, i.e. virtual or cloud environments, this could

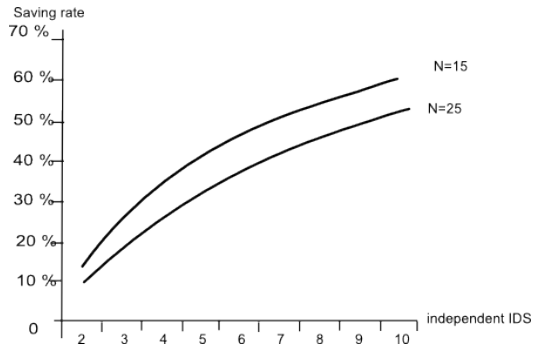

Fig. 3. Onetime cost savings based on 15 Analyzers and 4 changes per month.

consume a lot of time ($\frac{A!}{A! \cdot (A-2)!}$) and it depends in addition on number of changes and the average change costs ($I_{C_{Ch}}$). All this could be automated in a central IDS Manager by additional consistency checks. A smaller and linear impact based on number of changes (Ch) and change costs are the

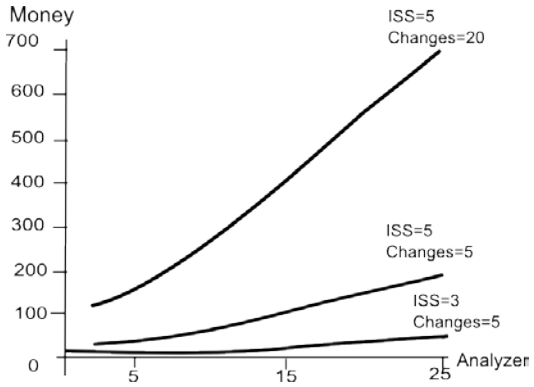

Fig. 2. Schematically development of savings in virtual and cloud environments based on different protected systems and services.

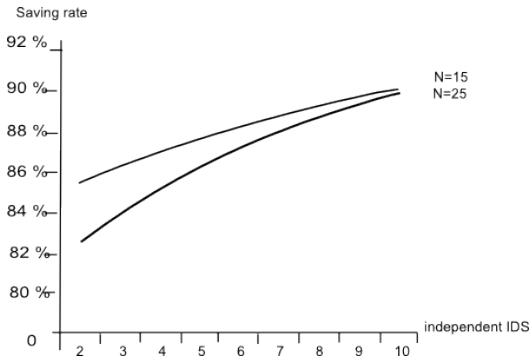

Fig. 4. Recurrent cost savings based on 15 Analyzers and four changes per month.

single values which infect this. All in all, monthly recurrent savings (S_r) could be represented as mathematical formula as:

$$S_r = \sum iss - 1 \cdot ((I_{C_{HW}} + I_{CS} + I_{D_{Ops}} + I_{C_M} + \frac{A! \cdot Ch \cdot I_{C_{Ch}}}{A! \cdot (A-2)! \cdot \sum (iss - 1)})$$

Most of these values are linear and result from the substituted IDS Manager. The consistency check is the single element that influences the impact nonlinear and makes the main economical value for a standardized format in complex environments.

4 Conclusion

This theoretical analysis of economical benefits demonstrates that a standardized parameterization format is already useful for operations when more than one IDS should be operated. The economical benefit grows up with every additional different Analyzer vendor of the Security Operations Center. All determined factors influence expenses and security level linear. Except the global security policy consistency check has non-linear curve related to expenses and security level. As illustrated in fig. 2 the economic benefit is effected by in-scope services and monthly change rate. The amount of Analyzers has the biggest and exponential influence to the savings. Fig. 3 illustrates the one time saving rates based on constant change rates and Analyzers. With 25 Analyzers the onetime costs with one supervising Manager saves 9.94 % compared to the classic architecture with 2 Managers. For 15 Analyzers there is a saving of 13.86 %. This rate increases up to 51.40 % by 15 Analyzers and 10 different in-scope services respectively 60.2 % for the same architecture but only 15 Analyzers. Recurrent savings are illustrated in fig. 4. The very high savings based on the omitted additional Managers. So the savings start with 82.46 % in the environment with 15 Analyzers respectively with 85.41 % by 25 Analyzers and increase up to 89.9 % for 15 Analyzers and 90.14 % by 25 Analyzers. The real saving rates depend on organizational structure, procurement conditions, etc. So this calculated saving rates could be a rough guidance value only. The onetime savings based on the centralization of all IDS Manager in one IDS Manager for all different Analyzers. This builds also the initial costs for IDS Managers without any IDS Analyzer operations expenses. The recurrent savings are linear affected by saved basic operation expenses and operational costs for the omitted additional Manager. The three calculations demonstrate that a supervising manager is economical in typically environments. A standardized parameterization provides significant one time and recurrent savings already in small IDS landscapes. The savings increase with every additional omitted Manager. The savings increase exponential with every additional Analyzer. The change rate is a not linear factor for the recurrent savings. In complex environments with heterogeneous systems and services IT like cloud environments the change rate is an important factor. In cloud environments services will be moved for hardware maintenance from one hardware to another. Network analyzer have to be adjust by every change of a host-based sensor or if the service was moved. This makes a standardized parameterization very attractive and economical for cloud environments. Based on the RoSI model the solution costs for an IDS will be decreased and it will be more economical to mitigate lower weighted risks with an IDS. The most economic way is to integrate new additional systems and services in an existing IDS management. All in all, the savings are significant and depend highly on existing environment, selected IDS and the complexity of the protected systems and services. One central supervising manager is already economically in small IDS environments. Based on the consistency check for the individual security policies, the amount of Analyzers is the major influencing dimension. Standardized IDS parameterizations fully deploy its economical and technical benefits in virtual and cloud environments.

References

[1] CERT / CC: CERT/CC Statistics 1988-2006, 2007, available online at http://www.cert.org/stats/ (last visit: 2007-06-13).

[2] J. Havrilla: Attack Sophistication vs. Intruder Technical Knowledge in Vulnerability Discovery: Bridging the Gap Between Analysis and Engineering, 2006, available online at http://www.pghrims.org/resources/policyholder/cert-2003-04-22-pghrisk.pdf (last visit: 2011 11 26).

[3] CERT/CC: Overview Incident and Vulnerability Trends, 27.11.2003, available online at http://www.pghrims.org/resources/policyholder/cert-2003-04-22-pghrisk.pdf (last visit: 2011 11 26).

[4] Bruce Schneier: Secrets & Lies, 2000

[5] A. Mizza: Return on Information Security Investment - Are you spending enough? Are you spending too much?, Jan 2005

[6] W. Sonnenreich, J. Albanese, B. Stout: Return On Security Investment (ROSI): A Practical Quantitative Model, available online at http://www.infosecwriters.com/text resources/pdf/ROSI-Practical Model.pdf, last visit 30.08.2012

[7] M. Boyle et al: Human Performance in Cybersecurity: A research Agenda, Proceeding of the Human Factors and Ergonomics Society Annual Meeting 2011, pp. 1115 - 1119, 2011

[8] ISO: Ergonomie der Mensch-System-Interaktion - Teil 110: Grundsätze der Dialoggestaltung (ISO 9241-110:2006); Deutsche Fassung EN ISO 9241-110:2006, Sept 2008

[9] H. Debar, D. Curry and B. Feinstein: The Intrusion Detection Message Exchange Format (IDMEF), 2007, RfC 4765, available online at http://www.ietf.org/rfc/rfc4765.txt, last visit 01. September 2007.

[10] B. Feinstein and G. Matthews: The Intrusion Detection Exchange Protocol (IDXP), 2007, RfC 4767, available online at http://www.ietf.org/rfc/rfc4767.txt, last visit 01. September 2007.

[11] M. Rose: The Blocks Extensible Exchange Protocol Core, Mar 2001, RfC 3080, available online at http://www.ietf.org/rfc/rfc3080.txt, last visit 01. September 2007.

[12] M. Wood, M. Erlinger: Intrusion Detection Message Exchange Requirements, March 2007, RfC 4766, available online at http://www.ietf.org/rfc/rfc4766.txt, last visit 01. September 2007.

[13] B.-C. Bösch: Ein einheitliches Austauschformat zum Parametrisieren verschiedener IDS, in UpTimes of German UNIX User Group Frühjahresfachgespräche 2012, pages 51 - 59, March 2012.

[14] B.-C. Bösch: Intrusion Detection Parameterization Exchange Data Model, 35th Jubilee International Convention on Information and Communication Technology, Electronics and Mircoelectronics 2012, May 2012.

[15] B.-C. Bösch: Intrusion Detection Parameterization Exchange Format, RfC-draft, 2012, work in progress.

[16] B.-C. Bösch: Standardized Parameterization of Intrusion Detection Systems, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), pp. 1 - 5, May 2012.

[17] B.-C. Bösch: Independent and Comprehensive Intrusion Detection Management, International Journal of Computer Science and Telecommunications (IJCST), pp. 1 - 6, Volume 3, Issue 7, July 2012.

[18] B.-C. Bösch: An Approach for Independent Intrusion Detection Management Systems, 7th Future Security Bonn, Sept. 2012

[19] B.-C. Bösch: Approach to Enhance the fficiency of Security Operation Centers to Heterogeneous IDS Landscapes, 7th International Workshop on Critical Information Infrastructures Security (CRITIS 2012) Lillehammer, Sept. 2012

[20] B.-C. Bösch: The Intrusion Detection Parameterization Exchange Format, unpublished

[21] German Federal ffice for Information Security: BSI - Leitfaden zur Einführung von Intrusion-Detection-Systemen, Oct 2002, available online at https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/ids02/index htm.html, last visit 26.08.2012

[22] SNORT: http://www.sort.org (last visit: 2011-12-03)

[23] Samhain: http://www.la-samhna.de/ (last visit: 2011-12-03)

[24] OSSec: http://www.ossec.net (last visit: 2011-12-03)

[25] Bro: http://www.bro-ids.org (last visit: 2011-12-03).