International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:7, No:8, 2013

Evaluation of State of the Art IDS Message Exchange Protocols

Robert Koch, Mario Golling and Gabi Dreo

Abstract— During the last couple of years, the degree of dependence on IT systems has reached a dimension nobody imagined to be possible 10 years ago. The increased usage of mobile devices (e.g., smart phones), wireless sensor networks and embedded devices (Internet of Things) are only some examples of the dependency of modern societies on cyber space. At the same time, the complexity of IT applications, e.g., because of the increasing use of cloud computing, is rising continuously. Along with this, the threats to IT security have increased both quantitatively and qualitatively, as recent examples like STUXNET or the supposed cyber attack on Illinois water system are proofing impressively. Once isolated control systems are nowadays often publicly available - a fact that has never been intended by the developers.

Threats to IT systems don't care about areas of responsibility. Especially with regard to Cyber Warfare, IT threats are no longer limited to company or industry boundaries, administrative jurisdictions or state boundaries. One of the important countermeasures is increased cooperation among the participants especially in the field of Cyber Defence. Besides political and legal challenges, there are technical ones as well. A better, at least partially automated exchange of information is essential to (i) enable sophisticated situational awareness and to (ii) counter the attacker in a coordinated way. Therefore, this publication performs an evaluation of state of the art Intrusion Detection Message Exchange protocols in order to guarantee a secure information exchange between different entities.

Keywords—Cyber Defence, Cyber Warfare, Intrusion Detection Information Exchange, Early Warning Systems, Joint Intrusion Detection, Cyber Conflict

I. Introduction

The idea of increased information exchange is not completely new. For instance Hill and Aguirre already observed the growing recognition that there would be high utility in integrating the output of different entities involved in network security, including routers, firewalls, proxies, as well as host-based and network-based Intrusion Detection Systems (IDS) [1]. Likely, they were thinking of heterogeneous entities, a mix of various vendors' products and government products and prototypes. In spite of several standardization efforts that would enable it, that level of integration has not occurred [2].

The President of the United States Barack Obama has clarified in 2009 that:

> It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country.

All authors are members of the Research Center CODE (Cyber Defence), Faculty of Computer Science, Universität der Bundeswehr München, D-85577 Neubiberg, Germany
E-mail: {robert.koch, mario.golling, gabi.dreo}@unibw.de

This fact is still valid today as Winterfeld et al. have identified [2]. Besides allowing a better intrusion detection, increased information exchange can also contribute to the following critical cyber challenges that are facing the U.S. (see Table I):

Sharing Information between internal departments is already subject to problems larger companies are facing. The reasons for this are various. Among others, due to the size of the organization (various locations) and the different cultures (languages / taxonomies), there are different communication flows. With regard to Cyber Warfare, sharing information posses a challenging task especially for the "information provider". While the organizations that receive the information may have a significant benefit, exposing a vulnerability, loosing reputation or limit liability may be great risks for those who provide the information and thus hamper the sharing of information [2]. Sharing of IDS data can be seen as the first step towards a more comprehensive approach of sharing information with regard to cyber security of an organization in general. If organization agree to share IDS logs, they may most likely also agree to share information on risk assessment, equipment, network structure and so on.

Situational Awareness, including Visualization, is the correlation and fusion of data from multiple sources that enables decision making. Situational awareness allows leaders to make informed decisions. There are many common operational pictures and dashboards today, but they fail to facilitate true risk posture understanding and to provide information in a format that enables decisions: Sharing of IDS-related messages can significantly contribute to a better situational awareness.

Systems Integration is the design to overcome the common practice of an organization purchasing multiple-point security systems (IDS, anti-virus, web protection) that do not work together, instead getting one system that coordinates and correlates protection activities. Each of these systems produces logs that need to be correlated together to provide a view of the overall system health and risk posture. Therefore, exchanging IDS logs between multiple vendors can also be seen as a step towards a better integration of independent systems.

Within the publication, the first part will give an overview of Intrusion Detection Systems in general, discussing the individual advantages and disadvantages of various approaches to Intrusion Detection. The next section will consider how the exchange of information between different IDS can have an essential impact on different stages of a Cyber Conflict. Even before an actual attack, an information exchange (in the sense of an early warning system) may significantly contribute to the creation of a common operational picture. In the main

TABLE I
EFFECTS OF INCREASED INFORMATION EXCHANGE *(bold)* ON CRITICAL CYBER CHALLENGES [2]

CYBER CHALLENGES	PSYCHOLOGICAL CHALLENGES	PROCESS CHALLENGES	TECHNICAL CHALLENGES
Deterrence	×		×
Policy and Legal Issues (Governance / International Agreements / Laws)	×	×	×
Sharing Information	×	×	×
Chain of Trust		×	×
Classification of Data	×	×	×
Cyber Rules of Engagement	×	×	×
Insider Threat	×	×	×
Lack of Common Definitions (taxonomy)		×	
Lack of Exercises that Test "Cyber Mission Assurance"		×	×
Metrics		×	×
Situational Awareness (including visualization)	×	×	×
Skill Shortage		×	
Stovepipes Between CNA / CND / CNE		×	×
Attribution	×	×	×
Auditing		×	×
Data Protection		×	×
Intrusion Detection			×
Resilence			×
Supply Chain	×	×	×
Systems Integration		×	×
Virtualization / Cloud Computing	×	×	×

phase (hot Cyber Warfare), the fast development of appropriate countermeasures - which need to be coordinated as well as enforced - comes into the main focus. Even in the period after the actual conflict, an information exchange is essential, since this phase is all about detecting the vulnerabilities that have been exploited (computer forensics) as well as identifying the attacker. Consequently, within the next section, a list of technical requirements to an exchange of information is derived. Afterwards, existing protocols on information exchange are presented. Therefore, an illustration of each protocol is given, emphasizing the Intrusion Detection Message Exchange Format (IDMEF) and its existing sub-protocols. In the last part of the publication, an evaluation is performed and the areas where more research is needed are depicted, before the conclusion is performed.

II. RELATED WORK

IDSs are used to identify attacks and unwanted behavior for about 30 years. According to the National Institute of Standards and Technology (NIST), an IDS is defined as follows: "An intrusion detection system is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents." [3]

A. Components of an Intrusion Detection System

An IDS consists of one or more of the following components [4] (see also Figure 1): Sensors, Analyzer and Manager.

A *Sensor* is the component that collects raw information from the data source and forwards detected occurrences (events) to the Analyzer. Common data sources include (but are not limited to) raw network packets, operating system audit logs, application audit logs, and system-generated checksum data.

The *Analyzer* evaluates data collected by Sensors for signs of unauthorized or undesired activity. If an event of interest has been detected, an alert is send to the Manager. Alerts typically contain information about the unusual activity that was detected, as well as the specifics of the occurrence.

Manager is a component or process from which the operator manages the IDS. Management functions typically include sensor configuration, analyzer configuration, event notification management, data consolidation and reporting.

Actions taken in response to an alert are summarized as *Response*. Responses may be undertaken automatically or initiated by a human. Sending a notification to the operator, which monitors the output of the IDS and initiates or recommends further action, is a very common response. Other responses include logging the activity; recording the raw data; terminating a network, user, or application session; or altering network or system access controls.

B. Detection Methods of Intrusion Detection Systems

Two main types of IDS are in use today: Knowledge-based and behavior-based systems. The first class of systems is using knowledge about negative events to identify unwanted activities. To gain acceptable results regarding false alarm rates, knowledge-based systems have to be configured strongly depending on the hosts and services of the network. However, a complete in-depth configuration of all systems is very time-consuming and the configuration has to be updated constantly. Small changes like an update can have a significant impact on the detection process. Therefore, the application of signature-based techniques in big network environments is often very difficult. Knowledge-based systems are reactive by nature and restricted to already known attacks. SNORT is a well-known example of a knowledge-based IDS [5].

The second class of systems is using models to describe the benign behavior of a network. The accurate modeling of network behavior is an active field of research. The difficulty

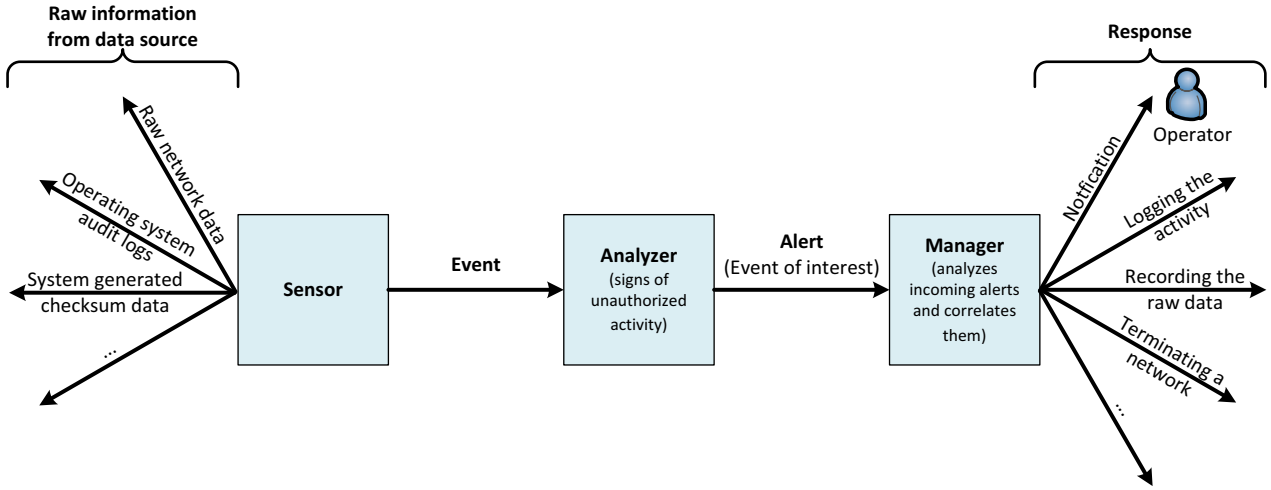

Fig. 1. Components of an Intrusion Detection System [4]

of behavior-based models is the possibility of misinterpretation of permittedm but unknown legal user actions, resulting in very high false alert rates.

C. Limitations of current Intrusion Detection Systems

Many different IDSs are available nowadays, both from commercial vendors as well as the open source community. All of these products have individual strengths and weaknesses (while for instance some IDS are aimed at detecting intrusions on the network, others are aimed at host operating systems, while still others are aimed at applications). Besides that fact, intrusions frequently involve multiple organizations as victims. Typically, those sites will use IDSs from different vendors. Thus, to enable a communication with the use of an common *Exchange Format* from one Analyzer to many Managers to help to correlate such distributed intrusions across multiple sites and administrative domains in a common format would facilitate the natural task of an IDS.

III. Scenario

Nations, as well as organizations, companies, (political) groups or individuals have different interests and priorities. This in general bears potential for tensions when own interests are followed and need to be pushed through against a competitor. With regard to nations, the evolving difference between the two competitors can range from dissents over tensions to searching for a solution with the use of forces; or in short the classical stages of a conflict. While this stages can be easily identified in conventional wars, the distinction between these stages is rather unprecise with regard to a cyber war, due to the nature of cyber threats and there effects. Because of the way the internet works, cyber attacks don't stop at the border of one nation. The high speed of the development of new malware and their diversity in combination with their polymorphic design to trick AV systems facilitates intrusions. In such cyber incidents, frequently multiple organizations are involved as victims (e.g. financial sites during ANONYMOUS *Operation Payback*, or multiple sites of the same target organization), which in turn makes cooperation necessary. Ideally, those sites have a solid security posture implemented, including an IDS. To counter threats, raw data must be put in context. Currently, this is mainly happening by examining raw data of a single source (*single IDS*). However, a much better result will be produced by correlating intrusion data of multiple sites and, if possible, even of administrative domains (especially in the *hot phase* of a cyber war). This will foster a better situational awareness of the cyber situation in the network and can be considered as a *operational level* (see Figure 2).

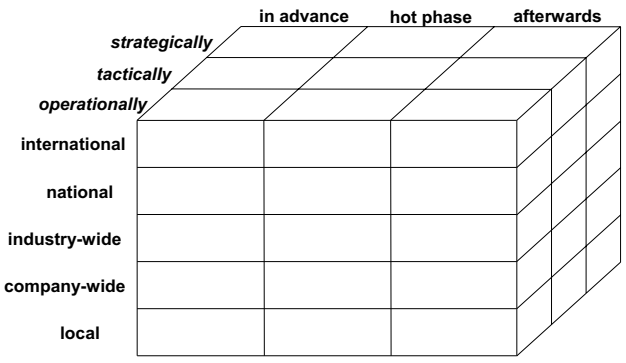

Fig. 2. Facets of an increased information exchange (Information Exchange Cube)

On a bigger scale, when we think of incidents that might arise to conflicts or even cyber wars, that operational situational awareness needs to be enriched with further information to generate a common operational picture (COP). On this *tactical level* we have left cyber security on company level and see cyber security primarily as an issue of national security as a governmental responsibility[1]. A combination of commercial and government information (including classified informa-

[1]Freedom to operate granted by the government, also if asset is owned by other entities

tion from intelligence sources) will provide a comprehensive view of the actual state of cyber security. A COP facilitates collaborative planning and assists all command echelons in achieving consistent situation awareness. Through the COP and thus the sharing of aggregated information, there is a great potential to improve the effectiveness in countering cyber threats throughout all stages of a conflict, especially when national or even international responses to cyber threats need to be coordinated to conduct concerted actions. Thus, already *in advance*, information exchange is essential for the whole CIS lifecycle (planning, design and procurement, implementation and accreditation, operation, enhancement, withdrawal) to improve the security (*strategical level*). Otherwise a once implemented security posture will become more and more outdated by time as it will not cover the recent threats (thus, information exchange *in advance* is of importance).

Due to organizational structures, funding and official cover, the most dangerous opponents are military and intelligence services, where the distinction between the two in some cases can't be done easily. Within the national and international treaties, the exchange of intrusion information is essential. With such a timely notification, the situational picture can be updated. This allows an actual check, whether the risk has changed and if so, the security posture needs to be modified.

Finally a distribution of the intrusion information will also allow limited forensic examination in case the attacked systems were destroyed (*afterwards*). Although, attribution is hard to achieve, knowing at least where an attack was originated allows to contact the country for internal investigations. Blaming a country for a single attack with limited evidence is risky. If there is an aggregation of attacks, the pressure on the need for internal investigation rises.

IV. Technical Requirements

Many requirements for data formats and exchange procedures for sharing information of interest to Intrusion Detection and Response Systems and to management systems, that may need to interact with them, have been defined, esp. in [6], [7] and [8]. Unfortunately, what has been written so far is not sufficient to cope with the scenarios shown in Section III in order to allow an efficient exchange of information between different IDS (as shown in Figure 3). Based on the scenarios presented, the following requirements can be derived:

1) Confidentiality, Integrity and Availability: Confidentiality, Integrity and Availability (CIA) are cornerstones for Information security. With regard to the exchange for IDS related data, the following requirements have already been identified and need to be applied [6], [7]:

- Reliable Message Transmission
- Interaction with Firewalls
- Mutual Authentication
- Message Confidentiality
- Message Integrity
- Per-source Authentication
- Denial of Service
- Degree of Confidence

2) Full Internationalization and Localization: As intrusion are becoming more and more decentralized, full internationalization and localization, that allows for sharing information between different time zones, is needed (time format). In addition, also time granularity and accuracy needs to be defined [6]. As different parts of an report may be written in a different natural language, the support of a multilingual use is also important [7].

3) Vendor Independance: As mentioned in RFC 4766 [6], exchange protocols have to be vendor independent. This implies the use of standardized exchange protocols and taxonomies with clear identifiers for the data detected, event information, analyzer location, alert identification etc.

4) Near Real-Time Capabilities: While the first three requirements have been identified by many resources, near real-time capabilities are widely neglected. But in order to react quickly on attacks, it is very essential that an correlation of data is available near real-time. Otherwise effective countermeasures are not possible.

5) Decision Support: Although situational awareness and the corresponding common operational picture are hard to archive, the complexity of the situation sometimes demands more support in order to make the right decision at the right time with the right information. So-called Decision Support Systems (DSS) are used to supports business or organizational decision-making activities intended to help decision makers compile useful information from a combination of raw data, documents, or personal knowledge to identify and solve problems and make decisions. DSS serves all three layers (operational, tactical and strategic layer) while preparing and planing of operations and helps to make decisions, which may be rapidly changing and not easily specified in advance.

Typical information, that decision support might present, are:

- Inventories of information assets including legal issues and correlated data from different sources (from all aspects of the information exchange cube)
- Comparative decisions from other cases
- Projected results of the decisions using knowledge based assumptions.

6) Human Interpretable Exploration of Relations: Particularly in data mining, the systematic application of methods, which are mostly statistical and mathematical, is used to identify a dataset with the aim of discovering previously unknown patterns. Data mining also deals with processing very large data sets (which could not be processed manually), for which efficient methods are needed. In essence, it is about extracting knowledge which is valid (in a statistical sense), previously unknown and potentially useful to determine certain regularities and hidden contexts. [9] defines it as a step in the knowledge discovery process to apply data analysis and discovery algorithms that provide a specific list of patterns (or models) of the data within acceptable performance limitations. This includes methods of classification, regression analysis, association analysis and cluster analysis. Unfortunatly, the results are sometimes not comprehensible. The results obtained by the machine must also be interpretable (explorative func-

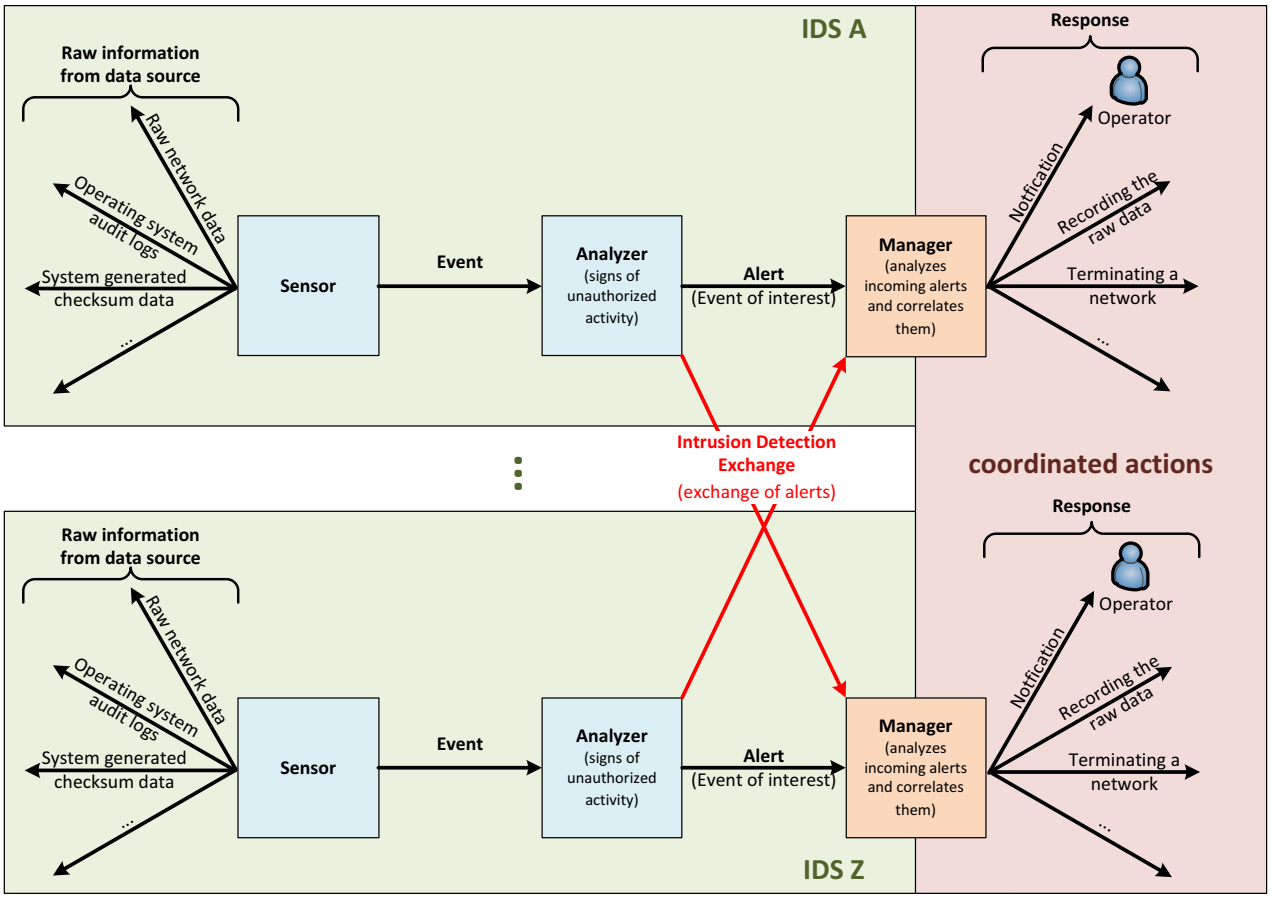

Fig. 3. Process of Information Exchange between IDSs

tion), so it get's clear WHY there is a relationship between the variables.

7) Scalability: Scalability describes the possibility of an approach to be deployable within a wide range of environments (from relatively small up to larger environments). In order to exchange informations in larger environments, information needs to be compressed in a compact way. One possibility in this regard would be the use of a hierarchical approach with clusters. In analogy to the Open Shortest Path First routing algorithm (OSPF) [10], for example, multiple domains can be formed. In OSPF, the overall majority of the routers exchange information only with others in their domain and only a few (so-called border routers) are used to mediate between two domains. This approach would also be adaptable to the exchange of IDS related information. Specific IDS of the particular domain would have to consolidate the knowledge of the domain and pass it to the parent domain in a compressed form.

8) Distributed Approach: Scalability is very much linked with an distributed approach. In order to avoid a single-point-of-error [11] no centralized IDS information exchange should be used. This is due to the fact that a centralized component could fail either intentionally or unintentionally, and as a consequence lead to an of blackout of the entire system.

9) Publish/Subscribe: Publish / subscribe describes a mechanism for observers to sign in and out in order to inform them about any changes. An object knows all its observers and reports any changes completely non-specifically to each registered observer. This requires no further knowledge about the object structure of the observers. In general, however, not all information about the state is exchanged - only the relevant parts of the information is passed on to the Observer, Subscribers have the ability to express their interest in an event, or a pattern of events, and are subsequently notified of any event, generated by a publisher, which matches their registered interest [12]. The strength of this event-based interaction style lies in the full decoupling in time, space, and synchronization between publishers and subscribers.

10) Need-to-know Principle: As a series of sensitive information is exchanged between IDS (data protection), the need-to-know principle should also be applied. It generally describes a security objective for handling secret information and denies a person to access the data if the information is not immediately required for the performance of the specific task of that person, even if that person - in principle - has access to such a data security level [13]. The need-to-know principle is one of the most fundamental security principles and limits the damage that can be done by a trusted insider. Failures

in implementing the need-to-know principle have contributed greatly to the damage caused by a number of recent espionage cases.

11) Resistance against False Data Injection: If an IDS is compromised by an attacker (as a consequence of an attack) or if the false positive rate is high (for instance due to the usage of an anomaly based system) false data is injected. Whether this is done intentionally or unintentionally, it has a huge impact on the correlation process. Thus, it might lead to wrong local decision making, and as a consequence an impact on the global decision making process is to be expected (domino effect). As a consequence, mechanisms for establishing trust and measuring the reliability of an IDS are needed.

V. Message Exchange

As already stated, exchanging information between multiple IDS can significantly contribute to a lot of tasks. As depicted in Figure 3, a communication flow from one Analyzer to many Managers is the aim of all IDS message exchange protocols, which in turn allows for a correlation of distributed intrusions across multiple sites and administrative domains. With regard to the exchange of IDS-related data, the syntax (exchange protocols) is clearly separated from the semantic (taxonomy). Consequently, the rest of this section is divided in those two corresponding subsections.

A. Exchange Protocols

This section deals with current data formats and exchange procedures for sharing information of interest to Intrusion Detection and Response Systems as well as Management systems.

1) Proprietary Protocols: For communications between IDS Analyzers and Managers, some (mainly older) systems use proprietary approaches. SAFEsuite decisions for instance uses SAFELink [14], an automated data collection and report distribution technology for multiple sources and destinations. Although this is somehow understandable, both from a historical point of view (because no standards for a common data exchange were available) as well as from a market perspective (since, for example a company doesn't want to give a competitor an insight into their own systems), we will not go further into details, because the idea of allowing an detailed exchange of information between systems from different vendors is not possible with proprietary protocols.

2) Simple Network Management Protocol (SNMP): The Simple Network Management Protocol [15] was designed to manage devices such as routers, switches, servers, workstations, printers or uninterruptible power supplies (UPS) from network management systems like HP Openview, OpenNMS or Nagios. Besides supervising devices, the protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. Therefore, the manager may send requests to agents, which are deployed on the managed device. With regard to the exchange of alerts, the more typical use of SNMP is the use of asynchronous notification from Agent/Analyzer to Manager. Some IDS use or can use Simple Network Management (SNMP) traps for sending data and/or communicating among components, for instance CyberWolf, Dragon Intrusion Detection System, ManHunt or SAFETNET [16]. SNMP provides the ability to exchange almost any kind of alert of suspicious activity or policy violation.

3) Common Intrusion Detection Framework (CIDF): The Common Intrusion Detection Framework (CIDF) was an attempt by the Defense Advanced Research Projects Agency (DARPA) during 1997-99 to develop an IDS interchange language, because no single IDS is able to recognize the full range of attacks [17]. CIDF was a research project and thus not designed for the commercial market. It contains of a high-level model, consisting of event generators, analyzers, databases, and responders and uses the Common Intrusion Specification Language (CISL) to communicate between the components. The syntax of the CISL with nested S-expressions and a fairly rich vocabulary in order to exchange messages on attacks is very similar to the multi-paradigm (functional, procedural) language LISP. The language includes nouns (subjects and objects) and verbs, such as "delete" or "open session". Although CISL is quite powerful, some authors found it to be to complicated, which in turn caused CISL/CIDF to be almost unrepresented in the market. However, CISL has had significant influences on the design of other efforts. Some ideas that were spawned from it, have experienced a rebirth in the Intrusion Detection Message Exchange Format (IDMEF).

4) Intrusion Detection Message Exchange Format (IDMEF): In order to "define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to management systems which may need to interact with them", the Internet Engineering Task Force (IETF) with its Intrusion Detection Exchange Format Working Group (IDWG), developed the *Intrusion Detection Message Exchange Format (IDMEF)*. As a "Lingua Franca" for Security Incident Management [18], IDMEF and its associated protocols enable a common language used to discuss intrusion detection events as a basis for cross-product event correlation. A lot of attention has been paid to the needs of IDS analysis, and to making the protocol work through firewalls in a straightforward way. Its message format is independent of the communication protocol.

IDMEF Communication Protocol (IDP) is the specification (not implementation) for the IDMEF communication protocol described in the same IDMEF requirement specification.There are two implementations to perform the physical transfer of intrusion detection information (see also Figure 4: the early one is called Intrusion Alert Protocol (IAP), The design of IAP was based on HTTP, which turned out to be unsuitable for several reasons and therefore did not make it to the RFC [19]. The newer and recommended one is *Intrusion Detection eXchange Protocol (IDXP)* [19].

IDXP in turn uses the *Blocks Extensible Exchange Protocol (BEEP)* [20] (which in turn uses TCP [21]). The Blocks Extensible Exchange Protocol (sometimes also abbreviated with BXXP) is a generic network protocol and as such not limited to be used by IDXP, but generally designed for asynchronous, connection-oriented applications and defined in RFC 3080. BEEP is centered around a frame mechanism, with

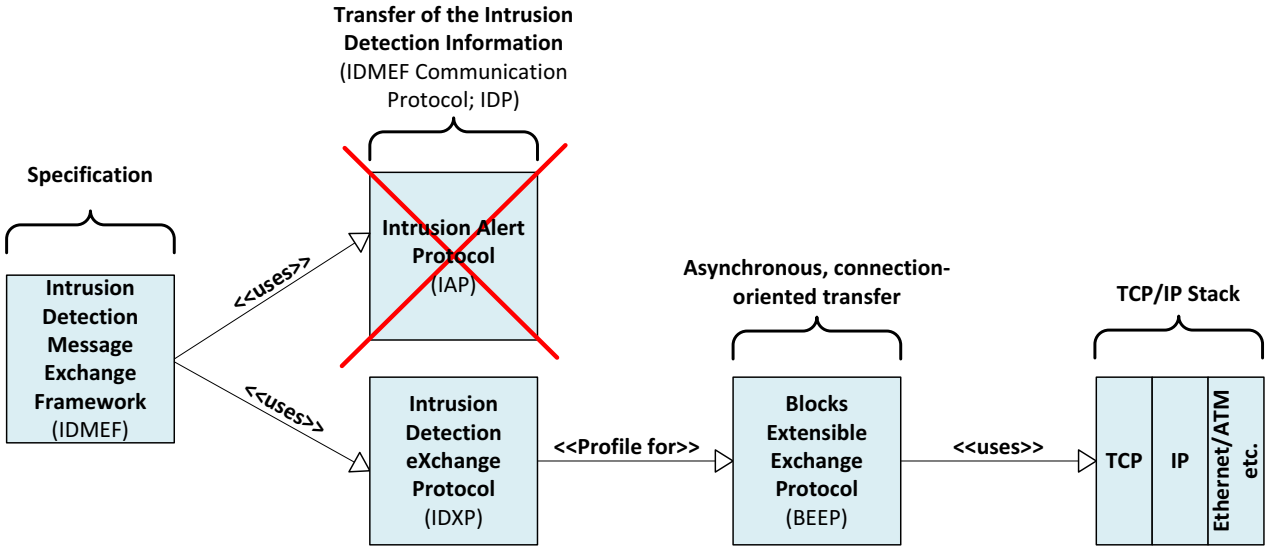

Fig. 4. Overview of the Intrusion Detection Message Exchange Format

can exchange independent messages between computers. The messages are using the Multipurpose Internet Mail Extensions (MIME) format. The exact definition of the message format is left to application developers (mostly text based, or - as in the case of IDXP: XML).

For BEEP, IDXP is a specification as well as a profile rather than a separate protocol. The IDXP profiles provide the parameters that will be used by BEEP during the setup and transfer of IDMEF data. In addition the RFC also specifies a possible encryption via the use of Transport Layer Security (TLS).

During session setup Analyzer and Manger exchange BEEP "greeting" messages [18]. The greeting identifies each entity as either an Analyzer or Manager. Data transfer takes place over full duplex stream oriented BEEP connections, which in turn use the underlying TCP protocol for reliable transfer of data. The BEEP security profiles provide the following additional capabilities [18]:

- Authentication of analyzer and manager
- Confidentially of messages
- Integrity of messages
- Protection from denial of service attacks
- Protection from message duplication

5) Incident Object Description and Exchange Format (IODEF): The Incident Object Description and Exchange Format (IODEF) effort was originally intended to define a data format as well as common exchange procedures for sharing information needed to handle an incident between different CSIRTs (Computer Security Incident Response Teams). The initial requirements and an initial draft of an XML implementation of a data model were developed [7]. The work for IODF has been stopped and taken over by the Format for Incident Report Exchange (FINE) effort sponsored by the Extended Incident Handling (INCH) working group within the IETF [18].

6) Format for Incident Report Exchange (FINE): The FINE effort has identified "Requirements for the format for incident information exchange (FINE)" [6] and will produce protocols for the exchange of incident information and statistics between managers in different organizations and management domains, between for example (i) a CSIRT and its users, (ii) CSIRT and law enforcement organizations and (iii) collaborating CSIRTS [18].

7) Intruder Detection and Isolation Protocol (IDIP): The Intruder Detection and Isolation Protocol (IDIP) is an infrastructure for integrating IDSs and automated response components [22]. Funded by DARPA, IDIP provides cooperation among intrusion detection systems, firewalls, routers, network management components, and hosts so that intrusions that cross multiple network boundaries can be automatically traced and blocked as close to the source as possible [19]. IDIP has been tested with a variety of IDSs, firewalls, and host-based responders. It provides a discovery coordinator API to allow components the access to services including data management, situation display, as well as access to network management and response policy management. IDIP uses CISL as the attack description language.

IDIP Systems are organized into communities. Each community is an administrative domain, with intrusion detection and response functions managed by a component called Discovery Coordinator. IDIP neighborhoods are collection of components with no other IDIP components between them. The emphasis in IDIP is on data management and secure communications between diverse components.

B. Taxonomies

A taxonomy or classification scheme is a unified method or model to classify attributes (possibly with the aid of a classification instrument) according to certain criteria into certain categories or classes. With regard to the processing of information, taxonomies need to have a mono-hierarchical

structure. Each attack vector is assigned to only one superclass, so that the overall classification maps a tree structure. Within this structure, elements related to the root contain more general information, whereas the stored knowledge is becoming increasingly specific the more the branches are growing. Through this type of classification of knowledge within hierarchical classes, a simple semantic (meaning) is created where individual attack vectors have a respective meaning.

Unfortunately, similar to Exchange Protocols, no single widely used common taxonomy is used. Different Exchange Protocols use different taxonomies to classify the attacks. However, depending on the particular taxonomy, it is possible to perform a limited mapping form one into another.

1) Vendor/User-Specific Taxonomies: Mainly due to historical reasons, firstly several vendor-specific taxonomies were created, which - usually in combination with a vendor-specific exchange protocol - have been used to enable the communication between multiple products of a single company (e.g., firewall, antivirus system and IDS) in order to exchange important information. Some of these vendor-specific taxonomies are kept secret while others became disclosed and are often used as a basis for further taxonomies.

2) Common Vulnerabilities and Exposures (CVE): Common Vulnerabilities and Exposures (CVE) is a dictionary for publicly known information security vulnerabilities, while the Common Configuration Enumeration (CCE) provides identifiers for security configuration issues and exposures [23]. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

CVE provides [19]:

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- A way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Free for public download and use
- Industry-endorsed via the CVE Editorial Board and CVE-Compatible Products

3) Bugtraq: Bugtraq is in its original meaning a mailing list, which is dedicated to computer security issues. It identifies weaknesses in computer programs, ways to use (so-called exploits) and approaches discussed in order to close these gaps. Bugtraq is a mailing list with a large number of contributions, because nearly all new vulnerabilities are addressed here. Bugtraq was created on the 5th of November 1993 by Scott Chasin in respond to the perceived inability of the existing security infrastructure on the Internet. It was Bugtraqs aim to publish vulnerabilities promptly and completely regardless of possible reactions of the affected software vendors. In July 1999, Bugtraq became property of SecurityFocus, which was in turn acquired by the U.S. software company Symantec on the 6th of August 2002. The Bugtraq vulnerability database is currently the Internet's premier source of vulnerability information [19]. Each vulnerability is assigned a unique "Bugtraq ID", so information about intrusions often contain a link to the equivalent Bugtraq ID.

4) Open Source Vulnerability Database (OSVDB): The Open Source Vulnerability Database (OSVDB) is an independent and open source database created by and for the community [19]. OSVDB was started in August 2002 at the Blackhat and DEFCON conferences and officially launched public on March 31, 2004. The goal is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities. It promotes greater, open collaboration between companies and individuals, eliminates redundant works, and reduces expenses inherent with the development and maintenance of in-house vulnerability databases [24].

5) Other examples of taxonomies: In addition to the taxonomies presented, there are of course many others that can't be listed here due to the brevity of this publication. Some of the more important ones are:

- US-CERT Vulnerability Notes Database: "The Vulnerability Notes Database provides timely information about software vulnerabilities. Vulnerability notes include summaries, technical details, remediation information, and lists of affected vendors. Many vulnerability notes are the result of private coordination and disclosure efforts." [25]

Numerous other databases provide actual security information, e.g.:

- Microsoft TechNet Security Bulletin [26]
- VUPEN Security Advisories [27]
- Secunia Advisories [28]
- SecurityTracker Vulnerabilities [29]

VI. Evaluation of IDS Message Exchange Protocols

In particular the Intrusion Detection Message Exchange Protocol and its correspondent sub-protocols have gained a high attention. With its 17 requirements (which - within this publication - are mainly subsumed under CIA, Full Internationalization/Localization and Vendor Independence) already far-reaching requirements have been identified. But as the scenario of Section III has already indicated, additional requirements have to be fulfilled before an sophisticated information exchange can be performed. For this purpose, this section and the corresponding Table II compares IDS Message Exchange Protocols with the requirements derived in Section IV. Since some of the IDS Message Exchange Protocols can use multiple taxonomies, for the sake of clarity, taxonomies are not considered within this section.

As depicted in Table II, none of the current approaches fulfills all requirements. Especially Decision Support, Human Interpretable Exploration of Relations, Scalability, Need-to-know principle and Resistance Against False Data Injection are not covered by existing protocols.

One of the bottlenecks of IDMEF that has not been mentioned so far is the usage of the eXtensilble Markup Language (XML). XML makes it easier to develop and deploy, but it comes with a performance cost. Due to the structure of XML, the data encoded is typically very large (for instance in comparison to JavaScript Object Notation; JSON), mainly because

TABLE II
OVERVIEW OF THE EVALUATION OF STATE OF THE ART IDS MESSAGE EXCHANGE PROTOCOLS

REQUIREMENTS	PROPRIETARY PROTOCOLS	SNMP	CIDF	IDMEF	IODEF	FINE	IDIP
Confidentiality, Integrity and Availability		+/-	+	+	+	+	+
Full Internationalization and Localization		+	+	+	+	+	+
Vendor Independence	-	+	+	+	+	+	+
Near Real-Time Capabilites		+/-	+/-	+/-	+/-	+/-	+/-
Decision Support		-	-	-	-	-	-
Human Interpretable Exploration of Relations		-	-	-	+/-	-	-
Scalability	-	-	-	-	-	-	+/-
Distributed Approach		-	-	-	-	-	+
Publish Subscribe		+	-	-	-	-	+/-
Need-to-know principle		-	-	-	+/-	-	-
Resistance Against False Data Injection		+/-	-	-	-	-	-

of XML's closing tags. Therefore parsing XML messages is still a relatively slow task today. Since the number of alerts received from IDSs is usually low, XML should work fine for the purpose [19]. However, firewalls, routers, and other network devices, are producing logs, which are hundred and thousand times higher than those of IDS. Thus, the XML dependency of IDMEF may become a bottleneck for extending IDMEF to network devices as well as for the usage of IDMEF in larger environments.

It also appears that the IDMEF data model fits very well with network IDSs, but it does not map well with non-IDS devices, such as, firewalls, NT Event Log, syslog, etc [19]. For that, a catch-all AdditionalData class was created to carry analyzer supplied information that does not fit into the data model.

Besides IDMEF, in particular the hierarchical approach of IDIP has to emphasized as a positive aspect.

VII. CONCLUSION

IDWG has successfully attracted participation of several industry leaders, such as, Cisco, NAI, HP, Boeing, IBM, ISS, MITRE, MSFT, Nokia, etc. It still remains to be seen whether IDMEF and IDXP will receive acceptance from commercial IDS vendors. Standards always take longer than expected for wide acceptance and IDWG is no exception. Once IDWG drafts become official RFC documents, we expect to see implementation from some of the IDS vendors, especially the ones who were involved with IDWG. The evolving correlation technologies will rely on such standards. Meta-IDS and enterprise security management vendors should adopt IDMEF early. IBM's Tivoli Risk Manager and ArcSight's Enterprise Security Manager are early adopters of IDMEF with demonstrated implementations. Another enterprise console vendor to announce support for IDMEF is eSecurity. Growth in deployment of Enterprise Security solutions in enterprises should also drive up the demand for such standards and interoperability. There are several tools and libraries available to help build IDMEF and IDXP applications. Most of them are accessible from Silicon Defense's IDWG Web page. Silicon Defense, a security research and consulting company, is actively involved with IDWG. It has also delivered a free open-source library and a plug-in to enable SNORT to output IDMEF XML alerts, which seems to be the most popular implementation available for IDMEF today. The lack of open standards for exchanging intrusion alerts and the lack of interoperability could potentially hamper the growth of IDS deployment and research. Although IDMEF and IDXP have not yet been blessed as standard, they are very close to becoming one and have already started to get traction for the research community, open source, and derivative standardization efforts. However, further work and success stories may be required to convince IDS vendors and wider intrusion detection communites of its usefulness. What HTML and HTTP did for Internet growth, IDMEF and IDXP can do with a likewise effect on research and deployment of intrusion detection technology. These are steps in the right direction and we must collaborate to take them further, being able to keep ahead of the hacker community again.

To date, most implementations of IDMEF are experimental. A few commercial efforts are being actively marketed. eSecurity stated that their agent technology uses a superset of the IDMEF standard (Sentinel is now part of NetIQ [30]). NetForensics (not reachable by BlackStratus [31]) indicated that they transport event information using XML over TCP but did not state that the IDMEF standard is being used.

A search of the Cisco web site retrieved no references to IDMEF. For NetIQ's [32] product "Vigilent Log Analyzer" (VLA), an Universal Agent is used to capture event information from devices for which a NetIQ agent is not available. Communications from the Universal Agent to the VLA server encodes the event information with IDMEF. The IDMEF/XML messages are transported over TCP but neither IDXP nor BEEP is used. An IDMEF plugin [33] has been developed for the well-known and widely used IDS SNORT [34]. This plug-in has been cited frequently in research studies. The documentation indicates that it is compatible with Snort 1.8.x. The original developer of SNORT founded SourceFire [35], a for profit company and has released a commercial version of SNORT 2.0. There is no mention of internal support for IDMEF at this time. The Prelude Project [36] is developing an open source hybrid network/host IDS and is using IDMEF. Although an IDMEF-like data model is used, the data is *not* transmitted in IDMEF format. They state that this is because of the overhead of XML – which is a common criticism. It is expected that as the standards settle, more implementations will appear. The growing need for centralized security event management will certainly foster this development.

REFERENCES

[1] S. Aguirre and W. Hill, "Intrusion detection fly-off: Implications for the united states navy," MITRE Technical Report MTR 97W096, Tech. Rep., 1997.
[2] S. Winterfeld and R. Rosenthal, "Understanding Today ' s Cyber Challenges," *Policy*, no. May, p. 28, 2011.
[3] "Guide to Intrusion Detection and Prevention Systems (IDPS)," 2007. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[4] M. Wood and M. Erlinger, "Intrusion Detection Message Exchange Requirements," RFC 4766, March, Tech. Rep., 2007. [Online]. Available: http://www.hjp.at/doc/rfc/rfc4766.html
[5] M. Roesch, "Snort-lightweight intrusion detection for networks," in *Proceedings of the 13th USENIX conference on System administration*. Seattle, Washington, 1999, pp. 229–238. [Online]. Available: http://www.usenix.org/event/lisa99/full_papers/roesch/roesch.pdf
[6] G. Keeni, R. Danyliw, and Y. Demchenko, "Requirements for the format for incident information exchange (fine)," *draft-ietf-inch-requirements-08. txt, IETF*, 2006.
[7] R. Danyliw, J. Meijer, and Y. Demchenko, "The incident object description exchange format," 2007.
[8] R. Holt, A. Winter, and A. Schurr, "Gxl: Toward a standard exchange format," in *Reverse Engineering, 2000. Proceedings. Seventh Working Conference on*. IEEE, 2000, pp. 162–171.
[9] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "From data mining to knowledge discovery in databases," *AI magazine*, vol. 17, no. 3, p. 37, 1996.
[10] J. Moy, "Ospf version 2," 1997, request for Comments: 2178.
[11] S. Zhuang, B. Zhao, A. Joseph, R. Katz, and J. Kubiatowicz, "Bayeux: An architecture for scalable and fault-tolerant wide-area data dissemination," in *Proceedings of the 11th international workshop on Network and operating systems support for digital audio and video*. ACM, 2001, pp. 11–20.
[12] P. Eugster, P. Felber, R. Guerraoui, and A. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys (CSUR)*, vol. 35, no. 2, pp. 114–131, 2003.
[13] P. Trommler, *The application profile model*. vdf Hochschulverlag AG, 2000.
[14] M. Surkan, "Safesuite spots net holes," *PC Week Netweek Dec*, vol. 16, 1996.
[15] J. Case, M. Fedor, M. Schoffstall, and C. Davin, *A simple network management protocol (SNMP)*. Network Information Center, SRI International, 1989.
[16] L. LaPadula, "State of the Art in CyberSecurity Monitoring - An Update," *Security*, no. September, p. 18, 2001. [Online]. Available: http://oai.dtic.mil/oai/oai?verb=getRecord\&metadataPrefix=html\&identifier=ADA458008
[17] S. Staniford-Chen, B. Tung, D. Schnackenberg *et al.*, "The common intrusion detection framework (cidf)," in *Proceedings of the information survivability workshop*, 1998.
[18] D. Corner, "Idmef-" lingua franca" for security incident management tutorial and review of standards development," *SANS Institute*, 2003.
[19] P. Kothari, "Intrusion detection interoperability and standardization," *SANS Institute*, 2002.
[20] M. Rose, "The blocks extensible exchange protocol core," 2001.
[21] M. Rose, "Mapping the beep core onto tcp," RFC 3081, March, Tech. Rep., 2001.
[22] D. Schnackenberg, K. Djahandari, and D. Sterne, "Infrastructure for intrusion detection and response," in *DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings*, vol. 2. IEEE, 2000, pp. 3–11.
[23] C. Vulnerabilities, "Exposures (cve), the mitre corporation," 2004.
[24] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *Security & Privacy, IEEE*, vol. 4, no. 6, pp. 85–89, 2006.
[25] "US-CERT Vulnerability Notes Database," 2013. [Online]. Available: http://www.kb.cert.org/vuls
[26] "Microsoft TechNet Security Bulletin," 2013. [Online]. Available: http://technet.microsoft.com/en-us/security/bulletin
[27] "VUPEN Security Advisories," 2013. [Online]. Available: http://www.vupen.com/english/security-advisories/
[28] "Secunia Advisories," 2013. [Online]. Available: http://secunia.com/advisories/
[29] "SecurityTracker," 2013. [Online]. Available: http://securitytracker.com/
[30] "NetIQ Sentinel," 2013. [Online]. Available: https://www.netiq.com/products/sentinel/
[31] "SIEM Solutions and Products," 2013. [Online]. Available: http://www.blackstratus.com/
[32] "NetIQ," 2013. [Online]. Available: https://www.netiq.com/
[33] "Snort IDMEF Plugin," 2013. [Online]. Available: http://sourceforge.net/projects/snort-idmef/
[34] "Snort :: Home Page," 2013. [Online]. Available: http://www.snort.org
[35] "Sourcefire Network Security Solutions," 2013. [Online]. Available: http://www.sourcefire.com
[36] "Prelude-IDS," 2013. [Online]. Available: https://www.prelude-ids.org

Robert Koch is a Research Assistant at the Universität der Bundeswehr München (UniBwM). He received his Diploma in Informatics in 2002 and his PhD in 2011 from the UniBwM. His main areas of research are network and system security with the focus on intrusion and extrusion detection in encrypted networks, security of COTS products, security visualization and the application of artifical intelligence. He has several years of experience in the operation of high security networks and systems.

Mario Golling is a PhD student at the Universität der Bundeswehr München (UniBwM), where he graduated in business informatics in 2007. His key aspects of research activity are network security, cyber defence, intrusion detection and next generation internet. He has many years of experience in running operational networks as well as teaching and training network administration/security. Among other things, he is a member of the Working Group IT Security of the UniBwM.

Gabi Dreo Rodosek holds the Chair of Communication Systems and Internet Services at the Universität der Bundeswehr München. She received her MSc. from the University of Maribora and her PhD from the Ludwig-Maximilians University Munich. She is spokesperson of the Research Center Cyber Defence (CODE), which combines skills and activities of various institutes at the university, external organizations and the IT security industry (for instance Cassidian, IABG or Giesecke & Devrient).