SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •
Special Focus

November 2013, Vol. 56 110103:1–110103:9
doi: 10.1007/s11432-013-5018-z

Data model extension for security event notification with dynamic risk assessment purpose

David LOPEZ[1,2], Oscar PASTOR[2] & Luis Javier GARCIA VILLALBA[1*]

[1]*Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA) School of Computer Science, Universidad Complutense, Madrid* 28040*, Spain*
[2]*Defence and Security Division, Systems Engineering for the Defence of Spain, S.A (ISDEFE), Madrid* 28040*, Spain*

Received July 7, 2013; accepted October 14, 2013

Abstract Dynamic risk assessment refers to a risk management framework where frequent updates of risk evaluation information are used to evaluate risk exposure, as close as possible to real-time. In this paper, we present the incident object description exchange format extended model for dynamic risk assessment. This format attempts to overcome the absence of integration and real-time communication between security systems and risk assessment tools. Our model is based on the incident object definition exchange format, which is commonly used in the computer security incident response teams community. This data model aims to facilitate a global vision of information systems risk by supplying real-time security events data to risk assessment tools based on renowned methodologies. We present a proof-of-concept scenario to demonstrate the usefulness of this integration and the proposed data model, and discuss the expected improvements.

Keywords dynamic risk assessment, risk management, DRA, IODEF-DRA, IODEF.

Citation López D, Pastor O, García Villalba L J. Data model extension for security event notification with dynamic risk assessment purpose. Sci China Inf Sci, 2013, 56: 110103(9), doi: 10.1007/s11432-013-5018-z

1 Introduction

Risk assessment (RA) and risk management (RM) are useful tools when applied to information systems (IS). They are used to assess risk exposure, drive management actions, and design an organizations risk mitigation plan for a given moment in time. Dynamic risk assessment (DRA) goes one step further, taking advantage of continuous risk exposure monitoring to allow a greater dynamism for real-time security decision making.

Previous analysis of DRA approaches applied to IS environments outlined how improvements can be made by integrating security systems with dynamic, or even real-time, risk assessment tools, while following renowned methodologies. The incident object description exchange format (IODEF) extended model for dynamic risk assessment (IODEF-DRA) that we propose in Section 2 is an attempt at this integration. The proposed data format is an evolution of the IODEF data model.

We present a detailed proof-of-concept, which aims to demonstrate the usefulness of the integration of security systems and DRA tools using the IODEF-DRA model. In the appendix, we suggest an XML prototype for the messages required in our model.

*Corresponding author (email: javiergv@fdi.ucm.es)

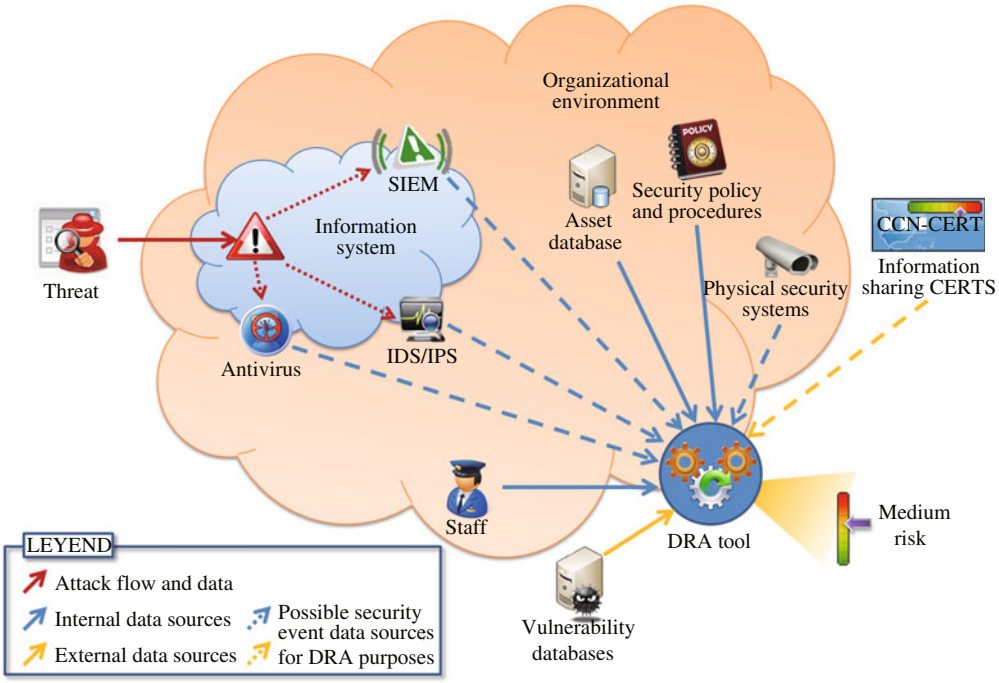

Figure 1 Dynamic Risk Assessment with integrated security systems using a real-time DRA tool.

Related works. A previous DRA state-of-the-art analysis summarized the different approaches applied to DRA [1]. Attention was drawn to the risk assessment features of systems that rely on real-time event monitoring (such as an intrusion detection system (IDS) or intrusion prevention system (IPS)) that have a narrow understanding of the IS and its global environment. Conversely, tools that implement methodological RA capture a higher level of information of the IS domain, which allows decision-making in alignment with organizational objectives and security policies. Finally, risk evaluation should take advantage of a greater quantity of sources [2], and profit from incident, threat and vulnerability knowledgebase sharing [3].

The integration of security tools (including physical tools that protect the IS's assets) and other information sources with methodological and dynamic RA tools may, therefore, result in more accurate risk management decisions. This integration requires RA tools to have continuous access to information about the IS's security status, as depicted in Figure 1. These inputs, adequately pre-screened to avoid an overload of the RA tool, shall be notified by security tools using communication interfaces and appropriate data models.

Standardization bodies, such as the internet engineering task force (IETF), have researched the development of standard information flows related to security incidents through the extended incident handling working group (INCH WG). They first proposed the experimental protocol known as intrusion detection message exchange format (IDMEF) [4], which focused exclusively on intrusion event information issued by an IDS. Several IDS providers adopted this format, but it was not suitable for a more complex environment [5].

Next, the incident object definition exchange format [6] was developed. Because it is an extension of IDMEF, the two are compatible. As shown in Figure 2 [7], IODEF comprises a root class "document" with a child node "incident", and a hierarchical structure of nodes called classes. For each notified incident, an instance of this document hierarchy is completed (typically by the CERT who circulates it) with information about the incident. Some of the classes are mandatory and must be included in the created instance, while others are optional. An IODEF document has its own lifecycle and information is added as the incident, or the tasks focused on its analysis, progress.

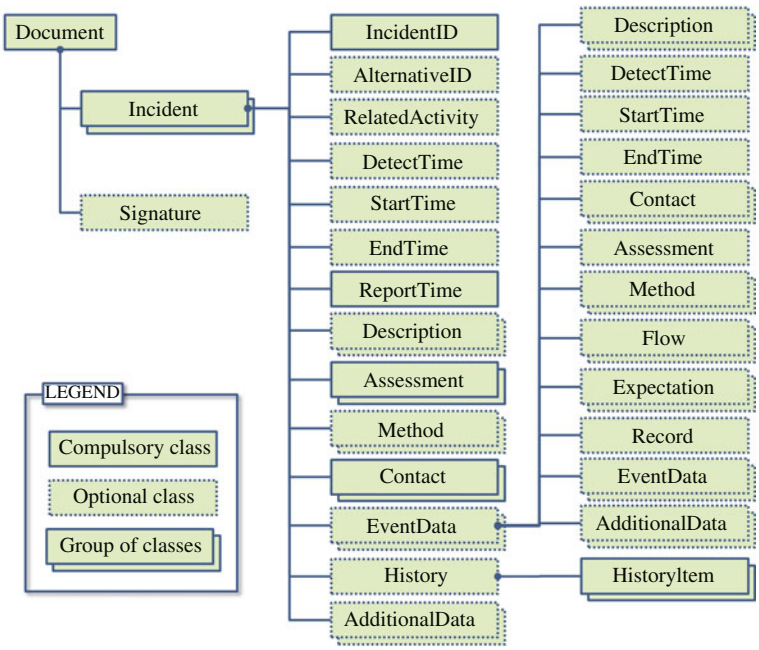

Figure 2 IODEF data model (IODEF INCH final version).

IODEF was conceived to help CERTs exchange information about incidents (in a broader sense than IDMEF), which could be automatically processed (although they were oriented to human use). Ad hoc applications using these models are implemented in CERT environments. These efforts have raised the maturity level of the IODEF model close to a standard for IS security incidents. This work is used as the base for our proposed extension. In addition, new extensions that rely on the IODEF data model are currently being developed to cover specific types of incidents [8].

2 Integrating security systems and dynamic risk assessment tools through an extended data model (IODEF-DRA)

2.1 Data model extension proposal (IODEF-DRA)

This IODEF extension is designed to be used for automated communication between security systems that are able to notify security events or incidents affecting an IS, and the deployed organization's RA tool, which is expected to be based on a methodological approach. Note that security systems protecting an IS could also be physical, such as a physical intrusion detection system.

The proposed IODEF for dynamic risk assessment extension embeds the compulsory classes defined by IODEF (a much-reduced set of the total classes) and adds a few additional classes. The remainder of non-compulsory IODEF classes is not required, except for the Assessment and EventData classes that are essential for IODEF-DRA. Interfaces adhering to IODEF-DRA should add data to the compulsory IODEF, IODEF-DRA (under the AdditionalData class), and IODEF Assessment classes (impact and confidence). According to the ISO [9], a security incident is defined as an event, or a series of events, threatening an IS with a high probability of compromising an organization's goals. The IODEF also has this structure if the events are clustered into an incident. Figure 3 depicts our proposed extension to the format.

The following classes are used to provide information for an event. They model factors that have an impact on risk evaluation, according to the RA methodologies previously analyzed.

• **AffectedAsset**. A new class, under the event AdditionalData, to identify the asset that is affected by the notified event. The identifier may be shared between the security system and the RA tool.

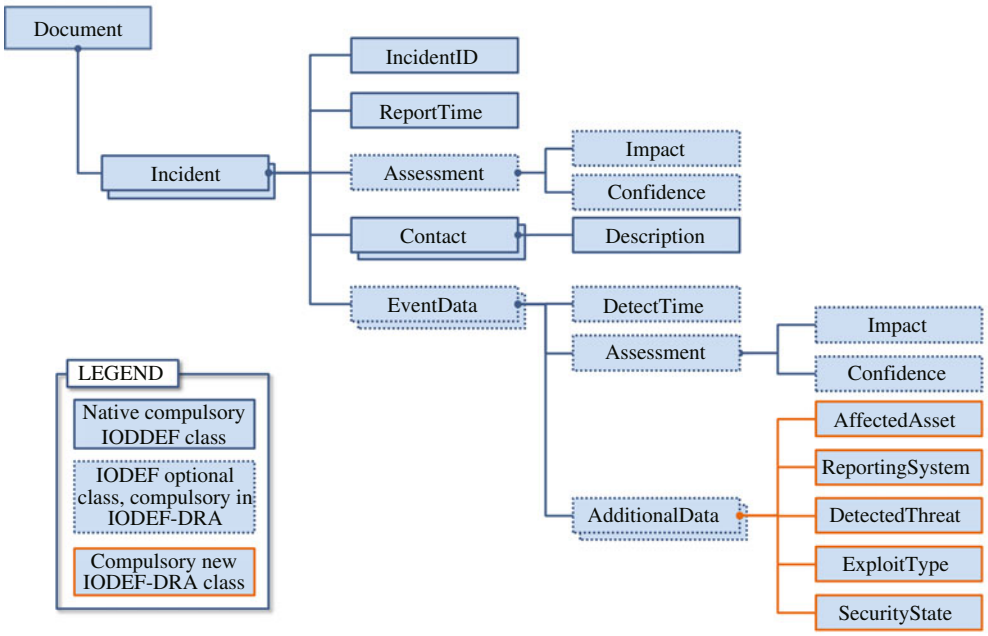

Figure 3 Extended IODEF data model for Dynamic Risk Assessment purposes (IODEF-DRA). Only IODEF classes relevant for this extension are shown.

• **DetectedThreat**. A new class, under the event AdditionalData, to identify the threat that triggered the monitored event, if a cause-effect relationship can be established. The identifier may be shared, or threat libraries can be used.

• **ExploitType**. A new class, under the event AdditionalData, to capture information about the exploited vulnerability. Several standard formats could be used when identifying exploits that affect the IS's components.

• **SecurityState**. A new class, under the event AdditionalData, to define the security system state. It notifies if the threat has been defeated or surpassed, or if a reaction is still possible.

• **ReportingSystem**. A new class, under the event AdditionalData, that comprises the identifier and the type of security system that notified the event. Many types of systems are possible, and include an IDS, a physical security system, or an informant CERT for generic incidents.

• **Assessment**. An optional IODEF native class that is compulsory under the Incident and Event classes. It gathers information about the initial assessment of the security system. It comprises the Impact and Confidence classes.

• **Impact**. An IODEF native class that is linked to the Assessment class, and is compulsory in this extension. It contains information about the severity and progress of the attack, from the point of view of a security system.

• **Confidence**. Similarly to Impact, this is compulsory in this extension. It lets the security system assign its own confidence level about the trustworthiness of the event data. It can also be used to notify whether the system is able to fully discard a false positive or not.

• **DetectTime**. A native IODEF class under EventData, which captures the time of detection in a unified and standardized format.

Because a security incident is a top hierarchy IODEF class, it may comprise several events or just one. Along with the Assessment class, it contains:

• **IncidentID**. A native IODEF class that uniquely identifies an incident.

• **ReportTime**. A native IODEF class that contains the reporting time in a unified and standardized format.

• **Contact**. A native IODEF class that contains contact details for the security system's administrator.

• **EventData**. A native IODEF class that was optional, but becomes compulsory in IODEF-DRA. An incident might include one or a list of EventData classes, each one containing its own information.

2.2 Required features for IODEF-DRA compliant tools

Additional features may be required by security systems to effectively implement the IODEF-DRA:

• Identification of the asset(s) under protection, or being affected in case of a security event. IDs must be shared with the RA tool.

• Issue notifications in response to a security event, dependent on a confidence threshold so that false positives are discarded.

• A notification message according to the proposed format (IODEF-DRA).

• Where possible, establish a secure communication channel with the RA tool.

On the other side, a methodological RA tool using the IODEF-DRA model should have the following functionalities:

• Assignment of unique asset IDs that are compatible with the model specification.

• Receive notification messages in real-time (when configured in push mode), or continuously check a repository for messages (pull mode).

• Import data according to the IODEF-DRA specification.

• Validate the input data and match the IDs with known assets, threats or vulnerabilities.

• Use updated data to reassess risks.

• Display the new risk assessment outcome, taking into account the confidence level issued by the security system.

• Ideally, verify the authenticity and integrity of notifications to avoid mistaken assessments.

3 Dynamic risk assessment with the IODEF-DRA extension: proof-of-concept

If we consider a RA over a simple IS with a reduced group of assets that include staff, remote IS premises, hardware and data, it is possible to generate an example attack tree (Figure 4). The tree shows the initial risk exposure for each node, dependent on the probability of a threat exploiting a vulnerability. A methodological RA may provide risk exposure taking into account organizational, technical and human factors. This scenario is typical when applying attack trees to RA. We use it to statically choose the best strategy and focus security resources on critical nodes.

In this example, a disgruntled employee can harm the organization in two ways. The employee may scan the network and launch an attack against a central data server. Alternatively, they may break into a remote unattended premises to destroy IS equipment, or to launch an attack through a remote server. The organization is most concerned with leaks of information, and the most plausible route for this is by a remote code execution through an unauthorized connection to a server and a later privilege escalation. In this scenario, the main advantages of integrating the security system and DRA tool (RA methodological tool adhering to IODEF-DRA) are:

• A DRA tool based on a methodological approach may know whether data stored on a server is to be considered critical; a security system administrator may not.

• An IS security system administrator does not typically have any information about the physical compromise of a remote premise, whereas a DRA tool could establish a relationship between a physical intrusion in a remote premise and a subsequent chain of events leading to a critical information leakage;

• The DRA tool may be aware of authentication measures or procedures in FTP connections from remote premises, and the data flow between them.

• The organization's environment enables communication between security systems (both physical and logical ones protecting the IS) and the embraced DRA tool, as shown in Figure 1. The DRA tool interacts with these systems receiving their notifications. The chain of events and interactions with the DRA tool are as follows:

1) A physical intrusion detection system notices an intruder in a remote IS unattended premise. It is hard to get a quick reaction from security staff because it is a remote premise. An intrusion system console notifies the DRA tool using an IODEF-DRA message (Appendix Message A).

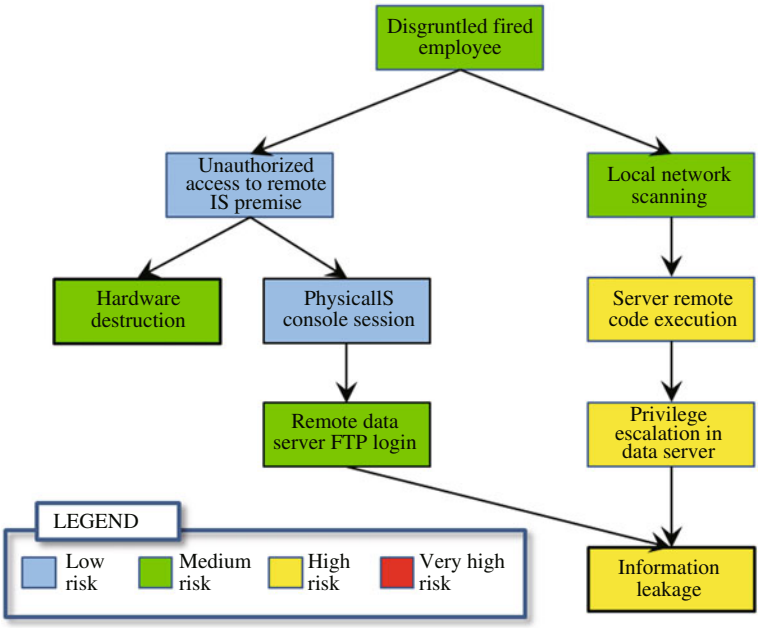

Figure 4 Attack tree example for the IODEF-DRA process. Risk outcomes may follow several approaches [10], but this is not the focus of this work, so we have simplified the process. A color code shows the baseline risk exposure level of each node, after an initial RA.

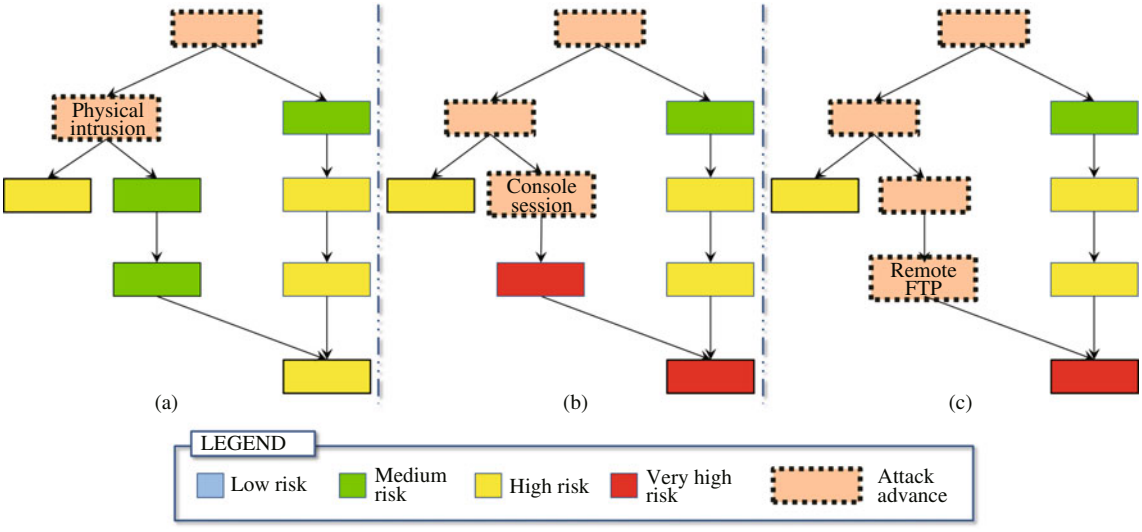

Figure 5 Dynamic Risk Assessment step-by-step progress (real-time integration of security systems and the DRA tool).

2) The DRA tool receives the message and reassesses the risk, evaluating new risk values for nodes that are exposed to the new IS environmental factors (Figure 5(a)).

3) After several failed login attempts, the intruder successfully connects to a system using the local console. Thus, a HIDS (host-based IDS) reacts, notifying the DRA tool about the "failed logins" security event, using a customized IODEF-DRA message (Appendix Message B).

4) The DRA tool processes this message and reassesses the risk exposure of the nodes (Figure 5(b)). In this context, the DRA tool judges that the attacker can easily gain access to the "Information leakage" node, because it is aware that ftp connections launched from remote units are never blocked, due to business requirements stated in the security policy. Consequently, the risk exposure rises to a higher level.

5) The attacker's next step is to launch a remote FTP login against the central data server. This time, a NIDS (network IDS) detects the ftp connection, because it does not follow custom communication protocols. It notifies the DRA tool with a new message (Appendix Message C).

6) In this case, the confidence that the FTP connection is a security event is lower, because it could be caused by a justified operational exception. Nevertheless, the DRA tool may be aware of the previous chain of events, and will undoubtedly use this information to support that the risk of information leakage is very high (Figure 5(c)).

7) The attacker may be now connected to the central data server and may have gained access to critical data.

If no further notice was taken of this event, data may be stolen through the ftp connection until someone arrives at the remote premise to check the physical intrusion. However, real-time monitoring of the risk using the DRA tool would have helped to make worthwhile decisions, such as closing ftp connections between the IS on the remote premise and the central data server. This may have caused negative effects to the business, but it would have been justified if the DRA tool assessed that there was an appropriately high risk of information leakage.

4 Conclusion and future work

There are several approaches that try to solve the challenges in DRA and dynamic risk management for ISs. They tend to focus on a specific dilemma at the detriment of other possible issues, although some techniques attempt a more holistic approach. Ideally, we should take into account all changes to the IS and its environment when reassessing risk.

The proposed IODEF-DRA data model attempts to fill one of the gaps in the existing DRA. It aims to integrate security systems that protect the IS throughout the organization, with RA tools that are based on sound methodological RA principles. Notifications of security events in the IS and its environment may be dynamically processed by the RA tool in real-time. Effective communication between an organization's security systems using the proposed model (or reliable external sources of information about security events), and DRA tools may bring about the following advantages:

1) An ability to update an RA process in real-time, enabling continuous risk monitoring. It may allow an instant awareness when a serious risk affects business goals, and reduce delays to reactions.

2) The enforcement of a methodological RA may be useful to both management and technical staff. It drives a homogeneous vision of risk throughout the organization that leads to an incident response better aligned with security policies.

3) The opportunity to take account assets, security components and policies, or other organizational factors beyond the IS architecture. By integrating the security systems and the methodological RA, the monitored domain is expanded to the IS and its environment.

This proof-of-concept scenario demonstrates how the proposed integration using IODEF-DRA can lead to the above advantages. First, it monitored and detected a rise in risk, taking into account the impact of a compromised asset on business goals. This led to a unified vision of risk, from both management and technical points of view, resulting in better decision making. Finally, it integrated the physical security systems protecting the IS environments, and took into account security policy factors to assess risk in real-time.

Future work will focus on the evolution of DRA tools that input data into IS environments, which might improve the quality and trustworthiness of risk assessments. We will focus on two objectives: first, the in-depth development of the IODEF-DRA model and its promotion, and second, the definition of other data feeding sources to allow much more diversity, which may improve the completeness of DRA.

References

1 López D, Pastor O, García Villalba L J. Dynamic risk assessment in information systems: State-of-the-art. In: Proceedings of the 6th International Conference on Information Technology, Amman, 2013. 8–10

2 European Network and Information Security Agency(ENISA). Standard II. http://www.enisa.europa.eu/activities/cert/background/inv/cert-activities/standardisation/standard-ii
3 Fernández D, Pastor O, Brown S, et al. Conceptual framework for cyber defense information sharing within trust relationships. In: Proceedings of the Fourth International Conference on Cyber Conflict(CYCON), Tallinn, 2012. 1–17
4 Internet Engineering Task Force (IETF). Intrusion Detection Message Exchange Format, 2007. http://datatracker.ietf.org/wg/idwg
5 Gorzelak K, Grudziecki T, Jacewicz P, et al. Proactive Detection of Network Security Incidents. European Network and Information Security Agency(ENISA) Report Deliverable, 2011. 114–116
6 Internet Engineering Task Force. The Incident Object Description and Exchange Format(IODEF), IETF Standards Track RFC5070. 2007. http://datatracker.ietf.org/wg/inch
7 TERENA–IODEF Working Group. Incident Object Data Model v.0.05 Final, 2002. http://www.terena.nl/tech/task-forces/tf-csirt/iodef/docs/iodef-datamodel-draft-003.html
8 IODEF Working Group. IODEF-Extension for Structured Cybersecurity Information(draft), TERENA Standards Track, 2013. http://tools.ietf.org/html/draft-ietf-mile-sci-07.html
9 BSI. Information Technology. Security Techniques. Information Security Incident Management. ISO/IEC 27035. 2011
10 Poolsappasit N, Dewri R, Ray I. Dynamic Security Risk Management Using Bayesian Attack Graphs. IEEE Trans Dependable Secur Comput, 2012, 9: 61–74

Appendix: IODEF-DRA messages example on XML format

Message A

⟨?xml version="1.0" encoding="UTF-8"?⟩
⟨Incident purpose="reporting"⟩
⟨IncidentID name="physicalAlert"⟩00001⟨/IncidentID⟩
⟨ReportTime⟩2012-03-10T20:13:05+00:00⟨/ReportTime⟩
⟨Assessment⟩
⟨Impact severity="medium" completion="succeeded"/⟩
⟨Confidence rating="high"/⟩
⟨/Assessment⟩
⟨Contact role="admin" type="person"⟩
⟨Description⟩Security Staff on site⟨/Description⟩
⟨/Contact⟩
⟨EventData⟩
⟨DetectTime⟩2012-03-10T20:13:02+00:00⟨/DetectTime⟩
⟨Assessment⟩
⟨Impact severity="medium" completion="succeeded"/⟩
⟨Confidence rating="high"/⟩
⟨/Assessment⟩
⟨AdditionalData⟩
⟨AffectedAsset type="site" assetID="remote-site"/⟩
⟨ReportingSystem type="physicalSecurityConsole" systemID="console01"/⟩
⟨DetectedThreat type="unauthorized access" threatID="Breakin"/⟩
⟨ExploitType vulnerabilityID="unknown"/⟩
⟨SecurityState state="supervised"/⟩
⟨/AdditionalData⟩
⟨/EventData⟩
⟨/Incident⟩
⟨/IODEF-Document⟩

Message B

⟨?xml version="1.0" encoding="UTF-8"?⟩
⟨Incident purpose="reporting"⟩
⟨IncidentID name="HostIDSAlert"⟩00015⟨/IncidentID⟩
⟨ReportTime⟩2012-03-10T20:18:33+00:00⟨/ReportTime⟩
⟨Assessment⟩
⟨Impact severity="low" completion="succeeded"/⟩

⟨Confidence rating=“high”/⟩
⟨/Assessment⟩
⟨Contact role=“admin” type=“person”⟩
⟨Description⟩Network administrator⟨/Description⟩
⟨/Contact⟩
⟨EventData⟩
⟨DetectTime⟩2012-03-10T20:18:25+00:00⟨/DetectTime⟩
⟨Assessment⟩
⟨Impact severity=“low” completion=“succeeded”/⟩
⟨Confidence rating=“high”/⟩
⟨/Assessment⟩
⟨AdditionalData⟩
⟨AffectedAsset type=“host” assetID=“Remoteserver”/⟩
⟨ReportingSystem type=“HIDS” systemID=“HIDS08”/⟩
⟨DetectedThreat type=“Local console login failure” threatID=“FailedLoginAttempts”/⟩
⟨ExploitType vulnerabilityID=“unknown”/⟩
⟨SecurityState state=“supervised”/⟩
⟨/AdditionalData⟩
⟨/EventData⟩
⟨/Incident⟩
⟨/IODEF-Document⟩

Message C

⟨?xml version=“1.0” encoding=“UTF-8”?⟩
⟨Incident purpose=“reporting”⟩
⟨IncidentID name=“NetworkIDSAlert”⟩00059⟨/IncidentID⟩
⟨ReportTime⟩2012-03-10T20:21:18+00:00⟨/ReportTime⟩
⟨Assessment⟩
⟨Impact severity=“low” completion=“succeeded”/⟩
⟨Confidence rating=“medium”/⟩
⟨/Assessment⟩
⟨Contact role=“admin” type=“person”⟩
⟨Description⟩Network administrator⟨/Description⟩
⟨/Contact⟩
⟨EventData⟩
⟨DetectTime⟩2012-03-10T20:21:13+00:00⟨/DetectTime⟩
⟨Assessment⟩
⟨Impact severity=“low” completion=“succeeded”/⟩
⟨Confidence rating=“medium”/⟩
⟨/Assessment⟩
⟨AdditionalData⟩
⟨AffectedAsset type=“host” assetID=“Fileserver”/⟩
⟨ReportingSystem type=“NIDS” systemID=“NIDS01”/⟩
⟨DetectedThreat type=“Remote FTP connexion” threatID=“RemoteFTP”/⟩
⟨ExploitType vulnerabilityID=“unknown”/⟩
⟨SecurityState state=“supervised”/⟩
⟨/AdditionalData⟩
⟨/EventData⟩
⟨/Incident⟩
⟨/IODEF-Document⟩