On Proposing a Model for Low-Interaction Honeypots Data Exchange

Cristine Hoepers[1,3], Antonio Montes[2,3], Nandamudi L. Vijaykumar[3]

[1]Computer Emergency Response Team Brazil – CERT.br
Brazilian Internet Steering Committee – CGI.br
[2]Renato Archer Research Center – CenPRA
Ministry of Science and Technology – MCT
[3]Computing and Applied Mathematics Laboratory – LAC
Brazilian National Institute for Space Research – INPE

cristine@cert.br, antonio.montes@cenpra.gov.br, vijay@lac.inpe.br

Keywords: honeypots, security incidents, data exchange.

In the past few years the number of computer security incidents on Internet connected networks has continuously increased (Computer Emergency Response Team Brazil (CERT.br) n.d., CERT Coordination Center n.d.). As a result, there is an increasing need of coordination and information exchange among different Computer Security Incident Response Teams (CSIRTs), as well as a growing need of automation and new data sources that could be used to identify attacks' trends.

The deployment of sensors in computer networks to gather malicious traffic is one of the methods used by CSIRTs and other security organizations to collect data for attack's trend analysis. One type of sensor that is being used lately is the honeypot, a security resource whose value lies in being probed, attacked, or compromised (Spitzner 2002).

Improved honeypots' information exchange would allow the correlation of attacks being conducted in different parts of the Internet, as well as a better understanding of those attacks. Although information exchange is a topic that has been investigated by the research group members of the The Honeynet Research Alliance (The Honeynet Project n.d.), there isn't any ongoing effort to create a standard format for honeypot's data exchange.

To allow the information to be shared easily, and to increase the automation, it is necessary to have a standard format to represent incident related data. Discussions about the advantages of a standard format for the exchange of information about incidents are being promoted by the Incident Handling community. The results of these discussions are being consolidated by the Internet Engineering Task Force (IETF) Extended Incident Handling Working Group (INCH). INCH is working in the proposal of a new Internet Standard, the Incident Object Description and Exchange Format (IODEF), that defines a data representation that provides a framework for sharing computer security incidents information commonly exchanged among CSIRTs (R. Danyliw, J. Meijer & Y. Demchenko 2006).

The IODEF definition started as one of the activities of the CSIRT's Task Force (TF-CSIRT) of TERENA (Trans-European Research and Education Networking Association). The initial development gave origin to the document "RFC 3067: TERENA's Incident Object Description and Exchange Format Requirements" (Arvidsson, Cormack, Demchenko & Meijer 2001), of February 2001. This document described for the first time the basic requirements for the definition of a format for incident data exchange.

The IODEF model represents incident related data in a structured way, giving to these data appropriate semantics, which allow a quick location of relevant information to handle an incident. This model is equally efficient to represent a subset of honeypots' related data. But, information like IP addresses being used by a honeypot, open ports, applied filtering mechanisms, emulated services and operating systems, among others, are not covered by the IODEF model.

To address this issue, an extension to the IODEF model and its utilization to represent data collected in honeypots is proposed in this work. This proposal is made taking into consideration that INCH is already working on a standard format for incident data exchange and that honeypots' data, by their malicious characteristics, are very similar to incident related data. A motivating fact for the use of IODEF is that this would allow the data collected not only to be correlated with data from other honeypots, but also with data related to incidents being reported to CSIRTs. In addition, tools developed to work with IODEF could be easily changed to work with honeypots' data.

The IODEF extension proposed in this work follows the requirements for extensions as defined by the IODEF Internet-Draft. We extended the model through aggregation, proposing the representation of honeypot-specific data at a new class, aggregated to one of the IODEF classes, as recommended in the IODEF Draft. With this choice, we achieved a satisfactory level of independence from the IODEF model. This is very important, because IODEF is still in its draft phase and, if it undergoes further changes, this will not affect the aggregated classes of this extension.

Our proposed extension also allows us to represent the data related to the attacks seen in the honeypots solely with the IODEF original model. This will facilitate the correlation of incident reports with honeypots' data. Other important feature is that attacks seen in honeypots can be used to generate incident reports in IODEF format, to be sent to the CSIRTs associated to the networks that originated the attacks.

References

Arvidsson, J., Cormack, A., Demchenko, Y. & Meijer, J. (2001), 'RFC 3067: TERENA's Incident Object Description and Exchange Format Requirements', http://www.ietf.org/rfc/rfc3067.txt.

CERT Coordination Center (n.d.), 'CERT/CC Statistics 1988-2006', http://www.cert.org/stats/cert_stats.html.

Computer Emergency Response Team Brazil (CERT.br) (n.d.), 'Incidents Reported to CERT.br', http://www.cert.br/stats/incidentes/.

R. Danyliw, J. Meijer & Y. Demchenko (2006), 'The Incident Object Description Exchange Format', http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-10.txt. Expires on March 20, 2007.

Spitzner, L. (2002), *Honeypots: Tracking Hackers*, 1st edn, Addison-Wesley Professional. ISBN: 0321108957.

The Honeynet Project (n.d.), 'Honeynet Research Alliance', http://www.honeynet.org/alliance/.