Análise comparativa entre o IDXP e uma variante IDMEF

Renato D. R. Fonseca, Leonardo C. Militelli, Adilson E. Guelfi, Volnys B. Bernal, João Antônio Zuffo

Laboratório de Sistemas Integráveis (LSI) - Escola Politécnica da Universidade de São Paulo (EPUSP)
Av. Professor Luciano Gualberto, trav. 3 nº158.
CEP: 05508-900 São Paulo - SP – Brasil

{rfonseca, leonardo, guelfi, volnys, jazuffo}@lsi.usp.br

Resumo. *O IDXP usa o formato IDMEF e propõe autenticação dos parceiros de comunicação, integridade e confidencialidade por meio do protocolo BEEP. O objetivo do trabalho é propor a integração do IDMEF com um modelo XML de assinatura digital de conteúdo, denominada variante IDMEF, proporcionando segurança da mensagem com o uso de qualquer protocolo de comunicação. Como resultado, o artigo discute uma análise comparativa entre o protocolo IDXP e a variante proposta.*

Abstract. *IDXP uses the format IDMEF and proposes partner authentication, integrity and confidentiality using BEEP protocol. The objective this work is to propose integration between IDMEF with an xml digital signature, called IDMEF variant, providing message's security using any communication protocol. As the result, this paper discusses a comparative analysis between the IDXP protocol and the IDMEF variant.*

1.Introdução

A proposta IDMEF (*Intrusion Detection Message Exchange Format*) [Fein02], além de apresentar o formato de mensagens de comunicação adotado entre componentes de uma solução de detecção de intrusão (*Intrusion Detection System* – IDS), também necessita de serviços de segurança no canal de comunicação, tais como, autenticação de parceiro, autoria, confidencialidade e integridade. Assim, uma contribuição à proposta IDMEF é agregar o serviço de autoria de mensagem, por exemplo, utilizando o *Xml Signature*. A recomendação [W3C02] define o *Xml Signature* como um formato *XML* para assinatura de conteúdos, provendo autoria, integridade e confidencialidade.

O objetivo deste trabalho é propor a utilização do proposta de formato de mensagens IDMEF com o modelo *XML* de assinatura de conteúdo, provendo autoria e integridade. Como objetivo secundário, o artigo comenta sobre um comparativo da "Variante IDMEF" com o IDXP (*Intrusion Detection Exchange ProtocoI*) [Fein02].

2. Segurança

2.1. Segurança de Mensagens

Uma das principais características relacionada à segurança de mensagens é o armazenamento. Portanto, as mensagens podem ser manipuladas localmente, sem a necessidade de comunicações externas. Desta forma, é desvinculado o tempo de uma sessão à existência de uma mensagem, a qual poderá ser consultada ao longo do tempo durante um período determinado ou não.

A troca de mensagens é torna versátil, como por exemplo, trocas de e-mail ou por requisições HTTP/POST. Porém, não é do escopo dos formatos de mensagens resolver questões sobre o gerenciamento e a garantia de entrega, os quais são partes integrantes da definição de protocolos seguros.

Atualmente, existem muitos formatos de mensagens seguras difundidos nos ambientes computacionais. Como por exemplo, PKCS#7 [PKCS7], PGP [Zimm96] e XADES [Centner04] [W3C03].

2.2. Segurança de comunicação

Essencialmente os protocolos de comunicação provêm segurança quanto à confidencialidade [Davis01], porém muitos deles também possibilitam a autenticação de parceiros e integridade dos pacotes trafegados. Para exemplificar alguns protocolos de comunicação seguros podem-se enumerar as seguintes soluções: SSL / TLS [RFC2246], IPSEC [RFC2411] e BEEP [Rose01]. Os protocolos de comunicação segura apresentam maior difusão em relação aos formatos de mensagens, devido sua ampla utilização na Internet. Desta forma, os protocolos se tornaram robustos, como por exemplo, o SSL, o qual pode ser encontrado inclusive em soluções de *hardwares* com objetivo de aumentar o desempenho.

2.3. IDMEF – Intrusion Detection Message Exchange Format

Normalmente, o sistema de detecção de intrusão (IDS) é uma solução composta por sensores, agentes e console de gerenciamento que, por muitas vezes, pertencem a diferentes fabricantes. Para facilitar o intercâmbio de informações entre esses componentes, se faz necessária a padronização de um protocolo de comunicação único. Com o propósito de satisfazer essa necessidade, surgiu o grupo IDWG (*Intrusion Detection Exchange Format Working Group*), pertencente ao IETF (*Internet Engineering Task Force*), o qual desenvolve a proposta de padronização do formato de dados e protocolos de comunicação para viabilizar a troca de informações.

O passo inicial para o processo de padronização foi a elaboração do documento *"*Intrusion Detection Message Exchange Requirements" [Wood02], o qual especifica proposta do formato das mensagens IDMEF e os requisitos necessários para sua implementação, além da definição do protocolo de comunicação IDP (*Intrusion Detection Protocol*).

Em seguida, o trabalho [Debar05] propõe a representação das informações trocadas entre os sistemas de detecção de intrusão utilizando o formato XML, o qual pode seguir a definição do tipo do documento (DTD). Desta forma, o formato XML provê versatilidade da manipulação de campos e variáveis.

2.4. IDXP - Intrusion Detection Exchange Protocol

Outro trabalho proposto pelo grupo IDWG é a especificação do protocolo de comunicação IDXP [Fein02] [Buch01] que atende todos os requisitos necessários para se adequar como protocolo de comunicação de mensagens IDMEF.

Na prática, o IDXP é formado pelo protocolo BEEP [Rose01], o qual contempla uma série de funcionalidades e mecanismos de controle e segurança que possibilitam, entre outras características, integridade, confidencialidade e autenticação de parceiros.

3. Análise comparativa entre a Variante IDMEF e o IDXP

A primeira questão é relativa ao não suporte do protocolo BEEP nos equipamentos e soluções de IDS, os quais requeririam atualizações para utilizar o IDXP. Deste modo, a "Variante IDMEF" apresenta vantagem em relação ao IDXP, pois devido ao uso do formato de mensagens XML existe a independência do protocolo de comunicação, tornando a solução isenta de atualizações, e mais diretamente adaptável aos meios de comunicação atuais.

A proposta de formato IDMEF apresenta vantagem quanto à sua compatibilidade devido existência de mecanismos de manipulação de XML, como a validação de um conteúdo XML por meio de um documento de definição (*Document Type Definition* – DTD).

A "Variante IDMEF" provê os serviços de segurança de autoria e integridade. Porém, não especifica modelos para a entrega e gerenciamento das mensagens, questões resolvidas pelo IDXP.

O IDXP apresenta uma preocupação importante em relação à autenticação de parceiros. Todavia, este ponto pode ser resolvido de outra forma, como por exemplo, a utilização da "Variante IDXP" com o protocolo SSL.

Concluindo, o IDXP está relacionado ao modelo de protocolos de comunicação seguros enquanto a "Variante IDMEF" opera com mensagens seguras.

4. Conclusão e trabalhos futuros

Este trabalho apresentou uma proposta denominada "Variante IDMEF" que utiliza a proposta IDMEF integrada com a recomendação *Xml Signature*.

A partir da análise comparativa foi possível identificar que o protocolo IDXP oferece como vantagens: mecanismos de garantia de entrega, autenticação de parceiros, integridade, confidencialidade. Entretanto, o IDXP apresenta como desvantangem que a maioria dos equipamentos atuais não suportam o protocolo BEEP. A "Variante IDMEF" apresenta vantagens: autoria de mensagens e trocas de mensagens sobre qualquer protocolo, inclusive sobre o SSL, o qual é a alternativa atualmente mais utilizada de protocolo de comunicação segura. Entretanto, a "Variante IDMEF" não trata da entrega e gerenciamento de mensagens, e também o tráfego de mensagens depende da escolha de um protocolo de comunicação segura ou não.

Este trabalho contribui para a definição de uma arquitetura de sistemas de detecção de intrusão que seja heterogênea e interoperável. Heterogênea sob o aspecto de definição

de uma base de elementos de fabricantes diferentes, que também resulta em soluções compatíveis, atigindo a interoperabilidade.

Uma possível evolução deste trabalho consiste no desenvolvimento de uma biblioteca de formatação de mensagens assinadas, a qual poderia ter como base para a biblioteca de código-fonte aberto LibIDMEF [LibID05].

5.Referências

[Bace01] Bace, R; Mell, P; "Intrusion Detection Systems", NIST - National Institute of Standards and Technology, Special Publication, 2001.

[Buch01] Buchheim, T.; Erlinger, M.; Feinstein, B.; Matthews, G.; Pollock, R.; Betser, J.; Walther, A.; "Implementing the Intrusion Detection Exchange protocol"; Computer Security Applications Conference, ACSAC 2001. Proceedings 17th Annual, 2001

[Centner04] Centner, M.; "XML Advanced Electronic Signatures", Master Thesis, 2004

[Debar05] Debar, H.; Curry, D.; Feinstein, B.; "The Intrusion Detection Message Exchange Format", 2005. Draft-ietf-idwg-idmef-xml-14, trabalho em andamento.

[Davis01] Davis, D., "Defective Sign & Encrypt in S/MIME PKCS#7, MOSS, PEM, PGP, and XML", Proceedings of the 2001 USENIX Annual Technical Conference.

[Fein02] Feinstein, B.; Matthews, G.; White, J.; "The Intrusion Detection Exchange Protocol (IDXP)", 2002, draft-ietf-idwg-beep-idxp-07, trabalho em andamento.

[LibID05] Poppi, S.; Migus, A.; McAlerney, J.; "LibIDMEF" http://sourceforge.net/projects/libidmef/, consulta ao site junho de 2005.

[PKCS7] RSA Laboratories, RSA Security; "PKCS-7: Cryptographic Message Syntax Standard", consulta ao site em Junho de 2005, 1993.

[RFC2246] Dierks, T.; Allen, C., "The TLS Protocol, Version 1.0", IETF, 1999. Disponível em www.faqs.org/rfcs/rfc2246.html.

[RFC2411] Thayer, R.; Doraswamy, N.; Glenn R., "RFC 2411: IP Security", IETF, 1998. Disponível em http://www.faqs.org/rfcs/rfc2411.html.

[Rose01] Rose, M.; RFC 3080: "The Blocks Extensible Exchange Protocol Core", IETF, 2001. Disponível em www.faqs.org/rfcs/rfc3080.html.

[W3C03] World Wide Web Consortium (W3C). *XML Advanced Electronic Signatures (XAdES), W3C,* 2003

[W3C02] World Wide Web Consortium (W3C). *XML – Signature Syntax and Processing (XMLDSig), W3C Recommendation*, 2002

[Wood02] Wood, M; Erlinger, M; "Intrusion Detection Message Exchange Requirements", 2002, trabalho em andamento.

[Zimm96] Zimmermann, P., "The Official PGP User's Guide," MIT Press, 1995.