Journal of Southeast University (English Edition) Vol. 22, No. 3, pp. 409 – 412 Sept. 2006 ISSN 1003—7985

Security integrated framework for semantic web based on social intelligence

Meng Qinghua[1,2] Ding Yongsheng[1]

([1]College of Information Science and Technology, Donghua University, Shanghai 201620, China)

([2]Department of Computer Science, Weifang University, Weifang 261401, China)

Abstract: An integrated security framework for a semantic web is proposed based on the social intelligence of an individual's avoiding harm and preserving transaction logic-integrity. The framework extends the semantic web model and controls the dynamic security of semantic web services, such as trust, logic and reasoning. It includes four layers, that is, a trust entrance layer, a social intelligence layer, a transaction layer, and a TCP/IP security protocols layer. The trust entrance layer deals with trustable features from users. Social intelligence layer is responsible for logical questions for a semantic web. The transaction layer carries out transaction reasoning. And the TCP/IP security protocols layer ensures security communication. These layers can cooperate to build closed-security-ring with different security grades. The integrated security framework provides an integrated security method for semantic web flow so that it is universal for various semantic web technologies.

Key words: integrated security framework; social intelligence; closed-security-ring; security-channel; semantic web

The semantic web[1] is a vision of a future Internet, which enables computers to interpret and extract web content much more effectively and precisely. But information assurance, security, and privacy also have become critical issues of applications of a semantic web. In addition to the specification of security (WS-security), Medjahed et al.[2-3] proposed some exploration from aspects of semantic web trust, and Yu et al.[4-6] proposed privacy policy management, but they only pay attention to policy control in OWL, and do not ensure the whole security for semantic web services.

Social intelligence is a kind of capability with which people can adjust their behavior under different and dangerous conditions to protect themselves[7]. Along with complication of application systems, it is necessary that social intelligence should be introduced into a semantic web to ensure confidentiality and integrity of data. If web services have been endowed with the social ability, web services can not only smartly manipulate complex business, but also automatically prevent themselves from being attacked.

In this paper, a security framework is proposed based on social intelligence, which matches with the whole semantic web model. So, it is universal for various semantic web technologies.

1 Social-Intelligence Inspired Security Integrated Framework for Semantic Web

1.1 Security in social intelligence

When people deal with tedious and secret business, the purpose of the secure logic-integrity intelligence is: ① To maintain equal security grade while they deal with the same security-grade transactions; ② To maintain logic-integrity for a complete transaction, while they process a more complex business which includes many proceedings; ③ To ensure that the process path be a closed ring while they provide a complex services for their clients. No matter what people do, the whole procedure should be controlled from beginning to end, and these processes should form a closed-procedure. In view of these facts, we can monitor the web services working procedures and make their path movements form a closed-ring.

1.2 Integrated security framework for semantic web

In order to guarantee the integrated security of a semantic web, we design a hierarchical control framework, as shown in Fig. 1. The framework is to guarantee the dynamic security, transaction integrity, self-regulation, self-inspection, and self-renewed for a semantic

Received 2006-04-25.

Foundation items: The National Natural Science Foundation of China (No. 60474037), Program for New Century Excellent Talents in University (No. NCET-04-415).

Biographies: Meng Qinghua (1970—), male, graduate; Ding Yongsheng (corresponding author), male, doctor, professor, ysding@dhu.edu.cn.

web. It includes four layers:

① Trust entrance layer This layer requires user authentication, which needs a unique user ID and represents a security grade of the web services. All operations of the web services are done in a corresponding secure channel. According to the national security standard, the secure channels of the web services have six secure grades.

② Social intelligence layer This layer monitors dynamic security features of web services, implements social intelligence features, and makes itself have the capability of self-judging and self-adjusting. The social intelligence layer can obtain some parameters from the intelligence interfaces of web services, and perceive dynamic security states and detect intrusions in order to protect the web services from attacks.

③ Transaction layer This layer is designed to satisfy business security. It responds to requests for web services in forms of transaction, and then the transactions are submitted, processed, audited, and logged. If there are any errors or defaults, transaction processing immediately is roll back. Online recovery for business can be automatically finished in this way.

④ TCP/IP security protocols layer This layer includes mainly some conventional security technologies such SSL, HTTPS, IPSEC, SET etc. These security methods work in the network layer, the transmitting layer, and the application layer of the TCP/IP reference model.

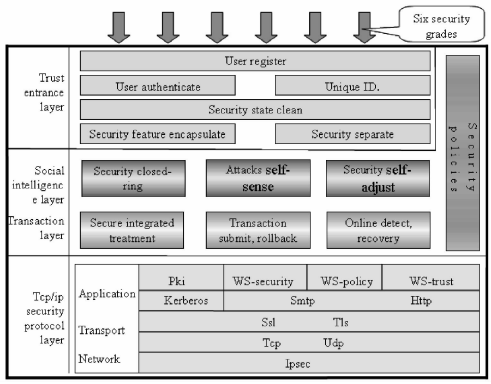

Fig. 1 Security control framework for semantic web

2 Closed-Security-Ring Mechanism for Semantic Web

The security access policies for semantic web services inspired by social intelligence include three parts: ① Closed-security-grade-ring, i. e. , all behaviors from a web service should have the same security-grade; ② Closed-transaction-integrity-ring, i. e. , service providing for users should be a whole item, the transaction should be fully completed; ③ Closed-visiting-path-ring, i. e. , the nodes passed through should compose a closed-ring as to an integral service.

The mathematical definition of a semantic web flow is expressed as $\mathrm{NIF} = (A, B, \mathrm{SC}, *, P, \geqslant)$, where A is a set of attributes, B is a set of secure behaviors, SC is the security grade of semantic web flow, $*$ defines the social intelligence characteristic for semantic web flow, P is a set of security policies, $\geqslant$ defines orders for different security grade semantic web flows and how to access each other normally.

Definition 1 Closed-security-grade-ring regulation

For interviewed web services sets (NIF_1, NIF_2, …, NIF_n), the regulation is expressed as

$$\mathrm{SC}_{\mathrm{NIF}_1} = \mathrm{SC}_{\mathrm{NIF}_2} = \ldots = \mathrm{SC}_{\mathrm{NIF}_n}$$

Definition 2 Closed-transaction-integrity-ring regulation

According to continuity and connection of transaction, directed graph $G\langle N, T_{\mathrm{trans}}\rangle$ is built along with the path of web services. Where N is MAC addresses or IP addresses of nodes where the web service passes, T_{trans} is the transmission time between neighboring nodes: $T_{\mathrm{trans}(i,j)} = T_{\mathrm{timestamp}(i)} - T_{\mathrm{timestamp}(j)}$, where $T_{\mathrm{timestamp}(i)}$ is the timestamp when the web services pass the node. Then the adjacent matrix $\boldsymbol{A}(G) = (a_{ij})_{n\times n}$ can be obtained from the directed graph $G\langle N, T_{\mathrm{trans}}\rangle$. According to the IP or MAC address of the related nodes when the web services pass, we can obtain

$$a_{jj} = \begin{cases} T_{\mathrm{trans}(i,j)} & \text{information from } i \text{ to } j \\ 0 & \text{information not from } i \text{ to } j \end{cases}$$

$\boldsymbol{A}(G)$ has features of symmetric matrix, i. e. , the transposed matrix of $\boldsymbol{A}(G)$ is itself:

$$\boldsymbol{A}^{\mathrm{T}}(G) = \boldsymbol{A}(G)$$

Definition 3 Closed-visiting-path-ring regulation

Judges whether the directed graph $G\langle N, T_{\mathrm{trans}}\rangle$ has a circuit. According to EULER circuit theorem, a directed graph has a circuit if and only if it is interconnected, i. e. , the out-degree and in-degree of each node are equal. The definition is given as

$$b_{ik} = \begin{cases} \mathrm{counter}\ (T_{\mathrm{trans}(i,j)}) & T_{\mathrm{trans}(i,j)} \neq 0, k = 0 \\ \mathrm{counter}\ (T_{\mathrm{trans}(j,i)}) & T_{\mathrm{trans}(j,i)} \neq 0, k = 1 \end{cases}$$

where $i, j \in (1, n)$ expresses MAC or IP address when web services pass through, k is 0 or 1, b_{i0} and b_{i1} express out-degree and in-degree of the node i, respectively. Behaviors of web services can compose a logic closed-ring if b_{i0} equals b_{i1}.

3 Case Study: Implementing Security Policy for Semantic Web Flow

3.1 Security policy for web service flow

We define several symbols. Some symbols express some attributes of a semantic web flow, and others denote operations of a semantic web flow. We also address several rulers for a semantic web flow. For instance, x, y, z express the semantic web flow; $\perp$ expresses a regulated security-grade flow which must obey corresponding security constraints; λw expresses a labeled semantic web flow which has its own security policy; $\langle e, M\rangle$ expresses the well-typed memory state of λw; other labels express security-grade, transaction operation, state transfer, etc.

Rule 1 Security marking It is important to change file permissions at run time. The following code changes the access control policy of the file w to label z. However, the original contents of w need to be wiped out to prevent them from being declassified, which provides stronger security assurance than an ordinary file system.

$$\lambda w\colon((x\colon \text{label}_{\perp}) * (\text{int}_x \text{ ref}_{\perp})_{\perp})_{\perp} \text{ref}_{\perp}(z\colon \text{lable}_{\perp})[\perp]$$
$$(\lambda(y\colon \text{int}_z \text{ ref}_{\perp})[\perp].\ w\colon = (x = z, y\colon \text{int}_x \text{ ref}_{\perp}))\text{ref}^{\text{intz}}0$$

Rule 2 Channel and flow security marking According to the regulation of closed-security-ring, we must identify the security channel and corresponding flows. Pairing a label to a web service flow, and storing the pairs in the reference of the flow represent the channel's security features. Therefore, we can check their security by tracking the flows' security labels. For example,

$$\lambda z\colon(((x\colon \text{label}_x)) * \text{int}_x)_{\perp} \text{ref}_{\perp} \lambda w\colon \text{lab}_w$$
$$\lambda(y\colon \text{int}_w)[\perp].\ z\colon = (x = z, y\colon \text{int}_x)$$

Rule 3 State changing If different web services exist in the same closed-security-ring and they perform a task together, we permit the flow change states from one to another. If pc $\in e\colon \tau$, and M is a well-typed memory such that $\langle e, M\rangle$ is a well-formed configuration, either e is a value or there exists e' and M' such that $\langle e, M\rangle \rightarrow \langle e', M'\rangle$.

Rule 4 Noninterference Let $\rightarrow *$ denote the transitive closure of the $\rightarrow$ relationship. The following theorem formalizes the claim that the type system of the web service enforces noninterference:

Suppose $x\colon \tau \in e\colon \text{int}_{\text{L}}$, and $H \subseteq \tau$ that, and given two arbitrary values v_1 and v_2 of type τ, and an initial memory M, if $\langle e[v_{i/x}], M\rangle \rightarrow * e\langle v_i', M_i'\rangle$ for $i \in \{1, 2\}$, then $v_1' = v_2'$.

3.2 Implementing policy for web service flow

For web services, security policies are embedded into XML document and use the related WS-policy specification to implement. The detail syntaxes are shown as follows:

```
〈wsp: Policy xmlns: wmlns: wsp = "…" xmlns: wsse = "…"〉
  〈wsp: PFWSF〉
    〈wsp: All wsp: Preference = "100"〉
      〈wsse: Security token〉
        〈wsse: Token type〉wsse: KerberosvSTGT〈/wsse: TokenType〉
      〈/wsse: Security token〉
      〈wsse: security channel〉
      〈wsse: Rule 1 (Security marking);
             Rule 2 (Channel and flow security marking);
             Rule 3 (State changing);
             Rule 4 (Noninterfererce)/〉
      〈/wsse: security channel〉
    〈/wsp: PFWSF〉
  〈/wsp: Policy〉
```

4 Conclusion

In order to ensure the complete security of a semantic web, a closed-security-ring network model is presented based on social intelligence. Different security channels having different security classes are designed in the model, and web services are transmitted and accessed in the channels. Therefore, the closed-security-ring can guarantee static and dynamic security for a semantic web.

References

[1] Berners-Lee T, Hendler J, Lassila O. The semantic web [J]. *Scientific American*, 2001, **184**(5): 34 - 43.

[2] Medjahed Brahim, Bouguettaya Athman. A multilevel composability model for semantic web services [J]. *IEEE Transactions on Knowledge and Data Engineering*, 2005, **17**(7): 954 - 968.

[3] Chun Soon Ae, Atluri Vijayalakshmi, Adam Nabil R, et al. Using semantics for policy-based web service composition [J]. *Distributed and Parallel Databases*, 2005, **18**(1): 37 - 64.

[4] Yu Ting, Winslett Marianne, Seamons Kent E. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation [J]. *ACM Transactions on Information and System Security (TISSEC)*, 2003, **6**(1): 1 - 42.

[5] Lee JinKyu, Upadhyaya Shambhu J, Rao H Raghav, et al. *Secure knowledge management and the semantic web* [M]. Special issue: The semantic e-business vision. New York: ACM Press, 2005. 48 - 54.

[6] Souzis Adam. Building a semantic Wiki [J]. *IEEE Intelligent Systems*, 2005, **20**(5): 87 - 91.

[7] de Ruyter B, Saini P, Markopoulos P, et al. Assessing the effects of building social intelligence in a robotic interface for the home[J]. *Interactive Compute*, 2005, **17**(5): 522 - 541.

基于社会智能的语义 web 安全集成框架

孟庆华[1,2] 丁永生[1]

([1] 东华大学信息科学与技术学院,上海 201620)
([2] 潍坊学院计算机科学系,潍坊 261401)

摘要:基于个体趋利避害和事务逻辑完整的社会智能特征,提出了一种语义 web 的安全集成框架. 该框架对语义 web 模型进行了扩展,控制语义 web 服务信任、逻辑、推理等方面的动态安全. 该框架包括 4 个层次:信任入口层、社会智能层、事务层和 TCP/IP 安全协议层. 信任层处理用户的信任特征,社会智能层控制语义 web 的逻辑问题,事务层负责事务推理,TCP/IP 安全协议层则保证安全通信. 这些安全层协同构建了具有不同安全等级的安全环. 该安全集成框架为语义 web 提供一种安全集成方法,为不同技术的安全协同提供了通用的安全解决框架.

关键词:安全集成框架;社会智能;安全环;安全通道;语义 web
中图分类号:TP309