Context-aware Alert Verification for Network Security using the Extension Method based on Basic-Elements

Hui Xu, Chunzhi Wang, Wei Liu and Xinlu Zong

School of Computer Science, Hubei University of Technology, Wuhan, China
xuhui_1004@hotmail.com

Abstract

As for network security, post-IDS alert analysis has become a fashion in view of collaboration and correlation, and context-aware alert verification is one of the main solutions. In order to guarantee a unified representation of related information and knowledge, this paper tries to introduce basic-elements and the extension method into the study on context-aware alert verification. This paper then proposes the use of basic-elements to realize the formal presentation of alert information and context information in a unified manner, and applies the extension method based on basic-elements for context-aware alert verification by utilizing the extension set and the extension analysis. The evaluation result of validation scenarios shows that, the proposed approach prospects a formalized way to context-aware alert verification for network security with an appropriate use of the extension method based on basic-elements.

Keywords: *Network Security, Context-aware Alert Verification, Basic-Element, Extension Method, Extension Set, Extension Analysis*

1. Introduction

Intrusion Detection System (IDS) has evolved as an important tool for network security, but the detection mechanisms of traditional IDSs have weaknesses including too fine grain, isolated alarming and lack of environmental consciousness. As for network security, post-IDS alert analysis should take the context into consideration in view of collaboration and correlation. Hence in this case, context-aware alert verification becomes a feasible way for network security. However, one of the main problems is how to guarantee a unified representation of related information and knowledge, in order to realize collaboration and correlation for the sake of network security.

Our prior work [1, 2, 3] discusses the issues related to the support of XML-based integrated network management for alert analysis, and tries to apply security ontology to represent security information, context information and correlation knowledge in a unified way, for the sake of post-IDS alert analysis. The application of security ontology realizes the unification of related information and knowledge, but still limits in the level of formalization. And in this case, the extension method prospects a promising way to improve the application of security ontology by means of formalization of a higher degree. In view of network security, the aim of this paper is then to introduce the extension method based on basic-elements including the extension set and the extension analysis into the research on context-aware alert verification.

The remainder of this paper is organized as follows. Section 2 introduces the definition of basic-elements, and proposes the formal presentation of alert information using affair-elements and the formal presentation of context information using matter-elements. Based on the unified representation of alerts and security-related contexts, Section 3 considers the

correlation problem for context-aware alert verification using the extension method from the extension set point of view. Furthermore, Section 4 demonstrates the realization of context-aware alert verification using the extension method from the viewpoint of the extension analysis based on divergence-tree for basic-elements, and then discusses issues related to several scenarios in order to validate the feasibility of the proposed approach. Section 5 concludes this paper.

2. Formal Representations of Alert Information and Context Information based on Basic-elements

In view of network security, the proposed approach utilizes basic-elements for unified formal representations of related information including alerts and contexts by means of affair-elements and matter-elements.

2.1. Formalization of Security Information based on Basic-elements

Aiming at the solving of contradictory problems of the reality world, the thinking of Extenics was first proposed by Prof. Cai in 1983 [4], and its basic theory is the extension theory containing matter-element theory [5] and extension mathematics as its two pillars.

From the viewpoint of network security, the Extenics-based approach is promising for the study on context-aware alert verification with the use of the extension innovative method system. In this case, as the logic cell of Extenics, basic-elements [6] that include matter-elements, affair-elements and relation-elements will be utilized to formalize security information in a unified manner.

Formula 1 demonstrates a common definition of basic-elements, in which $Object$ means the object for the research, with its characteristics $c_1, c_2, ..., c_n$ and corresponding values $v_1, v_2, ..., v_n$.

$$B = \begin{bmatrix} Object, c_1, v_1 \\ c_2, v_2 \\ ..... \\ c_n, v_n \end{bmatrix} \quad \ldots (1)$$

Base on Formula 1, the class for a type of basic-elements can be defined as Formula 2, in which $V_1, V_2, ..., V_n$ describe the value domains of characteristics $c_1, c_2, ..., c_n$ for the set of objects that is $\{Object\}$.

$$\{B\} = \begin{bmatrix} \{Object\}, c_1, V_1 \\ c_2, V_2 \\ ..... \\ c_n, V_n \end{bmatrix} \quad \ldots (2)$$

2.2. Formalization of Alert Information for Network Security using Affair-elements

As for the unified representation of alert information for network security, Intrusion Detection Message Exchange Format (IDMEF) [7] may be a choice. IDMEF is emerging as

an industry standard, and it can be used for interoperation between different IDSs. However, IDMEF is limited in standardizing various IDS formats, not widely applicable for the unified representation of various security alerts. Thus from this viewpoint, Formula 3 provides the formal representation of alert information using the class of affair-elements labeled as A_A, in which $\{Alert_x\}$ means a particular kind of alert objects, with its characteristics $c_{x1}, c_{x2}, ..., c_{xn}$ and corresponding value domains $V_{x1}, V_{x2}, ..., V_{xn}$.

$$\{A_A\} = \begin{bmatrix} \{Alert_x\}, c_{x1}, V_{x1} \\ c_{x2}, V_{x2} \\ ..... \\ c_{xn}, V_{xn} \end{bmatrix} = (\{Alert_x\}, c_x, V_x) \quad \ldots (3)$$

According to Formula 3, an affair-element for security alerts as an example is shown as Formula 4.

$$A_A = \begin{bmatrix} Alert_x, AlertID, v_{x1} \\ Confidence, v_{x2} \\ \text{Im } pact, v_{x3} \\ Method, v_{x4} \\ Time, v_{x5} \\ Signature, v_{x6} \\ \text{Re } action, v_{x7} \end{bmatrix} \quad \ldots (4)$$

2.3. Formalization of Context Information for Network Security using Matter-elements

As for the purpose of alert verification, context information is of great importance. Formula 5 describes the formal representation of context information for network security using the class of matter-elements labeled as M_C, in which $\{Context_y\}$ means a particular type of context objects, with its characteristics $c_{y1}, c_{y2}, ..., c_{yn}$ and corresponding value domains $V_{y1}, V_{y2}, ..., V_{yn}$.

$$\{M_C\} = \begin{bmatrix} \{Context_y\}, c_{y1}, V_{y1} \\ c_{y2}, V_{y2} \\ ..... \\ c_{yn}, V_{yn} \end{bmatrix} = (\{Context_y\}, c_y, V_y) \quad \ldots (5)$$

For the purpose of collaboration, context information in network security domain is mainly divided into following two types.

(1) Network and host information

As for context information in the field of network security, network information mainly includes service and privilege, while host information mainly consists of operation system and malicious software.

(2) Vulnerability information

In most cases, an attack is aiming at vulnerability of the source hosts. Hence, vulnerability information should be taken into consideration during the process of context-aware alert verification. Two main kinds of vulnerability information are included, which are one from CVE dictionary and the other one from Bugtraq vulnerability database.

Based on the analysis above, a unified representation of the matter-elements for context information in the field of network security is then presented as Formula 6.

$$M_C = \begin{bmatrix} Context_y, Service, v_{y1} \\ \quad Privilege, v_{y2} \\ \quad OperationSystem, v_{y3} \\ \quad MaliciousSoftware, v_{y4} \\ \quad VulnerabilityInformation, v_{y5} \end{bmatrix} \quad \ldots (6)$$

3. Application of the Extension Set for Context-aware Alert Verification

Since the unified representation of information for network security such as alerts and contexts has been formalized based on basic-elements, the asset correlation problem for context-aware alert verification can be considered using the extension method from the viewpoint of the extension set [6, 8, 9].

3.1. The Extension Set Point of View for Context-aware Alert Verification

When using the extension method from the viewpoint of the extension set, the formalization of asset correlation for context-aware alert verification is established as follows.

Suppose that the field X represents a set of the managed entities for network security, $x \in X$ is a managed entity, and $y = d(x)$ indicates the degree of threat suffered by x, then the extension set for X can be defined as $\overleftrightarrow{X} = \{(x, y, y') \mid x \in T_X X, y = d(x) \in I, y' = T_d d(T_x x) \in I\}$, in which $T = (T_X, T_d, T_x)$ means extension transformations representing the formalization of correlation knowledge in network security domain and I is the field of real numbers.

When T is not realized, the set of real attacks for network security can be formalized as the positive field of $\overleftrightarrow{X}$ that is $\overrightarrow{X} = \{(x, y) \mid x \in X, y = d(x) \rangle 0\}$, while the set of system-immune attacks for network security can be formalized as the negative field of $\overleftrightarrow{X}$ that

is $\overleftarrow{X} = \{(x, y) | x \in X, y = d(x) \langle 0\}$. And the zero point of $\overleftrightarrow{X}$ that is $\overleftrightarrow{X}_0 = \{(x, y) | x \in X, y = d(x) = 0\}$ reflects the critical condition between real attacks and system-immune ones for network security.

3.2. State Transition for Network Security using the Extension Set

From the viewpoint of the extension set, not only context-aware alert verification but also related security management actions can be formalized in a unified manner. Figure 1 proposes state transition for network security using the extension set.

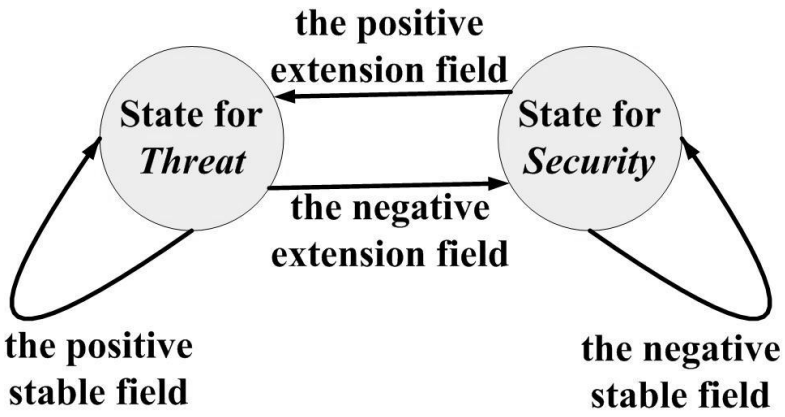

Figure 1. State Transition for Network Security using the Extension Set

As is indicated in Figure 1, when T_x representing the extension transformation for asset correlation in network security domain is realized, the action of context-aware alert verification to judge the alerts as real attacks that is the state for threat can be defined by the positive extension field, which is $\overleftarrow{X}^{+}(T_x) = \{(x, y, y') | x \in X, y = d(x) \leq 0, y' = d(T_x x) \rangle 0\}$, while the action of context-aware alert verification to judge the alerts as system-immune ones that is the state for security can be described by the negative stable field that is $\overleftarrow{X}_{-}(T_x) = \{(x, y, y') | x \in X, y = d(x) \langle 0, y' = d(T_x x) \langle 0\}$.

Furthermore, when T_x representing the extension transformation for management actions in the field of network security is realized, the case of successful threat elimination by countermeasure can be defined as the negative extension field, which is $\overleftrightarrow{X}^{-}(T_x) = \{(x, y, y') | x \in X, y = d(x) \geq 0, y' = d(T_x x) \langle 0\}$, and the case of failed threat elimination by countermeasure can be described as the positive stable field, which is $\overleftrightarrow{X}_{+}(T_x) = \{(x, y, y') | x \in X, y = d(x) \rangle 0, y' = d(T_x x) \rangle 0\}$.

4. Application of the Extension Analysis based on Divergence-tree for Context-aware alert Verification

Based on the correlation study of context-aware alert verification using the extension set, the extension method should be further utilized by applying the extension analysis based on divergence-tree to realize context-aware alert verification for the sake of network security.

4.1. Divergence-tree for Extension Analysis

First of all, Definition 1 describes the meaning of divergence for basic-elements, which is that B becomes B_e through extension by means of divergence analysis [6, 8, 9].

Definition 1 If B and B_e are two basic-elements, then the divergence of B to B_e through extension can be defined by $B-|B_e$

Figure 2 then provides a general model for divergence-tree of basic-elements.

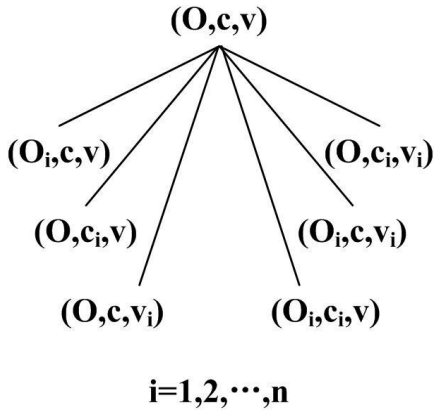

Figure 2. A General Model for Divergence-tree of Basic-elements

As is shown in Figure 2, related principles indicated from divergence-tree can be utilized for context-aware alert verification. Principle 1-3 presents one-variable divergence analysis for basic-elements, while Principle 4-6 demonstrates two-variable divergence analysis for basic-elements.

Principle 1 As for basic-element $B=(O,c,v)$, another object $O_i(1\le i\le n)$ can be extended to have the same value v for the same characteristic c, that is

$$B=(O,c,v) \ -| \ \{(O_1,c,v),(O_2,c,v),...,(O_n,c,v)\}$$

Principle 2 As for basic-element $B=(O,c,v)$, the same object O can be extended to have different characteristics $c_i(1\le i\le n)$ for the same value v, that is

$$B=(O,c,v) \ -| \ \{(O,c_1,v),(O,c_2,v),...,(O,c_n,v)\}$$

Principle 3 As for basic-element $B=(O,c,v)$, the same object O can be extended to have different values $v_i(1\le i\le n)$ for the same characteristic c, that is

$$B=(O,c,v) \ -| \ \{(O,c,v_1),(O,c,v_2),...,(O,c,v_n)\}$$

Principle 4 As for basic-element $B=(O,c,v)$, another object $O_i(1\le i\le n)$ can be extended to have the same value v for different characteristics $c_i(1\le i\le n)$, that is

$$B=(O,c,v) \ -| \ \{(O_1,c_1,v),(O_2,c_2,v),...,(O_n,c_n,v)\}$$

Principle 5 As for basic-element $B=(O,c,v)$, another object $O_i(1\le i\le n)$ can be extended to have different values $v_i(1\le i\le n)$ for the same characteristic c, that is

$$B=(O,c,v) \ -| \ \{(O_1,c,v_1),(O_2,c,v_2),...,(O_n,c,v_n)\}$$

Principle 6 As for basic-element $B=(O,c,v)$, the same object O can be extended to have different values $v_i(1\le i\le n)$ for different characteristics $c_i(1\le i\le n)$, that is

$$B=(O,c,v) \ -| \ \{(O,c_1,v_1),(O,c_2,v_2),...,(O,c_n,v_n)\}$$

4.2. Validation Scenarios

In order to explain the feasibility of the extension analysis based on divergence-tree for context-aware alert verification with the use of Principle 1-6, several scenarios are provided for the sake of validation.

Scenario 1 As for this scenario, the unified representation of matter-elements for context information in network security domain presented as Formula 6 will be considered.

Suppose that an alert targeting at a particular Backdoor vulnerability has been detected, but it is inconsistent with the context information existing for the current device, simply noted as $M_{C1}=[Context,\mathrm{MaliciousSoftware},\mathrm{Virus}]$. Indicated from the information, the device may be regarded as system-immune from this attack. However, the same device may possibly have other malicious software not obtained yet, and Principle 3 can then be used to formalize the renewal action of the context information for this device. A possible extension is $M_{C1}-|\{M_{C2},M_{C3},M_{C4},.....\}$, $M_{C2}=[Context,\mathrm{MaliciousSoftware},\mathrm{Worm}]$, $M_{C3}=[Context,\mathrm{MaliciousSoftware},\mathrm{Zombie}]$, $M_{C4}=[Context,\mathrm{MaliciousSoftware},\mathrm{Backdoor}]$. Thus the extended values for the characteristic $\mathrm{MaliciousSoftware}$ show that, the device may suffer from the underlying attack with detailed analysis of its Backdoor list.

Scenario 2 As for this scenario, the unified representation of matter-elements for context information in the field of network security proposed as Formula 6 will still be considered.

Suppose that an alert targeting at the Linux operation system has been detected, but it is inconsistent with the context information existing for the current device, simply noted as $M_{C5}=[Context_5,\mathrm{OperationSystem},\mathrm{WindowXP}]$. In this case, the device may be regarded as system-immune from this attack. However, other devices in the same network

may suffer from the underlying attack, and Principle 5 can then be utilized to formalize the collection action of the context information for this network. A possible extension is $M_{C5} - | \{M_{C6}, M_{C7}, M_{C8}, ...\}$, $M_{C6} = [Context_6, \text{OperationSystem}, \text{Linux}]$, $M_{C7} = [Context_7, \text{OperationSystem}, \text{Windows7}]$, $M_{C8} = [Context_8, \text{OperationSystem}, \text{Linux}]$. Thus devices indicated from M_{C6} and M_{C8} should be further considered for the possible attack.

The evaluation result of these validation scenarios above shows that, the proposed approach prospects a formalized way to context-aware alert verification for network security with an appropriate use of the extension method based on basic-elements.

5. Conclusions

The main contribution of this paper is to apply the extension method based on basic-elements to context-aware alert verification for network security. The proposed approach utilizes the basic-elements to formalize the representations of alert information and context information for the sake of unified management, and then makes use of the extension method for context-aware alert verification with the support of the extension set and the extension analysis based on divergence-tree, in order to promote the formalization level of network security from the viewpoint of asset correlation.

Acknowledgements

This work has been supported by the General Program for Natural Science Foundation of Hubei Province in China (No. 2012FFB00601), the Key Project for Scientific and Technological Research of Wuhan City in China (No. 201210421134), the Doctoral Scientific Research Fund from Hubei University of Technology (No. BSQD12029), the Provincial Teaching Reform Research Project of Education Department of Hubei Province in China (No. 2012273), the General Program for National Natural Science Foundation of China (No. 61170135), the National Natural Science Foundation of China for Young Scholars (No. 61202287), the Key Project for Natural Science Foundation of Hubei Province in China (No. 2010CDA011), the General Program for Natural Science Foundation of Hubei Province in China (No. 2011CDB075), the Key Project for Scientific and Technological Research of Education Department of Hubei Province in China (No. D20111409, No. D20121409), and the Twilight Plan Project of Wuhan City in China (No. 201050231084). The authors would like to thank all project partners for their valuable contributions and feedbacks.

References

[1] H. Xu, D. B. Xiao, X. Xia and Y. N. Chang, “A Collaborative Architecture for Post-IDS Alert Analysis”, Proceeding of 3rd International Conference on Computer Science and Education, Xiamen University Press, **(2008)**, pp. 666-671.
[2] H. Xu, D. B. Xiao, X. Xia and Z. Wu, “Collaborative Post-IDS Alert Analysis Based on Network Management Techniques”, Proceeding of 1st International Colloquium on Computing, Communication, Control, and Management, IEEE Press, **(2008)**, pp. 220-224.
[3] H. Xu, D. B. Xiao and Z. Wu, “Application of Security Ontology to Context-Aware Alert Analysis”, Proceeding of 8th IEEE/ACIS International Conference on Computer and Information Science, IEEE Press, **(2009)**, pp. 171-176.

[4] W. Cai, "Extension Set and Non-Compatible Problems", Journal of Scientific Exploration, vol. 1, in Chinese **(1983)**, pp. 83-97.
[5] W. Cai, "Matter-Element Analysis", Simplified Chinese version, Guangdong Higher Education Press, Guangzhou, **(1987)**.
[6] W. Cai, C. Y. Yang and B. He, "Preliminary Extension Logic", Simplified Chinese version, Science Press, Beijing, **(2003)**.
[7] H. Debar, D. Curry and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)", RFC4765, **(2007)**.
[8] L. X. Li, C. Y. Yang and H. W. Li, "Extension Strategy Generation System", Simplified Chinese version, Science Press, Beijing, **(2006)**.
[9] C. Y. Yang and W. Cai, "Extension Engineering", Simplified Chinese version, Science Press, Beijing, **(2007)**.

Authors

Hui Xu

She received a bachelor's degree in Computer Science and Technology from Huazhong Normal University, Wuhan, China in 2005, a master's degree in Computer Application Technology from Huazhong Normal University, Wuhan, China in 2008, and a doctor's degree in Radio Physics from Huazhong Normal University, Wuhan, China in 2010. Since 2006, she has been a certified computer system analyst in China. Now, she is a Lecturer at the School of Computer Science in Hubei University of Technology, Wuhan, China. Currently, her major field of study is network and service management.

Dr. Xu became a Member of Institute of Electrical and Electronics Engineers (IEEE) in 2007, a Member of Association for Computing Machinery (ACM) in 2007 and a Member of China Computer Federation (CCF) in 2008. She has authored or coauthored 1 book and 2 book chapters in the field of network management, 9 papers published by international journals, 4 papers published by Chinese journals, and more than 20 papers published by international conferences. In April 2008, she was awarded by International Association of Engineers (IAENG) for her first-authored paper presented to 2008 IAENG International Conference on Communication Systems and Applications. In July 2008, her biography was selected for inclusion in the 26th edition (2009) of the Marquis Who's Who in the World, California, USA. Additionally, she was a Session Co-Chair or a Paper Reviewer for 2nd&3rd&7th&8th International Conference on Computer Science and Education (ICCSE 2007&2008&2012&2013), a Session Chair for 1st International Symposium on Electronic Commerce and Security (ISECS 2008), a Paper Reviewer for 4th IEEE Conference on Industrial Electronics and Applications (ICIEA 2009), a Paper Reviewer for 3rd International Conference on Computer and Network Technology (ICCNT 2011), and a Paper Reviewer for Security and Communication Networks, an international journal published by Wiley Press.

Chunzhi Wang

She is a Professor at the School of Computer Science in Hubei University of Technology, Wuhan, China. She is also the Dean of the School of Computer Science in Hubei University of Technology, Wuhan, China. Currently, her major field of study is cooperative management.

Wei Liu

He is an Associate Professor at the School of Computer Science in Hubei University of Technology, Wuhan, China. Currently, his major field of study is Internet of Things.

Xinlu Zong

She is a Lecturer at the School of Computer Science in Hubei University of Technology, Wuhan, China. Currently, her major field of study is automated management.