SKRM: Where Security Techniques Talk to Each Other

Xiaoyan Sun, Jun Dai, Peng Liu
College of Information Sciences and Technology
Pennsylvania State University
University Park, USA
Email: xzs5052, jqd5187, pliu@ist.psu.edu

***Abstract*—Achieving complete and accurate cyber situation awareness (SA) is crucial for security analysts to make right decisions. To facilitate cyber SA, existing security tools, algorithms, and techniques like attack graph, should be integrated together to extract the most critical information and synthesize knowledge from different areas. Based on existing theories of situation awareness, a cyber SA model and an SKRM (Situation Knowledge Reference Model) model are constructed to enhance the coupling of current techniques to situation awareness to enable security analysts' effective analysis of complex cyber-security problems.**

***Keywords*-situation awareness; cyber security**

I. Introduction

To better secure a network, human decision makers should clearly know and understand what is going on in the network. This is basically what we call *cyber situation awareness (cyber SA)*. Human is the key role of cyber SA because only human can be "aware". Technologies regarding cyber security have made remarkable progress in the past decades. A lot of algorithms and tools are developed for vulnerability analysis, detection of attacks, damage and impact assessment, and system recovery, etc. These technologies significantly enhance human analysts cyber situation awareness and facilitate their network security management. Attack graph is one typical example. By combining vulnerabilities in the network, potential attack paths can be automatically generated with attack graph tools. Through generated attack paths, security analysts can clearly know how the attackers may exploit the network. Without attack graph, it is very difficult for them to construct reasonable attack scenarios for even a small network only by reading the vulnerability scan results, let alone for large scale enterprise network with hundreds to thousands of hosts. However, although these tools greatly ease the analysts work in some aspects, they do not explicitly consider the role of human operators when being designed. A lot of questions should be asked: can human analysts understand the output presented by these techniques? To what extent can the system facilitate human analysts cognition and situation awareness? What kind of information should be present to them for better situation awareness? Can they get the information they want when it is needed? Is the system responsive enough to support such interactive analysis? Is the interface user friendly? Apparently, without taking into account the role of human analysts, the capabilities of these techniques cannot be fully leveraged to effectively support situation awareness. In this paper, section 2 first introduces some key concepts of situation awareness and section 3 discusses how to apply SA to cyber field. Based on that, a SKRM model is proposed in section 4.

II. Situation Awareness Concepts

There have been a number of definitions towards situation awareness. The very first definitions are mostly related to aircraft domain, which are presented in the review from Dominguez [1] and Fracker [2]. Endsley [3] provides a formal definition of SA in dynamic environments: "*situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.*" From this definition, Endsley basically view situation awareness as containing three levels: *perception, comprehension*, and *projection*. Salerno et al. [4] slightly modified the above definition and define SA as "situation awareness is the perception ... and the projection of their status *in order to enable decision superiority*." Salernos definition implies the importance of situation awareness to the decision process. McGuinness and Foy [5] add a fourth level to Endsleys definition named *resolution*, which tries to identify the best path to follow to achieve the desire state change to the current situation. Resolution does not directly make decisions for humans regarding what should be done, but provides available options and the corresponding impact of these options to the environment. To help understand the four levels of SA, we use the analogy made by McGuinness and Foy to explain them: perception represents "What are the current facts?" Comprehension means, "What is actually going on?" Projection asks, "What is most likely to happen if ...?" And Resolution means, "What exactly shall I do?" Alberts et al. [6] provides another definition of situation awareness, which "*describes the awareness of a situation that exists in part or all of the battle space at a particular point in time*". For situation, they identify three main components: missions and constraints on missions, capabilities and intentions of relevant forces, and key attributes of the environment. For awareness, they say "*awareness exists in the cognitive domain*" and awareness is "*the result of a complex interaction between prior knowledge and current*

978-1-4673-2437-3/13/$31.00 ©2013 IEEE

perceptions of reality". This definition basically emphasizes the role of cognition in awareness and uncovers a fact that awareness is not just perceptions of reality, but also includes prior knowledge as a crucial factor. This explains why experienced analysts usually gain situation awareness more rapidly and accurately than novice analysts. Actually all the above definitions consider time as a basic element of SA. Decision makers rely on previous experience and prior knowledge to keep aware of changing environment, make decisions, and perform actions. As in the OODA (Observe, Orient, Decision, Act) loop [7], decisions and actions provide feedback to the environment again and a new cycle will start. Therefore, time is an essential element of SA.

III. Apply to Cyber Field: A Model of Cyber SA

Researchers from different communities have established various reference models or frameworks for situation awareness. Salerno et al. [4] construct a situation awareness framework based on Joint Directors of Laboratories (JDL) data fusion model [8] and Endsleys model of SA in dynamic decision making [3]. With the same definition of SA as in [5], Tadda and Salerno [9] propose a situation awareness reference model and provide clear definition to concepts such as entity, object, group, event, activity, etc. Both of the work demonstrates how to apply the established model to different domains.

The focus of this paper is not to establish a reference model for situation awareness, but to find a way to enhance human analysts SA by apply existing SA theories to cyber security field. Therefore, a model of cyber SA is constructed based on the work by Tadda and Salerno [9] and by Endsley [10], as shown in Figure 1. The key part of this model is an embedded sub-model we proposed: *Situation Knowledge Reference Model (SKRM)*. Simply put, SKRM is *a model that integrates cyber knowledge from different perspectives by coupling data, information, algorithms and tools, and human knowledge, to enhance cyber analysts situation awareness*. This following paragraphs will first explain the cyber SA model, and then justify why and how to establish SKRM.

In the cyber SA model in Figure 1, cyber situation awareness consists of four levels: perception, comprehension, projection, and resolution. The basic idea of this model is: taking input from data, information, tools and algorithms, and intelligence of human experts from different areas, SKRM enables the four levels of situation awareness. On the other hand, the output of SKRM, as well as data, information, system interfaces, and real world, all serve as human analysts information sources for cyber SA.

The perception level is different from the one in Tadda and Salernos model in [9]: Other than data and information, real world and system interface are explicitly included as the information sources of SA [3] [10] that are perceived by

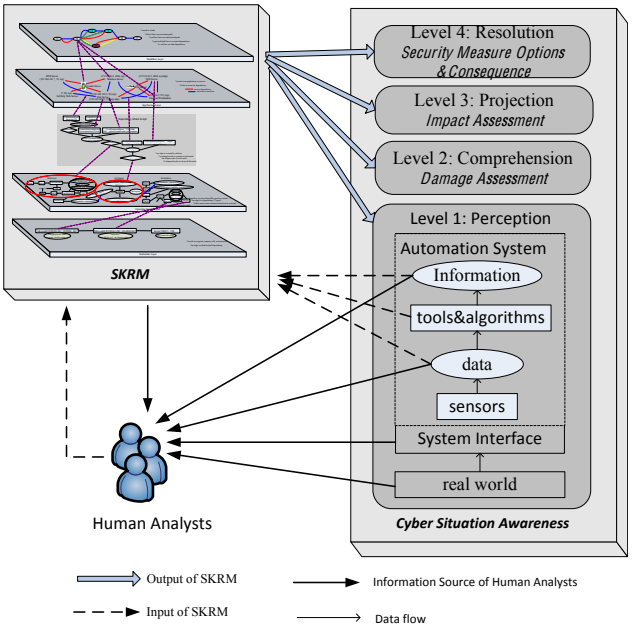

Figure 1. A Model of Cyber Situation Awareness

human analysts. System interface is directly related to the effectiveness of human cognition to system knowledge. Well-designed interface can present information and knowledge in an intuitive way and facilitate interactive analysis. In addition, information from real world is directly perceived by human analysts without being processed through automation systems. Such information influences human analysts' SA in some way, good or bad, although the "some way" is out of our research scope. For example, a piece of news regarding a recent popular attack pattern may trigger security analysts to relate it to similar symptoms found in their own network. Or their colleagues' talk about recent financial abnormality may implicitly confirm security analysts' inference of a computer being compromised.

In terms of cyber security, level 2 and 3 are mainly about impact assessment, which includes two parts [11]: assessment of current impact that is damage assessment, and assessment of future impact which mainly involves vulnerability analysis and threat assessment. Resolution level [5] is included in the model due to its importance for cyber security analysis: human analysts have a variety of security measures for security management, either confronting attacks by network hardening, or recovering from the damage caused by attacks. These security measures have different consequences towards network security. Thus human decision makers can choose the best option, at least that they think the best, based on the available security measures and the corresponding consequences.

IV. Proposed SKRM Framework

To better present SKRM framework, three questions should be answered: 1) Why do we need SKRM? 2) What

is the main structure of SKRM? 3) How can SKRM enable cyber situation awareness?

A. Why do we need SKRM?

We need SKRM for several reasons. First, *the isolation between different knowledge bases*. Cyber security has made significant advancement in a variety of areas, but these areas rarely "talk" to each other. When it comes to cyber SA, we have experts from different areas working on the same topic, but they cannot effectively communicate with each other. For example, system experts exactly know which file is stolen or modified, but they hardly know how this can impact the business level. On the other hand, business managers can rapidly notice a suspicious financial loss, but they won't relate it to an unallowed system call parameter inside the operating system. This is one reason for constructing SKRM: we need a model to integrate knowledge from different areas to break the isolation between them.

Second, *the isolation between techniques and human*. Human intelligence is the most powerful and valuable resource that needs to be well utilized in security analysis. Many microscopic tools, algorithms, and techniques are developed for specific purposes, but few macroscopic models or framework are provided to synthesize functions of these techniques, reduce the complexity of security problems and ease the cognition of human analysts. Therefore, we need to couple the available techniques to enhance cyber SA and construct a bridge between techniques and human analysts.

B. What is the main structure of SKRM?

Similar with the work by Tadda and Salerno[9], the key to construct SKRM is to identify relevant activities of interest. In terms of cyber SA, the activities of interest are mainly attacks, which may be associated with items ranging from business level processes, to network level applications and services, to operating system level entities, and finally to the lowest physical level devices (memory cells, disk sectors, registers, etc.). Based on this, the SKRM model is constructed, as shown in Figure 2.

SKRM model seamlessly integrates four abstraction layers of cyber situation knowledge, including *Workflow Layer, App/Service Layer, Operating System Layer* and *Instruction Layer*. As the layer goes down, information is presented in finer granularity in terms of technical details. These four layers are abstracted by categorizing isolated situation knowledge from different perspectives of network. Experts with expertise in different layers can communicate with each other on the same platform provided by SKRM.

Workflow layer is most human-understandable layer that mainly captures the mission or business processes within an organization or enterprise. Organizations take workflow management as the main technology for performing business processes [12]. A workflow typically consists of a number of tasks that are essential for fulfilling a business process.

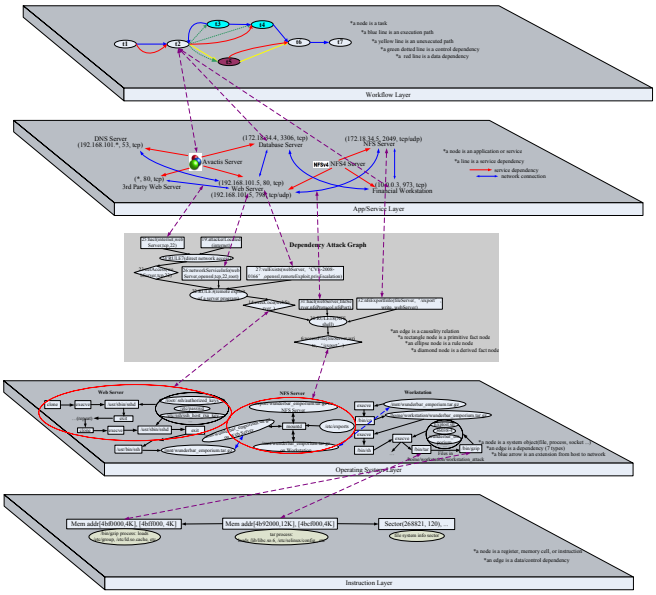

Figure 2. The Situation Knowledge Reference Model (SKRM)

Usually an organization keeps consistent and reliable workflows for their daily business. Attackers injecting malicious tasks or modifying data will cause abnormal behaviors in workflow. Therefore, workflow layer can enable cyber SA at business level. Workflow in this layer can be generated in two ways: either manually defined by business managers, or extracted from logs with workflow mining techniques [13], [14].

The function of business process relies on a variety application and services. A workflow can be divided into block tasks [15], which is actually a sub-workflow containing a set of atomic tasks. Therefore, the execution of a workflow depends on the execution of tasks, which then relies on corresponding application software. These applications have further dependence relationship on a set of services, such as web service, DNS service, etc. Therefore, *App/Service Layer* is incorporated into SKRM to capture the required applications and services for workflow execution, and the dependency relationship between them as well. Service discovery and dependency analysis techniques [16] can be applied to App/Service Layer.

Attackers compromise network by exploiting security holes existing in applications and services. These attacks will leave trace inside operating system, which could be deleted logs, prohibited access to password files, or abnormal system call patterns, etc. All these operating system objects, processes and files, as well as the dependency relationship between them, are included in *Operating System (OS) Layer*. Operating system layer usually adopts techniques of system level taint tracking [17] and intrusion recovery [18].

Instruction Layer can identify missed intrusions in operating system layer, and assist taint analysis and attack recovery at instruction level. Instruction layer maps the entities and

relationships on OS layer to memory cells, disk sectors, registers, kernel address space, and other devices. Techniques of intrusion harm analysis [19], including taint tracking and intrusion recovery, are often involved in instruction layer.

Attack Graph is not a specific layer in this stack, but rather an interconnection technique between App/Service Layer and Operating System Layer. By analyzing the vulnerabilities exist in the applications and services, attack graph can generate potential attack paths for the entire network. Through the attack paths, security analysts will know which hosts are most dangerous and need to be further scrutinized. Moreover, the corresponding system objects related to the vulnerable services or applications will be highlighted.

C. How can SKRM enable cyber situation awareness?

SKRM model is not simply a mapping of situation knowledge in different areas to the above abstraction layers. It is in fact an integration of data, information, algorithms and tools, and human knowledge through cross-layer interaction. It interconnects the perception level elements to elevate awareness to comprehension, projection, and resolution levels. SKRM model has the following characteristics that could enable the four levels of situation awareness:

1) Each abstraction layer generates a graph that covers the entire enterprise network. This ensures completeness of the overall network environment awareness.

2) Each abstraction layer views the same network from a different perspective and at a different granularity. These perspectives complement, assist and confirm each other for more accurate situation awareness.

3) Each abstraction layer leverages current available algorithms, tools, and techniques in its corresponding area to extract the most critical and useful information to present to human security analysts. Such techniques include but are not limited to workflow mining and attack recovery, service discovery and dependency analysis, system level taint tracking and recovery, and instruction level intrusion harm analysis, etc. Future developed algorithms, tools, or techniques can also be incorporated into SKRM to elevate its capability.

4) Cross-layer analysis is the *soul* of SKRM. SKRM captures cross-layer relationships by mapping, translating, bridging semantic gaps, and utilizing existing techniques such as attack graph. Performing *top-down, bottom up, and U-shape* cross-layer analysis can enhance the comprehension, projection and resolution levels of security analysts SA. For example, when business level abnormality such as financial loss is noticed, *top-down* analysis could find the damage caused by attackers in each abstraction layer: which service is compromised, which system file is deleted, or which memory cell is tainted, etc. This is an instance of *damage assessment*, corresponding to *comprehension level SA*. On the other hand, if an IDS alert is raised from operating system layer, a bottom-up analysis will find out how could the attack have future impact on the business level. This can be viewed as example of *impact assessment* or *threat assessment*, corresponding to *projection level SA*. If options of security measures and their corresponding impact are obtained through either bottom up or U-shape analysis, *resolution level SA* is achieved.

V. Conclusion

To achieve cyber situation awareness, the role of human cyber analysts should be considered explicitly into the design of security tools, algorithm, and techniques, such as attack graph. Therefore, based on existing theories of situation awareness, a cyber SA model and an embedded SKRM model are constructed to enhance the coupling of current techniques to situation awareness to enable security analysts' effective analysis of complex cyber-security problems. Current and future work is to demonstrate the potential capabilities of SKRM model for enabling cyber situation awareness.

VI. Acknowledgement

This work was supported by ARO W911NF-09-1-0525 (MURI), NSF CNS-0905131, and AFOSR W911NF1210055.

References

[1] C. Dominguez, "Can sa be defined," *Situation Awareness: Papers and Annotated Bibliography*, pp. 5,15, 1994.
[2] M. L. Fracker, "A theory of situation assessment: Implications for measuring situation awareness," in *Human Factors and Ergonomics Society Annual Meeting Proceedings*, vol. 32, 1988, p. 102-106.
[3] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, p. 32-64, 1995.
[4] J. J. Salerno, M. L. Hinman, and D. M. Boulware, "A situation awareness model applied to multiple domains," *Proceedings of SPIE*, vol. 5813, 2005.
[5] B. McGuinness and L. Foy, "A subjective measure of SA: the crew awareness rating scale (CARS)," in *Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia*, 2000.
[6] D. S. Alberts, J. J. Garstka, R. E. Hayes, and D. A. Signori, "Understanding information age warfare," DTIC Document, Tech. Rep., 2001.
[7] J. R. Boyd, "The essence of winning and losing," *Lecture notes*, 1996.
[8] I. Witthen and E. Frank, *Data Mining - Practical Machine Learning Tools and Techniques With Java Implementations*. New York and San Mateo, CA: Morgan Kaufmann Publishers, Academic Press, 2000.
[9] G. P. Tadda and J. S. Salerno, "Overview of cyber situation awareness," *Cyber Situational Awareness*, p. 1535, 2010.
[10] M. R. Endsley, "Theoretical underpinnings of situation awareness: A critical review," *Situation awareness analysis and measurement*, p. 332, 2000.
[11] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning *et al.*, "Cyber SA: situational awareness for cyber defense," *Cyber Situational Awareness*, pp. 3,13, 2010.
[12] M. Yu, P. Liu, and W. Zang, "Self-healing workflow systems under attacks," in *24th International Conference on Distributed Computing Systems*, 2004.
[13] W. Van der Aalst, B. van Dongen, J. Herbst, L. Maruster, G. Schimm, and A. Weijters, "Workflow mining: a survey of issues and approaches," *Data & Knowledge Engineering*, vol. 47, 2003.
[14] W. M. P. Van der Aalst, A. Weijters, and L. Maruster, *Workflow mining: Which processes can be rediscovered*. Citeseer, 2002.
[15] W. Van der Aalst, T. Weijters, and L. Maruster, "Workflow mining: Discovering process models from event logs," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, 2004.
[16] X. Chen, M. Zhang, Z. M. Mao, and P. Bahl, "Automating network application dependency discovery: Experiences, limitations, and new solutions," in *8th USENIX OSDI*, 2008.
[17] S. T. King and P. M. Chen, "Backtracking intrusions," in *ACM SIGOPS Operating Systems Review*, vol. 37, 2003, p. 223236.
[18] X. Xiong, X. Jia, and P. Liu, "SHELF: preserving business continuity and availability in an intrusion recovery system," in *ACM ACSAC'09.*
[19] S. Zhang, X. Jia, P. Liu, and J. Jing, "Cross-layer comprehensive intrusion harm analysis for production workload server systems," in *ACM ACSAC'10.*