Application for Network Security Situation Awareness

Pallavi Vaidya
Department of Information Technology
Vidyalankar Institute of Technology
Wadala Mumbai India

S. K. Shinde
Lokmnya Tilak college of Engineering
Kopar Khirane Navi Mumbai
India

ABSTRACT
This paper is based on the Network security situation awareness. It describes the framework designed to generate security graph. The proposed framework is easy to install and provides protection against denial of service and distributed denial of service attacks. It also displays security analysis of the sensors attached to the network

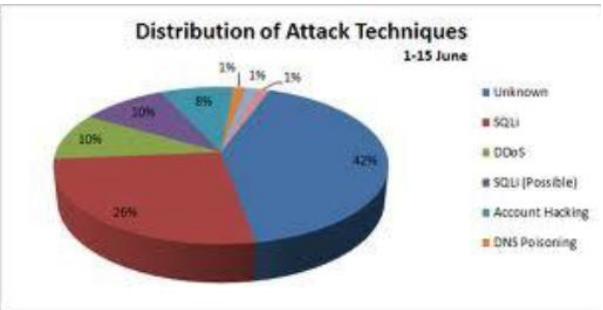
General Terms
Security, Network security situation awareness, Data fusion, D-S evidence theory.

Keywords
Network security situation awareness graph, Knowledge discovery

1. INTRODUCTION
In most organizations currently, a security management process consists of three independent domains; physical security domain, managerial security domain and technical security domain. It is very difficult to link these domains as the manager and managed objects are different although the security system is under the same governing structure. In other words, even when each security system is properly established, it is difficult to prevent or respond the security accident enterprise-wide when vulnerability is generated in a domain. Therefore, managing these three domains from the integrated viewpoint is needed to prevent or respond security accidents, and such security is called convergence. Situation Awareness is one of the key requirements for effective management of complex or geographically dispersed activities or events. Examples include defense activities, such as area surveillance, command and control, network-centric operations and asset protection, and many civilian activities, such as crisis management, event management and transport logistics. Situation awareness may apply, for instance, to the functionality, availability, capacity, data security, and alteration and development of networks and services. These aspects may refer to the following types of information, for example:

- Situation awareness regarding functionality comprises awareness of faults and disturbances as well as awareness of the interconnectivity of networks.
- Situation awareness regarding availability comprises awareness of networks' geographical coverage and service availability areas.
- Situation awareness regarding capacity may indicate network capacity and its adequacy or, on a more general level, the ability to provide certain communications services.
- Situation awareness regarding development and change indicates structural changes planned for networks and services or development prospects and needs.
- Situation awareness regarding data security comprises information about data security threats targeting the networks and services. [1]

2. PROBLEMS WITH NETWORK SECURITY
Along with the popularization of network, the threat it faces is growing bigger, for example, computer virus, Trojan horse program and DoS/DDoS attack are increasingly rampant.



According to Kasperskey survey, DDoS attacks were launched from computers located in 201 countries around the world in the year 2011. So as to guarantee the smooth running of network, presently adopted traditional technology of intrusion detection, firewall and virus detection are all in passive defense way and in independent working status, therefore, they don't have cognition on the network resource they are protecting for. And this cognition disjunction increases the time needed for operator to make a decision for alarm raised, and therefore, misses the optimal timing of handling. There exist several difficulties when implementing network security situation awareness.

1. The amount of alert events generated from various security sensors is tremendous and the false positive rate is too high.

2. The trivial alerts generated from large scale network attacks (e.g. DDoS) are very complex and the relationships among them are difficult to determine.
3. The data type of alert events generated from security sensors are very abundant, while there is a lack of knowledge needed by alert processing, and automatically acquiring these knowledge is rather difficult. [2]

3. EXISTING SYSTEM

Because network security situation technology is a newly emerging one, domestic and overseas research on this field is still at starting stage, and related research results are less common. Some research is based on information warfare ground situation awareness and some other emphasizes on improvement on traditional intrusion detection model.

Network security has been the eternal hot research spot, and it has undergone three phases: defense, detection and fault. However, there are still some security problems left, such as the complicated structure, and the kittle network attacks, so the network security issues are becoming more and more austere. The existed professional network security means, like IDS, Firewall and VDS can not reflect the security status of the network. Research on network security situational awareness makes elementary progress, but it still needs to refer to the mature theories and techniques of situational awareness applied in other fields. [8][9][12][14]

4. PROPOSED SYSTEM

The proposed project work summarizes the research progress of network security situation awareness, propose a framework for network security situation awareness based upon knowledge discovery, and apply the framework to the network security situation awareness system (Net-SSA). In this proposed system, we analyzed the existing problems of network security situation awareness and proposed a framework based on knowledge discovery. The framework consists of the modeling of network security situation and the whole process of the generation of network security situation. We have described the construction of the formal model for network security situation measurement based upon the D-S evidence theory, the extraction the frequent patterns and sequential patterns from the dataset of network security situation based upon knowledge discovery method and the transformation of these patterns to the correlation rules of network security situation, and the automatic generation of network security situation graph. We also present the application of the Net-SSA and show that the proposed framework supports for the accurate modeling and effective generation of network security situation.[15]

5. NETWORK SECURITY

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

5.1 Network security concepts

Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password, which is something the user 'knows'— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high-level analysis.

Communication between two hosts using a network may be encrypted to maintain privacy.

Honey pots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honey pots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honey pot.

5.2 Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

6. DATA MINING

Data mining (the analysis step of the knowledge discovery in databases process,[1] or KDD), a relatively young and interdisciplinary field of computer science[2][3] is the process of discovering new patterns from large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics and database systems.[2] The overall goal of the data mining process is to extract knowledge from a data set in a human-understandable structure[2] and besides the raw analysis step involves database and data management

aspects, data preprocessing, model and inference considerations, interestingness metrics, complexity considerations, post-processing of found structure, visualization and online updating.

The actual data mining task is the automatic or semi-automatic analysis of large quantities of data to extract previously unknown interesting patterns such as groups of data records (cluster analysis), unusual records (anomaly detection) and dependencies (association rule mining). This usually involves using database techniques such as spatial indexes. These patterns can then be seen as a kind of summary of the input data, and used in further analysis or for example in machine learning and predictive analytics. For example, the data mining step might identify multiple groups in the data, which can then be used to obtain more accurate prediction results by a decision support system.

The related terms data dredging, data fishing and data snooping refer to the use of data mining methods to sample parts of a larger population data set that are (or may be) too small for reliable statistical inferences to be made about the validity of any patterns discovered. These are used for large data populations.

7. KNOWLEDGE DICOVERY

Knowledge discovery is a concept of the field of computer science that describes the process of automatically searching large volumes of data for patterns that can be considered knowledge about the data. It is often described as deriving knowledge from the input data. This complex topic can be categorized according to 1) what kind of data is searched; and 2) in what form is the result of the search represented. Knowledge discovery developed out of the Data mining domain, and is closely related to it both in terms of methodology and terminology.

The most well-known branch of data mining is knowledge discovery, also known as Knowledge Discovery in Databases (KDD). Just as many other forms of knowledge discovery it creates abstractions of the input data. The knowledge obtained through the process may become additional data that can be used for further usage and discovery.

Another promising application of knowledge discovery is in the area of software modernization which involves understanding existing software artifacts. This process is related to a concept of reverse engineering. Usually the knowledge obtained from existing software is presented in the form of models to which specific queries can be made when necessary. An entity relationship is a frequent format of representing knowledge obtained from existing software. Object Management Group (OMG) developed specification Knowledge Discovery Met model (KDM) which defines ontology for the software assets and their relationships for the purpose of performing knowledge discovery of existing code. Knowledge discovery from existing software systems, also known as software mining is closely related to data mining, since existing software artifacts contain enormous business value, key for the evolution of software systems. Instead of mining individual data sets, software mining focuses on metadata, such as database schemas.

8. SELECTION OF PLATFORM

Windows® XP provides the most dependable version of Windows ever—with the best security and privacy features Windows has ever provided. Overall, security has been improved in Windows XP to help you have a *safe, secure, and private* computing experience. Windows XP is available in two editions—Windows XP Home Edition for home use, and Windows XP Professional for businesses of all sizes. Security features in Windows XP Home Edition make it even safer for you to shop and browse on the Internet. Windows XP Home Edition comes with built-in Internet Connection Firewall software that provides you with a resilient defense to security threats when you're connected to the Internet—particularly if you use always-on connections such as cable modems and DSL. Windows XP Professional includes all of the security capabilities of Windows XP Home Edition, plus other security management features. These important new security features will reduce your IT costs and enhance the security of your business systems. Windows XP Home Edition security services have been designed to be flexible, and take into account a wide variety of security and privacy situations that you'll face as a home user. If you are already familiar with the security model in Microsoft® Windows NT® version 4.0 and Microsoft® Windows® 2000, you will recognize many of the security features in Windows XP Home Edition. At the same time, you will also find a number of familiar features that have changed significantly, along with new features that will improve your ability to manage system security. For example, if you use the Internet to chat online or to send and receive e-mail, you may be vulnerable to hacker attacks. To protect you from these threats, Windows XP has incorporated enhanced security features that make your online experience even safer. Let's take a look at the important security and privacy features in Windows XP Home Edition that make you and your information more secure while you're having the most productive Windows user experience ever. Windows XP Professional includes a number of features that businesses can use to protect selected files, applications, and other resources. These features include access control lists (ACLs), security groups, and Group Policy—in addition to the tools that allow businesses to configure and manage these features. Windows XP offers thousands of security-related settings that can be implemented individually. The Windows XP operating system also includes predefined security templates, which businesses can implement without modifications or use as the basis for a more customized security configuration. Businesses can apply these security templates when they:

- Create a resource, such as a folder or file share, and either accept the default access control list settings or implement custom access control list settings.
- Place users in the standard security groups, such as Users, Power Users, and Administrators, and accept the default ACL settings that apply to those security groups.
- Use the Basic, Compatible, Secure, and Highly Secure Group Policy templates that have been provided with the operating system.

Each of the Windows XP security features—ACLS, security groups, and Group Policy—have default settings that can be modified to suit a particular organization. Businesses can also make use of relevant tools to implement and modify access control. Many of these tools, such as the Microsoft Management Console snap-ins, are components of Windows XP Professional. Other tools are included with the Windows XP Professional Resource Kit.

9. SELECTION OF LANGUAGE

For the implementation of this application flexible system implementation language is needed. Compilation should be relatively straightforward compiler, provide low-level access to memory, provide language constructs that map efficiently to machine instructions, and require minimal run-time support. Program should be compiled for a very wide variety of computer platforms and operating systems with minimal change to its source code. For Graphical User Interface programming, language chosen must be simple to uses, secure, architecture neutral and portable. Additional requirements of GUI are: 1) User interface management: Windows, menus, toolbars and other presentation components be supported by the language.2) Data and presentation management: language must contains a rich toolset for presenting data to the user and manipulating that data. 3) The Editor: The language should have a editor, a powerful and extensible toolset for building custom editors. 4) The Wizard framework: A toolset for easily building extensible, user-friendly Wizards to guide users through more complex tasks. 5) Configuration management: Rather than tediously write code to access remote data and manage and save user-configurable settings, etc., Java handles all this effectively.

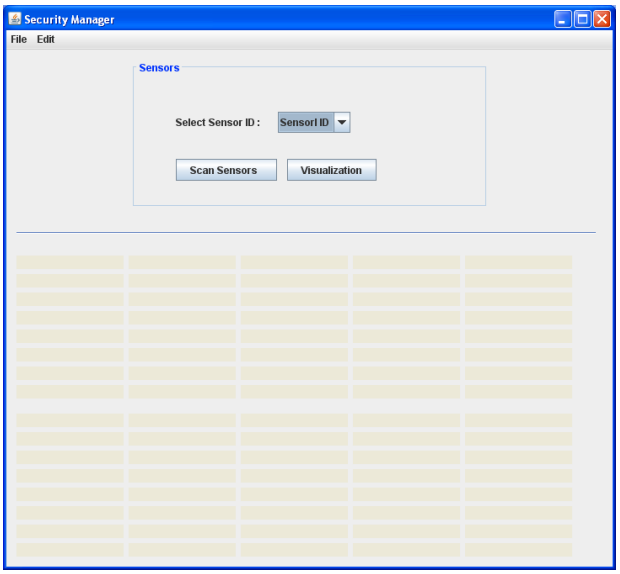
10. APPLICATION

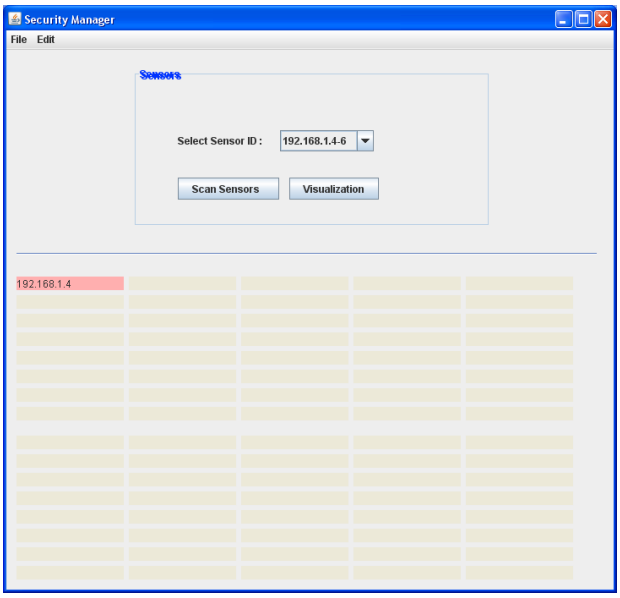
The application has three modules: Data processing server, KD agent and security expert. Data processing runs at the server side. It collects data and analyzes. KD agent runs at client side and sends s necessary information to the server. Security expert is a human interaction provided to decide the trusted and untrusted source. The drawback of any automated DSS is there is no human interaction. For implementation of this application flexible system, implementation language is needed. Compilation should be relatively straightforward compiler, provide low-level access. Hence Java is the better platform.

11. IMPLEMETATION

11.1 Data processing module

As it runs on the server it need s to collect all the information coming from the sensors connected to it. It scans the sensors connected to it.





11.2 KD agent

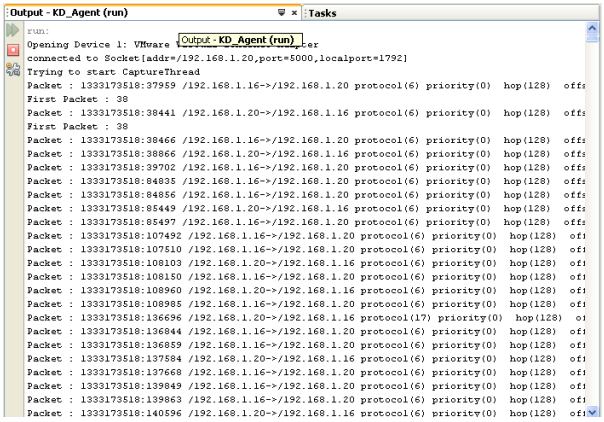
KD agent scans all the sensors and collects the information about activities in network. It is based on following steps:

11.2.1 Event simplification

It captures all the events and deletes redundant events.

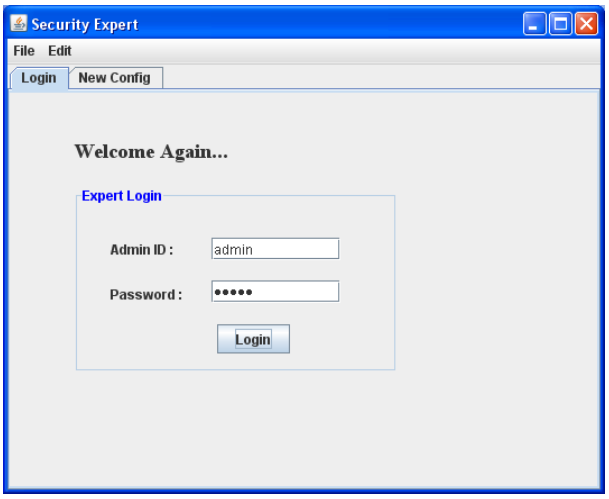
11.2.2 Event fusion

It depends on the D-S evidence theory of belief. This ensures that the false positive and false negative events are removed.[1][2][6][7] The following information is displayed as the output.

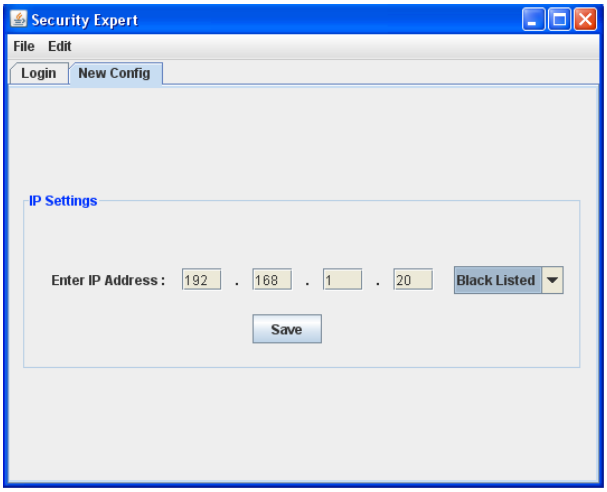


11.3 Security expert

This is the human factor added by this module. Here security expert can make decision. Security expert is a person who is given with administrative rights should be given to the person who is properly trained so that the social engineering attack can be avoided. To provide precautionary measures, Login name and password can be included. To provide mo re security administrator can be asked to change password periodically.



Security expert can update rules.



CONCLUSION

In this paper, we analyzed the existing problems of network security situation awareness [1] [3] and proposed a framework based on knowledge discovery. [4] The framework consists of the modeling of network security situation and the whole process of the generation of network security situation. We have described the construction of the formal model for network security situation measurement based upon the D-S evidence theory, the extraction the frequent patterns and sequential patterns from the dataset of network security situation based upon knowledge discovery method and the transformation of these patterns to the correlation rules of network security situation, and the automatic generation of network security situation graph. [4]. As this study continues, we plan to explore assessment of global security the problems of real-time predication of upcoming severe security attacks. [15]

12. ACKNOWLEDGMENTS

Our thanks to the Vidyalankar Institute of Technology for supporting and Prof. Avinash Shrivas who gave expert advice.

13. REFERENCES

[1] Bass, T., "Multi sensor Data Fusion for Next Generation Distributed Intrusion Detection Systems," Invited Paper 1999 IRIS National Symposium on Sensor and Data Fusion, pp.24-27, May 1999.

[2] Bass, T., "Intrusion Detection Systems and Multisensor Data Fusion," Communications of the ACM, Vol. 43, No. 4, April 2000.

[3] Endsley, M., "Toward a theory of situation awareness in dynamic systems, " Human Factors, Vol. 37, No.1, pp.32-64, 2005.

[4] Lai Jibao, Wang Huiqiang, and Zhu Liang, "Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory," 2006.

[5] Liu Mixi, Yu Dongmei and Zhang Qiuyu et aI., "Network Security Situation Assessment Based on Data Fusion, " 2008 Workshop on Knowledge Discovery and Data Mining, 2008.

[6] Yu Dong and Frincke, D., "Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory, " 43rd ACM Southeast Conference, March 18-20, 2005.

[7] Wang Huiqiang, Lai Jibao, and Ying Liang, "Network Security Situation Awareness Based on Heterogeneous Multi-Sensor Data Fusion and Neural Network, " Second International Multisymposium on Computer and Computational Sciences, 2007.

[8] Stefanos Manganaris, Marvin Christensen, Dan Zerkle, et al. A data mining analysis of RTID alarms. Computer Networks, 2000, 34(4):571-577

[9] Bass, T. and Robichaux, R., "Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations," Proceedings of IEEE Military Communications Conference, vol.1, pp.64-70, 200 I.

[10] Zhang Yong, Tan Xiaobin and Xi Hongsheng, "A Novel Approach to Network Security Situation Awareness Based on MUlti-perspective Analysis, " IEEE 2007 International Conference on Computational Intelligence and Security, 2007.

[11] Chen XZ, Zheng QH and Guan XH et aI., "Quantitative hierarchical threat evaluation model for network security, " Journal of Software, Vol. 17 , No.4, pp.885-897, April 2006, http://www.jos.org.cn/lOOO- 9825/17/885.htm, Accessed on Jun 2008.

[12] J Hall, J Pei, Y Yin. Mining frequent patterns without candidate generation. 2000 ACM. SIGMOD int'I Conf on Management of Data (SIGMOD'OO), DallaS, TX, 2000

[13] Mika Klemettinen. A knowledge discovery methodology for telecommunication network alarm databases. [Ph 0 dissertation]. Helsinki: University of Helsinki, Finland, 1999

[14] Haines JW, Lippmann RP, Fried OJ, Tran E, Boswell S, Zissman MA. DARPA intrusion detection system evaluation: Design and procedures. Technical Report 1062, Lexington: MIT Lincoln Laboratory, 1999.

[15] Lang F, Wang C, Gouqing M." A Framework for network security situation awareness based on knowledge discovery" 2010 2nd International conference on computer Engineering and Technology