网络安全态势感知所依赖的原始测量数据可以来源于不同型号、不同实现技术、不同开发与生产者的网络运行管理系统、网络安全管理系统、主机管理系统和应用管理系统,这些系统产生异构的运行监测数据和日志数据,需要采用流式数据处理方式在不同的时间窗口内完成融合处理任务.目前,这方面的研究明显是不够的,现有的大数据分析技术虽然可以提供一定的支持与借鉴,但这些方法对态势觉察的适用性还需要有针对性的研究.

(2) 不完全信息条件下的活动辨识

这个问题是指在测量系统存在漏报、误报以及信息缺失的前提下,如何尽可能准确地辨识出网络中存在的活动.这类研究可以认为是源自网络入侵检测领域,但在网络安全态势感知的范畴中被赋予了更为广泛的含义.互联网的流量具有重尾的特性,传统的研究往往关注流量行为的典型部分和主要部分,例如像流量分类,但在态势觉察中,不仅这些部分需要关注,小流量的零星行为也需要专注,例如 APT 检测的需要,而且不完全信息条件下这类活动的辨识更为困难.因此,这个领域需要更为精细的测量数据关联性分析方法.

(3) 网络活动的语义计算

从目前的实践看,网络攻击的意图识别基本上是手工完成的,即需要依靠人工经验的判断.鉴于人的能力约束和相关人力资源的不足,这种人工实现方式给网络安全态势感知的大规模应用带来极大的限制.因此,很有必要研究网络活动特征提取和意图识别的机器处理方法,以提高网络安全态势感知系统的自治能力.尽管网络入侵防范系统 IPS 领域的工作可以提供一定的基础,但从实现不同时间粒度的网络安全态势感知以满足从毫秒级攻击自动响应到 APT 检测的不同需要的角度看,都是远远不够的.

(4) 网络态势的可视化

网络安全态势感知所处理的海量异构测量数据及其处理结果需要有合适的表示方式来加以表达和应用,可视化技术是一个公认的可行支持.HSARPA 在它的战略研究计划中也提到需要研究可扩展的可视化方法来支持态势感知数据的使用,包括带准确地理定位的可视化方法、支持 Drill-down 的可视化分析方法以及适合不同用户使用和表达不同内容的可视化技术.

(5) 网络安全态势感知的协同

网络空间安全需要全球合作,至少在国家的层面要求合作的网络安全态势感知系统之间具有协同能力,就像 HSARPA 规划中所要求的那样.如果参照网络入侵检测领域的相关研究,对于合作机制的要求至少包括配置互操作性(即合作各方具有信息交换能力),需要有类似 SNMP 和 IPFIX 这样的标准协议;共享信息的语法互操作性,需要有类似 IDMEF 的标准数据结构;以及语义互操作性,例如描述网络安全态势的标准测度及其取值,这在网络入侵检测领域还是空白.此外,由于合作各方可能存在信息访问限制,如何实现信息共享与隐私保护的平衡把握,是需要研究的问题.

(6) 更为完善的态势投射方法

目前的态势投射方法基本都是静态的,不能适应网络安全态势感知的过程需要,因此需要研究相应的动态态势投射方法,例如基于非合作不完全信息动态博弈理论设计附带预警能力的态势投射方法.

6 结 论

网络安全态势感知包括网络安全态势觉察、网络安全态势理解和网络安全态势投射这 3 个层面,是一个完整的认知过程.它不仅仅是将网络中的安全要素进行简单的汇总和叠加,而是根据不同的用户需求,以一系列具有理论支撑的模型为支持,找出这些安全要素之间的内在关系,实时地分析网络的安全状况.

网络安全态势感知是网络安全领域的研究热点,尽管已经得到较长时间的关注,但仍未形成完整的体系和明确一致的目标.在现有的网络安全态势感知的研究中,将其视为网络安全事件应用大数据处理和可视化技术的汇总结果的观点和将其视为基于网络安全事件融合计算的网络安全状态量化表达的观点,都没有完整地反映其目标和任务;将其视为网络安全监测实现形式的观点则不够准确.为此,本文对网络安全态势感知概念进行重新定义,试图给出一个更为完整、清晰的描述,以期抛砖引玉.

目前,网络安全态势感知的研究是一个正处于发展中的课题,大部分研究都集中在重构攻击活动方面,基本都是网络入侵检测领域研究的延伸,已有很好的基础但也有很多问题需要研究和解决.另一方面,包括网络测量、网络流量行为学、网络管理技术、大数据处理技术、流式数据处理技术、可视化技术在内的其他相关领域的发展也为网络安全态势感知的研究提供了积极的支持.尽管网络安全态势感知的研究仍处于初级阶段,但是,随着各种相关技术和研究的不断完善,网络安全态势感知技术将走向成熟和实用,为保障网络的安全起到越来越重要的作用.

致谢 本文的匿名评阅者对文章内容,特别是对网络安全态势感知定义的完善提出了许多建设性的意见和建议,作者在此一并表示感谢.

References:

[1] Wang HQ, Lai JB, Zhu L, Liang Y. Survey of network situation awareness system. Journal of Computer Science, 2006,33(10):5−10 (in Chinese with English abstract).

[2] Bass T. Intrusion detection systems and multisensor data fusion: Creating cyberspace situational awareness. Communications of the ACM, 2000,43(4):99−105. [doi: 10.1145/332051.332079]

[3] Endsley MR. Toward a theory of situation awareness in dynamic system. Human Factors, 1995,37(1):32−64. [doi: 10.1518/001872095779049543]

[4] Franke U, Brynielsson J. Cyber situational awareness a systematic review of the literature. Computers & Security, 2014,46:18−31. [doi: 10.1016/j.cose.2014.06.008]

[5] Lenders V, Tanner A, Blarer A. Gaining an edge in cyberspace with advanced situational awareness. Security & Privacy IEEE, 2015,13(2):65−74. [doi: 10.1109/MSP.2015.30]

[6] Bearavolu R, Lakkaraju K, Yurcik W, Raje H. A visualization tool for situational awareness of tactical and strategic security events on large and complex computer networks. In: Proc. of the Military Communications Conf. (MILCOM 2003). IEEE, 2003. 850−855. [doi: 10.1109/MILCOM.2003.1290234]

[7] Erbacher RF, Frincke DA, Wong PC, Moody S, Fink G. A multiphase network situational awareness cognitive task analysis. Information Visualization, 2010,9(3):204−219. [doi: 10.1057/ivs.2010.5]

[8] Erbacher RF, Frincke DA, Wong PC, Moody S, Fink G. Cognitive task analysis of network analysts and managers for network situational awareness. Proc. of the SPIE Int'l Society for Optical Engineering, 2010,7530(1):423–426. [doi: 10.1117/12.845488]

[9] Government of Canada, Public Safety Canada. Canada's cyber security strategy. 2010. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

[10] Bass T, Gruber D. A glimpse into the future of id. The Magazine of USENIX & SAGE, 1999,24(3):40–49

[11] Chen P, Desmet L, Huygens C. A study on advanced persistent threats. In: Proc. of the IFIP. 2014. 63−72. [doi: 10.1007/978-3-662-44885-4_5]

[12] Mandiant. APT1: Exposing One of China's Cyber Espion age Unit. 2013. http://www.cfr.org/china/mandiant-apt1-exposing-one-chinas-cyber-espionage-units/p30020

[13] Chen XZ, Zheng QH, Guan XH, Lin CG. Quantitative hierarchical threat evaluation model for network security. Ruan Jian Xue Bao/Journal of Software, 2006,17(4):885−897 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/885.htm

[14] Xi RR, Yun XC, Zhang YZ, Hao ZY. An improved quantitative evaluation method for network security. Chinese Journal of Computers, 2015,38(4):749−758 (in Chinese with English abstract).

[15] Xin D, Gai WL, Wang L, Liu X, Hu JB. Survey of cyberspace situation awareness model. Journal of Computer Applications, 2013, 33(S2):245−250 (in Chinese with English abstract).

[16] Gong ZH, Zhuo Y. Research on cyberspace situational awareness. Ruan Jian Xue Bao/Journal of Software, 2010,21(7):1605−1619 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3835.htm [doi: 10.3724/SP.J.1001.2010.03835]

[17] Tadda GP, Salerno JS. Overview of cyber situation awareness. Springer US, 2010,46:15−35.

[18] Liu XW, Wang HQ, Lü HW, Yu JG, Zhang SW. Fusion-Based cognitive awareness-control model for network security situation. Ruan Jian Xue Bao/Journal of Software, 2016,27(8):2099−2114 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4852.htm [doi: 10.13328/j.cnki.jos.004852]

[19] Endsley MR. Final reflections: Situation awareness models and measure. Journal of Cognitive Engineering and Decision Making, 2015,9(1):101−111. [doi: 10.1177/1555343415573911]

[20] Endsley M. Situation awareness misconceptions and misunderstandings. Journal of Cognitive Engineering & Decision Making, 2015,9(1):4−32. [doi: 10.1177/1555343415572631]

[21] Goodall JR. Introduction to visualization for computer security. In: Proc. of the VizSEC. 2007. 1−17. [doi: 10.1007/978-3-540-78243-8_1]

[22] Erbacher R. Visualization design for immediate high-levelsituational assessment. Proc. of the ACM Int'l Conf. on Proc. Series, 2012,9(4):17−24. [doi: 10.1145/2379690.2379693]

[23] Shiravi H, Shiravi A, Ghorbani AA. A survey of visualization systems for network security. IEEE Trans. on Visualization and Computer Graphics, 2012,18(8):1313−1329. [doi: 10.1109/TVCG.2011.144]

[24] Cuppens F, Ortalo R. Lambda: A language to model a database for detection of attacks. In: Proc. of the 3rd Int'l Workshop on Recent Advances in Intrusion Detection (RAID 2000), Vol.1907. 2000. 197−216. [doi: 10.1007/3-540-39945-3_13]

[25] Bhatt P, Yano ET, Gustavsson PM. Towards a framework to detect multi-stage advanced persistent threats attacks. In: Proc. of the IEEE Int'l Symp. on Service Oriented System Engineering. 2014. 390−395. [doi: 10.1109/SOSE.2014.53]

[26] Roschke S, Cheng F, Meinel C. A new alert correlation algorithm based on attack graph. CISIS, 2011,6694(11):58−67. [doi: 10.1007/978-3-642-21323-6_8]

[27] Albanese M, Pugliese A, Subrahmanian VS. Scalable detection of cyber attacks. CISIM, 2011,245:9−18. [doi: 10.1007/978-3-642-27245-5_4]

[28] Mathew S, Upadhyaya S, Sudit M, Stotz A. Situation awareness of multistage cyber attacks by semantic event fusion. In: Proc. of the Military Communications Conf. 2010. 1286−1291. [doi: 10.1109/MILCOM.2010.5680121]

[29] Aleroud A, Karabatis G, Sharma P, He P. Context and semantics for detection of cyber attacks. Int'l Journal of Information & Computer Security, 2014,6(1):63−92. [doi: 10.1504/IJICS.2014.059791]

[30] Hutchins EM, Cloppert MJ, Amin RM. Intelligence driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: Proc. of the ICIW. 2011. 113−127.

[31] Julisch K. Clustering intrusion detection alarms to support root cause analysis. ACM Trans. on Information and System Security, 2003,6(4):443−471. [doi: 10.1145/950191.950192]

[32] Salah S, Maciá-Fernández G, Díaz-Verdejo JE. A model-based survey of alert correlation techniques. Computer Networks, 2013, 57(5):1289−1317. [doi: 10.1016/j.comnet.2012.10.022]

[33] Ourston D, Matzner S, Stump W, Hopkins B. Applications of hidden Markov models to detecting multi-stage network attacks. In: Proc. of the Hawaii Int'l Conf. on System Sciences. 2003. 9: 73−76. [doi: 10.1109/HICSS.2003.1174909]

[34] Katipally R, Yang L, Liu A. Attacker behavior analysis in multi-stage attack detection system. In: Proc. of the 7th Workshop on Cyber Security & Information Intelligence Research. 2011. 1−4. [doi: 10.1145/2179298.2179369]

[35] Ning P, Cui Y, Reeves DS. Constructing attack scenarios through correlation of intrusion alerts. In: Proc. of the 9th ACM Conf. on Computer &Communications Security. 2002. 245−254. [doi: 10.1145/586110.586144]

[36] Lin Z, Li S, Ma Y. Real-Time intrusion alert correlation system based on prerequisites and consequence. In: Proc. of the Int'l Conf. on Wireless Communications Networking and MobileComputing (WiCOM 2010). 2010. 1−5. [doi: 10.1109/WICOM.2010.5601285]

[37] Katipally R, Gasior W, Cui X, Yang L. Multistage attack detection system for network administrators using data mining. In: Proc. of the 6th Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW 2010). 2010. 1−4. [doi: 10.1145/1852666.1852722]

[38] Sadoddin R, Ghorbani AA. Real-Time alert correlation using stream data mining techniques. In: Proc. of the AAAI Conf. on Artificial Intelligence. 2008. 1731−1737.

[39] Katipally R, Gasior W, Cui X, Yang L. Multistage attack detection system for network administrators using data mining. In: Proc. of the 6th Annual Workshop on Cyber Security and Information Intelligence Research. New York: ACM, 2010. Article 51. [doi: 10.1145/1852666.1852722]

[40] Zhu B, Ghorbani AA. Alert correlation for extracting attack strategies. Int'l Journal of Network Security, 2006,3(3):244−258.

[41] Bateni M, Baraani A, Ghorbani AA. Using artificial immune system and fuzzy logic for alert correlation. Int'l Journal of Network Security, 2013(15):160−174.

[42] Wang CH, Chiou YC. Alert correlation system with automatic extraction of attack strategies by using dynamic feature weights. Int'l Journal of Computer and Communication Engineering, 2016,5(1):1−10. [doi: 10.17706/IJCCE.2016.5.1.1-10]

[43] de Alvarenga SC, Zarpel BB, Miani RS. Discovering attack strategies using process mining. In: Proc. of the 11th Advanced Int'l Conf. on Telecommunications. 2015. 119−125. [doi: 10.13140/RG.2.1.4524.4008]

[44] Qin XZ, Lee W. Statistical causality analysis of Infosec alert data. In: Proc. of the Int'l Symp. on Recent Advances in Intrusion Detection (RAID), Vol.2820. 2003. 73−93. [doi: 10.1007/978-3-540-45248-5_5]

[45] Zhai Y, Ning P, Iyer P, Reeves DS. Reasoning about complementary intrusion evidence. In: Proc. of the Computer Security Applications Conf. 2004. 39−48. [doi: 10.1109/CSAC.2004.29]

[46] Saad S, Traore I, Brocardo ML. Context-Aware intrusion alert verfication approach. In: Proc. of the Int'l Conf. on Information Assurance & Security. 2015. 53−59. [doi: 10.1109/ISIAS.2014.7064620]

[47] Alserhani F, Akhlaq M, Awan IU, Cullen AJ, Mirchandani P. MARS: Multi-Stage attack recognition system. IEEE Int'l Conf. on Advanced Information Networking & Applications, 2010,4(4):753−759. [doi: 10.1109/AINA.2010.57]

[48] Ning P, Xu DB, Healey CG, Amant RS. Building attack scenarios through integration of complementary alert correlation methods. In: Proc. of the NDSS. 2004. 97−111.

[49] Yanga SJ, Stotzb A, Holsoppleb J, Suditc M, Kuhld M. High level information fusion for tracking and projection of multistage cyber attacks. Information Fusion, 2009,10(1):107−121. [doi: 10.1016/j.inffus.2007.06.002]

[50] Saad S, Traore I. A semantic analysis approach to manage ids alerts flooding. In: Proc. of the Int'l Conf. on Information Assurance & Security. 2011. 156−161. [doi: 10.1109/ISIAS.2011.6122812]

[51] Sadighian A, Fernandez JM, Lemay A, Zargar ST. ONTIDS a highly flexible context-aware and ontology-based alert correlation framework. In: Proc. of the Revised Selected Papers of Int'l Symp. on Foundations & Practice of Security, Vol.8352. 2013. 161−177. [doi: 10.1007/978-3-319-05302-8_10]

[52] Saad S, Traore I. Extracting attack scenarios using intrusion semantics. LNCS, 2013,7743:278−292. [doi: 10.1007/978-3-642-37119-6_18]

[53] Saad S, Traore I. Semantic aware attack scenarios reconstruction. Journal of Information Security & Applications, 2013,18(1): 53−67. [doi: 10.1016/j.jisa.2013.08.002]

[54] Sadighian A, Zargar ST, Fernandez JM, Lemay A. Semantic-Based context-aware alert fusion for distributed intrusion detection systems. In: Proc. of the 2013 Int'l Conf. on Risks and Security of Internet and Systems (CRiSIS). 2013. 1−6. [doi: 10.1109/CRiSIS.2013.6766352]

[55] D'Aniello G, Loia V, Orciuoli F. A multi-agent fuzzy consensus model in a situation awareness framework. Applied Soft Computing, 2015,30:430−440. [doi: 10.1016/j.asoc.2015.01.061]

[56] Beaver J, Steed C, Patton R, Cui X, Schultz M. Visualization techniques for computer network defense. Proc. of the SPIE Int'l Society for Optical Engineering, 2011,8019(18):6−9. [doi: 10.1117/12.883487]

[57] Giura P, Wang W. Using large scale distributed computing to unveil advanced persistent threats. ASE, 2013,1(3):1−13.

[58] Yang SJ, Byers S, Holsopple J, Argauer B, Fava D. Intrusion activity projection for cyber situational awareness. In: Proc. of the IEEE Int'l Conf. on Intelligence and Security Informatics. 2008. 167−172. [doi: 10.1109/ISI.2008.4565048]

[59] Fava DS, Byers SR, Yang SJ. Projecting cyberattacks through variable-length Markov models. IEEE Trans. on Information Forensics & Security, 2008,3(3):359−369. [doi: 10.1109/TIFS.2008.924605]

[60] De Vel O, Liu N, Caelli T, Caetano TS. An embedded Bayesian network hidden Markov model for digital forensics. In: Proc. of the Int'l Conf. on Intelligence and Security Informatics (ISI 2006). 2006. 459−465. [doi: 10.1007/11760146_41]

[61] Lee D, Kim D, Jung J. Multi-Stage intrusion detection system using hidden Markov model algorithm. In: Proc. of the Int'l Conf. on Information Science andSecurity (ICISS 2008). 2008. 72−77. [doi: 10.1109/ICISS.2008.22]

[62] Farhadi H, AmirHaeri M, Khansari M. Alert correlation and prediction using data mining and HMM. ISeCure, 2011,3(2):77−101.

[63] Fachkha C, Bou-Harb E, Debbabi M. Towards a forecasting model for distributed denial of service activities. In: Proc. of the IEEE Int'l Symp. on Network Computing & Applications. 2013. 110−117. [doi: 10.1109/NCA.2013.13]

[64] Kim S, Shin S, Kim H, Kwon K, Hen Y. Hybrid intrusion forecasting framework for early warning system. IEICE Trans. on Information and Systems, 2008,E91-D(5):1234−1241. [doi: 10.1093/ietisy/e91-d.5.1234]

[65] Pontes E, Guelfi AE, Kofuji ST, Silva AAA. Applying multi-correlation for improving forecasting in cyber security. In: Proc. of the Int'l Conf. on Digital Information Management. 2011. 179−186. [doi: 10.1109/ICDIM.2011.6093323]

[66] Thonnard O, Dacier M. Actionable knowledge discovery for threat intelligence support using a multi-dimensional data mining methodology. In: Proc. of the IEEE Int'l Conf. on Data Mining Workshops. 2008. 154−163. [doi: 10.1109/ICDMW.2008.78]

[67] Qin X, Lee W. Attack plan recognition and prediction using causal networks. In: Proc. of the Computer Security Applications Conf. 2004. 370−379. [doi: 10.1109/CSAC.2004.7]

[68] Ren HL, Stakhanova N, Ghorbani AA. An online adaptive approach to alert correlation. In: Proc. of the DIMVA. 2010. 153−172. [doi: 10.1007/978-3-642-14215-4_9]

[69] Marchetti M, Colajanni M, Manganiello F. Identification of correlated network intrusion alerts. In: Proc. of the 3rd Int'l Workshop on Cyberspace Safety and Security. 2011. 15−20. [doi: 10.1109/CSS.2011.6058565]

[70] Ramaki AA, Khosravi-Farmad M, Bafghi AG. Real time alert correlation and prediction using Bayesian networks. In: Proc. of the ISCISC. 2015. 98−103. [doi: 10.1109/ISCISC.2015.7387905]

[71] Ramaki AA, Amini M, Atani RE. RTECA: Real time episode correlationalgorithm for multi-step attack scenarios detection. Computers & Security, 2014,49:206−219. [doi: 10.1016/j.cose.2014.10.006]

[72] Soleimani M, Ghorbani AA. Multi-Layer episode filtering for the multi-step attack detection. Computer Communications, 2012, 35(11):1368−1379. [doi: 10.1016/j.comcom.2012.04.001]

[73] Yan G, Lee R, Kent A, Wolpert D. Towards a Bayesian network game framework for evaluating DDoS attacks and defense. In: Proc. of the ACM Conf. on Computer & Communications Security. 2012. 553−566. [doi: 10.1145/2382196.2382255]

[74] Wu Q, Shiva S, Roy S, Ellis C, Datla V. On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks. In: Proc. of the Spring Simulation Multiconference. 2010. 1−8. [doi: 10.1145/1878537.1878703]

[75] Tang C, Wan GX, Zhang R, Xie Y. Modeling and analysis of network security situation prediction based on covariance likelihood neural. LNCS, 2012,6840:71−78. [doi: 10.1007/978-3-642-24553-4_11]

[76] Zhao WT, Yin JP, Long J. A cognition model of attack prediction in security situation awareness systems. Computer Engineering and Science, 2007,29(11):17−19 (in Chinese with English abstract).

[77] Chen XJ, Fang BX, Tan QF. Inferring attack intention of malicious insider based on probabilistic attack graph model. Chinese Journal of Computers, 2014,37(1):62−72 (in Chinese with English abstract).

[78] Ye Y, Xu XS, Qi ZC. Attack graph generation algorithm for large-scale network system. Journal of Computer Research and Development, 2013,50(10):2133−2139 (in Chinese with English abstract).

[79] Jose A. A survey about fuzzy cognitive maps. Int'l Journal of Computational Cognition, 2005,3(2):27−33.

[80] Lin ZG, Xu LZ, Yan XJ, Huang FC, Liu YP. A decision-making method on D-S evidence fusion information based on distance measure. Journal of Computer Research and Development, 2006,43(1):169−175 (in Chinese with English abstract). [doi: 10.1360/crad20060126]

[81] Xie P, Li JH, Ou X, Liu P, Levy R. Using Bayesian networks for cyber security analysis. IEEE/IFIP Int'l Conf. on Dependable Systems & Networks, 2010,23(3):211−220. [doi: 10.1109/DSN.2010.5544924]

[82] Poolsappasit N, Dewri R, Ray I. Dynamic security risk management using Bayesian attack graphs. IEEE Trans. on Dependable & Secure Computing, 2012,9(1):61−74. [doi: 10.1109/TDSC.2011.34]

[83] Tolman EC. Cognitive maps in rats and men. Psychological Review, 1948,55(4):189−208. [doi: 10.1037/h0061626]

[84] Szwed P, Skrzynski P. A new lightweight method for security risk assessment based on fuzzy cognitive maps. Int'l Journal of Applied Mathematics and Computer Science, 2014,24(1):213−225. [doi: 10.2478/amcs-2014-0016]

[85] Qu ZY, Li YY, Li P. A network security situation evaluation method based on D-S evidence theory. In: Proc. of the Int'l Conf. on Environmental Science & Information Application Technology, Vol. 2. 2010. 496−499. [doi: 10.1109/ESIAT.2010.5567380]

[86] Boyer S, Dain O, Cunningham R. Stellar: A fusion system for scenario construction and security risk assessment. In: Proc. of the 13th IEEE Int'l Workshop on Information Assurance. IEEE, 2015. 105−116. [doi: 10.1109/IWIA.2005.16]

[87] Wang L. Research on multiple classifier system based on fusion decision [MS. Thesis]. Xi'an: Xi'an University of Technology, 2008. 5−20 (in Chinese with English abstract).

[88] Wang J, Zhang FL, Fu C, Chen LS. Study on index system in network situation awareness. Computer Applications, 2007,27(8): 1907−1909 (in Chinese with English abstract).

[89] Cai X, Yang J, Zhang H. Network security threats situation assessment and analysis technology study. Int'l Journal of Security and Its Applications, 2012,7(5):217−224. [doi: 10.14257/ijsia.2013.7.5.20]

[90] Argauer BJ, Yang SJ. VTAC: Virtual terrain assisted impact assessment for cyber attacks. In: Proc. of the SPIE Defense & Security Symp. 2008,6973:69730F−69730F-12. [doi: 10.1117/12.777291]

[91] Wang L, Jajodia S, Singhal A, Noel S. *k*-Zero day safety: Measuring the security risk of networks against unknown attacks. European Conf. on Research in Computer Security, 2010,11(1):573−587. [doi: 10.1007/978-3-642-15497-3_35]

[92] Satty TL. The analytic hierarchy process. 1996. http://www.dii.unisi.it/~mocenni/Note_AHP.pdf

[93] Wang ZH, Zeng HW. Study on the risk assessment quantitative method of information security. In: Proc. of the 3rd Int'l Conf. on Advanced Computer Theory and Engineering. 2010. 529−533. [doi: 10.1109/ICACTE.2010.5579187]

[94] Ji XH, Pattinson C. AHP implemented security assessment and security weight verification. In: Proc. of the IEEE Int'l Conf. on Social Computing. 2010. 1026−1031. [doi: 10.1109/SocialCom.2010.153]

[95] Deng JL. Gray control system. Journal Huazhong Central China University of Science and Tedimelogy, 1982,10(3):1−10 (in Chinese with English abstract).

[96] Juan L, Tao L, Gang T. A network security dynamic situation forecasting method. In: Proc. of the Int'l Forumon Information Technology and Applications. 2009. 115−118. [doi: 10.1109/IFITA.2009.42]

[97] Lai JB, Wang HQ, Zhu L. Study of network security awareness model based on simple additive weight and grey theory. In: Proc. of the 2006 Int'l Conf. on Computational Intelligence and Security. 2006. 1545−1548. [doi: 10.1109/ICCIAS.2006.295320]

[98] Hu W, Li JH, Chen XZ, Jiang XH. Network security situation prediction based on improved adaptive grey verhulst model. Journal of Shanghai Jiaotong University, 2010,15(4):408−413. [doi: 10.1007/s12204-010-1025-z]

[99] Kotenko I, Doynikova E. Security evaluation for cyber situational awareness. In: Proc. of the High Performance Computing and Communications. 2014. 1197−1204. [doi: 10.1109/HPCC.2014.196]

[100] Ghosh N, Chokshi I, Sarkar M, Ghosh SK, Kaushik AK. NetSecuritas: An integrated attack graph-based securityassessment tool for enterprise networks. In: Proc. of the 2015 Int'l Conf. on Distributed Computing and Networking. 2015. 1−10. [doi: 10.1145/2684464.2684494]

[101] Liu P, Jia XQ, Zhang SZ, Xiong X, Jhi Y-C, Bai K, Li J. Cross-Layer damage assessment for cybersituational awareness. Advances in Information Security, 2009,46:155−176. [doi: 10.1007/978-1-4419-0140-8_8]

[102] https://www.dhs.gov/publication/fact-sheet-hsarpa

附中文参考文献:

[1] 王慧强,赖积保,朱亮,梁颖.网络态势感知系统研究综述.计算机科学,2006,33(10):5−10.

[13] 陈秀真,郑庆华,管晓宏,林晨光.层次化网络安全威胁态势量化评估方法.软件学报,2006,17(4):885−897. http://www.jos.org.cn/1000-9825/17/885.htm

[14] 席荣荣,云晓春,张永铮,郝志宇.一种改进的网络安全态势量化评估方法.计算机学报,2015,38(4):749−758.

[15] 辛丹,盖伟麟,王璐,刘欣,胡建斌.赛博空间态势感知模型综述.计算机应用,2013,33(S2):245−250.

[16] 龚正虎,卓莹.网络态势感知研究.软件学报,2010,21(7):1605−1619. http://www.jos.org.cn/1000-9825/3835.htm [doi: 10.3724/SP.J.1001.2010.03835]

[18] 刘效武,王慧强,吕宏武,禹继国,张淑雯.网络安全态势认知融合感控模型.软件学报,2016,27(8):2099−2114. http://www.jos.org.cn/1000-9825/4852.htm [doi: 10.13328/j.cnki.jos.004852]

[76] 赵文涛,殷建平,龙军.安全态势感知系统中攻击预测的认知模型.计算机工程与科学,2007,29(11):17−19.

[77] 陈小军,方滨兴,谭庆丰,张浩亮.基于概率攻击图的内部攻击意图推断算法研究.计算机学报,2014,37(1):62−72

[78] 叶云,徐锡山,齐治昌,吴雪阳.大规模网络中攻击图自动构建算法研究.计算机研究与发展,2013,50(10):2133−2139.

[80] 林志贵,徐立中,严锡君,黄凤辰,刘英平.基于距离测度的 D-S 证据融合决策方法.计算机研究与发展,2006,43(1):169−175. [doi: 10.1360/crad20060126]

[87] 王黎.基于融合决策的多分类器系统研究[硕士学位论文].西安:西安理工大学,2008.5−20.

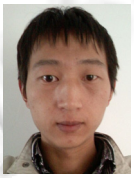
[88] 王娟,张凤荔,傅翀,陈丽莎.网络态势感知中的指标体系研究.计算机应用,2007,27(8):1907−1909.

[95] 邓聚龙.灰色控制系统.华中工学院学报,1982,10(3):1−10.

龚俭(1957－),男,上海人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络安全,网络管理.

胡晓艳(1985－),女,博士,讲师,CCF 专业会员,主要研究领域为计算机网络,未来网络体系结构.

臧小东(1985－),男,博士生,主要研究领域为网络安全,网络管理.



徐杰(1989－),男,博士生,主要研究领域为计算机网络.

苏琪(1989－),男,博士,主要研究领域为网络管理,网络测量.