DOI:10.12158/j.2096-3203.2020.02.024

电力监控系统的网络安全威胁溯源技术研究

李泽科[1]，陈泽文[1]，王春艳[2]，徐志光[1]，梁野[2]
（1. 国网福建省电力有限公司，福建 福州 350001；
2. 北京科东电力控制系统有限责任公司，北京 100192）

摘　要：为解决电力监控系统中网络安全威胁的防御问题，文中在借鉴国内外威胁溯源方法研究的基础上，分析了电力监控系统安全防护的要求，并结合电力二次系统安全防护特点，提出了建立事件发生链定位攻击源头的电力监控系统网络安全威胁溯源方法。首先对告警日志进行树状图建模，构建事件发生树，然后对发生树进行聚合得到初始的事件发生链集合，最后经过断链处理，得到最终的事件发生链集合。该方法能够自动对电力监控系统的告警数据进行有效分析，提取攻击事件，将原始告警处理成可直观展示的攻击图，实现关联主机的有效捕捉，帮助网络管理者实时监测网络安全状态，及时作出安全处置措施，保障网络、数据及设备等的安全。

关键词：电力监控系统；网络安全；威胁溯源；溯源技术；IP 溯源
中图分类号：TM732；TP391.1　　**文献标志码：**A　　**文章编号：**2096-3203(2020)02-0166-07

0　引言

电力监控系统中的安全威胁主要来自计算机网络内部威胁、计算机病毒、黑客攻击以及拒绝服务攻击等，导致文件被删除、篡改、程序运行错误或者死机，严重的将导致机密文件泄露[1—4]。国内外受网络攻击影响频繁发生的大停电事故不仅造成了巨大的经济损失，影响了电力系统的正常运行，也严重影响社会稳定[5—7]。我国电力监控系统的安全防护遵循国家信息安全等级保护制度，坚持“安全分区、网络专用、横向隔离、纵向认证”的方针[8—12]，安全区之间横向隔离，安全区内部采用防火墙和服务器等措施进行安全加固。

随着我国电力需求的不断增长及全国联网战略的实施，如何保证电网安全已成为电力系统迫切需要解决的问题。当前，国内外专家学者在威胁溯源技术研究方面取得了一定成果，研究主要集中在如何对攻击行为进行有效回溯[13—16]。在国外，Foroushani 等提出了一种基于网络数据流标记的 IP 溯源方法，即确定性流标记法（deterministic flow marking，DFM）[17]，该方法能够实现受害者对攻击者攻击位置的准确回溯，不足的是需要消耗大量的 CPU 和内存。在国内，Chunying Wang 等提出了基于符号模型检查算法（symbolic model checking algorithm，SMCA）和攻击图的一种能自动生成和分析攻击图的溯源方法[18]，该方法自动化程度高，回溯效果好，缺点是需要获得整个网络的拓扑结构，一旦攻击者攻破了系统，将获得整个网络的部署情况，具有较大的数据泄露风险[19—24]。

文中在前述安全威胁溯源方法基础上，从电力监控系统主动防御角度出发，探索研究电力监控系统的威胁溯源技术与方法，采用系统告警日志建立事件发生链实现威胁定位，解决现有威胁溯源方法存在溯源精度低、隐私数据泄露、系统资源消耗大等问题，提升电力监控系统的网络安全防护能力。

1　电力监控系统网络安全威胁溯源方法

电力监控系统主要采用基于网络安全日志及告警分析方式，从日志的采集、保存、分析、攻击图生成等环节引入安全思想，形成完整的攻击图，及时追究相关责任人员，提升电力监控系统用户异常行为的追溯能力。

文中采取构建事件发生链的方法来解决，利用存储的历史告警信息，建立基于 IP 关联的告警事件发生树，告警事件发生树经过处理后，得到最终事件发生链，通过计算威胁程度量化评分得到事件发生链威胁值。当事件发生链威胁值超过设定阈值时，则锁定为危险事件，给出提示信息，完成攻击路径的回溯，实现网络威胁溯源的目的。

电力监控系统网络安全威胁溯源流程见图 1。首先进行初始设置，建立告警类型及告警等级信息库，然后输入电力监控系统存储的原始告警日志，提取告警日志的 IP 信息形成初始事件发生树，再经过事件发生链建立模块形成事件发生链，分析互相连通的事件发生链、计算威胁评分，最终得到攻击

收稿日期：2019-10-08；修回日期：2019-11-19
基金项目：国家电网有限公司科技项目“电力监控系统安全监视预警和分析处置技术研究”（SGFJ0000DKJS1900279）

图及威胁提示信息。

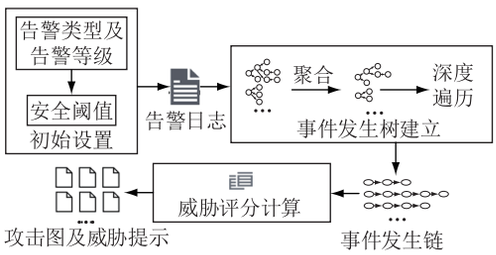

图 1 电力监控系统网络安全威胁溯源处理流程

Fig.1 Tracing process of power monitoring system network security threat source

1.1 告警等级及安全阈值设置

电力监控系统的日志类型、日志子类型、安全级别及告警等级设置,如表 1 所示。

表 1 日志类型及告警等级设置

Table 1 Log type and alarm level setting

日志类型	日志子类型	安全级别	告警等级
外设接入	并口插入告警通知	重要操作	1 级
	串口接入告警通知		
	USB 接入告警通知(无线网卡与存储接入)		
	IP 地址冲突		
异常访问	HTTP 服务访问异常	重要操作	1 级
	异常访问数据		
	FTP 异常访问		
	互联网控制消息协议(internet control message protocol,ICMP)服务访问异常归并		
	主机扫描		
	简单网络管理协议(simple network management protocol,SNMP)服务访问异常		
	分布式拒绝服务攻击(distributed denial of service,DDoS)事件		
	网络基本输入输出系统(network basic input/output system,NETBIOS)服务访问异常		
	动态主机配置协议(dynamic host configuration protocol,DHCP)服务访问异常		
异常登录	用户登录失败(超过阈值)	一般操作	0 级
	非法尝试登录失败告警通知(超过最大阈值)	紧急操作	2 级
高危操作	密通中断	重要操作	1 级
	关键目录中文件/权限变更告警通知	一般操作	0 级
	用户权限变更告警通知	一般操作	0 级
	验签错误	一般操作	0 级
	本地管理界面退出	一般操作	0 级
	开放非法端口	重要操作	1 级

定义告警类型与告警等级。将电力监控系统中日志类型分为外设接入、异常访问、异常登录及危险操作 4 种类型,安全级别分为一般操作、重要操作与紧急操作,告警等级分为 0 级、1 级和 2 级,设置告警类型与告警等级,便于后续步骤对事件发生链威胁程度的量化计算。安全阈值即威胁临界值,超过该值则锁定为疑似危险事件,应重点关注,安全阈值根据使用要求设置,可变更。

1.2 事件发生树建立

(1) 建立树节点。日志信息提取如表 2 所示,其中提取的 IP 地址表示事件发生树中节点,边表示从源地址到目的地址的告警事件(包含告警信息、开始时间、结束时间等)。

表 2 日志信息提取

Table 2 Log information extraction

日志信息	源主机 IP 地址	目的主机 IP 地址	告警事件
时间 1—时间 2 从 IP1 向目的主机 IP2 的某端口的主机扫描事件	IP1	IP2	主机扫描事件
时间 3—时间 4 从 IP3 向目的主机 IP4 的某端口的异常访问数据	IP3	IP4	异常访问数据
时间 5—时间 6 从 IP5 向目的主机 IP6 的某端口的 DDoS 事件	IP5	IP6	DDoS 事件

(2) 建立安全事件发生树。电力监控系统告警日志视作是数据源、目的首尾 IP 地址连接起来的巨型网络,网络的节点就是主机 IP 地址。安全事件发生树就是将这样的网络以树状图的形式构建出来,如图 2 所示。多事件的结构化表现形式即为安全事件发生树,发生树需要满足 3 个条件:

(a) IP 关联。后一个告警事件的源 IP 与前一个告警的目的 IP 相同。

(b) 因果相关。后一个告警事件与前一个告警事件在逻辑上构成因果关系。

(c) 时序性。后一个告警事件的开始时间大于前一个告警的开始时间,构成时序关系。

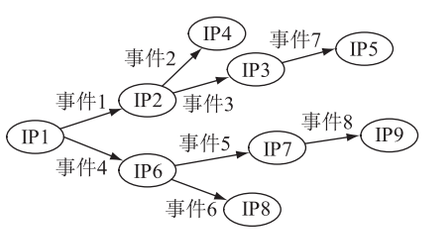

图 2 电力监控系统的事件发生树

Fig.2 Event tree of power monitoring system

接下来,需对建立的发生树进行聚合处理。如

果在发生树中发现后一个子节点与前一个子节点的告警类型、源 IP、目的 IP 均相同，则对二者进行聚合操作，将后者的结束时间覆盖前者的结束时间，并删除后一个子节点。聚合处理流程如图 3 所示。

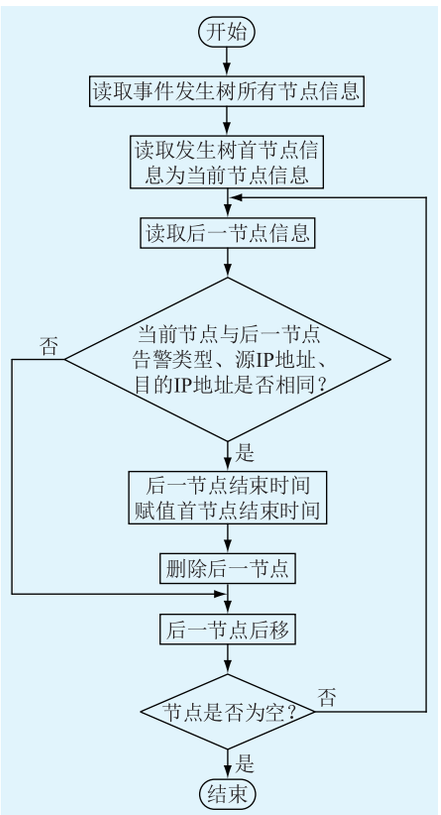

图 3　聚合处理流程

Fig.3　Aggregation process

1.3　拆分安全事件发生链

建立了安全事件发生树之后，就可以对当前的树状图进行深度遍历获得安全事件发生链了。在获取安全事件发生链时，首先要找到链首告警，链首告警意味着在此之前没有以该源 IP 为目的的告警发生。链首告警包括 2 种情况：一种是告警源 IP 对应的节点为无双亲节点；另一种是告警源 IP 对应的节点有双亲，但对应双亲告警的开始时间晚于该告警的开始时间。对应的，对安全事件发生树的深度遍历将进行 2 次，第 1 次，从所有的无双亲节点开始进行深度遍历，得到最终的事件发生链集合 C；第 2 次，再对剩余树节点进行深度遍历，得到剩下的发生链，并加入到最终的链集合 C 中。建立事件发生链流程如图 4 所示。

从事件发生树中拆分的发生链如图 5 所示。建立安全事件发生链之后，需要进行进一步的断链处理。如前述拆分的事件发生链的前后事件并不具备构成攻击行为的因果关系或时序关系，则进行断

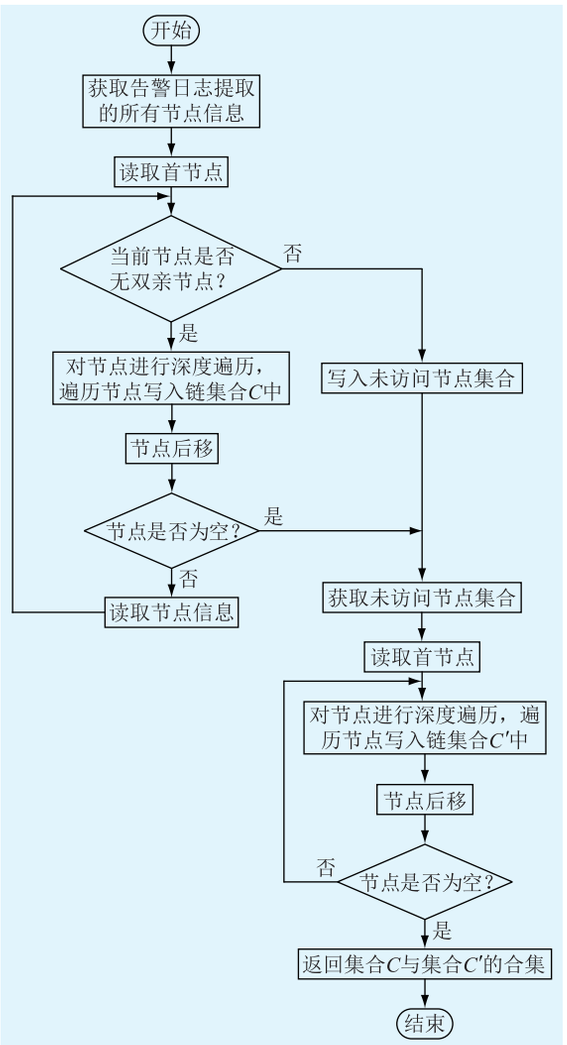

图 4　事件发生链建立流程

Fig.4　Event generation chain establishment process

链处理。因果关系规则即前一个告警事件为后一个告警事件的起因。在一条攻击链中，如果前后 2 个告警事件不存在因果关系，就不可能构成攻击事件，消除这种情况就需要对安全事件发生链进行断链处理。时序关系指假如 B 事件在 A 事件之后发生，且在 A 事件发生的时间内 B 事件没有发生，则称 A 事件与 B 事件间存在时序关系。同样的，如果前后 2 个告警事件不存在时序关系，也不可能构成攻击事件，消除这种情况也需要对安全事件发生链进行断链处理。如图 6 所示，事件 2 与事件 3 之间不存在因果关系或时序关系，则进行事件发生链的断链处理，将原有的安全事件发生链拆分为 2 个安全事件发生链。

1.4　构建威胁量化模型

生成安全事件发生链之后，需要对安全事件发生链进行威胁程度的量化评价，以便于电力监控系统维护人员着手维护，对监控系统的整体态势进行

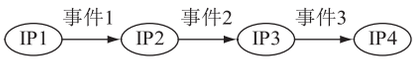

图 5 电力监控系统的安全事件发生链

Fig.5 Security event generation chain of power monitoring system

图 6 断链处理

Fig.6 Broken chain processing

感知。为此,本节构建基于安全事件发生链的威胁量化模型。模型涉及方面:告警等级,原始数据中直接附带此信息,参考价值较大;攻击尝试事件,同一时间内,相邻 IP 之间产生的其他告警事件可能是为攻击所作的尝试。威胁量化模型如表 3 所示,对事件发生链进行评分如表 4 所示。

表 3 威胁量化模型

Table 3 Threat quantization model

权重/%	因子		规则	得分
60	告警等级		0 级	1.0
			1 级	0.5
			2 级	0
40	攻击尝试事件	告警等级×80%	0 级	1.0
			1 级	0.6
			2 级	0.4
		告警数量×20%	(0,99]次	0.3
			[100,999]次	0.5
			[1 000,∞)次	1.0

表 4 安全事件发生链威胁程度评分

Table 4 Event occurrence chain threat degree score

事件发生链	时间1 用户异常登录 IP1 → 时间2 用户异常登录 IP2 → IP3	
发生链威胁评分:0.6	告警等级评分:1.0	0 级
	告警尝试事件评分:0	无

1.5 攻击图生成及威胁提示

根据 1.4 节计算的威胁程度量化计算的总评分,再根据 1.1 节设置的安全阈值,来锁定危险事件,进行威胁溯源。超过设置的安全阈值,则该条安全事件发生链被认定为疑似危险事件,危险事件及威胁提示将以可视化方式展示,生成便于运维人员理解的攻击图,经可视化处理后得到攻击图如图 7 和图 8 所示。

通过上述步骤在电力监控系统中采用建立安全事件发生链的方式来寻找网络事件发起者,查找网络攻击者,描绘出攻击报文在网络中的穿行路线,快速定位攻击源位置,从而找到攻击者,实现电力监控系统的网络安全威胁的溯源。

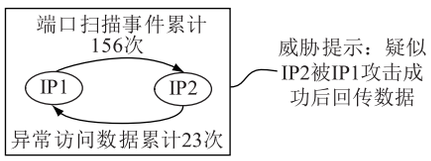

图 7 疑似攻击成功后回传数据

Fig.7 Return data after a successful attack

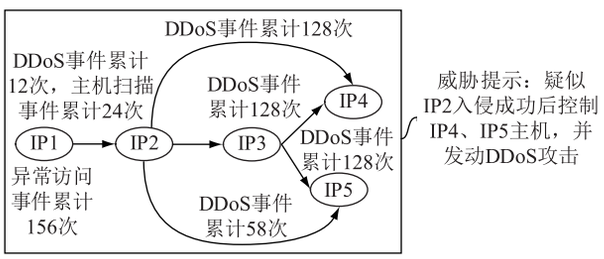

图 8 疑似入侵成功后控制多台僵尸主机并发动 DDoS 攻击

Fig.8 Control multiple zombie hosts after a successful intrusion and launch a DDoS attack

2 实验分析

实验数据选取某区域电力监控系统网络管理平台约 2 个月的告警日志,运用上述电力监控系统威胁溯源方法,验证文中所提方法与模型的有效性。

首先,进行初始设置,对抓取的管理平台日志按 1.1 节分类进行划分,分为系统内存异常、系统 CPU 负载异常、主机硬盘异常、网络异常、主机远程危险操作、外部设备接入异常及异常访问数据,设置系统安全阈值为 0.55。告警等级及告警级别划分如表 5 所示。

表 5 实验分析中告警等级与告警级别划分

Table 5 Classification of alarm levels and alarm levels in experimental analysis

告警分类	告警子分类	告警等级	告警级别
主机状态信息	系统内存异常	紧急操作	2 级
	系统 CPU 负载异常	紧急操作	2 级
	主机硬盘异常	紧急操作	2 级
	网络异常	紧急操作	2 级
异常登录	主机远程危险操作	一般操作	0 级
外设接入	外部设备接入异常	重要操作	1 级
异常访问	异常访问数据	重要操作	1 级

然后,建立安全事件发生树。以 2019 年 6 月 5 日到 6 月 7 日的告警日志为例,合计 153 510 条告警,进行树节点构建和聚合处理,得到 7 368 条告警,数据去冗效果如表 6,经过聚合处理后,分支减少为原数据的 5.99%。

表 6 某区域电力监控告警日志聚合处理效果

Table 6 Effect of aggregation of power monitoring alarm logs in a certain area

数据处理	告警条数	占原数据比率/%
原始告警日志	153 510	100
聚合处理	7 368	5.99

接下来,对构建的安全事件发生树进行深度遍历后得到安全事件发生链,确定告警间的因果关系如表 7 所示,再经因果关系和时序关系判断处理,设置时序关系中的时间窗口为 2 h,最终得到安全事件发生链 739 条,占原数据的 6.58%,见表 8。

表 7 因果关系

Table 7 Causal relationship

因果	系统内存异常	系统 CPU 负载异常	主机硬盘异常	网络异常	主机远程危险操作	外部设备接入异常	异常访问数据
系统内存异常	0	0	0	0	0	0	0
系统 CPU 负载异常	0	0	0	0	0	0	0
主机硬盘异常	0	0	0	0	0	0	0
网络异常	1	1	1	0	0	0	0
主机远程危险操作	1	1	1	1	0	0	0
外部设备接入异常	1	1	1	1	0	0	0
异常访问数据	1	1	1	1	0	0	0

表 8 某区域安全事件发生链处理效果

Table 8 Effect of chain processing in a certain area

数据处理	安全事件发生链条数	占原数据比率/%
初建安全事件发生链	11 237	100
非因果关系处理	10 027	81.19
非时序关系处理	739	6.58

最后,得到安全事件发生链后,绘制攻击图,并运用威胁量化模型,计算攻击图中的安全事件发生链的威胁评分,以下就其中 2 个示例做出分析,图 9 为根据文中提出模型与方法生成的“疑似攻击成功后回传数据”攻击图。

计算事件发生链的威胁评分为 0.516,因未超过设置的安全阈值 0.55,所以系统未给出威胁提示信息。

图 10 为根据文中提出模型与方法生成的“疑似入侵成功后控制多台僵尸主机,并发动 DDoS 攻击”攻击图。

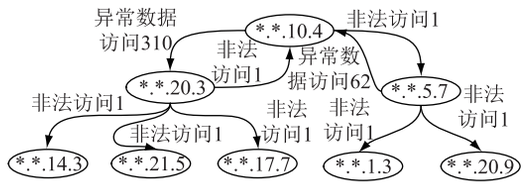

图 9 疑似攻击成功后回传数据

Fig.9 Return data after the suspected attack succeeds

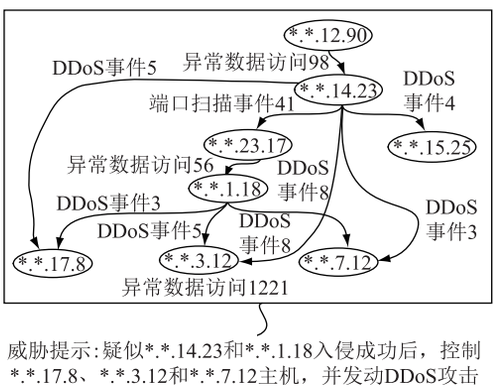

图 10 疑似入侵成功后控制多台僵尸主机并发动 DDoS 攻击

Fig.10 Control multiple zombie hosts after a successful intrusion and launch a DDoS attack

计算安全事件发生链的威胁评分为 0.572,已超过安全阈值 0.55,所以系统给出了威胁提示信息。

系统效率方面,处理电力监控系统网络管理平台的 3 d 告警日志,系统 CPU 占用率、内存占用率、攻击图生成时间情况如表 9 所示。

表 9 某区域安全事件发生链处理系统资源使用情况

Table 9 Resource usage of chain processing system in a regional security incident

系统资源	使用情况
CPU 占用率/%	48(Total2.5 GHz)
内存占用率/%	38(Total7.9 GB)
攻击图生成时间/s	125

实验结果证明了文中提出的电力监控威胁溯源方法的有效性,因果、时序关联确保了攻击事件间的相关性,成功提取了疑似攻击事件并锁定了危险源,为电力监控系统的威胁溯源奠定了基础,且系统资源使用情况在合理范围内,符合电力监控系统资源使用要求。

3 结语

文中提出了一种电力监控系统网络安全威胁溯源方法。该溯源方法分别针对告警日志相互独立、冗余多、粒度差异大、类型多样,且安全事件发生链含有噪声的问题提出了按照 IP 跳转提取安全

事件发生链、安全事件发生树的子节点合并及剔除法的解决方案。相比较其他威胁溯源技术,文中方法的显著特点是依靠少量的先验知识自动提取攻击事件,采用沿 IP 跳转提取攻击轨迹方法,建立基于安全事件分析的事件发生链,并采用可视化方式直观展示告警信息,提升了网络安全威胁溯源的准确度和自动化实现程度。

随着电力监控系统网络规模的不断扩大和渐趋复杂,复杂的网络环境暗藏着巨大的挑战与机遇,网络攻击手段也越来复杂多样,网络威胁溯源尤为重要。威胁溯源技术研究仍需要在现有研究成果基础上进一步深化,未来网络安全威胁溯源工作应该是技术与管理相结合,在多个层面解决问题的系统工程,网络威胁溯源技术仍有待长期的探索研究。

参考文献:

[1] 郑国晨. 电力系统二次安全防护现状与建议[J]. 通讯世界,2018 (9):91-92.
ZHENG Guochen. Current status and suggestions on secondary security protection of power system[J]. Communications World, 2018 (9): 91-92.

[2] 张召亮,孙萌. 电力监控系统二次安全防护改造方案设计与实现[J]. 河南城建学院学报,2019 (1):60-64.
ZHANG Zhaoliang, SUN Meng. Design and implementation of secondary security protection reform scheme for power monitoring system[J]. Journal of Henan Cheng Jian University, 2019 (1): 60-64.

[3] 杨钊. 电力监控系统二次安全防护策略研究[J]. 电工技术,2018(13):118-119,122.
YANG Zhao. Research on secondary security protection strategy of power monitoring system[J]. Electrical Engineering Technology,2018 (13):118-119,122.

[4] 李楠芳,邵巍,王旭,等. 电力监控系统的二次安全防护要点分析 [J]. 中国新通信,2018,20(2):213.
LI Nanfang,SHAO Wei,WANG Xu,et al. Analysis of secondary safety protection points of power monitoring system[J]. China New Communications,2018,20(2):213.

[5] 周孝信,郑健超,沈国荣,等. 从美加东北部电网大面积停电事故中汲取教训[J]. 电网技术,2003,27(9):1-2.
ZHOU Xiaoxin,ZHENG Jianchao,SHEN Guorong,et al. Learn from the large-scale blackouts in the northeastern United States and the United States[J]. Power System Technology,2003,27 (9):1-2.

[6] 刘念,余星火,张建华. 网络协同攻击:乌克兰停电事件的推演与启示[J]. 电力系统自动化,2016,40(6):144-147.
LIU Nian,YU Xinghuo,ZHANG Jianhua. Network synergy attack: deduction and enlightenment of Ukrainian blackout event [J]. Automation of Electric Power Systems, 2016, 40 (6): 144-147.

[7] 李中伟,佟为明,金显吉. 智能电网信息安全防御体系与信息安全测试系统构建:乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化,2016,40(8):147-151.
LI Zhongwei,TONG Weiming,JIN Xianji. Construction of intelligent grid information security defense system and information security test system: reflections on and enlightenment from Ukrainian and Israeli State Grid attacks [J]. Automation of Electric Power Systems,2016,40(8):147-151.

[8] 高夏生,黄少雄,梁肖,等. 电力监控系统安全防护要素[J]. 电脑知识与技术,2017,13(8):212-214,222.
GAO Xiasheng, HUANG Shaoxiong, LIANG Xiao, et al. Safety protection elements of power monitoring system[J]. Computer Knowledge and Technology,2017,13(8):212-214,222.

[9] 章伟华. 电力监控系统网络安全防护探讨[J]. 信息记录材料,2017,18(6):46-47.
ZHANG Weihua. Discussion on network security protection of power monitoring system[J]. Information Recording Materials, 2017,18(6): 46-47.

[10] ALIREZA I, MOHAMED O, MOHD F. Accurate ICMP traceback model under DoS/DDoS attack[C]//15th International Conference on Advanced Computing and Communications, Assam,2007.

[11] 国家电力监管委员会. 电监信息 62 号电力行业信息系统安全等级保护基本要求[Z]. 2012.
National Electricity Regulatory Commission. Electricitysupervision information No. 62 basic requirements for security level protection of power industry information systems[Z]. 2012.

[12] 国家发展和改革委员会. 发改委 14 号令电力监控系统安全防护规定[Z]. 2014.
National Development and Reform Commission. Development and reform commission No. 14 order power protection system safety protection regulations[Z]. 2014.

[13] 陈周国,蒲石,祝世雄. 一种通用的互联网追踪溯源技术框架[J]. 计算机系统应用,2012,21(9):166-170.
CHEN Zhouguo, PU Shi, ZHU Shixiong. A general internet tracking and traceability technology framework[J]. Computer Systems,2012,21(9):166-170.

[14] 郝尧,陈周国,蒲石,等. 多源网络攻击追踪溯源技术研究[J]. 通信技术,2013,46(12):77-81.
HAO Yao,CHEN Zhouguo,PU Shi,et al. Research on traceability and traceability of multi-source network attacks [J]. Communication Technology,2013,46(12):77-81.

[15] 杨泽明,李强,刘俊荣,等. 面向攻击溯源的威胁情报共享利用研究[J]. 信息安全研究,2015,1(1):31-36.
YANG Zeming, LI Qiang, LIU Junrong, et al. Research on threat intelligence sharing and utilization for attack sources [J]. Information Security Research,2015,1(1):31-36.

[16] 李德全,徐一丁,苏璞睿,等. IP 追踪中的自适应包标记[J]. 电子学报,2004,32(8):1334-1337.
LI Dequan,XU Yiding,SU Puyin,et al. Adaptive packet marking in IP tracking[J]. Chinese Journal of Electronics,2004,32 (8): 1334-1337.

[17] BURCH H, CHESWICK B. Tracing anonymous packets to their approximate source[C]//Usenix Systems Administration Conference(LISA), 2000.

[18] WANG C, DU N, HUI J. Generation and analysis of attack graphs[J]. Procedia Engineering, 2012, 29: 4053-4057.

[19] STONE R. Centertrack: an IP overlay network for tracking DoS floods[C]//Usenix Security Symposium, 2000.

[20] 卿昱,杨志聪. 基于SOA的栅格安全服务研究[J]. 信息安全与通信保密,2009(2):79-84.
QING Yu, YANG Zhicong. Research on grid security service based on SOA[J]. Information Security & Communication Security, 2009(2): 79-84.

[21] DUFFIELD N G, GROSSGLAUSER M. Trajectory sampling for direct traffic observation[J]. IEEE/ACM Transactions on Networking, 2001, 9(3): 280-292.

[22] 李超,罗凌璐,王德辉,等. 智能变电站过程层网络监测与故障定位系统设计与实现[J]. 电力工程技术,2019,38(2): 117-122.
LI Chao, LUO Linglu, WANG Dehui, et al. Design and implementation of process layer network monitoring and fault location system for intelligent substation[J]. Electric Power Engineering Technology, 2019, 38(2): 117-122.

[23] 席荣荣,云晓春,金舒原,等. 网络安全态势感知研究综述[J]. 计算机应用,2012,32(1):1-4,59.
XI Rongrong, YUN Xiaochun, JIN Shuyuan, et al. A review of network security situational awareness research[J]. Computer Applications, 2012, 32(1): 1-4, 59.

[24] 王慧强,赖积保,朱亮,等. 网络态势感知系统研究综述[J]. 计算机科学,2006,33(10):5-10.
WANG Huiqiang, LAI Jibao, ZHU Liang, et al. A review of network situational awareness systems[J]. Computer Science, 2006, 33(10): 5-10.

作者简介:


李泽科

李泽科(1977),男,学士,高级工程师,从事调度自动化管理工作(E-mail: lizeke@139.com);

陈泽文(1975),男,博士,高级工程师,从事电力监控系统安全防护工作;

王春艳(1979),女,学士,高级工程师,从事电力监控安全防护技术研究工作。

Network security threat tracing technology of power monitoring system

LI Zeke[1], CHEN Zewen[1], WANG Chunyan[2], XU Zhiguang[1], LIANG Ye[2]

(1. State Grid Fujian Electric Power Co., Ltd., Fuzhou 350001, China;
2. Beijing Kedong Electric Power Control System Co., Ltd., Beijing 100192, China)

Abstract: On the basis of the research results of domestic and foreign threat tracing methods, in order to solve the problem of network security threat defense in power monitoring system. This paper combines with the requirements of power monitoring system security protection and the characteristics of power secondary system security protection by establishing the source of event location chain attack. The method firstly models the alarm log tree, constructs an event generation tree, and then aggregates the occurrence tree to obtain an initial event generation chain set. Finally, after the chain breaking process, the final event generation chain set is obtained. The method can automatically analyze the alarm data of the power monitoring system, extract the attack event, and process the original alarm into an attack map that can be visually displayed, thereby effectively capturing the associated host, and helping the network manager to monitor network security status in real time. So that timely safety measures are taken to ensure the safety of the network, data and equipment.

Keywords: power monitoring system; network security; threat traceability; traceability technology; IP traceability

(编辑　陈静)