基于网络协议和页面特征的物理设备发现

冯健飞,张 毅,马 迪,张京京
(国防科学技术大学 计算机学院,湖南 长沙 410073)

摘 要:互联网存在着大量网络摄像头、PLC、传感器等物理设备,对这些设备进行自动发现有助于了解其分布和部署情况;从人机物多域融合的角度表示物理设备,有助于全面刻画物理设备,并为跨域攻击分析提供支持。文中提出一种基于网络协议报文和 Web 页面特征在互联网中发现物理设备的方法。该方法主要通过 HTTP、SNMP 和 PPTP 协议的握手报文头部信息和物理设备访问控制 Web 页面的结构特征发现物理对象并获取物理对象的基本信息,然后通过预置的产品信息库充分感知设备硬件信息,通过 IP 信息库获知设备物理地点和社会域属性,从而实现对物理对象的人机物多域融合分析。最后利用文中所提出的方法,开发了物理对象感知和分析系统 NetThing,并对运用文中方法获取的物理设备数据进行了分析和验证。

关键词:互联网;物理设备;协议报文;Web 页面
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2016)05-0031-05
doi:10.3969/j.issn.1673-629X.2016.05.007

A Searching Physical Devices Method Based on Internet Protocols and Web Page Features

FENG Jian-fei, ZHANG Yi, MA Di, ZHANG Jing-jing
(School of Computer Science, National University of Defense Technology, Changsha 410073, China)

Abstract: There are many physical devices in the Internet, including webcams, PLC, sensors etc. Searching and finding these physical devices helps to know more about their distribution and deployment. Describing physical devices in "social cyber physical multi-domain" model is also good for fully depicting them and analyzing possible existence of cross-domain threats. A method for finding physical devices in the Internet based on the protocols' datagrams and Web page features is proposed. This method mainly uses the shake hands datagrams of HTTP, SNMP, PPTP and the features of Web pages to find physical devices and get their basic information. Then it expands hardware information of the devices through the products information base, and social domain information, such as location information, through the IP information base. At last, a proto type system named NetThing is developed using method proposed, and the data of experiments is analyzed and verified.

Key words: Internet; physical devices; protocol datagram; Web page

0 引 言

随着网络规模的不断扩大,越来越多的物理设备接入到互联网中,包含了被感知的现实对象、感知信息的传感器件、信息处理设施[1],比如无线家用 WIFI 热点、网络摄像头及温度传感器等。而由于部分用户安全意识的淡薄,这类设备存在较大的安全隐患。

2014 年底,华为公布了家庭网关的 RomPager 漏洞。RomPager 是小型网络设备内置的网页服务器,攻击者可能利用该漏洞获取管理员权限或者发起拒绝服务攻击[2]。而同样采用了 RomPager 的中兴[3]和 TP-Link[4]设备也发布了相似的漏洞。除了路由器外,网络摄像头等新兴网络设备也面临较大安全隐患,比如江苏省警用摄像头被境外控制的重大安全事件[5]。除了网络设备外,以"震网蠕虫"为代表的通过摆渡攻击等方式破坏工业设施的案例也越来越多[6],且这些攻击大部分具备 APT 攻击特性。

网络设备的安全隐患主要来自于三方面:一是网络设备系统自身的漏洞;二是设备配置时的漏洞;三是

收稿日期:2015-06-23 **修回日期**:2015-09-24 **网络出版时间**:2016-05-05
基金项目:国家自然科学基金资助项目(61170285)
作者简介:冯健飞(1991-),男,硕士研究生,研究方向为计算机网络与信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160505.0815.038.html

管理的疏忽[5]。

在网络漏洞挖掘中,目标对象范畴已经涵盖了数据通信网络基础设施[7]。发现这些目标的存在,为后续安全防护提供了依据。

目前发现物理对象的方法有 Snoogle[8]、Microsearch[9]、MAX[10]、OCH[11]、Dyser[12]等模型,这些模型都是针对无线传感器网络所设计的,部分思想可借鉴到在互联网中发现物理对象上。关于物理对象的多域融合研究模型有 Cyber-Physical System[13]、Social Cyber Physical System[14]、Physical-Cyber-Social Computing[15],而这些模型都需要可行的技术方法提供物理对象的多域信息,这也是文中工作的一个重要应用。

文中描述了基于常见的网络协议握手报文和 Web 页面的特征发现网络设备的方法。分析了 HTTP、SNMP 和 PPTP 协议报文中可能存在的物理设备信息,量化分析了作为设备登录界面的 Web 页面的结构特征,并通过设备信息库和 IP 信息库将信息向社会域和物理域进行扩展。最后基于文中的方法设计开发了原型系统 NetThing,并对实验数据进行了分析。

1 NetThing 系统概述

目前主流的联网物理设备都提供了基于 Web 页面的访问和控制接口,在缺乏有效的防火墙隔离下,这些页面有可能被远程访问。据此,文中设计了基于常见的网络协议报文和设备登录页面特征的物理设备发现系统,取名为 NetThing。

NetThing 系统基本结构如图 1 所示,总共分为三层。第一层为报文获取和协议预处理层,主要工作是对某特定IP进行HTTP、SNMP、PPTP协议的探测分析。第二层为信息扩展部分,主要是对上一步获取的信息进行丰富。首先,进行 Web 页面分析,主要是针对 HTTP 协议返回状态为 200 OK 的情况进行分析,提取页面基本信息和主要关键字。其次,对于某些可以获取具体型号的设备,可以预置设备的信息库,通过型号匹配获取关于设备硬件的详细参数。最后,对于 IP 信息,可以通过查询已有的数据库,获取某个 IP 的地理位置、AS 号以及所属的 ISP 等,从而进一步扩展设备的信息。统一将信息存入数据库对外提供查询接口,查询效果如图 2 所示。输入关键字 router,返回含有 router 的 IP 和详细信息。

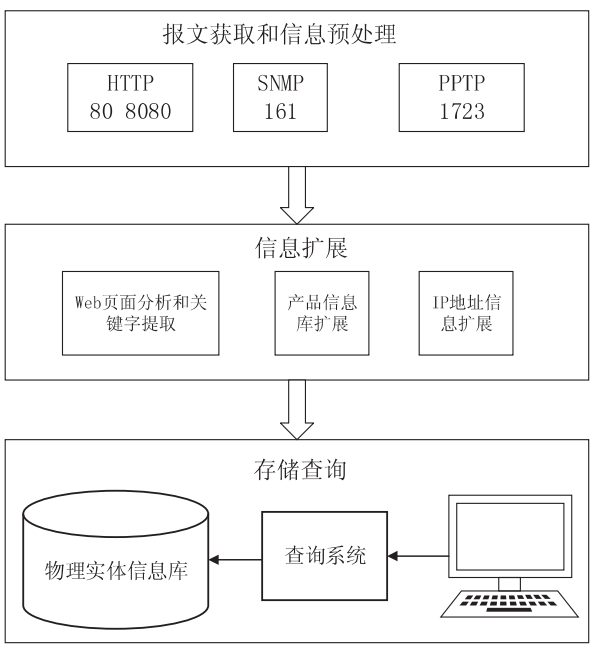

图 1 系统结构

图 2 结果展示界面

2 设备信息挖掘和多域扩展

2.1 协议应答报文分析和 Web 页面分析

文中主要涉及到了 HTTP、SNMP 和 PPTP 协议的握手报文,这些报文的头部都可能含有基本的关于物理设备的描述。基本方法是对某一 IP 的上述协议的工作端口发送请求报文,如果收到应答报文,提取其中的有价值字段进行统计分析。

对 HTTP 协议,首先提取应答报文中的 server 字段。在各大厂商设备的访问控制界面的响应报文中,该字段常带有关于厂商或者设备的简单描述,为确定该设备的存在提供了一定的依据。如果含有 location 字段,也进行提取,此字段一般指示了服务器地址迁移后的新地址。

对于返回状态为 401 Unauthorized 的报文,含有 WWW-Authenticate 字段。该字段规定了信息的加密方式,对于很多网络设备,这个字段也提供了设备的型号信息。

SNMP(Simple Network Management Protocol),即简

单网络管理协议,是用来对互联中由众多软硬件厂商生产的网络设备进行管理的一组协议。向 SNMP 代理进程发送 GET 查询报文就可能返回被管理系统的相关信息。文中主要查询了 OID 为.1.3.6.1.2.1.1.(1,4,5,6).0 的对象,分别可以获取被管理系统的基本信息、联系人、机器名和机器所在位置信息。

PPTP(Point to Point Tunneling Protocol),即点对点隧道协议,是目前 VPN 的主要支持协议。通过简单地向 PPTP 服务器发送建立连接请求报文,就可以收到一个应答报文,该报文的 hostname 和 vendor string 字段对该服务器的所属机构和设备厂商进行简单的描述,从而反映了设备和拥有该设备的机构的基本信息。这进一步扩展了一个设备的社会属性。

2.2　多域信息扩展

主要通过三个途径对信息进行扩展,分别是 Web 页面分析、产品信息库匹配和 IP 信息库扩展。

首先对 HTTP 协议返回状态为 200 OK 的情况,进行 Web 页面分析。图 3 显示了 HTTP 报文获取和页面分析的流程。

第一步读取 HTML 文档信息,提取 HTML 文档的 title 字段和 meta 字段,在 meta 字段中分别提取 keyword、description、author 子字段。下一步提取页面的纯文本内容,并计算文本长度。在此基础上,进一步将含有大写字母和数字的单词提取出来,因为对于一个物理设备的描述很可能涉及到设备厂商等专用名词和具体参数指标。

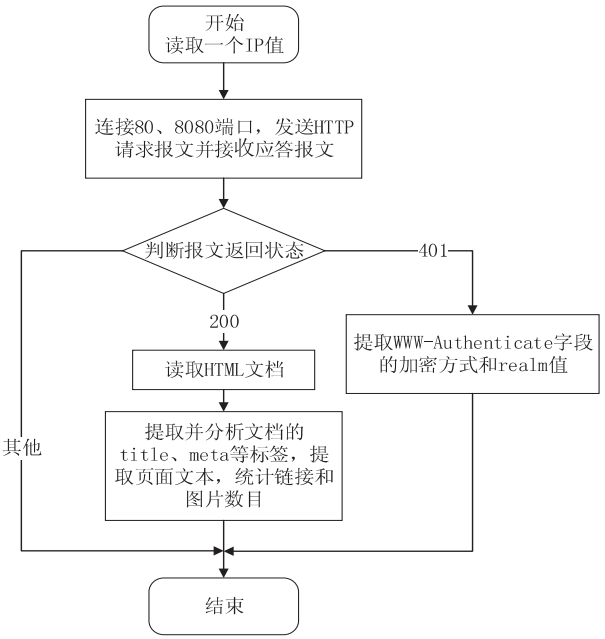

图 3　HTTP 报文和 Web 页面分析

进一步分析是否含有用户名密码输入框,主要是通过对 HTML 的 input 标签的 id 和 name 属性采用如下正则表达式进行匹配:

(us)+e*(r)+|(name)+|(login)　　(1)

p+((ass)+|w+(or)*d+)　　(2)

式(1)匹配了诸如 username、user、login 等常见的用户名表述方式;式(2)匹配了诸如 password、pass 等常见的密码的表述方式。

如果匹配成功,则表示含有用户名和密码输入框,从而证明该页面很可能是一个设备的登录页面。接下来统计页面中的图片和链接数量,并保存链接内容。最后提取页面中表格内的文本信息,并计算表格文本信息长度及其所占页面文本信息长度的比例。

在通过产品信息库匹配进行信息扩展中,首先搜集了常见产品的基础参数信息,并将它们结构化存储在数据库中。对于发现的可以确定其产品型号的网络设备,在信息库中匹配查询出具体记录,从而扩展设备的详细参数信息。

最后 IP 地址信息扩展是通过网络中已有的数据库进行匹配查询,例如对于 IP 地址 36.72.231.20,可以获取如下信息:

City: Semarang. Country: Indonesia. Organization: PT Telkom Indonesia. ISP: PT Telkom Indonesia. ASN: AS17974

其中包含了该地址所处的地理位置、所属的组织机构以及网络服务供应商等,这些信息同时也与对应的物理设备关联,从而对此物理设备形成了从自身物理信息,到网络信息,再到社会域信息的多域融合的全面描述。

3　基于重要字段的搜索结果排序

对搜索结果采用传统的倒排方式进行索引。具体过程如图 4 所示。

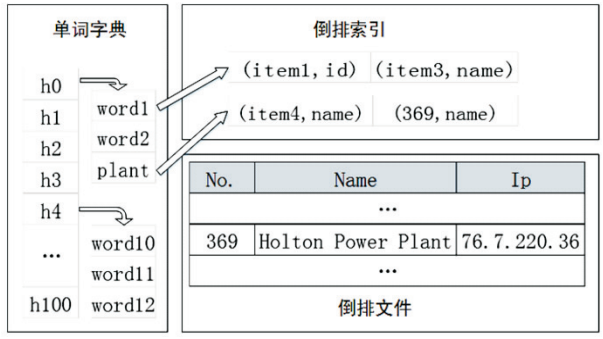

图 4　倒排索引

单词字典采用哈希加链表的形式构造。对于给定的搜索词,首先计算其哈希值,然后通过哈希值索引对应的单词链表找到该单词,接着访问该单词的倒排索引。倒排索引中同时记录了某条记录的索引值 itemX 和该记录中含有此单词的字段,比如 title、host 等。最后根据记录的序列号查询该条记录的详细信息。

在搜索结果的排序上,按照含有搜索单词的字段的重要性进行排序。首先对不同字段赋予不同的权重,比如一个单词在 title 字段或者 realm 字段出现,赋予比在页面文本中出现更高的权重。在赋予权重之后,可以计算出每条记录对其包含的每个单词的权重。

假设对某一查询 Q,得到的结果 R 中含有 m 条命中记录:

$R = (I_1, I_2, \cdots, I_m)$

其中第 k 条记录 I_k 命中了 N_k 个字段:

$I_k = (F_{k1}, F_{k2}, \cdots, F_{kn_k})$

字段 F_t 权重为 P_t。在此基础上,对于记录 I_k,其匹配权重为:

$$S_k = \sum_{i=1}^{i=n_k} P_{ki} \tag{3}$$

其中,P_{ki} 是 F_{ki} 的权重,从而根据 S_k 的值对 I_k 进行排序。

当命中记录较少时,还应当推荐相似度高的命中记录。首先要提出相似度的衡量方法。可以认为地理位置相近或者是产品型号相近的记录与用户的搜索要求相近。可以将地理位置、产品型号等组成树状结构,记录从根节点到叶节点的路径作为叶节点的向量表示,例如对地理位置有如下构造:

China Hunan Changsha (1,4,1)

China Hunan Yueyang (1,4,2)

对产品型号有如下构造:

Huawei AR-1200 (1,1,1)

Huawei AR-1220(1,1,2)

对于向量 $\boldsymbol{\alpha}$ 和 $\boldsymbol{\beta}$,夹角的余弦计算公式为 $\cos\theta = \dfrac{\boldsymbol{\alpha}\cdot\boldsymbol{\beta}}{|\boldsymbol{\alpha}|\cdot|\boldsymbol{\beta}|}$。该值越大,表明向量夹角越小,其相关性也就越大。

依然假设 F_t 的权重为 P_t。对某查询 Q:$w_1, w_2, w_3 \cdots$,其中 w_i 是第 i 个查询关键词,$\boldsymbol{\alpha}_t$ 是 w_t 的向量表示。第 k 条记录 I_k 的命中字段为:

$(F_{k1}, F_{k2}, \cdots, F_{kn_k}, f_{k1}, f_{k2}, \cdots, f_{kx_k})$

对于记录 I_k,其匹配度为:

$$S_k = \sum_{i=1}^{i=n_k} P_{ki} + \sum_{j=1}^{j=x_k} \frac{\boldsymbol{\alpha}_j \cdot \boldsymbol{\beta}_{kj}}{|\boldsymbol{\alpha}_j| \cdot |\boldsymbol{\beta}_{kj}|} \tag{4}$$

其中:P_{ki} 是 F_{ki} 的权重;$\boldsymbol{\beta}_{kj}$ 是 f_{kj} 字段对应的向量;$\boldsymbol{\alpha}_j$ 是 $\boldsymbol{\beta}_{kj}$ 对应的查询单词的向量。

根据 S_k 的值对 I_k 进行排序。

4 实验结果及分析

为了确保实验的准确性,采用了随机生成 IP 地址的方法。首先根据 IANA 的分配情况,随机选择了 12 个 A 类地址,涵盖了 ARIN、RIPE NCC、APNIC 三大机构。随机且不重复地生成 IP 地址后三个字节,共生成了 288 000 个 IP,对这些 IP 进行协议分析和 Web 页面分析。下面分别介绍获取的物理信息,并提取作为设备登录页面的 Web 页面的特征。

4.1 结果统计

所有的 HTTP 协议返回 5 305 条,其中 server 字段统计结果排名第三的是 RomPager/4.07 UPnP/1.0,共出现 377 次,这是大部分家用网络设备内置的网页服务器。

返回 401 状态的共 1 072 次,对 realm 字段进行统计,前几位分别是 Broadband Router,BEC 7800TN R2,TD-8817,ZXV10 W300S,TD-W8101G,这些都是网络设备。其中 TD 开头的是 TP-link 的家庭网络路由器型号,这对后续的通过产品库进行信息扩展提供了依据。在加密方式上,有 1 046 个为 Basic,10 个为 Digest,13 个为指定。说明绝大部分只是采用简单方式对用户名和密码进行加密,这存在被窃取和仿冒的危险。

另外,从 SNMP 报文中提取出了 Netopia 3341,Netopia 2246N-VGx,Netopia 4652,Netopia 3341,Netopia 3346N-ENT 等设备型号,也为后续分析提供了线索。

4.2 设备登录页面特征分析

实验中 HTTP 协议返回 200 OK 状态的共 2 706 个。对这些页面进行分析,含有用户名和密码输入框的为 315 个,假设这些是设备的登录页面,对这些页面进行分析。

对页面特征进行统计,结果显示绝大部分页面纯文本信息长度小于 1 000 B,链接数目小于 5 个,图片数目小于 10 张,而表格文本长度占页面文本长度的比例则分布较为随机,没有具体特征体现。页面文本长度统计如图 5 所示,页面链接数量统计如图 6 所示。

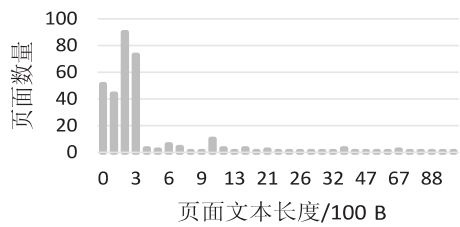

图 5 页面文本长度统计

图 6 页面图片数量统计

进一步对页面中的文字进行统计,在 title 字段出现次数最多的词是 Login,共 95 次,configuration 和 router 并列 72 次。对所有的链接提取统计,发现出现

次数最多的前几项为:http://www. arris. com 有 204 次,http://mikrotik. com 有 72 次,http://www. mikrotik. com/有 8 次。这些都是相关厂商的页面。

5　结束语

文中提出一种基于网络协议报文和 Web 页面特征在互联网中发现物理设备的方法,并通过多种手段扩充了设备的信息,对设备进行了物理、信息和社会多域描述。实验还存在一些不足之处,比如在 Web 页面分析中,某些页面需要根据脚本或者 location 字段进行二次跳转,对这些页面进一步分析会扩充发现的物理设备的数目。通过该文,可以认识到互联中存在很多没有高级安全防护措施的设备,主要是小型化家用网络设备,这其中潜在着较大的网络安全隐患。

参考文献:

[1] 于海宁,张宏莉,方滨兴,等. 物联网中物理实体搜索服务的研究[J]. 电信科学,2012,28(10):111-119.

[2] 华为技术有限公司. 安全预警-涉及华为家庭网关产品的多个 RomPager 漏洞[EB/OL]. 2014-12-19. http://www.huawei. com/cn/security/psirt/security - bulletins/security - advisories/hw-407667. htm.

[3] 中兴通讯公司. 中兴通讯家庭网关产品受多个 RomPager 漏洞影响[EB/OL]. 2015-01-09. http://support. zte. com. cn/support/news/LoopholeInfoDetail. aspx? newsId = 1006322.

[4] 红黑联盟. 多个 TP-Link 路由器 RomPager 拒绝服务漏洞[EB/OL]. 2014-06-22. http://www. 2cto. com/Article/201406/310905. html.

[5] 张　庆,宋　芬,沈国良. 网络设备安全措施分析与研究[J]. 网络安全技术与应用,2008(8):33-34.

[6] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报,2015(1):40-53.

[7] 张友春,魏　强,刘增良,等. 信息系统漏洞挖掘技术体系研究[J]. 通信学报,2011,32(2):42-47.

[8] Wang H, Tan C C, Li Q. Snoogle: a search engine for pervasive environments[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(8): 1188-1202.

[9] Tan C C, Sheng B, Wang H, et al. Microsearch: when search engines meet small devices[C]//Proceedings of the 6th international conference on pervasive computing. Sydney, Australia: [s. n.], 2008: 93-110.

[10] Yap K K, Srinivasan V, Motani M. MAX: human - centric search of the physical world[C]//Proceedings of 3rd conference on embedded networked sensor systems. San Diego: [s. n.], 2005: 166-179.

[11] Frank C, Bolliger P, Mattern F, et al. The sensor internet at work: locating everyday items using mobile phones[J]. Pervasive and Mobile Computing, 2008, 4(3): 421-447.

[12] Ostermaier B, Romer K, Mattern F, et al. A real-time search engine for the web of things[C]//Proceedings of internet of things. Tokyo, Japan: [s. n.], 2010: 1-8.

[13] Krämer B J. Evolution of cyber-physical systems: a brief review[M]. New York: Springer, 2014.

[14] Horváth I. What the design theory of social-cyber-physical systems must describe, explain and predict[M]//An anthology of theories and models of design. London: Springer, 2014: 99-120.

[15] Sheth A, Anantharam P, Henson C. Physical-cyber-social computing: an early 21st century approach[J]. IEEE Intelligent Systems, 2013, 28(1): 78-82.

(上接第 30 页)

[18] 黄程韦,金　赟,王青云,等. 基于语音信号与心电信号的多模态情感识别[J]. 东南大学学报:自然科学版,2010,40(5):895-900.

[19] Busso C, Deng Z, Yildirim S, et al. Analysis of emotion recognition using facial expressions, speech and multimodal information[C]//Proc of the sixth international conference on multimodal interfaces. USA: IEEE, 2004: 205-211.

[20] Hoch S, Althoff F, Mcglaun G, et al. Bimodal fusion of emotional data in an automotive environment[C]//Proc of IEEE international conference on acoustics, speech, and signal processing. USA: IEEE, 2005: 1085-1088.

[21] Sayedelahl A, Araujo R, Kamel M S. Audio-visual feature-decision level fusion for spontaneous emotion estimation in speech conversations[C]//Proc of 2013 IEEE international conference on multimedia and expo workshops. USA: IEEE, 2013: 1-6.

[22] Tato R, Santos R, Kompe R, et al. Emotion space improves emotion recognition[C]//Proceedings of the 2002 international conference on speech and language processing. USA: IEEE, 2002: 2029-2032.