Pulling the Curtain on Airport Security
Billy Rios
Xssniper@gmail.com
@xssniper
How to get put on the no-fly list...
Why are you doing this?

- Just an average Joe
- Interest in ICS, Embedded and Medical devices
- I travel a lot
Lessons Learned by a Young Butterbar

• Show respect
• Accept Responsibility
• Trust, but Verify
Show me the Money… (budget.house.gov)

- > 50,000 people at more than 400 airports across the country and an annual budget of $7.39 billion (2014)

- TSA receives about $2 billion a year in offsetting collections under current law, through air-carrier and aviation-passenger security fees. The largest of the fees, in terms of total collections, is the Aviation Passenger Security Fee (sometimes called the September 11th Security Fee), which brings in about $1.7 billion a year.

- By law, the first $250 million of passenger-security fees is set aside for the Aviation Security Capital Fund, which provides for airport-facility modifications and certain security equipment.
Show me the Money...

One guy

no budget

and a laptop
Disclosure

All issues in this presentation were reported to DHS via ICS-CERT >6 months ago
Response?

• Our software “cannot be hacked or fooled”
• “add their own software and protections.”
• <silence>
• Spoke with Morpho last week
Scenarios

(1) TSA doesn’t know about the security issues in their software

(2) TSA knew about the security issues, developed their own custom fixes, never told the vendors... and is hording embedded zero day vulnerabilities and leaving other organizations exposed?
Recommended Security Guidelines for Airport Planning, Design and Construction

Revised: May 2011
CHECKPOINT DESIGN GUIDE (CDG)
Revision 4.0
August 29, 2012

Prepared for the
Transportation Security Administration (TSA)
Office of Security Capabilities (OSC)
<table>
<thead>
<tr>
<th>Equipment</th>
<th>Quantity</th>
<th>Power Requirements</th>
<th>IT Requirements</th>
<th>Additional Information</th>
</tr>
</thead>
</table>
| TDC Podium CAT/BPSS (generic) | 1 per 2 lanes, +1 for odd numbered lanes, +1 if checkpoint leads International Flights | - Non-dedicated  
- 20A, 125V, 180W/plaque  
- Z-Hot, 3-Wire Grounding  
- NEMA 5-20R Duplex Receptacle  
- Power cord length is unknown at the time of this printing | - Data Drops = 2  
- Cable/Cat5 cable  
- The cable length from the termination point in the IT cabinet to the data outlet in the work area shall not exceed 200ft.  
- If data drop cannot be secured when the checkpoint is closed, a locking device is required. Coordinate with TSA HQ IT Security. | - The TDC function can be supported by either a TDC Podium or a CAT/BPSS  
- The CAT/BPSS may be on a wheeled cart or it may sit on floor. |
2.3 BIN CART

Bins are the gray containers located on a cart at the front and back of each checkpoint lane. Passengers use bins to divest themselves of their personal belongings such as purses, carry-on bags, backpacks, laptops, shoes, jackets, etc. Bin carts are similar to a hand cart or dolly that allows for the transport of a large number of bins without requiring excessive lifting or carrying by a TSA agent. In the past, bin transport by the TSOs was the primary cause of on-the-job injuries at checkpoints. Hand-carrying of bins is no longer endorsed by TSA. TSA recommends that bin carts be pushed upstream through an ADA or access gate. Ideally, an ADA or access gate should exist at every lane but this is not always possible. When there is insufficient space for an ADA or access gate, the bin cart should be pushed upstream against passenger flow through the WTMD.

Bin carts can be one or two bins wide with bins stacked on top to slightly below the handle which equates to approximately 40 bins. Each lane requires a bin cart at each end. TSA recommends maintaining about 60 bins per lane divided across each end. A fully-loaded bin cart should be located at the start of the divest tables on the non-sterile side of the lane for passenger pick-up. The other bin cart should be positioned at the end of the composure rollers on the sterile side so that the TSA agent can collect empty bins after passengers have picked up their belongings. Refer to Figure 2-9 for bin cart dimensions. The bin cart width times two should be factored into the overall length of the checkpoint lane when designing a new checkpoint or reconfiguring an existing checkpoint.

Figure 2-9 Bin Cart

![Bin Cart Diagram]
<table>
<thead>
<tr>
<th>IT Requirements</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data Drops = 2</td>
<td>• The TDC function can be supported by either a TDC Podium or a CAT/BPSS.</td>
</tr>
<tr>
<td>• Cat5e / Cat6 cable</td>
<td>• The CAT/BPSS may be on wheels or it may sit on floor.</td>
</tr>
<tr>
<td>• The cable length from the termination point in the IT cabinet to the data outlet in the work area shall not exceed 295’.</td>
<td></td>
</tr>
<tr>
<td>• If data drop cannot be secured when the checkpoint is closed, a locking device is required. Coordinate with TSA HQ IT Security.</td>
<td></td>
</tr>
</tbody>
</table>
Figure 4-1  SSCP Data Connectivity Diagram

- TDC & CAT/BPSS PODIUM
- TSA IT CABINET (EXISTING)
- WALL MOUNT KRONOS TIME CLOCK
- CAT 6 Patch Panel
- LANE 1 AT/X-RAY
- PANIC & DURESS BUTTON
- LANE 2 AT/X-RAY
- PANIC & DURESS BUTTON
- LANE 2 ET@ AIT
- 2-LANE AVS SETUP LANE 1 & 2
- AVS
- BLS
- ETD

- STSO Podium
- LANE 3 AT/X-RAY
- PANIC & DURESS BUTTON
- LANE 3 ET@ AIT
- SINGLE-LANE AVS SETUP LANE 3
- AVS
- BLS
- ETD

- EXTERIOR
- INTERIOR PRIVATE SCREENING ROOM
IT Program Assessment
TSA - Security Technology Integrated Program (STIP) (2010)

Review
The DHS Chief Information Officer conducted a comprehensive program review of the TSA - Security Technology Integrated Program (STIP) on April 15, 2010. The STIP program, a joint effort co-funded by the Passenger Screening Program (PSP) and Electronic Baggage Screening Program (EBSP), is a TSA-wide Enterprise system that delivers data from passenger and baggage screening security technologies (in a common format) in order to facilitate data interchange/exchange through a single network for effective communication and metrics reporting. STIP has Enterprise Management, Configuration Management, Resource Management and Equipment Maintenance capabilities.
A Quick Lesson on Backdoors
I can't believe it, Jim. That girl's standing over there listening and you're telling him about our back doors?

[Yelling] Mr. Potato Head! Mr. Potato head! Backdoors are not secrets!

Yeah, but your giving away our best tricks!

They’re not tricks!
A Word About Backdoors

• Malicious account added by a third party

• Debugging accounts that someone forget to remove

• Accounts used by Technicians for Service and Maintenance
Technician Accounts == Backdoors

• Often hardcoded into the software
• Applications which depend on the passwords
• Business process which depend on passwords
• External software which depend on passwords
• Training which train technicians to use these passwords
Technician Accounts == Backdoors

- Can be discovered by external third parties (like me!)
- Cannot be changed by the end user (in most cases)
- Once initial work is completed, these passwords usually scale
Rapiscan 522B

RAPISCAN THREAT IMAGE PROJECTION

HIT

MISS
NUMBER_ERG_BIT  12 ; After classify energy
ENERGY_TYPE_FLAG  0 ; 0 == DUAL ENERGY, 1 == HIGH, 2 == LOW
CLASS_TBL_CLASS_DIV  349 349 349 ; 1st interval 349-240, 2nd
CLASS_TBL_ENERGY_DIV  20 300 301 900 ; 1st interval 0-100; 100-30

[MAP_CONTROL]
FULL_MAP_FILE  C:\rapiscan\lut\r522bp_f.map
SKIP_MAP_FILE  C:\rapiscan\lut\r522bp_s.map

[SYS_INFO]
OPID_OPTION  0 ; 0 = disable
FOOTMAT_OPTION  0 ; 0 = disable
RAP_PASSWORD  2830
CURTAIN_SW_DELAY  40
FOOTMAT_OPEN_DELAY  50
MONOCHROME_FLAG  0 ; 0 = color, 1 = monochrome
EXTRA_SCAN_CTRL  0 ; 0 = disable (for Auto Bringback)
BIDIR_SCAN_FLAG  0 ; 0=FWD,1=REV,2=BIDIR,3=FW+AB,4=REV+AB
SAFETY_TRIP_OPTION  0 ; 0 = disable
<table>
<thead>
<tr>
<th>User_ID</th>
<th>First_Name</th>
<th>Middle_Init</th>
<th>Last_Name</th>
<th>CharCntInPassword</th>
<th>Password</th>
<th>AccessCode</th>
<th>ActiveCode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0011</td>
<td>Service</td>
<td></td>
<td>Engineer</td>
<td>0</td>
<td>0011</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1234</td>
<td>Temporary</td>
<td></td>
<td>SCREENER</td>
<td>0</td>
<td>1234</td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>
Log On

TIP
Data Integrity problem in User's record

OK Cancel
try {
    if (Checkpassword()){
        Authenticate();
    }
    Else{
        AuthFail();
    }
}
catch{
    ShowErrorMessage();
    Authenticate();
}
“TSA has strict requirements that all vendors must meet for security effectiveness and efficiency and does not tolerate any violation of contract obligations. TSA is responsible for the safety and security of the nearly two million travelers screened each day.”

"Questions remain about how the situation will be rectified and the potential for unmitigated threats posed by the failure to remove the machinery," the committee's Republican and Democratic leaders wrote in a Dec. 6 letter to the men. "It is our understanding that these new components -- inappropriately labeled with the same part number as the originally approved component -- were entirely manufactured and assembled in the People's Republic of China."

“The referenced component is the X-ray generator, a simple electrical item with no moving parts or software.”

He described the piece as "effectively, an X-ray light bulb."

6500407-001 RevD
Kronos MADE IN CHINA
Interesting Items

• VxWorks on PowerPC
• VxWorks FTP
• VxWorks Telnet
• Web server
  • Server: Allegro-Software-RomPager/4.32
  • WWW-Authenticate: Basic realm="Browser"
value = 127 = 0x7f
-> devs
drv name
  0 /null
  1 /tyCo/0
  1 /tyCo/1
  2 /aioPipe
  5 /bpf/dhcpc
  5 /bpf/dhcpc-arp
  6 /pty/telnet.S
  7 /pty/telnet.M
  8 /beeper
  9 /MLkeypad/local
 10 /IOSIMkeypad/
  3 /flash0/
 11 /reader/bc/local
 12 /reader/bc/remotel1
 13 /reader/bc/remote2
 14 /reader/bc/wand
 15 /reader/mag/local
 16 /lcd
 17 /reader/prox/local
 18 /reader/prox/remote

value = 1 = 0x1
-> ifShow
fec (unit number 0):
  Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 192.168.0.102
  Broadcast address: 192.168.0.255
  Netmask 0xffffffff Subnetmask 0xffffffff
  Ethernet address is 00:40:58:04:29:16
  Metric is 0
  Maximum Transfer Unit size is 1500
  0 octets received
  0 octets sent
  2210 packets received
  882 packets sent
  876 unicast packets received
  878 unicast packets sent
  1334 non-unicast packets received
  4 non-unicast packets sent
  0 input discards
  0 input unknown protocols
  0 input errors
  0 output errors
  0 output errors
  0 collisions; 0 dropped

lo (unit number 0):
  Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
  Type: SOFTWARE_LOOPBACK
  Internet address: 127.0.0.1
  Netmask 0xff000000 Subnetmask 0xff000000
value = 0 = 0x0
-> cd "app"
value = 0 = 0x0
-> ls
.
.. M8M.jar
WebC.out
value = 0 = 0x0
->
value = 25 = 0x19

-> java

Usage: java [-options] class

where options include:
- help         print out this message
- version      print out the build version
- v -verbose   turn on verbose mode
- debug        enable remote JAVA debugging
- noasyncgc    no effect. Asynchronous GC support was removed.
- verbosegc    print a message when garbage collection occurs
- noclassgc    disable class garbage collection
- ss<number>   set the maximum native stack size for any thread
- oss<number>  set the maximum Java stack size for any thread
- ms<number>   set the initial Java heap size
- mx<number>   set the maximum Java heap size
- mr<number>   set the red heap reserve size
- my<number>   set the yellow heap reserve size
- D<name>=<value> set a system property
- classpath <directories separated by colons>
  list directories in which to look for application classes
- bootclasspath <directories separated by colons>
  list directories in which to look for system classes
- Xrun<library>[::<option>=<value>,...]
  load library on startup
- verify       verify all classes when read in
- verifyremote verify classes read in over the network [default]
- noverify     do not verify any class

value = 1 = 0x1
BootLine="tffs(0,0)Null:/flash0/os/vxWorksZ e=192.168.0.0"
hostname="Null"
ipAddr="192.168.0.102"
subnetMask="fffff00"
gateway="192.168.0.1"
deviceId="444444"
bootBuildNbr="1000"
ftpUserName="SuperUser"
ftpPassword="2323098716"
basicAuth="yes"
dhcp="no"
dhcpLeaseTime="-1"
hostServerIP="127.0.0.4"
keypad="telephone"
ModemId="@2"
String s6 = (String)hashtable.get("TelnetChoice");
if(s6 != null & & s6.compareTo(DBTransaction.yesNo[0]) == 0)
{
    String s1 = M8MAApp.devMgr.request("get|Configuration|nvParams^ftpUserName");
    if(s1.equals("?"))
    {
        String s2 = M8MAApp.devMgr.request("set|Configuration|nvParams^ftpUserName#SuperUser");
        s2 = M8MAApp.devMgr.request("set|Configuration|nvParams^ftpPassword#2323098716");
        flag = true;
    }
    else
    {
        String s3 = M8MAApp.devMgr.request("get|Configuration|nvParams^ftpUserName");
    }
Protected Object
216.9.106.24
San Francisco International Airport
Added on 26.05.2014
Boulder Creek
Details

HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="Browser"
Content-Type: text/html
Transfer-Encoding: chunked
Server: Allegro-Software-RomPager/4.32
Connection: close

Telnet
at400-1 login:

HTTP
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="Browser"
Content-Type: text/html
Transfer-Encoding: chunked
Server: Allegro-Software-RomPager/4.32
Connection: close

FTP
220 UnWorks (5.4.2) FTP server ready
530 Login failed.
214-The following commands are recognized:
HELP USER PASS QUIT LIST MLST
RETR STOR CWD TYPE PORT PWND
OPEN USER ALIAS TFILE USER

Backdoors...

- FTP and Telnet - SuperUser:2323098716
  - config\devCfg.xml file
  - MaintValidation.class file within the m8m.jar

- Web - KronosBrowser:KronosBrowser

- ~6000 on the Internet, two major airports
Here’s a thought...

• Foreign made main board on TSA Net that can track which TSA personnel are on the floor at any given moment

• Hardcoded FTP password/backdoor

• Hardcoded Telnet password/backdoor which gives up a VxWorks shell

• Hardcoded Web password/backdoor
Does TSA know Kronos 4500’s have Chinese made main boards?

Does the TSA know the software has hardcoded backdoors?
Trust but Verify the Engineering
<table>
<thead>
<tr>
<th>Name</th>
<th>Standard Location</th>
<th>Calibrated Location</th>
<th>Selected</th>
<th>Current Strength</th>
<th>Alarm Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNT</td>
<td>6.070</td>
<td>6.555</td>
<td>+0.040</td>
<td>+0.040</td>
<td>750.0</td>
</tr>
<tr>
<td>NITRO</td>
<td>3.830</td>
<td>4.136</td>
<td>-0.100</td>
<td>+0.120</td>
<td>750.0</td>
</tr>
<tr>
<td>RDX</td>
<td>6.350</td>
<td>6.857</td>
<td>-0.040</td>
<td>+0.040</td>
<td>1000.0</td>
</tr>
<tr>
<td>PETN</td>
<td>7.990</td>
<td>8.629</td>
<td>-0.040</td>
<td>+0.040</td>
<td>150.0</td>
</tr>
<tr>
<td>HMX</td>
<td>7.070</td>
<td>7.635</td>
<td>-0.040</td>
<td>+0.040</td>
<td>1500.0</td>
</tr>
<tr>
<td>AM NO3</td>
<td>4.532</td>
<td>4.884</td>
<td>-0.040</td>
<td>+0.040</td>
<td>1500.0</td>
</tr>
<tr>
<td>TATP</td>
<td>4.120</td>
<td>4.449</td>
<td>-0.040</td>
<td>+0.040</td>
<td>750.0</td>
</tr>
<tr>
<td>TATP2</td>
<td>4.440</td>
<td>4.795</td>
<td>-0.040</td>
<td>+0.040</td>
<td>750.0</td>
</tr>
<tr>
<td>SnklsPwdr</td>
<td>7.449</td>
<td>8.044</td>
<td>-0.040</td>
<td>+0.040</td>
<td>250.0</td>
</tr>
<tr>
<td>COCAINE</td>
<td>7.936</td>
<td>8.570</td>
<td>-0.040</td>
<td>+0.040</td>
<td>750.0</td>
</tr>
<tr>
<td>HEROIN</td>
<td>8.822</td>
<td>9.527</td>
<td>-0.040</td>
<td>+0.040</td>
<td>750.0</td>
</tr>
<tr>
<td>THC</td>
<td>8.757</td>
<td>9.457</td>
<td>-0.040</td>
<td>+0.040</td>
<td>500.0</td>
</tr>
<tr>
<td>METHAM</td>
<td>5.753</td>
<td>6.213</td>
<td>-0.040</td>
<td>+0.040</td>
<td>500.0</td>
</tr>
<tr>
<td>AMPHET</td>
<td>5.664</td>
<td>6.117</td>
<td>-0.040</td>
<td>+0.040</td>
<td>500.0</td>
</tr>
<tr>
<td>MDMA</td>
<td>6.375</td>
<td>6.884</td>
<td>-0.040</td>
<td>+0.040</td>
<td>500.0</td>
</tr>
<tr>
<td>MDA</td>
<td>6.275</td>
<td>6.776</td>
<td>-0.040</td>
<td>+0.040</td>
<td>500.0</td>
</tr>
<tr>
<td>MORPH</td>
<td>7.596</td>
<td>8.203</td>
<td>-0.040</td>
<td>+0.040</td>
<td>750.0</td>
</tr>
<tr>
<td>Ephedrine</td>
<td>5.953</td>
<td>6.429</td>
<td>-0.040</td>
<td>+0.040</td>
<td>1000.0</td>
</tr>
<tr>
<td>Neg-CAL</td>
<td>6.070</td>
<td>6.555</td>
<td>-0.080</td>
<td>+0.080</td>
<td>1000.0</td>
</tr>
<tr>
<td>Pos-CAL</td>
<td>7.936</td>
<td>8.570</td>
<td>-0.080</td>
<td>+0.080</td>
<td>500.0</td>
</tr>
</tbody>
</table>
Itemiser

- X86 (Pentium Processor)
- Windows CE
- Disk on chip with ~7.5 meg main program
- PS2, Floppy, USB
- IrDA?!?!!?!!
File System

• ITMSCE.exe (Main Application)
• Users.bin (User Accounts)
• Config.bin (Settings for detection)
• Options.bin
• History.bin
• Alarms (folder)
Drive in drive C is Ac
Volume Serial Number is 2525-15FY
Directory of C:\

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG</td>
<td>33</td>
<td>04-02-82</td>
</tr>
<tr>
<td>SYS</td>
<td>18,526</td>
<td>02-14-97</td>
</tr>
<tr>
<td>AUTOEXEC/BAT</td>
<td>51</td>
<td>08-30-82</td>
</tr>
<tr>
<td>NW</td>
<td>6,456,335</td>
<td>08-04-82</td>
</tr>
<tr>
<td>LOADEPC/EXE</td>
<td>95,668</td>
<td>07-11-82</td>
</tr>
<tr>
<td>DOC-SST/BAT</td>
<td>259</td>
<td>08-30-82</td>
</tr>
<tr>
<td>ITKSSH</td>
<td>18</td>
<td>02-02-82</td>
</tr>
<tr>
<td>COMMAND/CON</td>
<td>28,547</td>
<td>02-14-97</td>
</tr>
<tr>
<td>HIMEM/SYS</td>
<td>29,136</td>
<td>09-30-93</td>
</tr>
<tr>
<td>CHL/BIN</td>
<td>58</td>
<td>05-26-11</td>
</tr>
<tr>
<td>SERIAL</td>
<td>12</td>
<td>05-13-94</td>
</tr>
</tbody>
</table>

11 file(s)  6,629,833 bytes
619,793,664 bytes free

C:\> copy *.sys a:
Overwrite A:\CONFIG.SYS (Yes/No/All)? A
C:\> A:\HIMEM.SYS
C:\> 2 file(s) copied

C:\> copy *.com a:"
xor eax, eax
and ecx, 3
rep movsb
mov edi, offset a695372 ; "695372"
or ecx, 0xffffffff
repne scasb
not ecx
sub edi, ecx
<table>
<thead>
<tr>
<th>Name</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator 1</td>
<td>Operator</td>
</tr>
<tr>
<td>Maintenance 1</td>
<td>Maintenance</td>
</tr>
<tr>
<td>Administrator 1</td>
<td>Administrator</td>
</tr>
<tr>
<td>Super User 1</td>
<td>Super User</td>
</tr>
<tr>
<td>D. Hansen</td>
<td>Administrator</td>
</tr>
<tr>
<td>J. Eggen</td>
<td>Operator</td>
</tr>
<tr>
<td>C. Henke</td>
<td>Administrator</td>
</tr>
<tr>
<td>D. Winger</td>
<td>Operator</td>
</tr>
<tr>
<td>K. Eckelberg</td>
<td>Administrator</td>
</tr>
<tr>
<td>R. Owen</td>
<td>Operator</td>
</tr>
<tr>
<td>J. Kempt</td>
<td>Operator</td>
</tr>
</tbody>
</table>
Users on the user menu Itemiser

- Operator 1
- Maintenance 1
- Administrator 1
- Super User 1
- <various user accounts>
Users in the Binary

• Operator 1
• Maintenance 1
• Administrator 1
• Super User 1
• Administrator 2
• Super User 2
### Users in the Binary vs User Menu

#### Binary
- Operator 1
- Maintenance 1
- Administrator 1
- Super User 1
- Administrator 2
- Super User 2

#### User Menu
- Operator 1
- Maintenance 1
- Administrator 1
- Super User 1
Two Backdoor Accounts

• Administrator 2: 838635
• SuperUser 2: 695372
Advisory (ICSA-14-205-01)
Morpho Itemiser 3 Hard-Coded Credential

Original release date: July 24, 2014

**Legal Notice**

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

**OVERVIEW**

Independent researchers Billy Rios and Terry McCorkle have identified hard-coded credentials in the Morpho Itemiser 3. Morpho has not produced a patch, update, or new version that mitigates this vulnerability.
MITIGATION

Morpho has decided not to address this vulnerability at this time.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.
Blame the vendor?
This is actually, TSA’s Fault

- TSA depends on this equipment to do their job
- TSA operators do not have the expertise to detect exploited devices
- TSA has not conducted adequate threat models on how these devices are designed from a cyber security standpoint
- TSA has not audited these devices for even the most basic security issues
- Vendors develop devices to meet TSA requirements
- TSA certifies devices it deems satisfactory
- We pay for all this...
I hope that someone (maybe the GAO?) trusts what the TSA is telling us about their devices, but verifies the engineering is a reality.
If you have embedded devices, I would hope you would do the same for your devices BEFORE you fork over the $$!
Questions?