$100 SiLK Network Flow Sensor

Ron Bandes
John Badertscher → Dwight Beaver
Agenda

- What are: SiLK? a Micro-server? Arch Linux ARM?
- Server choices (Raspberry Pi vs. PogoPlug)
- Network Infrastructure – (taps, adapters etc.)
- Design/Implementation choices (Network locations)
- Installation Procedures
- Server Configuration
- Server Management (updates, logs, memory)
- Problems – Things We Would Have Done Differently
What is SiLK?

Tools for the collection and analysis of network flow data

http://tools.netsa.cert.org
What are Micro-Servers?

Characteristics: Small, Low Wattage, Silent

• Raspberry Pi
• PogoPlug
• Typically run Arch Linux [ARM] operating system
What is Arch Linux ARM?

Lightweight Linux OS; well supported by user community

Minimalist – Simplicity - Full control by end-user, targeting competent Linux users

https://github.com/archlinuxarm
Raspberry Pi

- Linux server intended for hobbyists $40
- Includes a graphics adapter (HDMI)

PogoPlug E02

- Intended as a Network Attached Storage (NAS) device $25 on eBay
- Not intended as an all-purpose server
- No console. SSH only

http://www.crunchbase.com/company/cloud-engines
http://mediastreamers.productwiki.com/pogoplugin-video
Server Comparison

<table>
<thead>
<tr>
<th>PogoPlug v2 (E02)</th>
<th>Raspberry Pi model B</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No Console</td>
<td>• Dual VideoCore IV (HDMI)</td>
</tr>
<tr>
<td>• ARMv5te Marvell Kirkwood</td>
<td>• ARMv6h ARM1176JZFS</td>
</tr>
<tr>
<td>• 1.2 GHz processor clock</td>
<td>• 700 MHz processor clock</td>
</tr>
<tr>
<td>• 256 MB RAM</td>
<td>• 512 MB SDRAM</td>
</tr>
<tr>
<td>• 128 MB NAND FLASH</td>
<td>• SD, MMC, SDIO slot</td>
</tr>
<tr>
<td>• 4 USB 2.0 jacks</td>
<td>• 2 USB 2.0 jacks</td>
</tr>
<tr>
<td>• Gigabit Ethernet</td>
<td>• 10/100 Mbps Ethernet (USB)</td>
</tr>
<tr>
<td>• No Real Time Clock</td>
<td>• No Real Time Clock</td>
</tr>
<tr>
<td>• Includes enclosure &amp; power supply</td>
<td>• User provides enclosure &amp; power supply</td>
</tr>
</tbody>
</table>
Alternative Platforms

- Raspberry Pi
- Old laptop/desktop
- Virtualization!
Network infrastructure choices

Taps, adapters etc.

- Cheap managed or “smart” switches
  
  Netgear GS108T-NAS
  
  - VLANs
  - LAGs
  - Port Mirroring
  - $80

- Iptables on a wireless access point (OpenWRT)
  
  - iptables -A PREROUTING -t mangle -j ROUTE --gw <sensor ip> --tee
  
  - iptables -A POSTROUTING -t mangle -j ROUTE --gw <sensor ip> --tee
Solution Components

$100 Solution

- PogoPlug server ($25)
- NoName Ethernet Adapter ($4)
- MikroTik switch as network tap ($40)
- 16 GB Flash Drive ($10)
2nd Ethernet Adapter

- For network monitoring – 10/100 Mbps $3.75
- The 1st adapter is for server management

http://www.tmart.com/Rj45-Ethernet-10-100-USB-Network-Adapter-Purple_p123164.html
Network Tap

- MikroTik RB260 switch w/SPAN port $40

http://www.lanmart.ru/blogs/review-mikrotik-rb260gs

Design & Implementation Choices

- Network monitoring locations
- Separate analysis server or combined node
- Implications of flash storage
Network Monitoring Locations

Between edge router and cable modem

- Easy constriction point for monitoring
- Outside the Network Address Translation (NAT)

On LAN

- Inside the NAT
- Hard to place when a residential router is used
  - Need to interpose tap between the LAN switch and the router component, which is NOT exposed in residential router
Tap between Router and Cable Modem

Router

Switch (tap)

YAF (sensor)

Cable Modem
Residential Routers

Switch

DHCP Server

Firewall

Router

NAT

Monitor here?!

Internet

Wireless Access Point
Configuring the Tap

- Port 1 – Switch management
- Ports 2&6 – Unused
- Ports 3&4 – Link to be tapped (rtr & cable mdm)
- Port 5 – Monitoring port 4

http://www.tapmytrees.com/
# Switch (tap) Configuration

## MikroTik SwOS

<table>
<thead>
<tr>
<th></th>
<th>Port1</th>
<th>Port2</th>
<th>Port3</th>
<th>Port4</th>
<th>Port5</th>
<th>SFP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forwarding</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From Port 1</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From Port 2</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From Port 3</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From Port 4</td>
<td>□</td>
<td></td>
<td>□</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From Port 5</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From SFP</td>
<td>□</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Port Lock</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Lock</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock On First</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Port Mirroring</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mirror Ingress</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>Mirror Egress</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>Mirror To</td>
<td></td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td>□</td>
</tr>
</tbody>
</table>
Repurposing Non-Hobbyist HW

- PogoPlug requires you to register on pogoplug.com before you can SSH into your device.
- This could be a problem if you bought the PogoPlug on eBay and the original owner registered it.
- PogoPlug can be repurposed for a variety of applications (e.g., Tor Relay, NAS, Streaming Server etc.)
Installation Procedures

1. Install Arch Linux ARM
2. Update Arch Linux ARM*
3. Install 2\textsuperscript{nd} Ethernet adapter
4. Install YAF
5. Install SiLK

*Run Update FREQUENTLY
*When in doubt…update \textit{again}!

http://www.aquacityplumbing.com/images/pages/Plumbing-Installation.jpg
Installation Challenges

- Arch Build System: `buildpkg & pacman`
- `Systemd` vs. `init`
- `vi` vs. `vim`
- `U-Boot` boot-loader
  - Installed on internal Flash, not mass storage
  - Arch Linux requires newer `U-Boot` than what comes on the PogoPlug

http://wwiimodeller.co.nz/wp-content/uploads/1355087242_s_010_basic_boxes_small.jpg
Server Configuration

1. Create “service” to bring up 2\textsuperscript{nd} Ethernet adapter
2. Create service for rwflowpack
3. Create service for YAF

\begin{figure}
\centering
\includegraphics[width=\textwidth]{server_configuration_diagram}
\end{figure}
Management procedures

Arch Linux ARM updates

Logging

• Logs will eventually fill storage if you don’t rotate them
• FLASH memory has a limited number of writes
  — Minimize writing by minimizing logging
It works!

```bash
[root@pogotor system]# rwfilter --type=in,inweb --all=-
| rwuniq --fields=dip
| dIP | Records |
| 192.0.2.212 | 55 |
```

```bash
[root@pogotor system]# rwfilter --type=out,outweb --all=- | rwuniq --fields=sip
| sIP | Records |
| 192.0.2.212 | 49 |
```

```bash
[root@pogotor system]# rwfilter --type=all --all=- | rwuniq --fields=type
| type | Records |
| outweb | 33 |
| in | 18 |
| out | 16 |
| inweb | 37 |
| ext2ext | 30 |
```
Performance & Metrics

Raspberry Pi

• No PCI BUS
• NIC lives on USB bus
• 700 MHz processor main bottle neck
• YAF starts dropping packets around 55 Mbps
• No application labeling
Problems: Things We Would Have Done Differently…

- You don’t get what you don’t pay for…
  - Effort (Opportunity Cost)
  - Bandwidth
- Update management
- U-Boot
- PogoPlug becomes a brick

Software Problem with ARMv5

Unaligned memory word accesses on ARMv5 processors have results that are “implementation defined.” Some Memory Management Units may handle this improperly.

It also helped (a lot) having CERT developers, Emily Sarneso and Dan Ruef, available to help.
Questions?

http://cuteoverload.files.wordpress.com/2012/10/8024316149_438e648edf_b1.jpg%3Fw%3D560