Secure and Reliable Firewall Systems based on MINIX 3

Rüdiger Weis
Beuth Hochschule für Technik Berlin
MINIXCon 2016
MINIX 3 is initially targeted at the following areas:

- Applications where very high reliability is required
- Single-chip, small-RAM, low-power, $100 laptops
- Embedded systems
- Education (e.g., operating systems courses at universities)
Minix3 Features

- POSIX compliant
- Full C source code supplied under a BSD-type licence.
- Networking with TCP/IP
- **Device drivers run as user processes**
- **High degree of fault tolerance**
TFH-Berlin Diplomarbeit: Netfilter

- Diplomarbeit, Juli 2007, TFH Berlin
- Brian Schüler
- Analysis and Porting of a network filtering architecture on Minix-3

Rüdiger Weis
Secure and Reliable Firewall Systems based on MINIX 3
Minix3 versus Linux

Linux System

Minix3 Mikrokernel

Minix Userspace

Firewall

Vulnerable Area

Secured Area

Network Packets

Firewall coupled with Kernel

Firewall decoupled from Kernel

MINIX 3 System

Minix Userspace

Firewall

Minix Microkernel

Secure and Reliable Firewall Systems based on MINIX 3
### Minix3 Netfilter in USERMODE

<table>
<thead>
<tr>
<th></th>
<th>Linux Netfilter</th>
<th>Minix Netfilter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crash Attack</td>
<td>System Crash</td>
<td>Restart Process</td>
</tr>
<tr>
<td>Executable Code</td>
<td>Owned System</td>
<td>Owned Usermode Process</td>
</tr>
</tbody>
</table>
MINIX 3 - Reliability

http://www.minix3.org/reliability.html

- Reduce kernel size
- Cage the bugs
- Limit drivers’ memory access
- Restrict access to kernel functions
- Restrict access to I/O ports
- Restrict communication with OS components
- Reincarnate dead or sick drivers
- Survive bad pointers
- Tame infinite loops
- Limit damage from buffer overruns
- ...

Rüdiger Weis
Beuth Hochschule für Technik Berlin
Secure and Reliable Firewall Systems based on MINIX 3
Firewall Virtualisation

- Weis, Schüler, Flemming:
- Towards Secure and Reliable Firewall Systems based on MINIX 3
Virtualisation

Incoming unfiltered network traffic

Filtered network traffic

Harmless Packets
Malicious Packets

Virtualization Layer
MINIX3 Firewall
LINUX
Router Hardware

Secure and Reliable Firewall Systems based on MINIX 3