

Secure and Reliable Firewall Systems based on MINIX 3

Rüdiger Weis

Beuth Hochschule für Technik Berlin

MINIXCon 2016

Minix3

<http://www.minix3.org/>


MINIX 3 is initially targeted at the following areas:

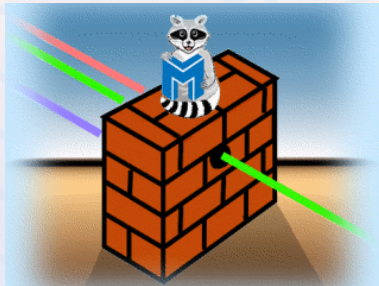
- Applications where very high reliability is required
- Single-chip, small-RAM, low-power, \$100 laptops
- Embedded systems
- Education (e.g., operating systems courses at universities)

Minix3 Features

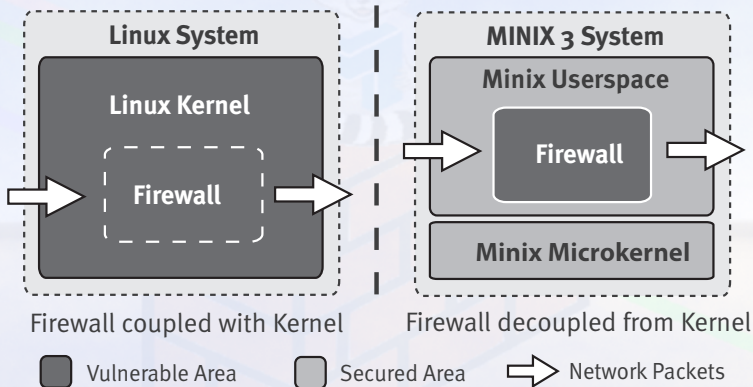
- POSIX compliant
- Full C source code supplied under a BSD-type licence.
- Networking with TCP/IP
- **Device drivers run as user processes**
- **High degree of fault tolerance**

TFH-Berlin Diplomarbeit: Netfilter

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



Minix3 versus Linux



Minix3 Netfilter in USERMODE

| | Linux Netfilter | Minix Netfilter |
|-----------------|-----------------|------------------------|
| Crash Attack | System Crash | Restart Process |
| Executable Code | Owned System | Owned Usermode Process |

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
- ...

Firewall Virtualisation

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



Virtualisation

