Trusted computing applied in Open Power Linux

Qiuyin Mao, R&D Director
Zhiqiang Tian, Senior BIOS Engineer

Beijing Neu Cloud Oriental System Technology Co. Ltd.
(NCO China)
Agenda

- NCO(China) introduction
- Background
- Demonstrated Features
- Our experience
- Benefit

Join the conversation at #OpenPOWERSummit
Beijing Neu Cloud Oriental System Technology Co., Ltd

- Leading High Performance Server Manufacturer in China, Invested By IBM
- Teamsun’s Holdings Subsidiary

Neu Cloud is committed to the events focusing on the IBM POWER servers manufacturing, the localization and the well matched platform and ecological system. Owing to establish a comprehensive ecological system and manufacturing chain, Neu Cloud infuses substantial R&D into the domains of server, database, middleware, virtualization, cloud computing and big data. What’s more, joint great efforts with leading enterprises by reaching agreements to chart a promising future.
The computer system security problem is more and more emphasized by the Chinese government and it has created its own security standards. Open POWER as a new open platform, it urgently needs to achieve China's trusted computing security standard and provides the prototype system that conforms to the specifications in order to satisfy the demands of the development of Open POWER ecosystem in China.
Demonstrated Features

Trusted motherboard: As the RTM of the Trusted computing, provides the highest security solution.
Demonstrated Features

TPCM card:
- Embedded in mother board that has the highest security standard but it need design new platform board
- As a PCIE device, implements TPCM and no HW change in system. It can work after PCIE device is ready during BIOS post stage.
- As a USB device, it can only work after OS loads its’ driver.
Demonstrated Features

Implemented trusted chain pass from RTM to application
Demonstrated Features
Based on the white list and trusted database to implement Trusted Computing in OS kernel.
Demonstrated Features

Support TPCM card in open power firmware level to support open power virtualization
Demonstrated Features

Apply the open power trusted computer node to China security Cloud system
Our experience

We choose Linux as the application OS and it is easy to port the whole trusted computing software stack to other UNIX like OS such as AIX.
Our experience

Join the conversation at #OpenPOWERSummit
Our experience

* We developed Linux release version based on Debian and can support Loongson, ARM, X86/AMD and Power
* We setup a strong automated building and testing infrastructure to speed up the development
Our experience

- Security Enhanced Power Linux Architecture

- Application (Web Service...)

- SW support level (SDK)

- Trusted SW level (Service, API)

- Secured Linux Kernel

- Trusted immune system (Trusted kernel)

Join the conversation at #OpenPOWERSummit
Our experience

“White list” is a kind of new computing operation and protection mode, it utilize active immunization through identification, state metric, confidential storage function so that it can timely recognize "own" or threat and block harmful substances into the body.
Our experience

Trusted Computing Architecture

Identify
Get subject, object

Control
Set subject access rule
right, wrong

Alert
Audit system behavior

System Manage
Security Manage
Audit Manage

Trusted Immune Management Platform
Our experience

- Security Hole Detect Service
- Security Trend Service
- SW certification service
- Audit Service
- Trusted Policy Service
- Trusted SW Service
- Immune Service

Join the conversation at #OpenPOWERSummit
Benefit

The prototype implementation on the open power system that abides by the security standards of China provides strong support for the comprehensive power system promotion and in the meantime it provides a powerful guarantee for the development of power ecosystem in China high security level market. It enriches the China ISV and IHV’s options range with this total solution from hardware to software.