社区与发行版

openSUSE miniSummit @Scale13x – summary

Hi Geekos, here is a small summary of our Thursday February 19th openSUSE miniSummit event here at SCALE 13x.

Located in Century AB room, a 80 seats room, the average attendance rate was varying between 50% and 85%.

Qualifying the attendance 50% or more were not related to SUSE / openSUSE, which had a good wealth of questions and feedback.

The day started by a talk about openSUSE / SUSE Xen and openstack by Peter Linnel and Russel Pavlicek.

One hour later Manu Gupta has presented all the bolts and nuts about Google Summer of Code at openSUSE.

We then go for lunch, and corridor exchanges.

I opened the afternoon with my talk “them + me = we” about breaking mythic frontier.

Then, just after a small break, Mark Fasheh, a member of filesystem SUSE Labs group, had a talk about the project Duperemove: dedupe on btrfs (have a look of the source on github, and the package available on obs).

The day continued with a Town Hall talk by myself and Peter running an open discussion with attendees. With interesting remarks and feedback from openSUSE users, and also complete foreigners. For example, the way systemd was introduced in openSUSE distribution was appreciated (having choice during 2 versions). It was an unstressfull, open and positive exchange.

To follow, Bryan Lunduke and Peter animated a talk about “the 10 things you would love about SUSE and openSUSE if you only you knew…”

I did really enjoy the way they numbered the slides … Freschy, punchy, funky, the kinda talk I would like to see again at OSC15.

To finalize the day, Markus Feilner for Linux Magazine (Germany) talked about openQA.

I found the day interesting and a perfect mix between openSUSE and SUSE during this day, confirming the excellent partnership we have.

Thanks you to the sponsors of this day and to all those who helped make it happen.

Links : SCALE picture album day 1 : by Françoise on G+

openSUSE miniSummit day album : Bruno’s Album on G+

Follow the news on G+ channel

Stay tuned for more news during this week-end.

软件与系统

Boot Guard 与 Coreboot

Coreboot 作为得到 FSF 青睐的开源 BIOS 方案，已经随着 Chromebook 的发布成长了不少。不过若是您想要在新近购买、搭载 Intel Broadwell 处理器上的壕笔记本使用 Coreboot 的话，死了这条心吧……

由于各方面的限制，在市场上找到一块兼容主流 CPU 且被 Coreboot 支持的桌面级主板相当困难，支持的笔记本则更少了。而这个问题很可能会随着 Broadwell 处理器的铺开变得更加严峻。

近日PCWorld发布了一篇文章，简单介绍了 Intel 在 Broadwell 处理器上引入的名为 Boot Guard 的技术。

简单来说，该技术允许 OEM 厂商将使用非对称密钥签名的公钥部分烧入 CPU，这样意味着未经厂商签名的 BIOS 固件将会被 CPU 拒绝执行。

根据 Intel 方面的表示，这些技术主要是为了避免黑客通过修改固件的方式，绕过 UEFI 固件中 Secure Boot 的安全保护。不过从技术上来讲，Boot Guard 提供了两种模式：

- Verified Boot 模式下会验证固件签名，且将完全拒绝未通过验证固件的运行
- Measured Boot 模式下将启动过程的信息记录到 TPM（可信任平台模组）中，交由操作系统去做后续进一步处理。

和 Secure Boot 模式状态可以由用户翻遍 UEFI 后再禁掉不同，Boot Guard 的模式是由 OEM 在出厂前决定的。而几乎所有的笔记本厂商在搭载 Broadwell 笔记本出厂前都将 Boot Guard 设为了第一种模式，在带来安全性的一定提升，与 Coreboot 等第三方固件永别了。

当年对 Secure Boot 开炮且实现 Linux 支持的 Matthew Garrett 在自己的博客上再次开轰，认为 Intel 引入的 Boot Guard 技术在某种程度上可以说是逼迫厂商在安全与自由之间做抉择，结果是消费者的选择自由以“大多数的安全”名义被剥对了。他认为，对于整个行业来讲，引入一项新技术时应同时考虑安全与自由，而非对立起来。

如同某个在 Phoronix 读者评论中所说的，安全关乎的是谁掌握着钥匙。如果您被安全的门紧紧保护起来了，但是却没有钥匙，那恐怕只能是监狱。