Karthik Jayaraman

University of Oslo

LinuxCon 2012

San Diego, August 29 to 31

Background

I am a PhD student at the University of Oslo and my research is centered around Design, Standardization and innovation in mobile software ecosystems such as Android. The focus of my research lies in the periphery of technology engineering, socio-technical aspects such as stakeholders and institutions and economics of platforms such as Android and their ecosystems.

The LinuxCon is a leading annual technical conference on Linux and open source. LinuxCon is known for attracting leading speaking talent from a cross-section the Linux community, industry and academia. One of the key focus of LinuxCon 2012 has been embedded Linux and Android. There were various sessions on technical aspects such as Android security, SDK, backward compatibility, app stores and their economic and legal aspects were presented and debated in the conference.

The conference provided a platform for understanding the current developments around Android and also the future roadmap for the evolution of various embedded Linux technologies. The usefulness of this conference for my research came from the lectures that were relevant to my research and the interactions with the speakers and participants (developers, industry veterans and academicians) on some of the topics that I am currently investigating.

On Mobile apps, app stores and compliance

Mobile apps have become key accelerators of commerce for many businesses. Apps and app stores now cater to PC's, mobile devices such as tablet, web platforms, and cloud computing devices and various vendors offer their own marketplaces for service specific apps. Due to the increase in the usage of FOSS in apps there are also various violations of the open source licenses and some developers are unaware or just do not care about these violations.

The speaker described the violations of FOSS licenses as being caused by a failure to comply with four key license obligations. The obligations that were analyzed and presented at the conference were the below.

The GPL and LGPL license requires app developers who use the FOSS code to provide source code or an offer to get the source code and provide a copy of the license , the FOSS code used in apps that are based on the Apache software license requires app developers to provide a copy of the license and provide notices/attributions. The presenter of the talk described that 71% of the apps that they scanned failed to comply with these requirements, leading to a serious violation of the licensing agreement. Some of the reasons for the failure to comply were lack of awareness on licensing obligations and lack of resources that could help with the process of compliance. Some of the mobile apps that later achieved compliance did so by adding an offer for to download source code or a copy of the license but a majority of the apps resolved their compliance issues by removing the non-compliant open source components altogether. The talk was useful in understanding open source compliance issues related to Android and how the stakeholders are affected by the lack of awarness.

Android Security

One of the key strengths of Android is its open nature but it also makes Android easier to infect with malicious code. Various exploits have been created that can cause Android to skip user approval for certain actions, enabling the device to send information to hackers or record calls without the user knowing about it.

The talk on security enhanced Android discussed some of the key issues related to Android security and how the security issues can be fixed. The focus of a security enhanced Android is to prevent data leakage by apps, prevent bypass of security features, enforce legal restrictions on data, protect integrity of apps and data. The speaker described Kernel security in the existing Android releases as being enforced through App isolation and sandboxing, Any app in the Android system can run native code and the access control is based on the Linux discretionary access control (DAC). Some of the problems with DAC is that access to data is entirely at the discretion of the owner/creator of the data. Some processes such as root (uid 0) can override and some objects (e.g. sockets) are unchecked. The security policies are hardcoded and scattered.

The speaker described a security enhanced Android system where the policy enforcement is based on Mandatory Access Control (MAC) for Linux, which enforces a system-wide security policy based on security labels. This can confine flawed and malicious applications and prevent privilege escalation, which are observable in the existing Android framework.

The speaker demonstrated the benefits of SELinux through various cases of running exploits on processes such as the Android volume Daemon and how enforcing system-wide SELinux policies can secure the system from hackers trying to exploit the vulnerabilities of the existing DAC based Android system. The talk helped key security issues related to the design of the Android platform and how these issues can impact the overall ecosystem.

Conclusion

This was a very useful conference, I attended various talks on Android and its ecosystem, building embedded Linux systems for various devices and security related issues. Talks on the future of Android on automobiles provided a new perspective on how the Android ecosystem in the future will be extended based on the context of spaces (living room, automobiles, public areas) and device centric such as tablets and cellphones. Thanks to the NUUG foundation, I was able to collect relevant data from this conference, which will be useful for my current and future research pursuits.