Technische Universität München

Enhanced Android Security to prevent Privilege Escalation

Bachelorarbeit in Informatik

Janosch Maier

Outline

- Android Security – Fitting together?
- Evaluated Defense Mechanisms
  - Virtualization
  - SEAndroid
  - User Interaction
- Live Demo
- Conclusion

Technische Universität München

Enhanced Android Security to prevent Privilege Escalation

Bachelorarbeit in Informatik

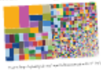
Janosch Maier

Outline

- Android Security – Fitting together?
- Evaluated Defense Mechanisms
  - Virtualization
  - SEAndroid
  - User Interaction
- Live Demo
- Conclusion

Android & Security?

Android Fragmentation



Privilege Escalation?

Root Exploits

IPC Exploits

Companies need Data Isolation

SEAndroid

Other kernel hardening possible as well (e.g. restrict setuid)

```
# Device types
type exynos_device, dev_type;
```

[illegible]

Policies control file access:
No policy – No access!

Virtualization

In-App-Virtualization
- All business apps are locked in a container
- Communication with host system?

System Virtualization
- Multi Boot
- Strict separation
- Root exploits (on host)

Demo Videos

Have a close look...

User Interaction

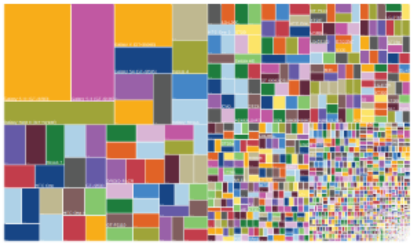
Something like this for all intents?
- User knows what is legit...?
- EULA-phenomenon

Conclusion

Increased Security
- Multi-Boot + SELinux
- Merge needed
- Better security in 4.3

Android & Security?

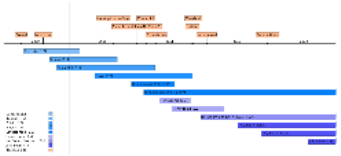
Android Fragmentation



Source: http://opensignal.com/reports/fragmentation-2013/ (26/09/2013)

Privilege Escalation?

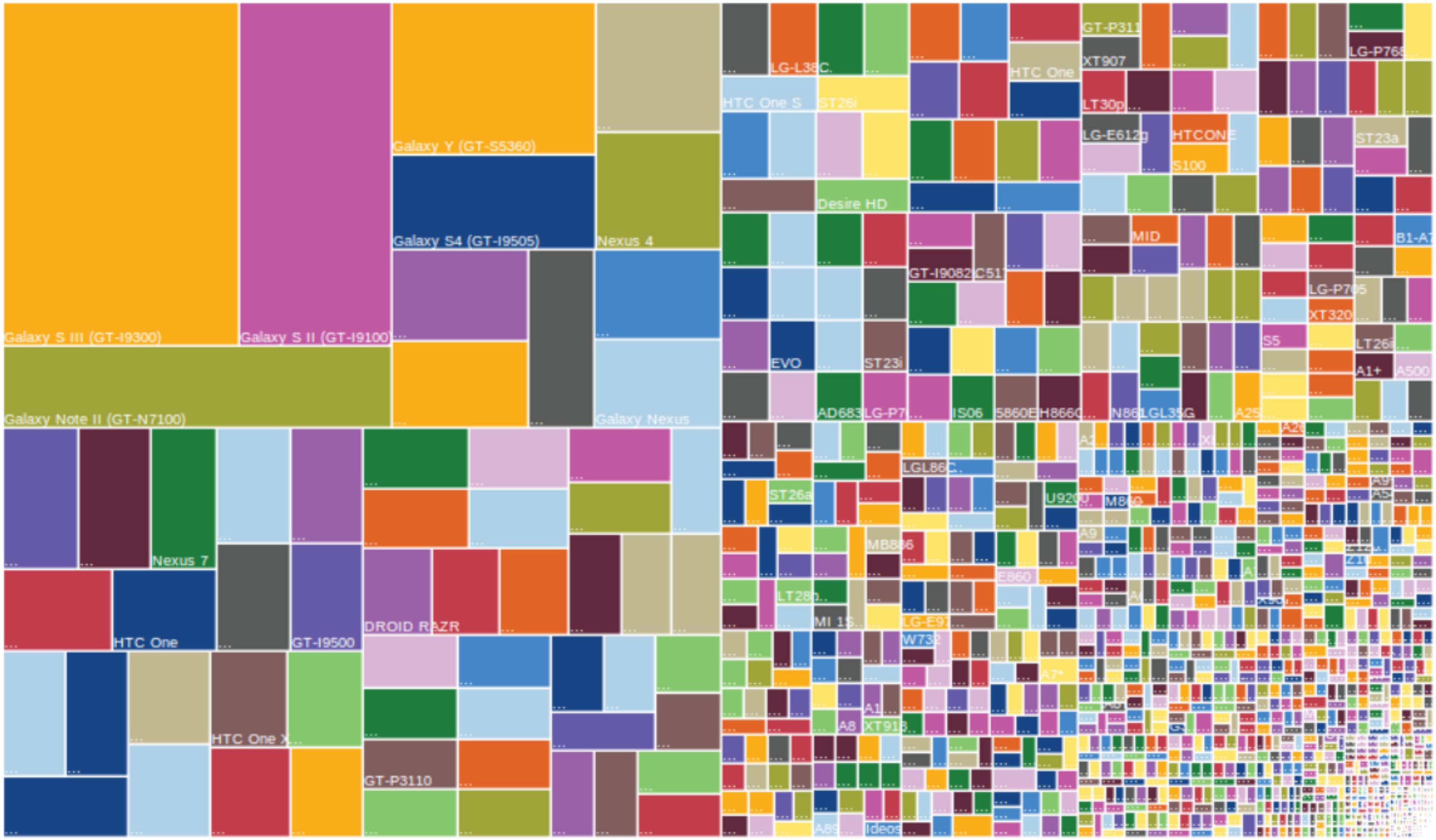
Root Exploits



IPC Exploits

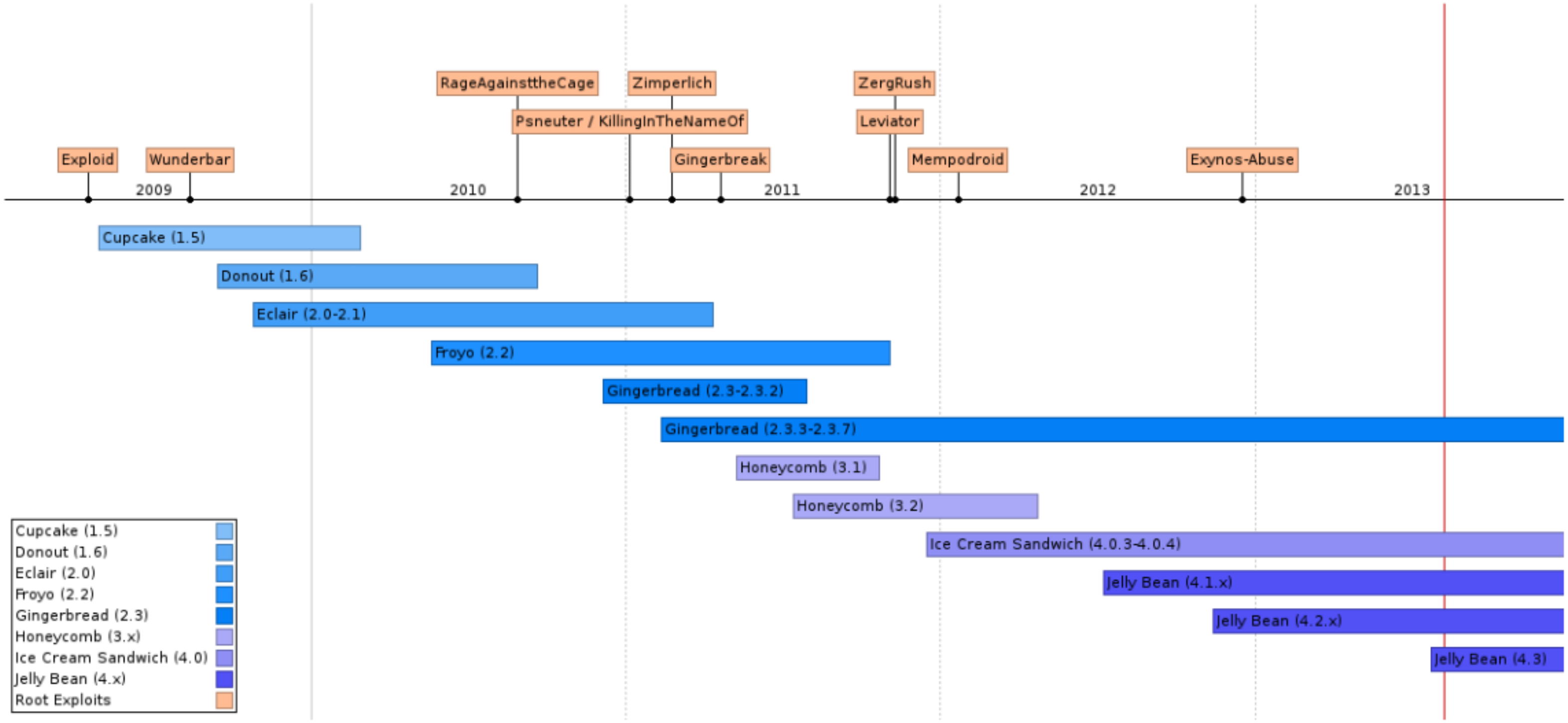
Companies need Data Isolation

Android Fragmentation



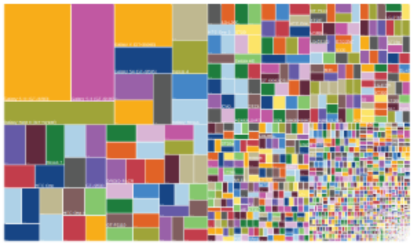
Source: http://opensignal.com/reports/fragmentation-2013/ (26/09/2013)

Root Exploits



Android & Security?

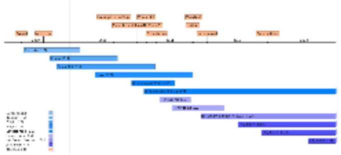
Android Fragmentation



Source: http://opensignal.com/reports/fragmentation-2013/ (26/09/2013)

Privilege Escalation?

Root Exploits



IPC Exploits

Companies need Data Isolation

Outline

- Android Security – Fitting together?
- Evaluated Defense Mechanisms
  - Virtualization
  - SEAndroid
  - User Interaction
- Live Demo
- Conclusion

Android & Security?

Android Fragmentation

Privilege Escalation?

Root Exploits

IPC Exploits

Companies need Data Isolation

SEAndroid

Other kernel hardening possible as well (e.g. restrict setuid)

```
# Device types
type asyncs_device, dev_type;
```

Policies control file access:
No policy – No access!

Virtualization

In-App-Virtualization
- All business apps are locked in a container
- Communication with host system?

System Virtualization
- Multi Boot
- Strict separation
- Root exploits (on host)

Demo Videos

Have a close look...

User Interaction

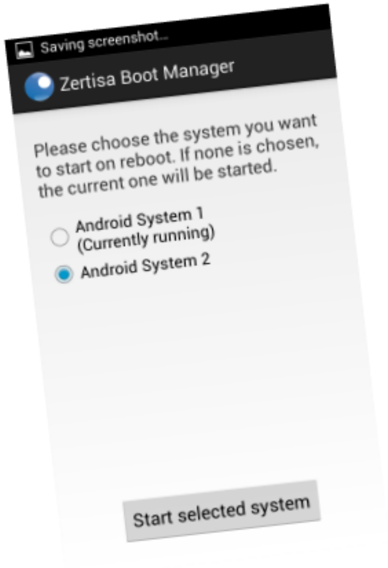
http://goo.gl/fownE1

Something like this for all intents?
- User knows what is legit...?
- EULA-phenomenon

Conclusion

Increased Security
- Multi-Boot + SELinux
- Merge needed
- Better security in 4.3

Virtualization



Saving screenshot...

Zertisa Boot Manager

Please choose the system you want to start on reboot. If none is chosen, the current one will be started.

○ Android System 1 (Currently running)

● Android System 2

In-App-Virtualization

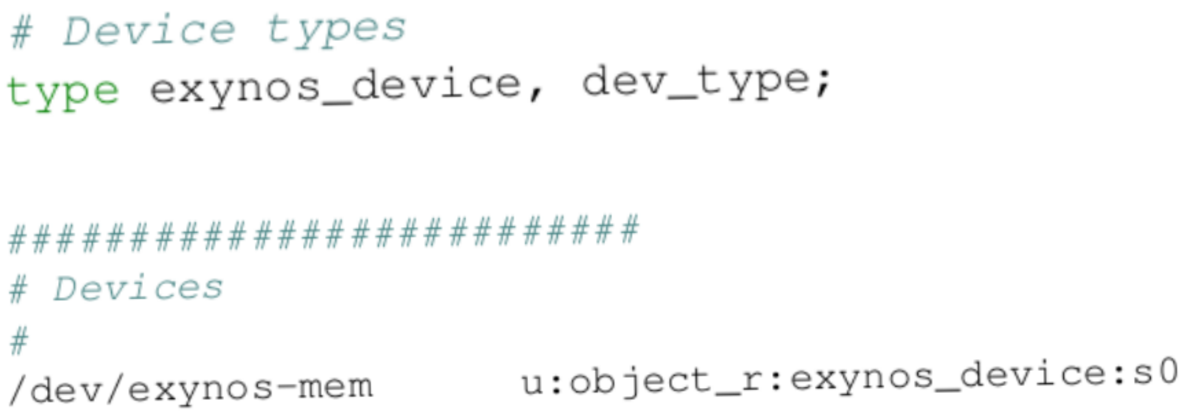
- All business apps are locked in a container
- Communication with host system?

System Virtualization

- Multi Boot
- Strict separation
- Root exploits (on host)

SEAndroid

Other kernel hardening possible as well (e.g. restrict setuid)



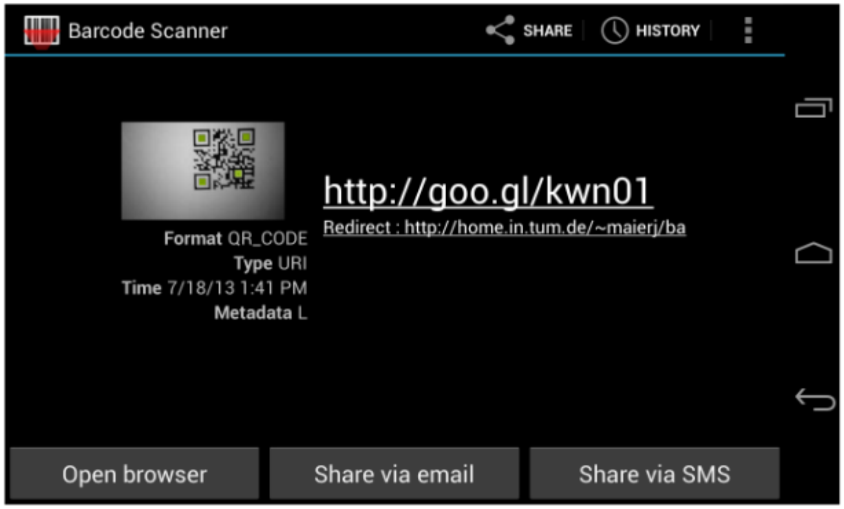
```
# Device types
type exynos_device, dev_type;


#########################
# Devices
#
/dev/exynos-mem          u:object_r:exynos_device:s0
```

Policies control file access:

No policy – No access!

User Interaction



http://goo.gl/kwn01

Redirect : http://home.in.tum.de/~maierj/ba

Format QR_CODE
Type URI
Time 7/18/13 1:41 PM
Metadata L

Something like this for all intents?

- User knows what is legit...?
- EULA-phenomenon

Outline

- Android Security – Fitting together?
- Evaluated Defense Mechanisms
  - Virtualization
  - SEAndroid
  - User Interaction
- Live Demo
- Conclusion

Android & Security?

Android Fragmentation

Privilege Escalation?

Root Exploits

IPC Exploits

Companies need Data Isolation

Virtualization

In-App-Virtualization
- All business apps are locked in a container
- Communication with host system?

System Virtualization
- Multi Boot
- Strict separation
- Root exploits (on host)

SEAndroid

Other kernel hardening possible as well (e.g. restrict setuid)

```
# Device types
type anyone_device, dev_type;
```

Policies control file access:
No policy – No access!

Demo Videos

Have a close look...

User Interaction

http://goo.gl/fownE1

Something like this for all intents?
- User knows what is legit...?
- EULA-phenomenon

Conclusion

Increased Security
- Multi-Boot + SELinux
- Merge needed
- Better security in 4.3

Demo Videos

Have a close look…

Conclusion

Increased Security

- Multi-Boot + SELinux
- Merge needed
- Better security in 4.3

Questions?

maierj@in.tum.de

More Info?

http://phynformatik.de/de/publications/

Questions?

maierj@in.tum.de

More Info?

http://phynformatik.de/de/publications/