Taming the Robots

Enhancing Security of Multi-Personality Mobile Devices

Matthias Lange, Toorcon San Diego, Oct. 20th, 2012
mlange@sec.t-labs.tu-berlin.de

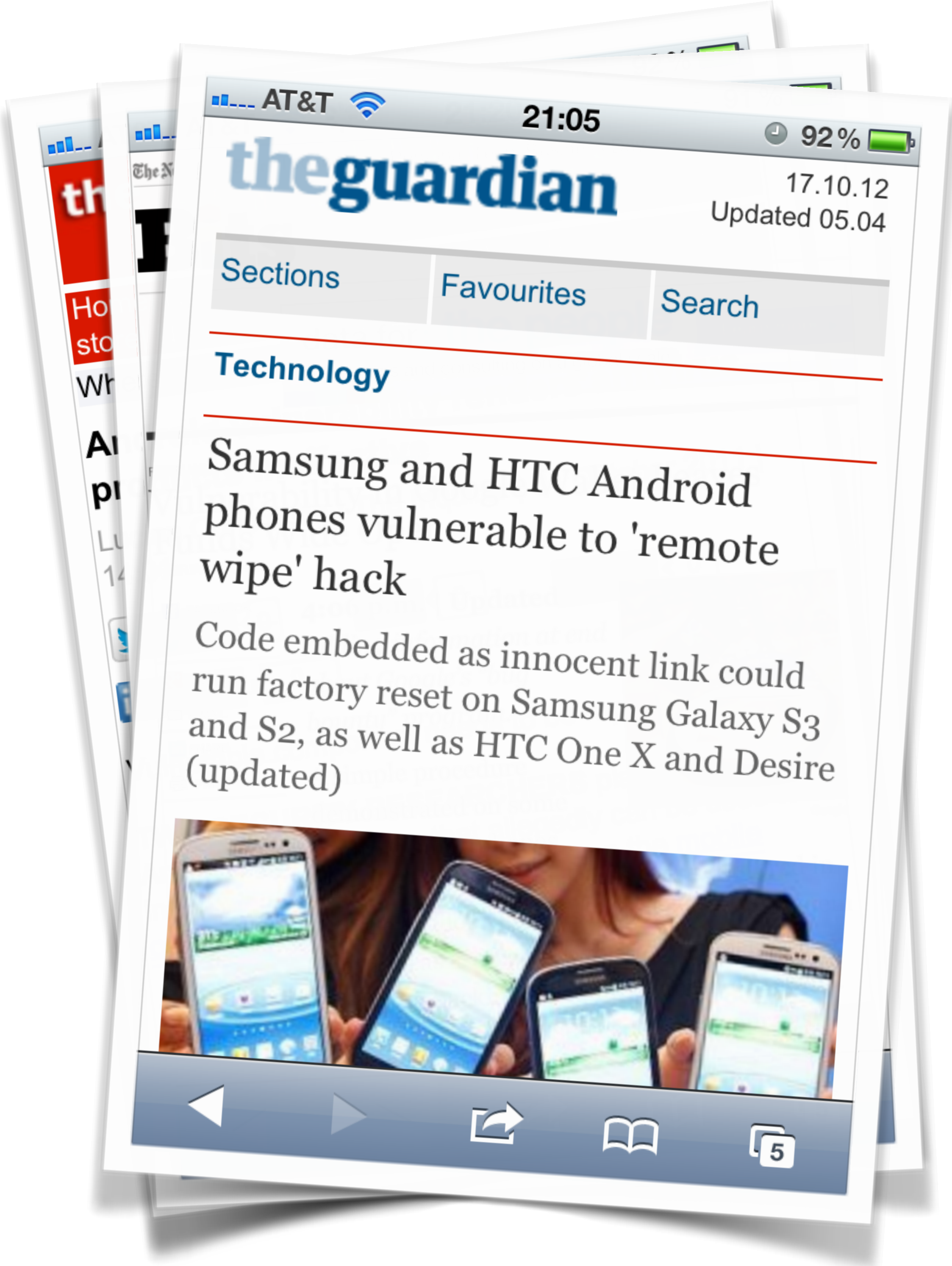
This talk is not about
breaking things

picture © www.norebbo.com

Motivation

Security

- Emerging threats
- Existing OS not secure



17.10.12
Updated 05.04

Technology

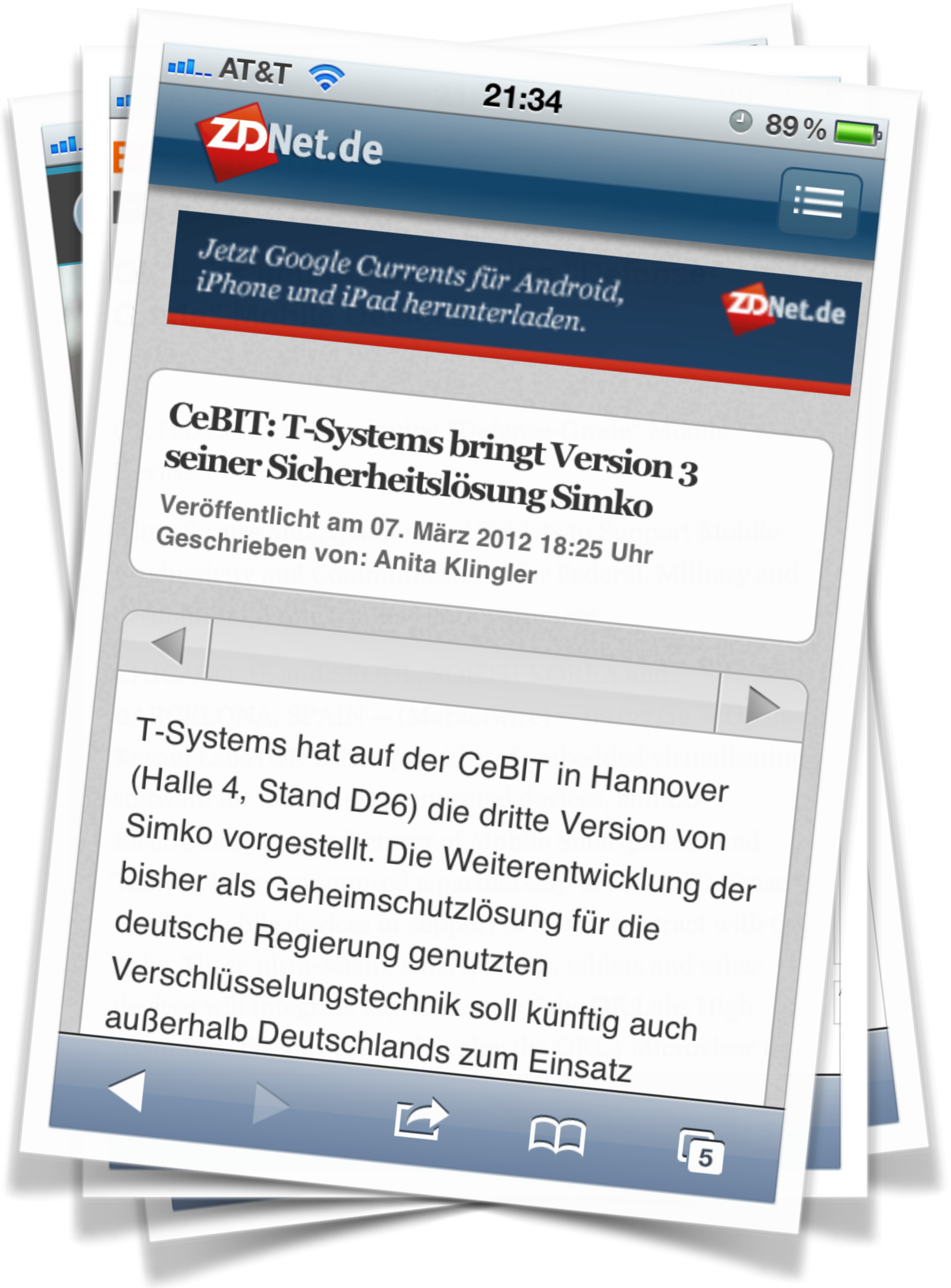
Samsung and HTC Android phones vulnerable to 'remote wipe' hack

Code embedded as innocent link could run factory reset on Samsung Galaxy S3 and S2, as well as HTC One X and Desire (updated)

BYOD and Secure Smartphones

- Multi-Personality

- Governments



Jetzt Google Currents für Android, iPhone und iPad herunterladen.

CeBIT: T-Systems bringt Version 3 seiner Sicherheitslösung Simko

Veröffentlicht am 07. März 2012 18:25 Uhr
Geschrieben von: Anita Klingler

T-Systems hat auf der CeBIT in Hannover (Halle 4, Stand D26) die dritte Version von Simko vorgestellt. Die Weiterentwicklung der bisher als Geheimschutzlösung für die deutsche Regierung genutzten Verschlüsselungstechnik soll künftig auch außerhalb Deutschlands zum Einsatz

Future Applications

- Secure text and voice
- NFC
- eHealth

How we gonna do this?

picture © www.norebbo.com

Patch OS?

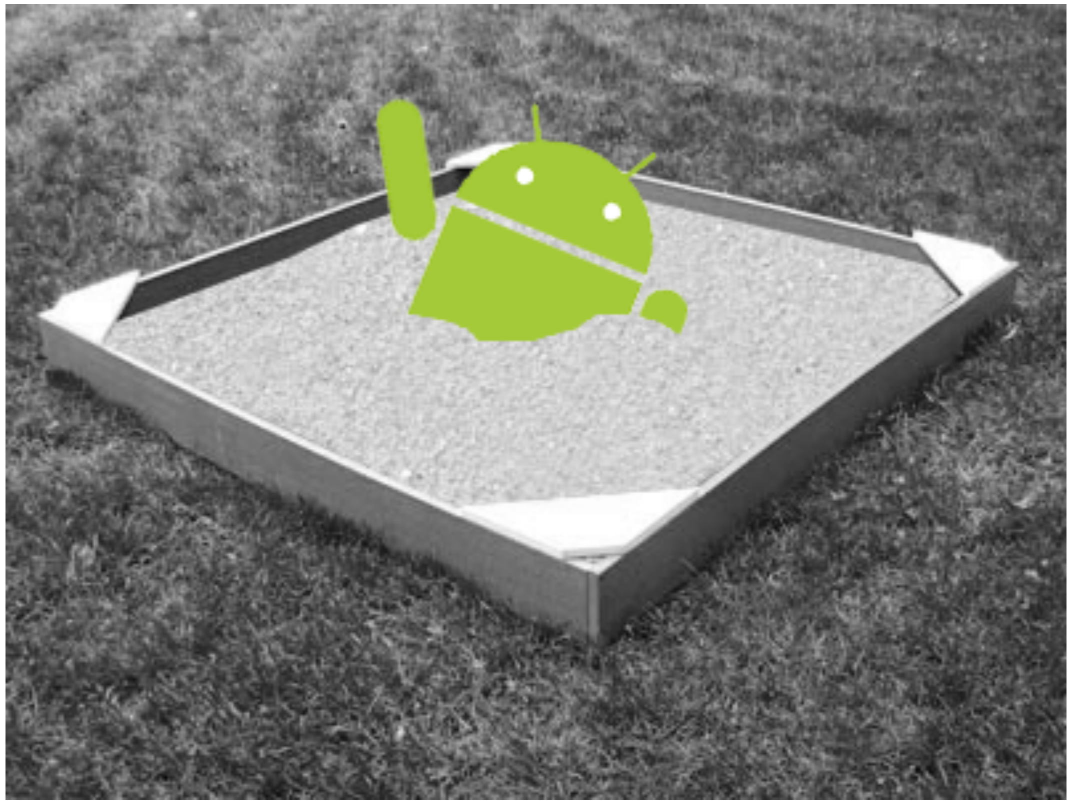
Bad update record
Fragmentation

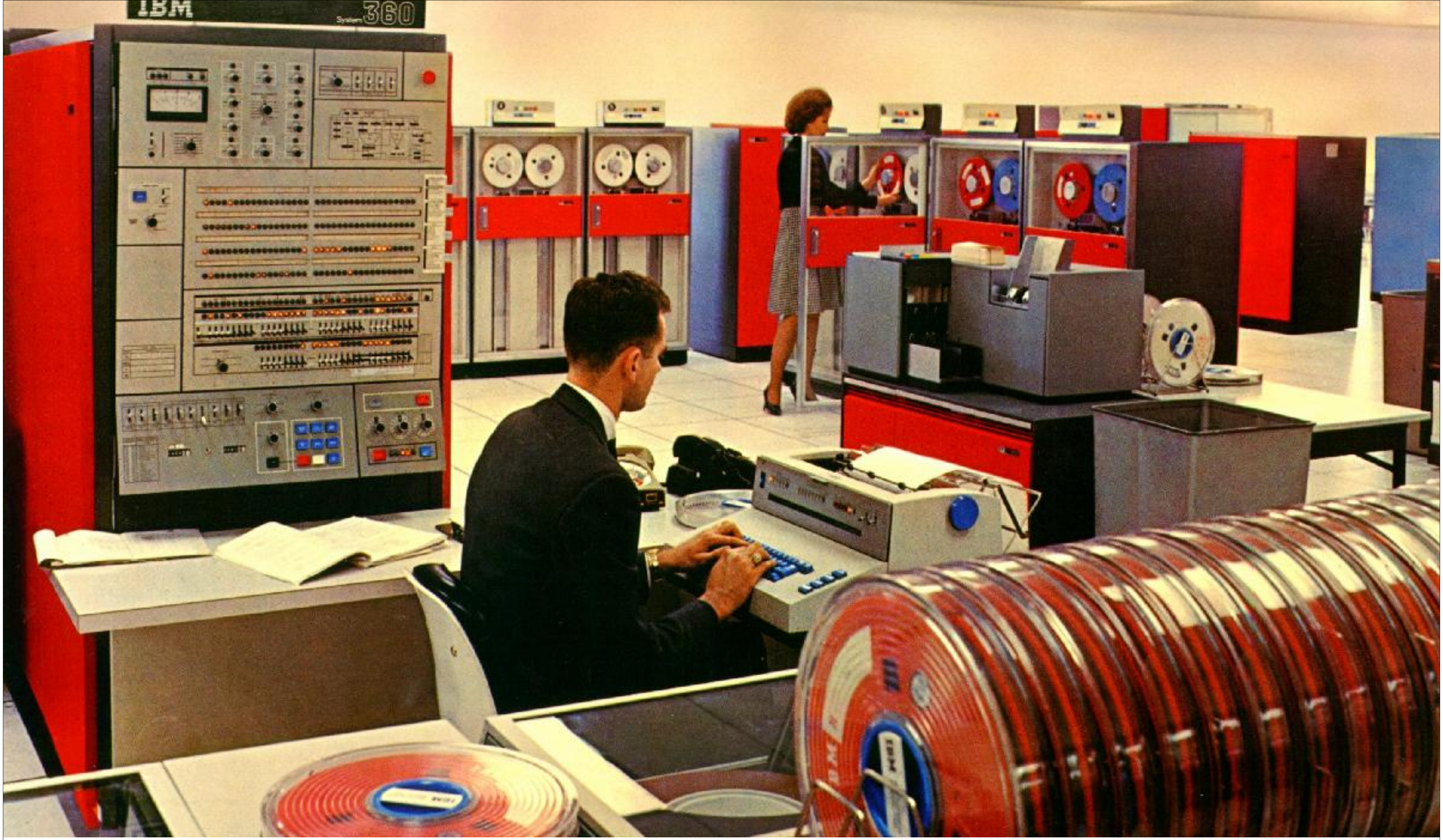
Add security layer?

Change middleware
Improve permission model

Sandbox Android

Using Virtualization

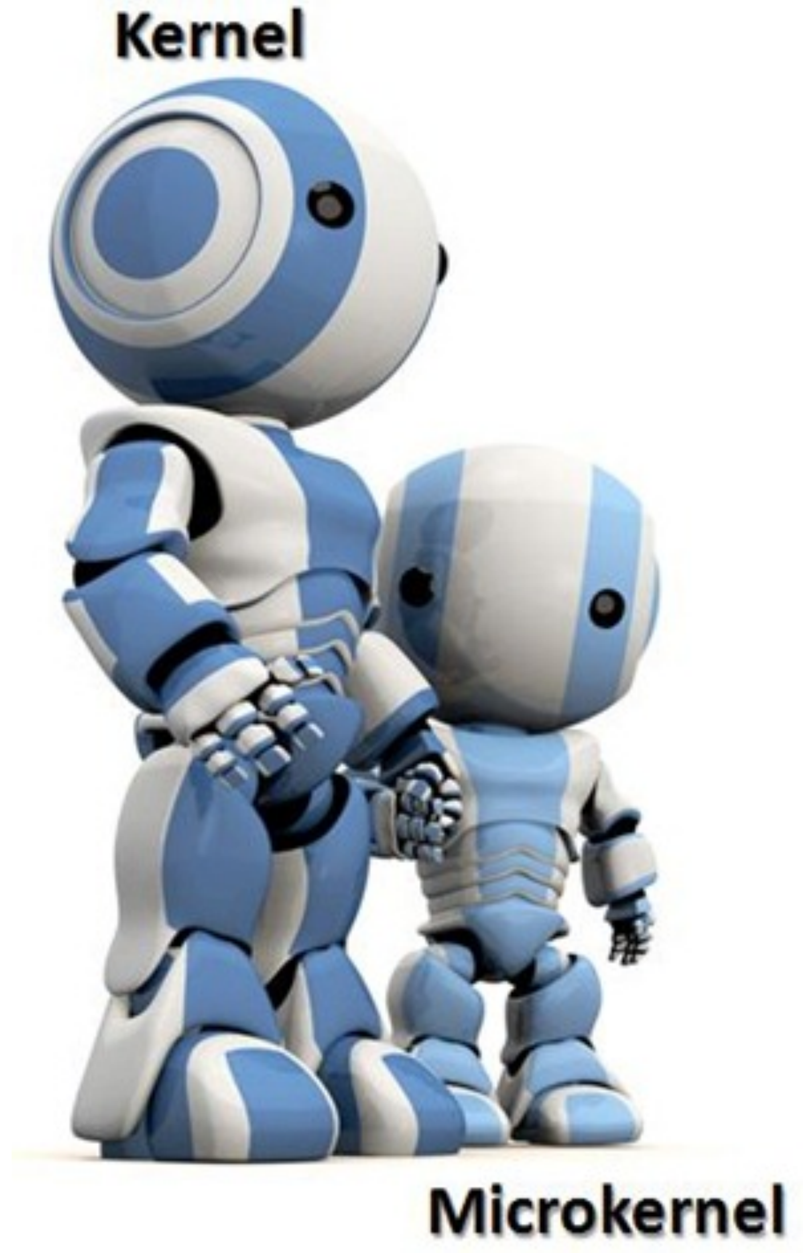




Virtualization is known
since the 60s

Microkernel as Hypervisor

- Less code, less errors
- Improvements over monolithic kernels
  - Fault isolation
  - Improved acces control
  - Flexibility
- Needs runtime environment



Fiasco.OC + L4Re

- Microkernel + runtime environment
  - x86 and ARM, SMP support
  - SVM, VT-x
  - L4Re provides basic services

Virtualization - L4Linux

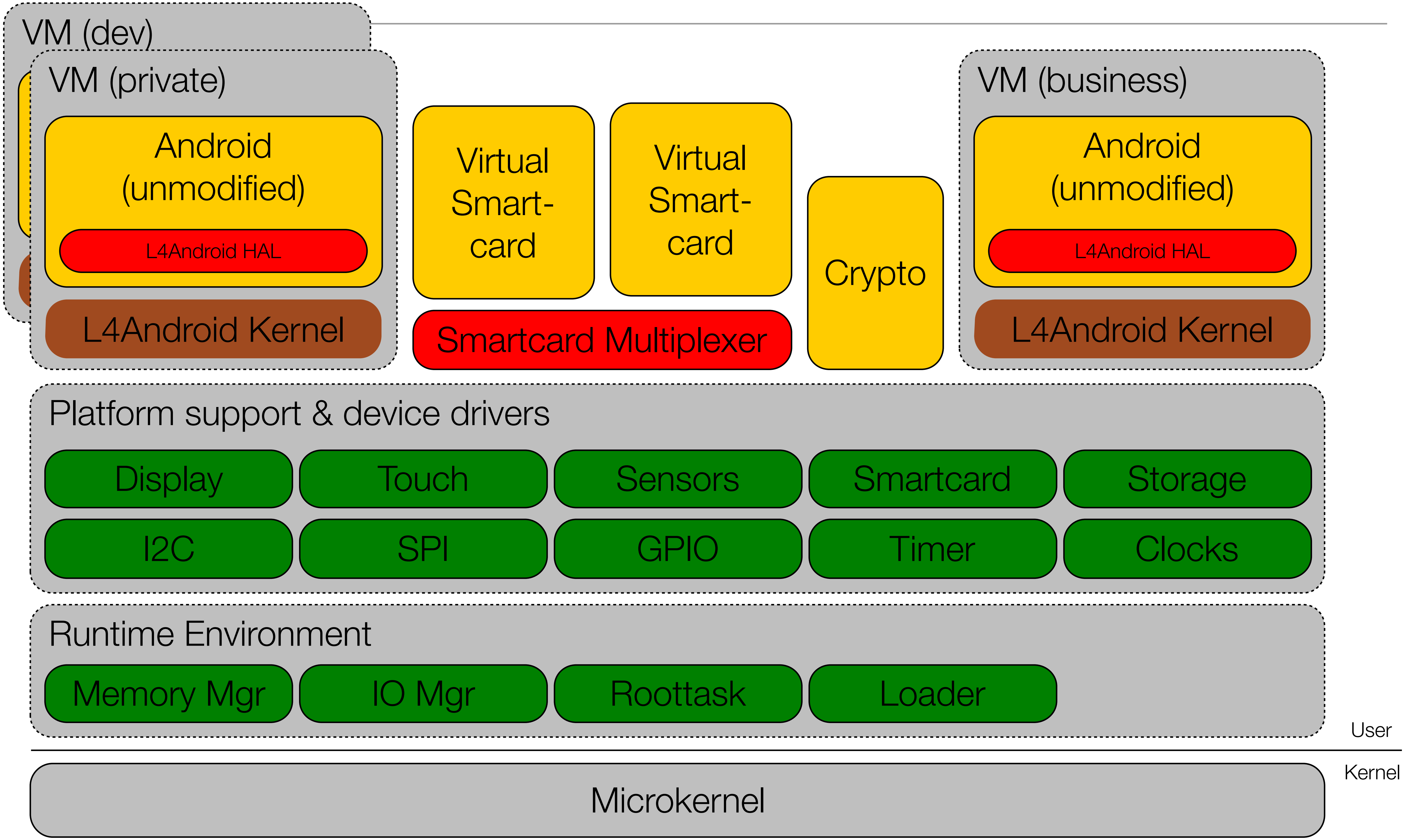
- User space port of Linux kernel
- Binary compatible
- Current version 3.5
- Applicable to non-virtualizable platforms

L4Android Framework

- Paper at ACM SPSM ’11*
- Demo on Samsung Galaxy S2 at HotMobile ’12
- Open source project
    - See www.l4android.org
    - Source code
    - Demo images

*L4Android: A Generic Operating System Framework for Secure Smartphones

L4Android Architecture



Results

- No hardware modifications or extensions required
- Supports x86 and ARM
  - Generic HW interface for both architectures
- Reasonable performance with multiple Androids
- Support for Samsung Galaxy S2

Applications

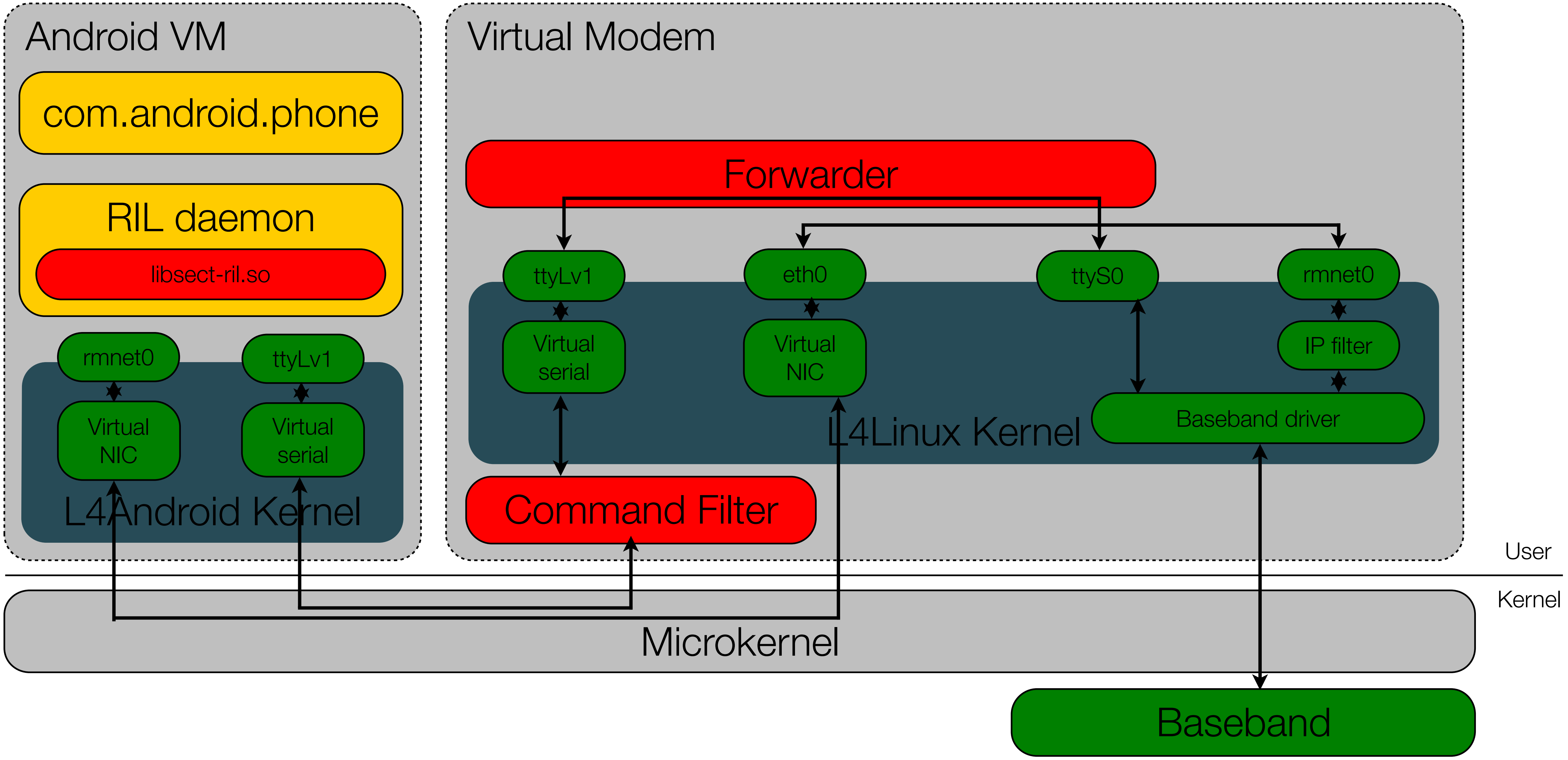
picture © www.norebbo.com

The Virtual Modem

- Paper at IEEE DSN ’12*
- Prevent signaling attacks on phone
- Protect user from cellular trojans

*Taming Mr. Hayes: Mitigating Signaling Based Attacks on Smartphones

Virtual Modem Architecture



Virtual Modem Results

- Mitigate known signaling attacks
- Prevent premium number SMS
- Hinders SMS controlled botnets

What is SimKo?

SimKo3

- **Si**chere **M**obile **Ko**mmunikation
- Confidential governmental communication
- Meet requirements to handle confidential data
- Existing Windows Mobile solution EOL

SimKo3 Prototype

- Developed as an R&D project by SecT
- Architecture based on L4Android framework
- Samsung Galaxy S2 (Exynos4 SoC)
- Demonstrated at Cebit 2012, product available by end of 2012

Thank you!

Questions?