John Floren

Introductio Android

Inferno

Bibliography



Hellaphone: Replacing the Java in Android

John Floren

Sandia National Labs

July 2012

Collaborators: Joshua Landgraf, Joel Armstrong

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S.

Department of Energy's National Nuclear Security Administration under contract DE-AC03-94AL85000. SAND 2012-5278C.

Biography

- Computer engineer by training (RIT)
- Been interested in operating systems since high school
- · Work for Sandia National Labs, California
 - High performance computing
 - Mobile

Hellaphone

Introduction

- Security
- · I like open source and Sandia is down with that
- Goal: open up as much of my work as possible

John Floren

- Introduction
- Android
- Inferno
- Bibliography

Smartphones

- Totally ruling the world
- A computer in my pocket? Awesome!
 - It can make phone calls too?
- Nifty sensors: camera, GPS, accelerometer
- Read email, browse the web, take pictures, get driving directions, play games
- Manage your passwords, 2 factor auth, Google Wallet



John Floren

Introduction Android

memo

Bibliography

Why smartphones kinda suck

- Blackberry, iPhone, Windows: all closed-source
- RIM will decrypt your messages for the government [6][5]
- iPhone
 - Tracks your movements [1]
 - DoS attack via SMS [2]
- Windows
 - Nobody has one!
 - DoS'd via SMS [7]
- CarrierIQ [3]

John Floren

Introduction

Android Inferno

Bibliography

But Android is still cool, right?

- Linux-based
- Open-source
- Tons of devices (phones, tablets, laptops)
- Write your own applications-no developer fees, no market fees!
- You can hack the OS if you want
- · Big community of developers and OS hackers

John Floren

Introduction

Android

Inferno

Bibliography

Android kinda sucks too

- I have to program in WHAT?
- · Vendors have no incentive to update the OS
 - How much do you trust Joe Random's ICS Rom?
- Security ain't so hot
 - DEF CON 19: fake OTA updates
 - CarrierIQ
 - Malicious apps [4]
- About 15 million lines of code, not including Linux.
 - Not very documented-hope you like digging!
- 1.2 GHz processor, 512 MB of RAM, runs like a dog



John Floren

- Introduction
- Android
- Inferno
- Bibliography

Android as a Linux platform

- Android is unattractive for hacking, sure
- Really just a thick layer of Java spread on top of a thin Linux cracker
- Mostly standard Linux underneath
- · Comes with a little busybox environment
 - Cyanogenmod ships a rather nice environment with bash etc.
- · Let's scrape away the Java and build on Linux
- Bonus: we'll get tons of compatible hardware with all the drivers already written



John Floren

- Introduction
- Android
- Inferno
- Bibliography

Inferno

- Open-source operating system from Bell Labs, now owned by Vita Nuova
- Implements the Dis virtual machine
- Runs natively or hosted on Linux/Windows/OS X/Plan 9
- Inspired by Plan 9
- Compiles fast, launches fast
 - Runs in a few megabytes
 - About 1 million LOC total
 - This includes the applications and code for native booting (which we don't use)
- Why not run it on top of Android's Linux?
 - We get all the hardware drivers (binary blobs, yay!)
 - Makes updating Inferno easy-no flashing ROMs



John Floren

Inferno

Android - Java = Linux

- Bibliography
- The first thing we do, let's kill all the Java
- Every Java process spawns from "zygote"
- Eliminate it from /init.rc
- But / is reset every boot!
- You can build your own custom ROM
- Or use our script to grab the running boot image, modify it, and reflash

John Floren

- Introductior
- Android
- Inferno
- Bibliography

Android + Inferno = Hellaphone

- Adapt Inferno to build for Android
- Use AGCC script to build Inferno with Android compilers and libs
- Most of the Linux code is suitable
- Some tweaks were needed in bits of assembly or C
- Had to create support for various bits of hardware
 - Framebuffer adapted from OLPC code
 - Mouse code to parse touchscreen inputs
 - Convert /dev/input events to text and make it available
- Hack the window manager to make it suitable for a phone.

John Floren

Introduction

Android

Inferno

Bibliography

The old Inferno window manager

	200
% ps grep Charon back stop 209 209 michael 382 382 michael	next http://www.vitanuova.com/inferno/index.html
Acne Newcol Kill Putall Dump Exit /appl	
New Cut Paste Snarf Sort Zerox Delcol /appl/cmd/bind.b Del Snarf Limbo Look	New Cut Paste Snarf Sort Z /usr/michael/ Del Snarf Glevelopment acros
<pre> } flags := sys->MREPL; arg=:nit(args); while((0 := arg->opt0) != 0)</pre>	Idemo/ demo2/ im.b architectures im.b im.b im.b im.b im.b im.b im.b im.b im.b im.b im.b im.b im.b im.c im.b im.c im.b im.c im.b im.c im.b im.c im.b im.c im.c im.c
arg = nil; /appl/cmd/auth/ Del Snarf Get Look khangelogin.b logind.b countersigner.b mKille createsignerkey.b passwd.b keyfs.b signer.b keysrv.b verify.b	auxi/ auxi/ bit2git.b brt2git.b broke.b broke.b cat.b cat.b cat.bl

John Floren

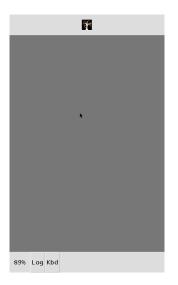
Introduction

Androic

Inferno

Bibliography

The new phone-friendly window manager



John Floren

Introduction

Android

Inferno

Bibliography

The drop-down menu

× 8	8				
Files	Edit				
Charon	Manua1				
Shell	Dialer				
SMS	->System				
->Misc	->Games				
89% Log Kbd					

John Floren

Introduction

Android

Inferno

Bibliography

It has a browser too

Charon ? 🗆 🕳 🗙									
back s	top nex	t http	://www.	vitanuo	va.com/				
3	vita nuova inferno								
			HOME	PRODUCT	<u>s</u> l <u>sour</u>	<u>ions</u> I <u>re</u>	CURCES	DOWNLO	DADS
	A compact operating building cross-platform distrik								
	Image Manage Manage								
-						1			27
Done									snarf
									×
Esc	Tab		, ,	. 1	r)	-			<-
1	2	3	4	5	6	7	8	9	0
٩	w	•	•	1	У	u		٠	P
a	\$	đ	r	9		J.	ĸ	н	;
z	x	¢	v	b		m	,		1
Caps	shift)	•	CU	~	E	nter

John Floren

- Introduction
- Android
- Inferno
- Bibliography

Phone-specific stuff

- devphone talks to the radio
 - Presents a file system interface
 - To make a phone call: echo 'dial 15551234567' > /phone/phone
 - To receive incoming calls, read from /phone/phone
 - Read will block until a call is incoming
 - Similar interface for SMS
- Nobody wants to make phone calls like that
- So we wrote a dialer app and an SMS app
- Also made early drafts at WiFi and audio drivers (both semi-functional)

John Floren

Introduction

Android

Inferno

Bibliography

Dialing application

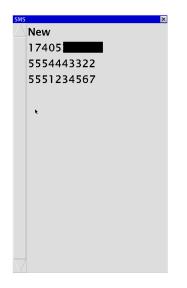
Dialer							
15551122331							
1	2	3					
4	5	6					
7	8	9					
*	0	#					
Dial							
Hang up							
Speaker							
Status: inactive ()							

John Floren

Introduction

Android

Inferno



SMS application

Send message Back We: This string can be replaced in the client by the sender's name if desired, later.									ın	
Them: The client used to send messages should prepend "Me: " to messages it sends, then add them to this file.										
I am typing a message to send Send									nd	
Kbd										×
Esc	Tab		· ·		t	1	-	-		<-
1	2	3	4	5	6	7		8	9	0
٩	w	٠	٢	۲	У	u		•	۰	p
a	\$	۴ď	r	9		J		ĸ	1	;
z	x	¢	۷	b		m		,	÷	1
Caps	shift						tri	~ Enter		

Neat things to try

- Inferno sandboxing one instance of OS per app
- Security hacks
 - If accelerometer reads > 10G, wipe the SD card
- Fun with 9P

Hellaphone

Inferno

- Easy to access your files at home
- Easy to share files with nearby phones
- Use 9P to export your phone's devices and control them from your PC
 - Anti-theft programs are now easy
 - Just import your phone's GPS device and camera
 - (Thief is probably pretty perplexed anyway)

Conclusion

- It's not that hard to strip down Android for your own purposes
- With a bit more work, Inferno could be a viable smartphone OS
 - It's fast

Hellaphone

Inferno

- It's light
- It's easy to work on
- It already comes with a bunch of software and infrastructure, you're not going from scratch
- No app store, but if you didn't write it yourself, you can't trust it anyway, right?

John Floren

Android

Inferno Ribliografi

Get in!



Code at http://bitbucket.org/floren/inferno

John Floren

- Introduction
- Android
- Inferno
- Bibliography

Bibliography I

- Alasdair Allan. Got an iPhone or 3G iPad? Apple is recording your moves. http://radar.oreilly.com/2011/04/apple-location-tracking.html, April 2011.
- [2] Dan Goodin. Hijacking iPhones and other smart devices using SMS. http://www.theregister.co.uk/2009/07/31/smart_phone_hijacking/, July 2009.
- [3] Dan Goodin. BUSTED! Secret app on millions of phones logs key taps. http://www.theregister.co.uk/2011/11/30/smartphone_spying_app/, November 2011.
- [4] Dan Goodin. Malicious apps infiltrate Google's Android Market. http://www.theregister.co.uk/2011/12/12/android_market_malware/, December 2011.
- [5] Kathleen Hall BlackBerry to co-operate with police after youths used BBM to organize riots. http://www.computerweekly.com/news/2240105290/ Blackberry-to-co-operate-with-police-after-youths-used-BBM-to-organise-riots.
- [6] Josh Haliday, BlackBerry wins the battle but not the war in India. http://www.guardian.co.uk/technology/2010/sep/01/blackberry-india-rim, September 2010.
- [7] Tom Warren. Windows Phone SMS attack discovered, reboots device and disables messaging hub. http://www.winrumors.com/ windows-phone-sms-attack-discovered-reboots-device-and-disables-messaging-hub/, December 2011.