



Windows Phone 7 OEMS – Microsoft BlueHat Executive Briefings

Alex Plaskett – November 2011



Main Objectives

- High level overview
- Demonstrate that OEM's negatively impact the security posture of phones
- Provide independent viewpoint on security
- Provide thoughts for future



Introduction



Who am I?

- Security Consultant @ MWR InfoSecurity
- Presented on WP7 at 44con, T2 etc..
- Breaking stuff for fun for a while ③



What this talk will cover

- OEM Features and Risks
- OEM Vulnerabilities
- Future Thoughts



Platform OEM Comparisons

- WP7: HTC, Samsung, LG, Dell
- Android: Acer, HTC, LG, Motorola
- iOS: Apple
- BBOS: RIM

⇒ WP7 and Android: greater attack surface/more complex security ecosystems



WP7 Security Model

- Process Sandbox
- Code Signing
- Centralised Security Policy
- Exploit Mitigations

Chamber Based Security Model тсв Elevated **Rights Standard Rights**

Least Privilege Chamber



WP7 OEM Features

Third Party Development	OEM/MO Development
Managed Code Only	Managed + Native Code
User space Only	User space and Kernel
LPC Sandbox Applications	Up to high privilege chambers
No accessible services	Globally Accessible Services



WP7 OEM Risks

- Vulnerabilities in OEM Apps or Drivers
- Privileged Application Functionality
- Extra Delay in Patching OEM Code
- Vulnerabilities in OEM code misattributed to MS vulnerabilities?



Vulnerabilities



Other Platform OEM Vulnerabilities

Android
 HTC Browser INSTALL Permissions
 HTC Sound Recorder
 HTC Logger

iPhone / BlackBerry:
 N/A



WP7 Potentially Dangerous OEM Functionality

- Samsung Diagnostic Application
- LG MFG Application
- HTC Debug Code



Concerning OEM Code

IDA - C:\Users\user\Documents\Research\HTC\drhtc.i64 (drhtc.dll)						
File Edit Jump Search View Debugger Options Windows Help						
🚰 🔚 🔄 🖛 🗣 🐂 🛍 🖏 🛸 🖡 🐛 🗛 🗛 🖬 📾 📾 💣 👉 🛪 🖆 🗙 🕨 🗖 🗖 No debugger 🔷 🔻 🗊 🚏 🎬 🖾 🖉						
f Functions window Image: Comparison of the second	×	IDA View-A	s' Str	ings window	💟 🖸 Hex View-A 🗵 🖪 Structures 🗵 🔃 Enums 🗵 🛐 Imports 🗵	
Function name	-	Address	Length	Tv	pe String	
f sub_EF952E30		text:EF953	00C 00000012	un	nic 04/26/10	
<u>f</u> sub_EF952E38		text:EF9530	00000020	: un	iic [+] core 2.0 released	
f sub_EF95406C		(s) .text:EF953	04C 00000012	un	nic 04/30/10	
<u>f</u> DHC_Init		(s) .text:EF953	00000032	un	iic [+] htc bridge framework	
<u>f</u> DHC_Deinit		(s) .text:EF953	00000012	un	nic 05/03/10	
f DHC_Open		(s) .text:EF953	0000006C	: un	iic [+] core 2.1 released & re-arch. drhtc code structure	
<u>f</u> DHC_Close		(s) .text:EF9531	00000012	un	nic 05/05/10	
<u>F</u> DHC_Read		text:EF9531	L28 0000003C	: un	iic [+] htc shim module framework	
<u>f</u> DHC_Write		's' .text:EF9531	164 00000012	un	iic 05/11/10	
<u>F</u> DHC_Seek		text:EF9531	L78 0000004E	un	iic [+] policy faker and certificate faker	
f DHC_PowerDown		's' .text:EF9531	LC8 00000012	un	05/12/10	
<u>f</u> DHC_PowerUp		text:EF9531	LEO 0000046	un	ic [+] controller of developer unlock	
F DHC_IOControl		(s) .text:EF953	228 00000074	un	iic [+] force all managed/hybrid Yamanote apps to native ones	
f sub_EF9540D8	Ŧ	's' .text:EF9532	29C 00000012	un	nic 05/13/10	
< III •	•	's' .text:EF9532	2B0 000007E	un	ic [+] core 2.2 stable released, fix all klocwork critical issues	
Line 13 of 202		's' .text:EF9533	330 00000012	un	nic 05/14/10	
R Graph overview	×	's' .text:EF953	344 0000003A	un	ic [-] remove certificate faker	
IDA - C:\Users\user\Documents\htclvstuff\	htclv.i	db (htclv.dll)				
File Edit Jump Search View Debugger Options Windows Help						
🖻 🔒 🗄 今 マ 今 マ 🏥 備 橋 🍓 🔍 🔊 🌆 🖬 🕼 🛷 🛤 儲 🦑 マ 🖑 🛋 🕨 💭 🔲 🔲 😡 No debugger 🛛 🔍 🗄 🗊 🚏 🖺 🖼 万						
F Functions window		IDA View-A 🛛	's' Strings wir	ndow 🗵	O Hex View-A ≥ ▲ Structures ≥ Enums ≥ ™ Imports ≥ Exports	
Function name	A	dress	Length	Type St	tring	
f LVModInitialize	's	.text:10001210	000000A6	unic [k	K][LoaderVerifier] after re-enabling developer unlock, now its state is '%s'\r\n	
f LVModUninitialize	's	.text:100012D8	0000009A	unic [k	K][LoaderVerifier] backdoor-fixing developer unlock to 'enabled' state\r\n	
f LVModAuthenticateFile	's	.text:10001398	0000008C	unic [k	[LoaderVerifier] current developer unlock state: %d (hRes: %08x)\r\n	
7 LVModRouting	's	.text:10001428	00000080	unic [k	C[[LoaderVerifier] enabling developer unlock (hRes: %08x)\r\n	
f IVModAuthorize	's	.text:10001118	0000062	unic [k	([LoaderVerifier] take %s(%s) as Native app.\r\n	
f IVModGetPageHashData		text:100011F8	0000012	unicdi	isabled	
F IVModCloseAuthenticationUandle		text:100011F9	00000010	unic of	nabled	
		tott1000104C	00000000	unic El	more and a second se	
		dete:1000104C	00000000	unic IV	miou na 20. stars Mars Mars - Disala - 20. stars Date Mark 19. stars Circ 20. stars - Circ 20. stars - 1. st	
4	S	.data:100030C8	00000000	unic p	rop:v5ystem.itemiNameDisplay;v5ystem.DateiNodified;v5ystem.Size;V5ystem.FileCount;v5ystem.Author	

Line 13 of 36



WP7 OEM Vulnerabilities

- HTC Kernel Arbitrary Read/Write
- Samsung PROVXML Privilege Escalation



Browser Exploitation

- Samsung Diagnostic Application
 For Debugging
- Samsung PROVXML Vulnerability For File System Access
- => Not Directly Using OEM Vulnerabilities
- Browser lacks
 ID_CAP_INTEROPSERVICES



Demo



Identified Problems

- Gap between MS and OEM code quality
- OEM's introduce dangerous features to offer customers / internal developers extra functionality at the potential expense of security
- MSFT gets blamed for OEM mistakes?



Future Thoughts



Mango and onwards

- Restricts method I used to debug and develop exploits against the platform (ID_CAP_INTEROPSERVICES) and new web browser.
- However, design and policy still allows OEM applications to use driver functionality
- OEM code could still expose MS to an unnecessary level of risk



Discussion Points

- Better Integration between MS SDL with OEM's Development?
- More granular permissions for OEMs

 Provide secure APIs for OEM
 requirements?
- Does MS have oversight in what the OEM's are shipping?
- More stringent controls on what OEM's ship?



Conclusions

- Strong Granular Security Model
- Attackers need multiple vulnerabilities
- MS needs to motivate OEM's to deliver better code
- Attackers could use OEM vulnerabilities



Questions?