

USB attacks need physical access right? Not any more...

Andy Davis, Research Director NCC Group





Agenda

- The problem with USB bugs
- The USB bugs I've found and how I found them
- Demo: iOS 7 bug
- A contrived example of a remote USB bug via Bluetooth
- Demo: Windows hidparse.sys bug
- USB redirection via RDP
- Demo: Windows 2012 usbaudio.sys bug (triggered remotely)
- The implications for future USB bugs
- Mitigation strategies to reduce the risks
- · Conclusions and further research



The problem with USB bugs

- Physical access required
- Vendors aren't really interested
- Local bugs have their place, but have a limited impact









Recent high profile USB host bugs

- CVE-2011-2295: Oracle Sun Solaris USB Local Buffer Overflow Vulnerability
- CVE-2012-3723: Apple Mac OS X USB Hub Descriptor bNbrPorts Heap overflow
- MS13-027: The Windows 8 RNDIS kernel pool overflow
- CVE-2013-3200: Microsoft Windows USB Descriptor Handling Local Privilege Escalation





How I first started finding USB bugs (2011)

- Arduino microcontroller
- Fuzzer written in C++
- Only emulates USB HID devices
- Only allows semi-automated fuzzing
- Has found bugs in:
 - Windows 7
 - Windows XP
 - OS X
- Limitations not really fast enough to emulate most USB devices







USB fuzzer – the next generation (2012)

- Dedicated USB test equipment hardware
- USB capture and playback
- Emulates any USB host or device
- Understands and analyses the different USB device classes
- Uses a scripting language to generate USB traffic
- Costs approx. USD1200 (plus specific class analysis options)
- · Limitations doesn't have a software API to control it







How I find them now (2013...)

· Facedancer and umap



\$ sudo python umap.py -P /dev/ttyUSB0 -i



The USB host assessment tool Andy Davis, NCC Group 2013 Version: 1.0

Based on Facedancer by Travis Goodspeed

For help type: umap.py -h

01:01:00 - Audio : Audio control : FR Protocol undefined 01:02:00 - Audio : Audio streaming : FR Protocol undefined 02:02:01 - CDC Control : Abstract Control Model : AT commands V.250 02:03:ff - CDC Control : Telephone Control Model : Vendor specific 02:06:00 - CDC Control : Ethernet Networking Control Model : No class-specific protocol required 03:00:00 - Human Interface Device : No subclass : None **SUPPORTED** 06:01:01 - Image : Still image capture device : Bulk-only protocol 07:01:02 - Printer : Default : Bidirectional interface 08:06:50 - Mass Storage : SCSI : BBB **SUPPORTED** 09:00:00 - Hub : Default : Default **SUPPORTED** 0a:00:00 - CDC Data : Default : Default 0b:00:00 - Smart Card : Default : Default

https://github.com/nccgroup/umap





What has umap found most recently?

• CVE-2014-1287 : iOS 7 arbitrary code execution in kernel mode







Demo: iOS 7 bug







Contrived example of remote USB bug

- Discovered a null-pointer dereference in hidparse.sys in 2011
- Microsoft not interested not really a security issue
- Triggered by inserting a malicious device
- HID report descriptor is parsed during enumeration phase
- Blue screen occurs



Contrived example of remote USB bug



Windows (all versions) - not patched





What else uses HID report descriptors?

- · Bluetooth keyboards!
- During pairing, report descriptor is parsed
- Very tenuous, as this isn't really a USB bug it's a HID parsing bug
- First attempt to move away from direct physical access





I have a spare Arduino...

Small, portable, programmable USB device to trigger USB vulnerabilities:







Demo: hidparse.sys bug via Bluetooth







USB Redirection via RDP

Numerous legacy "High-level" redirection capabilities:

- Easy Print
- Drive Redirection
- Smart Card Redirection
- Plug-and-Play Device Redirection
- Input Redirection
- Audio Redirection
- Port Redirection





Problem with High-level USB redirection







Problem with High-level USB redirection







Problem with High-level USB redirection







Enter "RemoteFX USB Redirection"...





Image: www.norcalblogs.com

RemoteFX USB Redirection



RemoteFX USB Redirection	RDP High-Level Device Redirection
Does not require drivers on the client	Requires drivers for the device to be installed on the client
Requires the device driver to be installed on the server	Generally does not require drivers on the server
Uses one redirection method for many types of devices	Uses a specific, unique method for each type of device being redirected
Forwards URBs to and from the device over the RDP connection	Exposes high-level device functionality in the remote session by using an optimized protocol for the device type
Enables only one session to use a device at a given time; the local client cannot use the device while an RDP session is using it	Enables any number of sessions to access the device simultaneously, including the local client
Is optimized for the LAN, like the rest of RemoteFX	Works with both LAN and WAN

Enable RemoteFX on the client



C: <> gpupdate /force

Computer Configuration\Administrative Templates\Windows Components \Remote Desktop Services\Remote Desktop Connection Client\ RemoteFX USB Device Redirection

Allow RDP redire	ection of other supported R	emoteFX USB devices from this computer	
Previous Setting	Next Setting		
Not <u>C</u> onfigured Enabled Disabled	Comment: Supported on:		× + ×
			-
Options:		Help:	
RemoteFX US8 Redir Adminstrators and U	ection Access Rights Jsers	This policy setting allows you to permit RDP redirection of other supported RemoteFX USB devices redirected through this mechanism will no longer be available for local usage on this computer. This is because RDP will replace the selected supported RemoteFX USB devices driver with the Remote Desktop RemoteFX USB redirection device driver to facilitate RDP redirection of these devices. If you enable this policy setting, you can choose to give the ability to redirect other supported RemoteFX USB devices driver in the Administrators group on the computer. If you disable or do not configure this policy setting, other supported RemoteFX USB devices are not available for RDP redirection by using any user account.	. E

Enable RemoteFX on the client



Remote Desktop Connection	Remote Desktop Connection
Remote Desktop Connection	Remote Desktop Connection
General Display Local Resources Programs Experience Advanced Remote audio Configure remote audio settings. Settings Settings	Local devices and resources Choose the devices and resources on this computer that you want to use in your remote session. Smart cards Ports
Keyboard Apply Windows key combinations: Image: Construction of the strength of the strengt of the strength of	Drives Other supported Plug and Play (PnP) devices Vother supported RemoteFX USB devices USB camera
Local devices and resources Choose the devices and resources that you want to use in your remote session. Printers Clipboard More	Which devices can I use in my remote session? OK Cancel
Options Connect Help	































Demo: usbaudio.sys bug via RDP





Image: us.cdn4.123rf.com



The implications for future USB bugs

- Windows USB bugs no longer need local physical access
- Remote exposure of the Windows kernel has been increased
- What were local DoS bugs can now remotely "blue-screen" a server
- May apply to other (non-Windows) remoting technologies





How can you reduce the risks?

- If RemoteFX is not required on the server, turn it off
- If RemoteFX is required specify GUIDs of authorised USB devices
- Do not enable RemoteFX USB remoting on clients
- Minimise the use of USB "High-level" remoting via RDP
- Be more cautious of "local" vulnerabilities and apply the patches











Conclusions and further research

- Physical access is no longer a requirement to trigger Windows USB bugs
- RemoteFX USB remoting has exposed more of the Windows kernel to attackers
- Need to investigate other remoting technologies e.g. Citrix
- The Internet of Things is full of USB possibilities ©





Questions?

Andy Davis, Research Director NCC Group andy.davis 'at' nccgroup 'dot' com







UK Offices

Manchester - Head Office Cheltenham Edinburgh Leatherhead London Thame

European Offices

Amsterdam - Netherlands Munich – Germany Zurich - Switzerland



North American Offices

San Francisco Atlanta New York Seattle



Australian Offices

Sydney