Charles T.W. Truscott Watters

@r0ss1n1

Network Protocol Analysis, Fuzzing, Debugging, Vulnerabilities, & Source Code Analysis

MSDN / RFC -> Recommend specifications for applications implementing network protocols

Fuzzing -> Variable Length fields interpreted predominantly by C/C++ applications and device drivers,

computer program structures interpreting ASCII, Unicode hexadecimal, binary values

Debugging -> Vendor, open-source userland or kernel land debugging for processes or device drivers,

x86 / x86_64 & custom add-ons to aid exploit writing process, e.g. msfpescan, !heap, !mona, pykd, pydbg

Vulnerabilities -> Integer Overflow, Stack Overflow, Heap Overflow, Read Primitive, Write Primitive, Use-After-Free,

VTABLE Overwrite, Double Free, e.t.c. (MITRE CWE C/C++)

Application Analysis, Fuzzing, Debugging, Vulnerabilities, & Source Code Analysis

Intel Microprocessor Language Applications Interpreted by Operating System (such as ntokrnl.exe) -> Applications

translate to machine language for the operating system and processor architecture, e.g. resolving API calls to OS API, narrowing to syscalls

Fuzzing -> Mostly File-Format or Network-Function or input-based, e.g. variable lengths, variable ASCII / Unicode sequences

Debugging -> x86 or x86_64 userland debugging with x64dbg or WinDBG

Mobile App Analysis, Fuzzing, Debugging, Vulnerabilities, & Source Code Analysis

Android or iOS -> Very vendor specific, requires Google's adb or Apple's XCode. Apps are rolled out from

the store for delivery to devices. Can be run in an emulator.

Mobile App Vulnerabilities -> Mostly File Format, e.g. several CVEs for rendering ASCII characters or interpreting JPEGs

out of widely used apps, e.g. Facebook, Instagram, Twitter, vulnerable to file format fuzzing discovered exploit code.

Other vulnerabilities in mobiles such as in protocols and protocol stacks. Left my Galaxy Note

vulnerable for over a year while DNSBIND was subservient to a buffer-overflow in a DNS query, all attacks must have ported this

to Android or the Galaxy Note via private contractor

Web Browser Analysis, Fuzzing, Debugging, Vulnerabilities, & Source Code Analysis

Analysis -> Biggest players in the Web Browser game are Chrome (Google), IE & Edge (Microsoft),

Firefox (Mozilla), Portable Firefox distributed by third parties (e.g. Tor Browser), Opera, Safari (Apple)

Fuzzing -> Manual Introspection of API calls to browser functionality, such as the C/C++ higher

level construct of writing new parts of the Javascript, node.JS e.t.c. Programming Language

Fuzzing, vulnerabilities -> Interprets file formats, can enumerate and evaluate functionality via documentation

or generalisations of Web 2.0 features, OS file formats, Javascript languages, browser functionality

Debugging and Source Code Analysis -> Can BINDIFF different revisions of browsers release to release,

predominantly reverse engineering in IDA (Windows, Mac), Ghidra (made by NSA), test ASM interpreting browser

functionality such as interpreting client-side languages; device drivers, DLLs, portable executable format files, DSOs, APKs, KEXTs, e.t.c.

Charles T.W. Truscott Watters 2481 Byron Bay NSW 2481 0421533702