Security Now! #481 - 11-11-14

Certificate Transparency

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- Microsoft's **>>>Mega Red Alert<<<** Patch Tuesday
- A surprising event in the Net Neutrality struggle
- Steve's just back from Las Vegas... presenting SQRL.
- Important BELKIN N750 Router Firmware Update.

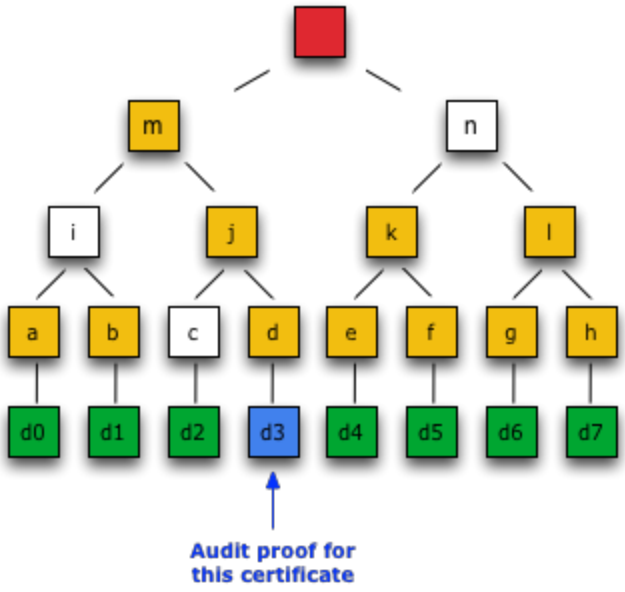

Figure 5

Security News:

Mega Patch Tuesday!

- https://technet.microsoft.com/library/security/ms14-nov
- 16 patch bundles resolving 33 known vulnerabilities,
- (2 of the bundles appear to be delayed and held back)
- MS14-066
  - This security update resolves a privately reported vulnerability in the Microsoft Secure Channel (Schannel) security package in Windows. The vulnerability could allow remote code execution if an attacker sends specially crafted packets to a Windows server.
  - Exploitability Index: 1 - "More Likely"
  - Mitigating Factors: "Microsoft has not identified any mitigating factors for this vulnerability."

    - Workarounds: "Microsoft has not identified any workarounds for this vulnerability."

- FAQ:
    - What might an attacker use the vulnerability to do?
        - An attacker who successfully exploited this vulnerability could run arbitrary code on a target server.
    - How could an attacker exploit the vulnerability?
        - An attacker could attempt to exploit this vulnerability by sending specially crafted packets to a Windows server.
    - What systems are primarily at risk from the vulnerability?
        - Server and workstation systems that are running an affected version of Schannel are primarily at risk.
- Four shiny new TLS cipher suites added:
    - 2-RSA, 2-DH (PFS), all GCM (Galois Counter Mode)

- Also... CRITICAL Remote Code Execution Vulnerabilities:
    - Windows OLE (Object Linking and Embedding)
    - Internet Explorer:
        - <quote> This security update resolves seventeen privately reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer…
    - XML Code Services
    - Microsoft Office
        - Three privately reported vulnerabilities in MS Office.
    - TCP/IP (IOCTL) processing…
        - <quote> This security update resolves a publically reported vulnerability in TCP/IP that occurs during input/output control (IOCTL) processing. This vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of another process. If this process runs with administrator privileges, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

- Windows Audio Service
- .NET Framework
- Sharepoint Foundation
- Remote Desktop Protocol
- IIS Restriction Feature Bypass
- Active Directory Federation Services
- IME (Input Method Editor) for Japanese!
- Kernel Mode Driver... attacker places a specially crafted TrueType on a Windows share and gets a victim to enumerate it.

Obama wants to reclassify ISPs as Telecommunications Carriers
http://www.vox.com/cards/network-neutrality/why-did-the-court-rule-the-fccs-network-neutr

ality-rules-illegal

Steve's just back from Las Vegas.

- FIDO's Brad Hill

Belkin Issues Firmware Fix for Router Vulnerability

- Belkin has a fix for a vulnerability in its N750 dual band router (offered since 2011 and still on the market) that could be exploited by people using guest networks to gain root access. Users are urged to update the firmware to F9K1103_WW_1.10.17m.
- A vulnerability in the router's guest network web interface allows an unauthenticated remote attacker to gain root access to the operating system of the affected device. The vulnerability enables control over a part of heap memory where a variable that forces the execution of a CGI and also the variable with the name of the CGI to be executed, are stored.
- Routers running F9K1103_WW_1.10.16m would be affected unless owners switched off unprotected guest networks... which are turned on by default.
- Metasploit now has an automated remote takeover module... so "War Driving" could really mean "war."
- The Metasploit module enables access to the router's telnet server directly from the guest network to the root shell.
- TRIVIAL to expoit and also to verify:
- https://labs.integrity.pt/advisories/cve-2014-1635/

SpinRite

http://www.reposter.net/2014/10/universal-fix-for-windows-ksod/

Universal fix for windows KSOD (Oct, 2014)

Ever had your Windows installation inexplicably die leaving your computer unusable without a fix? I have – more times than I'd like to count. The last time this happened was yesterday when Windows 7 would only boot into a black screen with a movable cursor, also known as the blacK Screen Of Death. It was a serious case considering none of the safe modes or repair function in the Windows boot options would work; each option would universally end in either a KSOD or the classic BSOD after hanging on aswRvrt.sys during safeboot. After exhaustively eliminating all possible "regular" fixes that were available on the internet, I decided it was time for the big guns: Steve Gibson's Spinrite.

Prior to trying Spinrite I first tried Kaspersky's Rescue Disc 10 which was entirely useless for my case. After booting from the rescue USB dongle I would always get a "Missing Operating System" error in the boot screen. Not reassuring. I have long been a fan of Steve Gibson's Security Now podcast, which is why I knew of the tool. I knew the tool would be one of the few things that might do the trick, so I gave it a shot. After about an hour running Spinrite 6, and a few reboots later, my Windows 7 installation was working perfectly as if nothing had ever happened. Spinrite saved the day.

TL;DR Spinrite saved my machine from a perpetual and otherwise unbeatable KSOD scenario and my guess is that if you are having KSOD problems then Spinrite is one of few things that might help you too.

Certificate Transparency

RFC 6962
"Certificate Transparency"
This document describes an experimental protocol for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed, in a manner that allows anyone to audit certificate authority (CA) activity and notice the issuance of suspect certificates as well as to audit the certificate logs themselves. The intent is that eventually clients would refuse to honor certificates that do not appear in a log, effectively forcing CAs to add all issued certificates to the logs.

Append-Only Log Property:
Provable that:
Any particular version of the log is a full proper superset of any particular previous version.
In other words: All certificates claimed to have been added, have indeed been added.

(Fun with Merkle Hash Trees)
Gnutella, LimeWire, Bitcoin,

Trust:
Merkle trees avoid the need to blindly trust logs

Auditable.