Security and Proprietary Software

By Roy Schestowitz
Created 21/05/2021 - 7:00pm
Submitted by Roy Schestowitz on Friday 21st of May 2021 07:00:39 PM Filed under Security [1]

- **SSH CA for host keys** [2]

  An SSH CA is a key pair used to sign, or certify, other SSH keys. Such a signed key is called a certificate. An SSH client can be configured to implicitly trust host certificates created using specific CA keys. This makes it easier and more secure to log into new hosts.

- **Colonial Pipeline Lessons: Ransomware (and Security) Steps Everyone Should Take** [3]

  From the SolarWinds hack to the Colonial Pipeline ransomware attack, cybersecurity has entered into public consciousness like never before.

  How can you avoid falling victim to a cyber attack? Start with the assumption that perfect cybersecurity doesn't exist, and then make your network and data so hard to hack that cybercriminals give up and look elsewhere.

- **Security updates for Friday** [4]

  Security updates have been issued by Arch Linux (ceph, chromium, firefox, gitlab, hedgedoc, keycloak, libx11, mariadb, opendmarc, prosody, python-babel, python-flask-security-too, redmine, squid, and vivaldi), Debian (lz4), Fedora (ceph and python-pydantic), and openSUSE (cacti, cacti-spine).
Holes in the WiFi [5]

The discoverer of the KRACK attacks against WPA2 encryption in WiFi is back with a new set of flaws in the wireless-networking protocols. FragAttacks is a sizable group of WiFi vulnerabilities that (ab)use the fragmentation and aggregation (thus "Frag") features of the standard. The fixes have been coordinated over a nine-month period, which has allowed security researcher Mathy Vanhoef time to create multiple papers, some slide decks, a demo video, patches, and, of course, a web site and logo for the vulnerabilities.

Three of the vulnerabilities are design flaws in the WiFi standards, so they are likely present in all implementations, while the other nine are various implementation-specific problems. The design flaws may be more widespread, but they are much harder to exploit "because doing so requires user interaction or is only possible when using uncommon network settings". That means the real danger from FragAttacks lies in the programming errors in various WiFi implementations. "Experiments indicate that every Wi-Fi product is affected by at least one vulnerability and that most products are affected by several vulnerabilities."

Apple Accuses Microsoft of Using Epic in Legal Attack [6]

Apple Inc. injected a new level of intrigue in its bitter court fight with Epic Games Inc., suggesting the Fortnite maker was acting as a stalking horse for Microsoft Corp. and withholding evidence.

The iPhone maker made the accusations Wednesday night in a filing asking a judge to make an adverse credibility finding against Lori Wright, an Xbox executive who testified in the trial on behalf of Epic. That would mean the judge could ignore her testimony.

Source URL: http://www.tuxmachines.org/node/151444

Links:
[4] https://lwn.net/Articles/856902/rss
[5] https://lwn.net/Articles/856044/