

The Last Month in InfoSec

February 2016 Edition

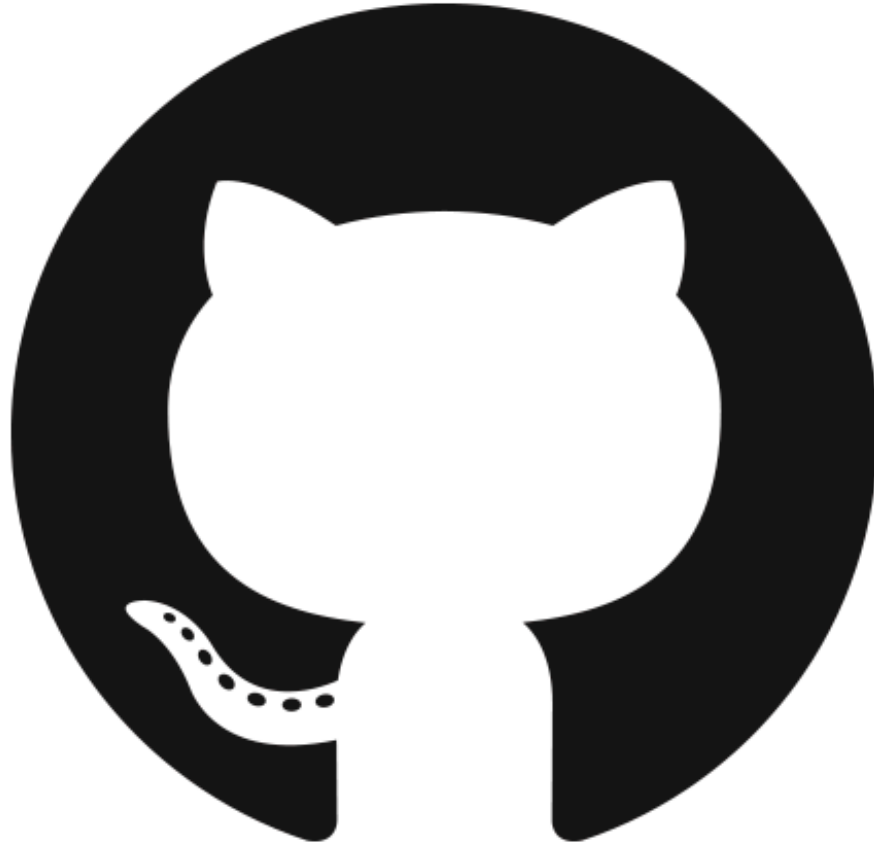
Joe T. Sylve, M.S.

NOLASec

February 24, 2016

Disclaimer

- The views expressed during this talk (and in general after drinks) are mine alone and do not necessarily reflect those of Blackbag Technologies, 504ENSICS Labs, or NOLASec, Inc.
- They may or may not also be shared by Vico and Andrew (but who cares what those guys think?)



Grab a Copy of These Slides

<https://github.com/jtsylve/slides>

Socat...

CRYPTO WTF? OF THE MONTH

Socat Backdoor?

- Hard-Coded NON-PRIME parameter in Diffie-Hellman exchange
 - Advisory: <http://goo.gl/ojKiqk> (NON-SSL!)
 - Write up: <http://goo.gl/JX4mDJ> (NON-SSL!)

Socat Backdoor?

- The Commit
 - <http://goo.gl/uxUdFH> (NON-SSL!)

“Socat did not work in FIPS mode because 1024 instead of 512 bit DH prime is required. Thanks to Zhigang Wang for reporting and sending a patch.”

... help us Dan Kaminsky. You're our only hope!

DNS IS BROKEN AGAIN

CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow

- All versions of glibc since 2.9
 - November 13, 2008
- DNS client side resolver is vulnerable
 - getaddrinfo()
- The vulnerability relies on an oversized (2048+ bytes) UDP or TCP response, which is followed by another response that will overwrite the stack.

CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow

- Initial Google Write up: <https://goo.gl/kluvj1>
- Qualys Writeup : <https://goo.gl/0e41U4>
- Dan Kaminsky's Rant: <http://goo.gl/wfv0f8>
(NON-SSL!) (WTF Dan DNS-Sec Kaminsky?)

... FBI likes it in the back door!

JUDGE ORDERS APPLE TO DECRYPT ALLEGED TERRORIST'S IPHONE

iPhone Decryption Shenanigans

- Brian will talk in depth about this tonight
- The Court Order: <https://goo.gl/ZgLWES>
 - “... bypass or disable the auto-erase function whether or not it has been enabled ...”
 - “... enable the FBI to submit passcodes to the SUBJECT DEVICE for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol...
 - “... when FBI submits passcodes to the SUBJECT DEVICE, software on the device will not purposefully introduce any additional delay between passcode attempts...”

... but wait there's more!

IN OTHER NEWS

In Other News

- Two more High Severity OpenSSL bug found
 - <https://goo.gl/ATUysV>
- 500 Gbps DDOS!
 - <https://goo.gl/vFLHy5>
- Lenovo SHAREit several vulns
 - Including hard-coded password....
 - <http://goo.gl/o2vq0P> (NON-SSL!)

In Other News

- Man sees odd data, think fitbit is broken.
Reddit figures out that his wife is pregnant.
 - <https://goo.gl/5Y5tnF>
- Overload a city's power grid by hacking internet-connected home air conditioners
 - <http://goo.gl/pscpuj> (NON-SSL!)