

SBOMs The Hard Way:

Hacking Bob the Minion

Larry Pesce, Product Security Research and Analysis Director
DEF CON 32 IoT Village

FINITE STATE



Larry Pesce

Product Security Research and Analysis Director, Finite State

- ~~Reformed~~ Penetration Tester
- Paul's Security Weekly podcast co-host (19 years!)
- SANS/GIAC GICSP, GAWN, GCFA, GCIH
- Principal Instructor @ SANS
- Recent convert to the Oxford Comma
- Enjoys long walks on the beach, weighed down by his ham radio (DE KB1TNF)



Larry Pesce*

Product Security Research and Analysis Director, Finite State

- ~~Reformed~~ **Penetration Tester**
- **Paul's Security Weekly podcast co-host (19 years!)**
- **SANS/GIAC GICSP, GAWN, GCFA, GCIH**
- **Principal Instructor @ SANS**
- **Recent convert to the Oxford Comma**
- **Enjoys long walks on the beach, weighed down by his ham radio (DE KB1TNF)**

*** as a Despicable Me villain**


In the Beginning, There Were SBOMs

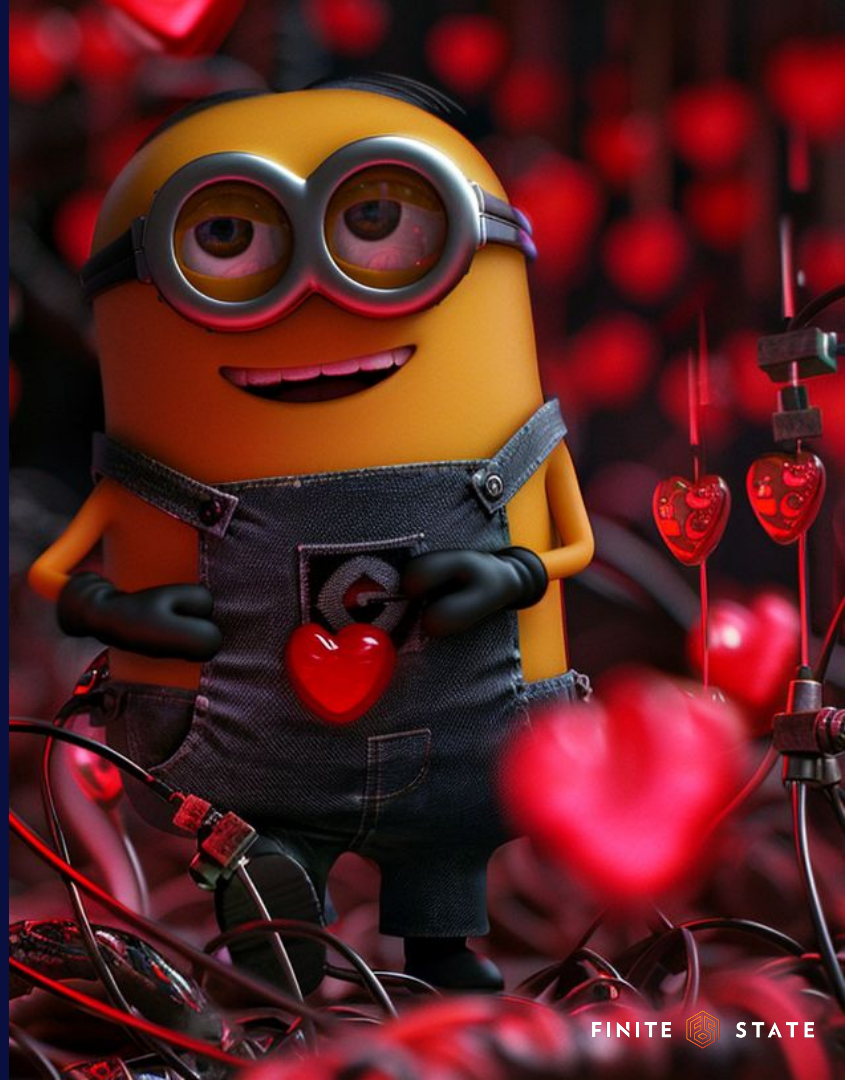
SBOM inevitability

- US regulations/initiatives
  - Omnibus, 524B, Cyber Trust Mark
- EU regulations
  - CRA, …
- General benefits
  - Software inventory, 1st and 3rd party
  - Enrichment
  - SBOMs for Evil



I :heart: SBOMs

- Find new devices, firmware, versions
- Extraction and RE
- Discovery of “known” issues/vulnerabilities
- Verification of CPE match, CVE detection
- Occasional hackery, 0-day discovery, many surprises
- The end result is so much fun!



FINITE STATE

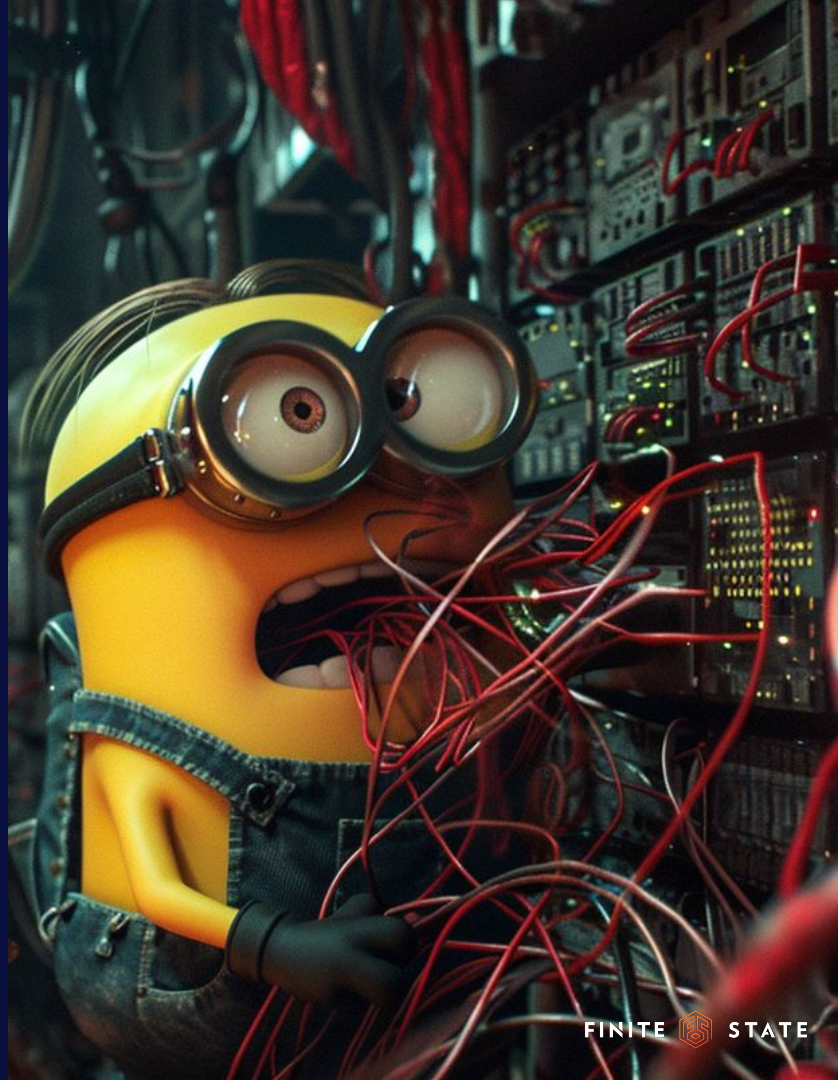

Suddenly a Wild Bob appears...

Davolink AX-1800

- AKA Bob the Minion
  - WiFi6, 802.11ax
  - Easy Mesh
  - WPA3
- Interesting hardware…
  - 128M Flash
  - 256M DRAM
- No current OpenWRT support
- $70-ish via Amazon
- Kevin variety with WiFi 6E
  - $130 via Amazon








Firmware? What Firmware?
FINITE STATE

No firmware

- WebUI “Check for Updates”
  - No updates…
  - No capture from network
- Support forums
  - Different English and Korean versions
  - No one asking, no one giving
- No downloads in Support section of website




No SBOM...


No Fun!
FINITE STATE


...but Brain Surgery is Fun!

Get the Brains!

- No easy downloads means we do this the hard way…
- Board inventory
- Serial?
- JTAG?
- SPI?

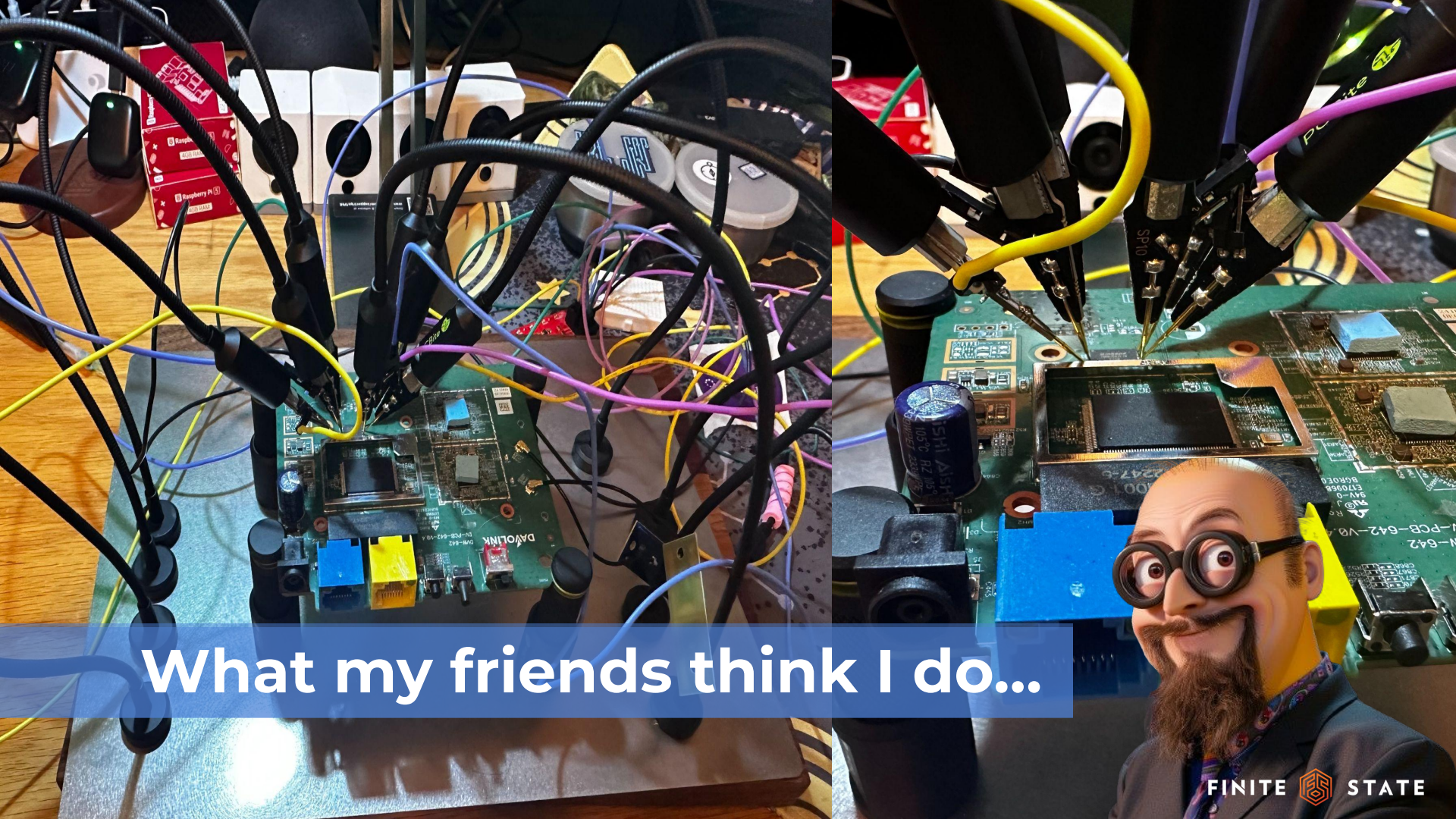






What society thinks I do...

*https://www.wired.com/story/intel-lab-istare-hack-chips/


What my friends think I do...
FINITE STATE


What I think I do...
FINITE STATE


What I really did...
FINITE STATE

Winbond W25N01GV

spiflash

3V 1G-BIT
SERIAL SLC NAND FLASH MEMORY WITH
DUAL/QUAD SPI
BUFFER READ & CONTINUOUS READ



FINITE STATE

The Challenges

- PCbites, no accurate read
  - ...see flashrom support
- Soldered flash let the magic smoke out
  - Kill one, buy two more
  - This is getting expensive... but free (work) trip to DEF CON 32!
- Bus Pirate 3.6, 5
  - Not enough memory (128M)
  - Bus Pirate 5 docs are lacking
  - Other tools with same failure
  - No dediprog ($$) or FT2322 on hand
- flashrom fail
  - No NAND support, chip support
- Pi with SPI bitbang? FAIL
  - https://www.mageirias.com/articles/hardware_hacking/dumping_a_winbond_w25n01gvzeir/dumping_a_winbond_w25n01gvzeir.html



Nailed it!

- Cheap adapter attached to a RasPI 4
  - Off board chip removal
- flashrom fork with NAND support
  - https://github.com/froloffw7/flashrom
- Unmerged commit (?) with Winbond W25N01GV chip support
  - manual patch to flashchips.c include/flashchips.h
  - https://ticket.coreboot.org/issues/523

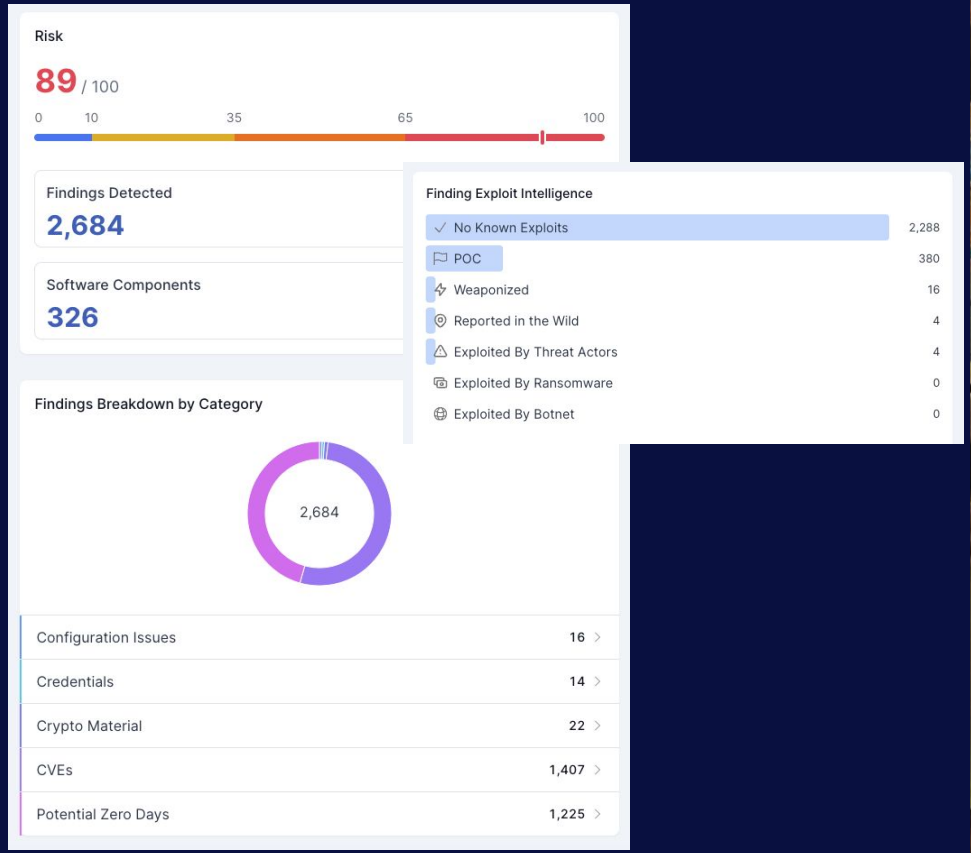
```
0x000030: 30 31 47 56 20 20 20 20 20 20 20 20 20 20 20 20 01GV
0x000040: ef 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x000050: 00 08 00 00 40 00 00 00 00 00 00 00 40 00 00 00 ....@.......@...
0x000060: 00 04 00 00 01 00 01 14 00 01 05 01 00 00 04 00 ................
0x000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x000080: 08 00 00 00 00 bc 02 10 27 32 00 00 00 00 00 00 ........'2......
0x000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x0000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x0000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x0000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x0000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x0000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x0000f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 3d ...............=
Found WINBOND flash chip "W25N01GV" (131072 kB, SPI) on linux_spi.
===
This flash part has status UNTESTED for operations: ERASE WRITE WP
The test status of this chip may have been updated in the latest development
version of flashrom. If you are running the latest development version,
please email a report to flashrom@flashrom.org if any of the above operations
work correctly for you with this flash chip. Please include the flashrom log
file for all operations you tested (see the man page for details), and mention
which mainboard or programmer you tested in the subject line.
Thanks for your help!
Reading flash...
```



FINITE STATE


The Treasure

AN SBOM!

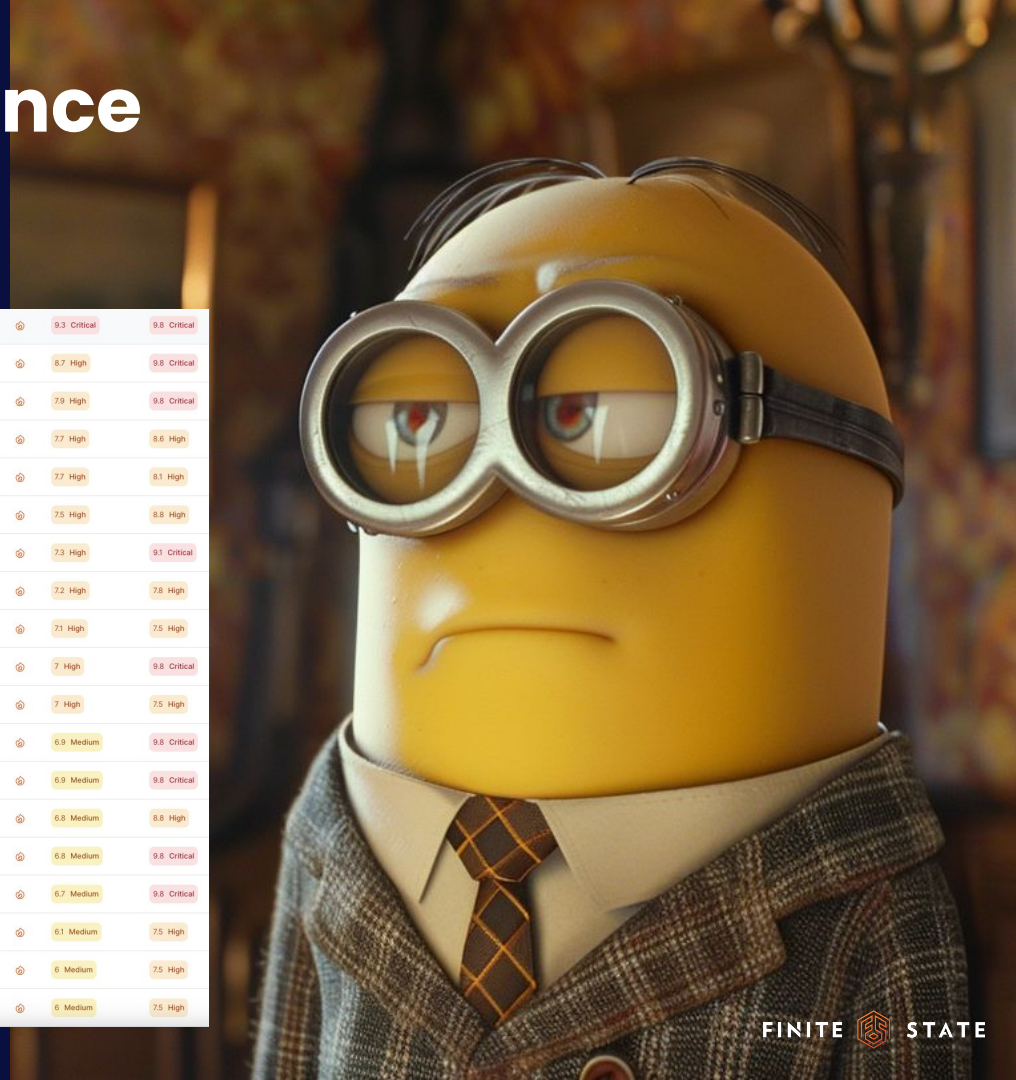

Risk
89 / 100
0
10
35
65
100
Findings Detected
2,684
Software Components
326
Finding Exploit Intelligence
No Known Exploits 2,288
POC 380
Weaponized 16
Reported in the Wild 4
Exploited By Threat Actors 4
Exploited By Ransomware 0
Exploited By Botnet 0
Findings Breakdown by Category
2,684
Configuration Issues 16
Credentials 14
Crypto Material 22
CVEs 1,407
Potential Zero Days 1,225



….and Exploit intelligence

- So much to unpack…
- CVSS scoring with EPSS tempering
- Lots of network based attacks with available exploits
  - 79 with various status
  - …without counting Linux kernel stuff

CVE-2022-1292 - OpenSSL:1.1.1n	9.3 Critical	9.8 Critical
CVE-2016-2148 - BusyBox:1.22.1	8.7 High	9.8 Critical
CVE-2022-32221 - curl:7.66.0; cURL:7.75.0	7.9 High	9.8 Critical
CVE-2020-8616 - bind-libs:9.11.2-P1-1	7.7 High	8.6 High
CVE-2021-22901 - cURL:7.75.0	7.7 High	8.1 High
CVE-2022-28391 - busybox:1.28.4; BusyBox:1.22.1	7.5 High	8.8 High
CVE-2021-22945 - cURL:7.75.0	7.3 High	9.1 Critical
CVE-2016-6301 - BusyBox:1.22.1	7.2 High	7.8 High
CVE-2016-2147 - BusyBox:1.22.1	7.1 High	7.5 High
CVE-2022-37434 - zlib:1.2.11-1	7 High	9.8 Critical
CVE-2023-50387 - Dnsmas… dnsmasq-debuginfo:2.86	7 High	7.5 High
CVE-2022-34835 - U-Boot:2020.01	6.9 Medium	9.8 Critical
CVE-2023-38545 - libcurl4-32bit:7.79.1; cURL:7.75.0	6.9 Medium	9.8 Critical
CVE-2017-16544 - BusyBox:1.22.1	6.8 Medium	8.8 High
CVE-2022-32207 - cURL:7.75.0	6.8 Medium	9.8 Critical
CVE-2022-30767 - U-Boot:2020.01	6.7 Medium	9.8 Critical
CVE-2019-5747 - BusyBox:1.22.1; busybox:1.28.4	6.1 Medium	7.5 High
CVE-2020-8169 - curl:7.66.0-3	6 Medium	7.5 High
CVE-2020-8285 - curl:7.66.0-3	6 Medium	7.5 High




The Spoils

Credentials

- 3 valid users, 2 undocumented…
- *bob* user?!
  - Password of *bob*
- Hashcat for the remaining users
  - So far, unsuccessful…
  - Possible .kr character set

```
→  etc cat passwd.ori
root:$1$$iH.ncJhU.b13wJb3iLPKq/:0:0:root:/var/tmp:/bin/ash
admin:$1$$mz7MkSOrgCzFz25kgxTQF0:0:0::/var/tmp:/bin/dvsh
nobody:x:0:0::/var/tmp:/dev/null
bob:$1$ovCE1ysJ$lJ52bYgo3kb9penoV.Rh..:1:1:WebUser:/var/tmp:/dev/null
```



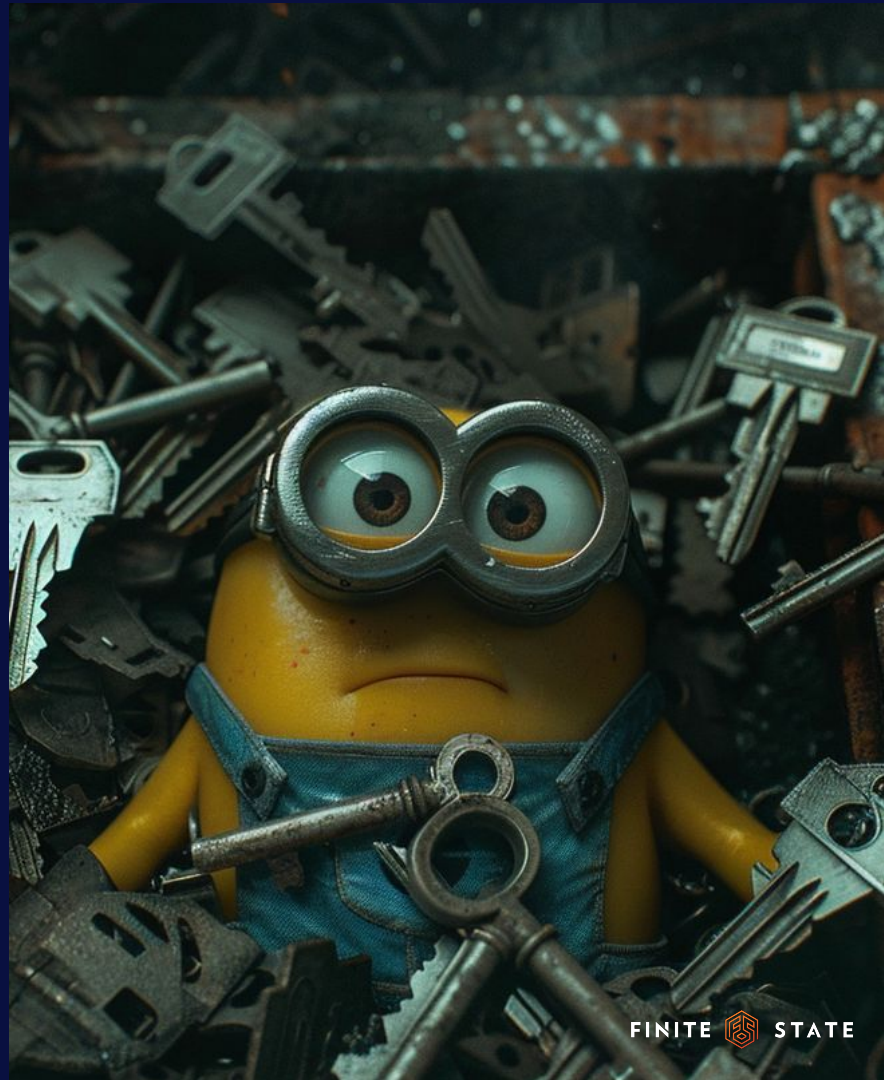
FINITE STATE

Key Material

- **Private keys/certificates**

```
➜  etc cat private.key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAqmox7VWd10TzjFYRtVrbLC/8jftvlD1NbNnkvze28gW2aiEA
JXxH2TSWx3kUJ0lyP0g61/CGjUbFIbGu1rpDCqOb+e7G9szXSXl92WObNBCKsWB6
jWlY80CxrNobhcUpU142KDdcPtS403yuMY0VpoTMPdCQo0u10/VbbzGZeLwU36CT
yLQINib58vXgmVDynVos2OpBd+gbvedigyb5lhZWF1qsC/CkZCpK3xKJ7lkBaUxa
mHgf82m3fSkwtZCOqdE4GwvSHddq8BvD0fPtlMh2feNQl6tkKJIkxCgllUjtrTl6
jWy3rjCRfkZM4hqGnJY3MZdiYV1iDRpHZSRvLQIDAQABAoIBACXY3evC1wJHOvvQ
5a/sVL7UjXeO/vHiR37ESaw6GHRZ1nBtkdXBa0ePCWmVt2ceRbROO1tX/NoFfKSG
DLl9toP3YB267Q9E4Q9dXxjXqVF/1v2b2rvrSKkFljA4ZGJqLkpoowh9ewwtPDsj
9p/koIlR9vZHisfpeaFwXXUtg9MvPWbFzSPY/wmp4BR1lkDixZENcoe8PZnR4M4C
gEVRwiZfbckA9QZGHjj3t5EK5rbMpGhllf05YiszTU9CM8NrEmbdRMeeNckMAaCK
VuhtXQjqEXPJ1QnJGNPiL56Zo1ZXvQ2pfWRwcXITpqNh8zjkVOL6pz/VlUIij1Uf
qOTfvoECgYEA2uQh8jGYKZ6C8D6/dgr4/KlgnPZDgRYmnjhX1zKlQzLPOqg1f9jd
I741TKcBez+/Eufkg7mo6Wld3M6sKdfIzF8gd1mVFI3dYDGALH8+oa30/ZuaZZV/
zrXtuDC+qh3CzeBS+xPFJTu8EVXAqmo7WN1UBJBgrQvgipk9xmm3daECgYEAx04x
J9Tgi6+0DEQXjbUAqUm8ZZB27C0R6U5GWot680JXjLI7a+seihL9KYsp8wVJ3Ygt
Yte2+CAIStnVvhwL3VgLvoqkCo9mZIGlks6UNFium/m1KRE5PT328Li/cCzpj/j3
rlCEoDWvbU2JDcK38VfGtIeOGo964Y3N8LZTtg0CgYBChMl8HG4tV6pa7/anHLaF
scNWb9Abzmt18ZFgKFfoj+xB2xRHAdRSJF92J9pfZgPe7vGWxjj6lbacf4H6RUUU
NmRbYLHZSTNZJDHbU9/oqjUZBMxqyn/Ihaj0LHwEnn6wqdcNzfg/VGPWsMSYBSh7
3ObHbEi0zcMy21bWkRHbgQKBgQCt9Ghg/KOUKCI9Bn2MWKwgFdSSzRmPH/NfL8um
IdGJWqExkyrcEZZRKyu9w9I0Y6xJ6B69A8yWGtdCBYlSagZNBhkSEM4GzYywMpxC
W33thm24g6WEF51e/6N2DbpBfWHKIKKFiY+IifL4stDpqseDpXowfZQhSJQXI/7Y
lzrPTQKBgA/apL6+2B6WeLB9dZCuMVnCvAvtMU+NVB7nVw78V3hOZ3vV8GPWTs+7
/ZsrYa8pTTLdsuQB384xoR5MCYf5b4IKGZiRYYqHIaEk63/55qHKYpia1kGzOK3s
j13655Ij2Pp/rhnisk5UamGuxDGBkHuOtmVNLWmUaWbdNPCDMfL6
-----END RSA PRIVATE KEY-----
```

```
➜  etc cat private.pem
-----BEGIN CERTIFICATE-----
MIID0zCCArugAwIBAgIJAKcVFWzKkqCnMA0GCSqGSIb3DQEBCwUAMH8xCzAJBgNV
BAYTAktPMQ0wCwYDVQQIDARkYXZvMQ0wCwYDVQQHDARkYXZvMQ0wCwYDVQQKDARk
YXZvMQ0wCwYDVQQLDARkYXZvMQ0wCwYDVQQDDARkYXZvMSUwIwYJKoZIhvcNAQkB
FhZzdXBwb3J0QGRhdm9saW5rLmNvLmtyMCAXDTIxMDUxODA0NTYzMVoYDzQ3NTkw
NDE1MDQ1NjMxWjB/MQswCQYDVQQGEwJLTzENMAsGA1UECAwEZGF2bzENMAsGA1UE
BwwEZGF2bzENMAsGA1UECgwEZGF2bzENMAsGA1UECwwEZGF2bzENMAsGA1UEAwwE
ZGF2bzElMCMGCSqGSIb3DQEJARYWc3VwcG9ydEBkYXZvbGluay5jby5rcjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKpqMe1VnddE84xWEbVa2ywv/I37
b5Q9TWzZ5L83tvIFtmohACV8R9k0lsd5FCdJcj9IOtfwho1GxSGxrta6Qwqjm/nu
xvbM10l5fdljmzQQirFgeo1pWPNAsazaG4XFKVNeNig3XD7UuNN8rjGNFaaEzD3Q
kKNLtdP1W28xmXi8FN+gk8i0CDYm+fL14JlQ8p1aLNjqQXfoG73nYoMm+ZYWVhda
rAvwpGQqSt8Sie5ZAWlMWph4H/Npt30pMLWQjqnROBsL0h3XavAbw9Hz7ZTIdn3j
UJerZCiSJMQoJZVI7a05eo1st64wkX5GTOIahpyWNzGXYmFdYg0aR2Ukby0CAwEA
AaNQME4wHQYDVR0OBBYEFFRubNCfToR9Qslo4OXNGAUqsHMKMB8GA1UdIwQYMBaA
FFRubNCfToR9Qslo4OXNGAUqsHMKMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggEBABi20JFV5W5qAJhSlHvhIwNV1Noly+hR/y9bYr7K8nxHYR9h8W7PoSqc
wI6brguYaCBEcl8VtavqxR21orSG8DpK+srYT54TcZHrpLA4jZ2Of8JDbwDxwOtV
tulOPvRhVTnkMH2kMmW+BHSBz0lTiCUlitwTwXNDyJFOkoocIAbv52pVSsqemimF
xgRKYqkjqlyd8nd0u4HXZsk4c66ZF02CSAiFtCLQ0doKTdT8+DrGcfrkR+v41RSA
FNWCA0lowvJ/emcX8aNBjKRT/5n2gO7lxmChy4akRIeng2g+D7l/ZXIA18Bjt3eh
0jHmySo2Zy/UbJn+R7Tmt/gjU7fKCSM=
-----END CERTIFICATE-----
```



FINITE STATE

Web app

- JavaScript (ew) for the client frontend
  - Client side Captcha
- Custom web server
  - Integrated functionality ala BusyBox
  - Needs time, emulation or other access
- Command injection?
  - ...in the password reset function?

```
  sVar2 = strlen(acStack_110);
  if ((9 < sVar2) && (local_114 == 7)) break;
  gen_printf(
            "a password must be 10 characters including one special character and alphanumeric cha
            racters.\n"
            );
  if (param_1 < 2) {
    return 0;
  }
}
snprintf(acStack_90,0x80,"echo -e \"%s\n%s\n\" | busybox /bin/passwd %s > /dev/null 2>&1",
         acStack_110,acStack_110,local_120);
dv_system(acStack_90);
return 0;
```



FINITE STATE

Other goodies

- Scripts, scripts and scripts
  - IP addresses at LG Uplus, Korea Telecom, and Chunghwa Telecom
  - “Snapshot” upload
- Custom shell?
  - Default user shell of /bin/dvsh
  - May be a /bin/ash clone
    - But…why?
- Kernel version?
  - 4.4.140 - bleeding edge for IoT



TODO

- OpenWRT support
  - My call to action to the community
  - I bet the WiFi chipset is the hardest part…
- Emulation with {Firmadyne, FAT, QEMU, FirmAE}
- Brain transplant!
  - I bricked one, but have “blank” flash
  - Flashrom “unsupported” write
- Ongoing reporting to Davolink





Thank you!

larry.pesce@finitestate.io

FINITE STATE


Thank you!
larry.pesce@finitestate.io
A huge thanks to Edwin Shuttleworth for the assist!
FINITE STATE