ALPC is in Danger: ALPChecker Detects Spoofing and Blinding Attacks

Anastasiia Kropova,
Igor Korkin, Ph.D.

Who we are

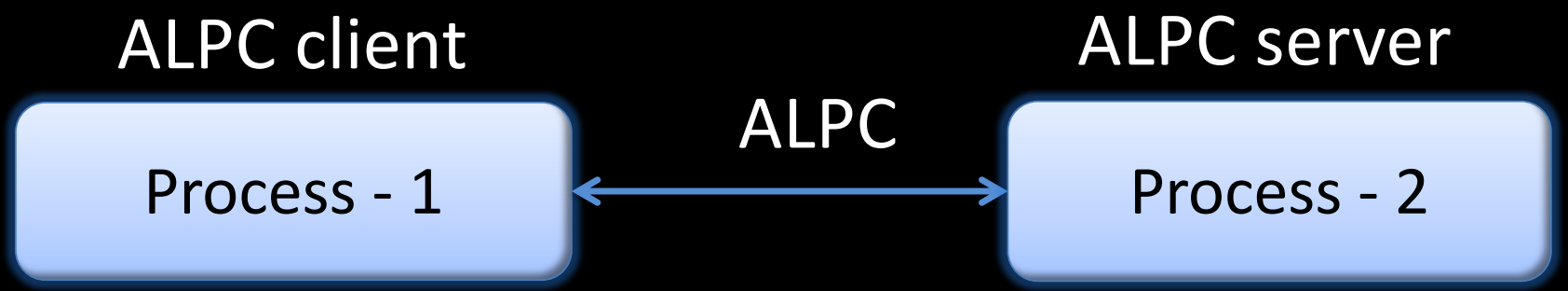
Anastasiia Kropova

- Bachelor of Cyber Security
- alumni of NRNU MEPhI (Moscow Engineering Physics Institute)
- Cryptology and Cybersecurity Department

Igor Korkin, Ph.D.

- Independent Security Researcher
- Speaker at BlackHat, HITB, CDFSL, SADFE
- sites.google.com/site/igorkorkin

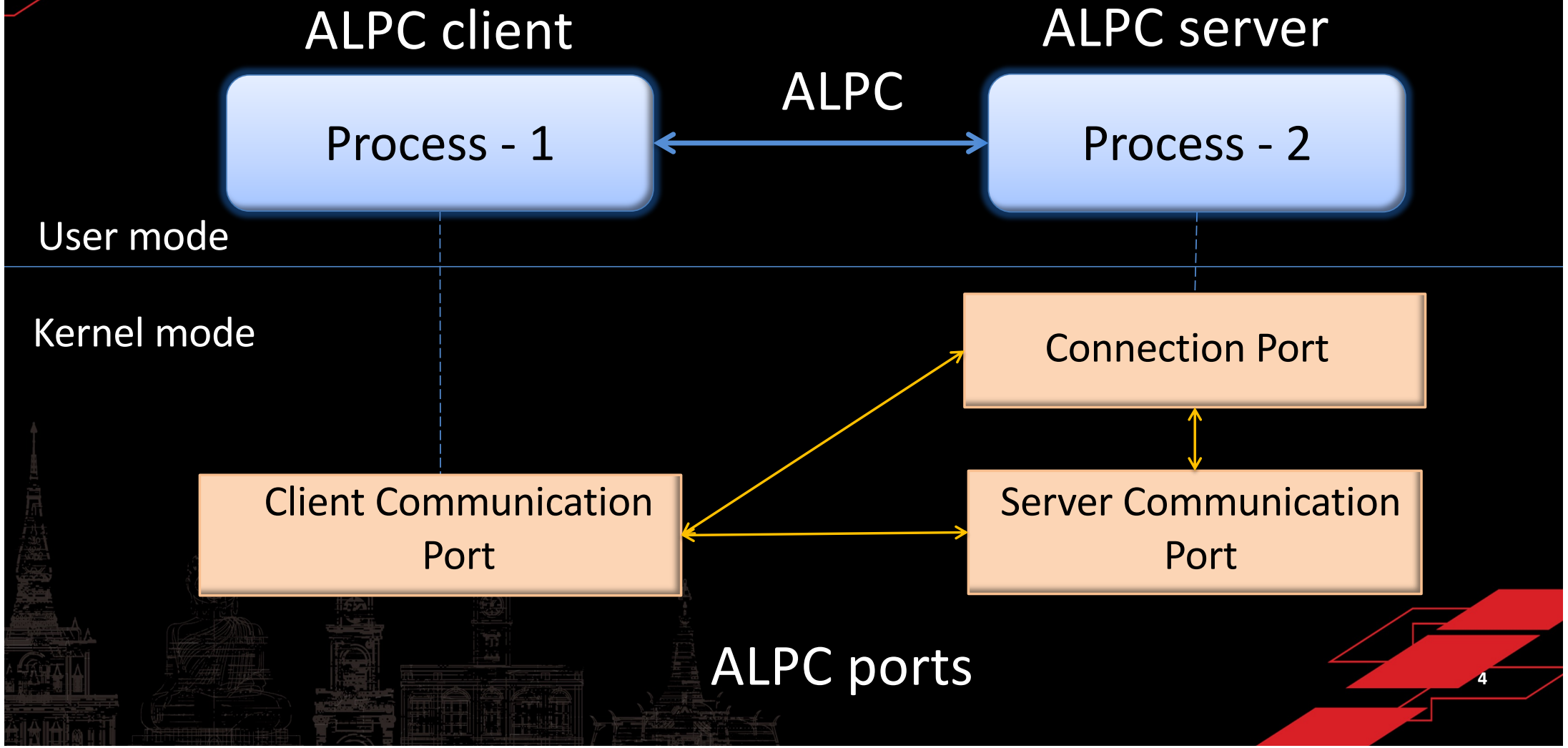
Interprocess communication in Windows



Interprocess communication cases:

- Usage of dynamic-linked libraries;
- Verification of the authenticity of the user to perform the operation on his behalf;
- Getting input text;
- Creation or removal of threads;
- D-COM-object interaction.

Interprocess communication in Windows – ALPC architecture



ALPC port structures

ALPC_PORT
PortListEntry
CommunicationInfo
OwnerProcess
PendingQueue
WaitQueue
CanceledQueue
MainQueue

ALPC_COMMUNICATION_INFO
ConnectionPort
ClientCommunicationPort
ServerCommunicationPort
HandleTable
CloseMessage

```
(nt!_ALPC_PORT*) 0xffffa109f2a559c0          0xffffa109`f2a559c0 struct _ALPC_PORT *
  PortListEntry                              struct _LIST_ENTRY [ 0xffffa109`f2bd6a20 - 0xffffa109
  CommunicationInfo                          0xffff898a`35b5b360 struct _ALPC_COMMUNICATION_INFO *
    ConnectionPort                           0xffffa109`f375acf0 struct _ALPC_PORT *
    ServerCommunicationPort                  0xffffa109`f2bd6a20 struct _ALPC_PORT *
    ClientCommunicationPort                  0xffffa109`f2a559c0 struct _ALPC_PORT *
    CommunicationList                        struct _LIST_ENTRY [ 0xffff898a`35b37498 - 0xffff898a
    HandleTable                              struct _ALPC_HANDLE_TABLE
    CloseMessage                             0xffff898a`35d3abd0 struct _KALPC_MESSAGE *
  OwnerProcess                               0xffffa109`f410d080 struct _EPROCESS *
  CompletionPort                             0x00000000`00000000
  CompletionKey                              0x00000000`00000000
```

Kernel mode attacks using Windows Kernel Drivers

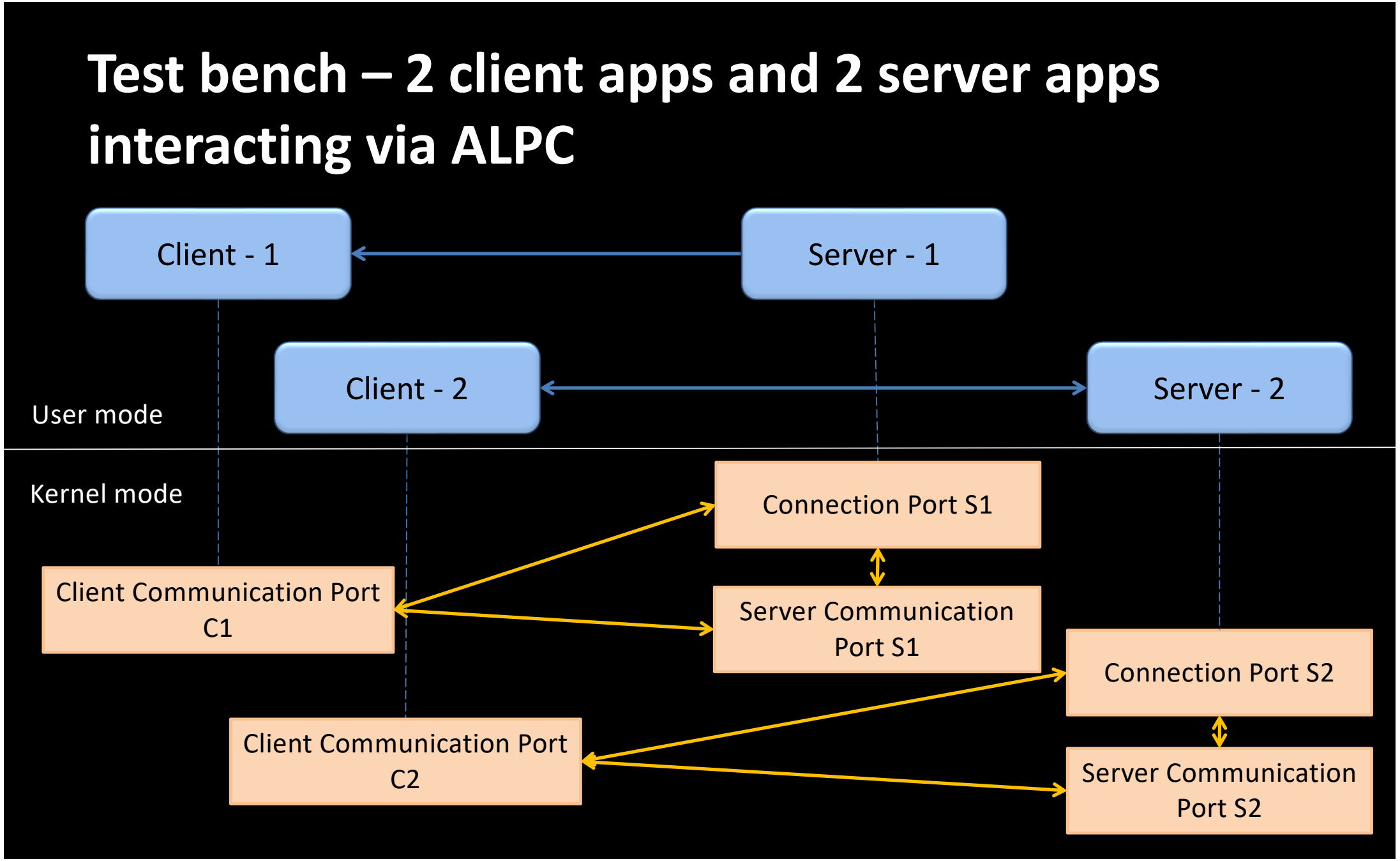
Kernel driver attacks in 2022-2023

- Bring your own vulnerable driver (BYOVD)
- Malware drivers signed with leaked certificates
- UEFI security threats

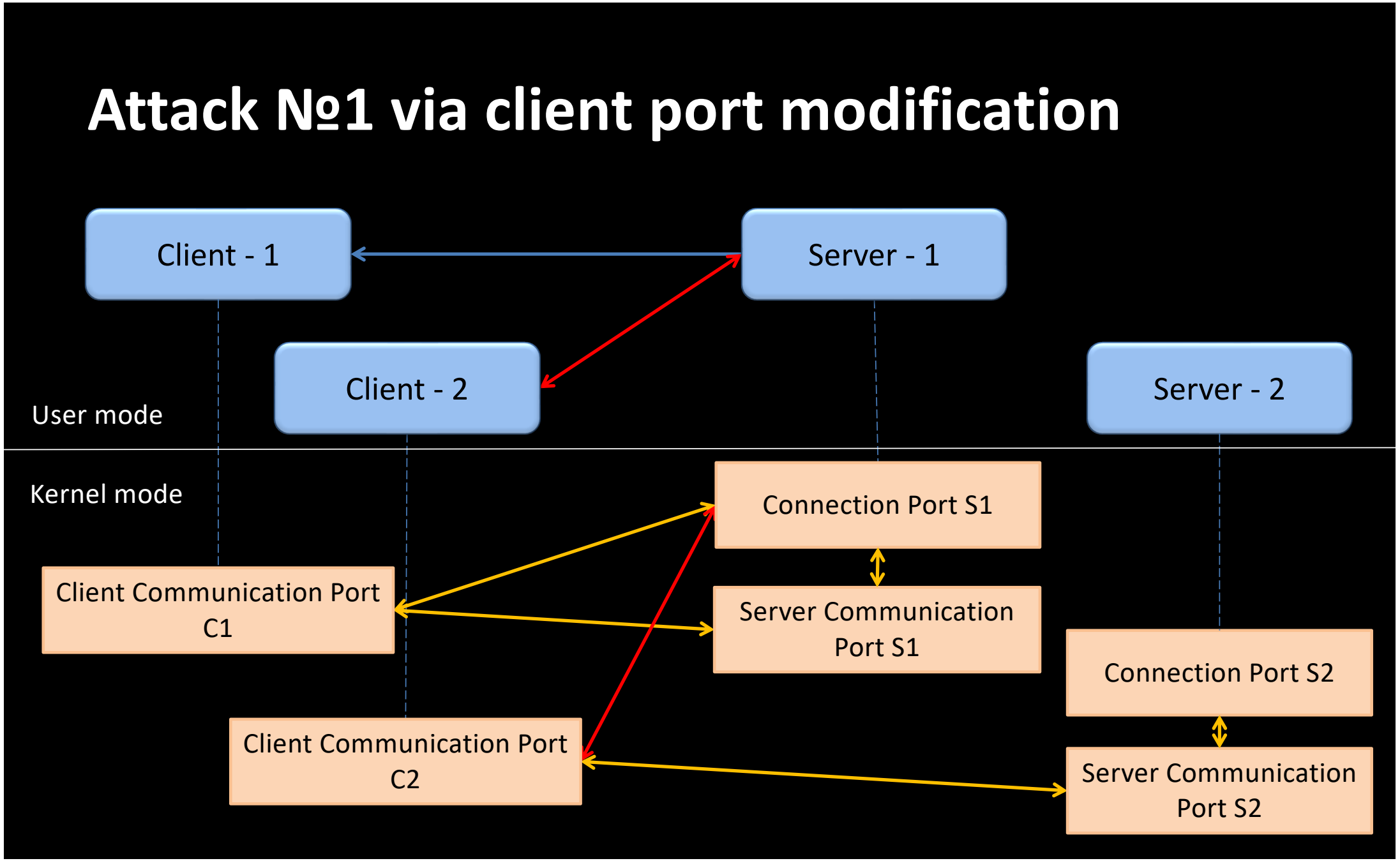
- Pogonin and Korkin at the ADFSL and Rootcon conferences in 2022 gave more than 50 attack examples, accomplished using these techniques;
- Rapid7 experts gave 30 malware examples that use buggy signed drivers (2022);
- TrendMicro experts analyzed low-level threads evolution in Windows and made a conclusion about actuality of kernel-level threads (2023)

Binarly team guys first payed attention to ALPC vulnerability. In 2022 at LABScon and Ekoparty conferences they demonstrated attack on WMI based on disabling ALPC connection.

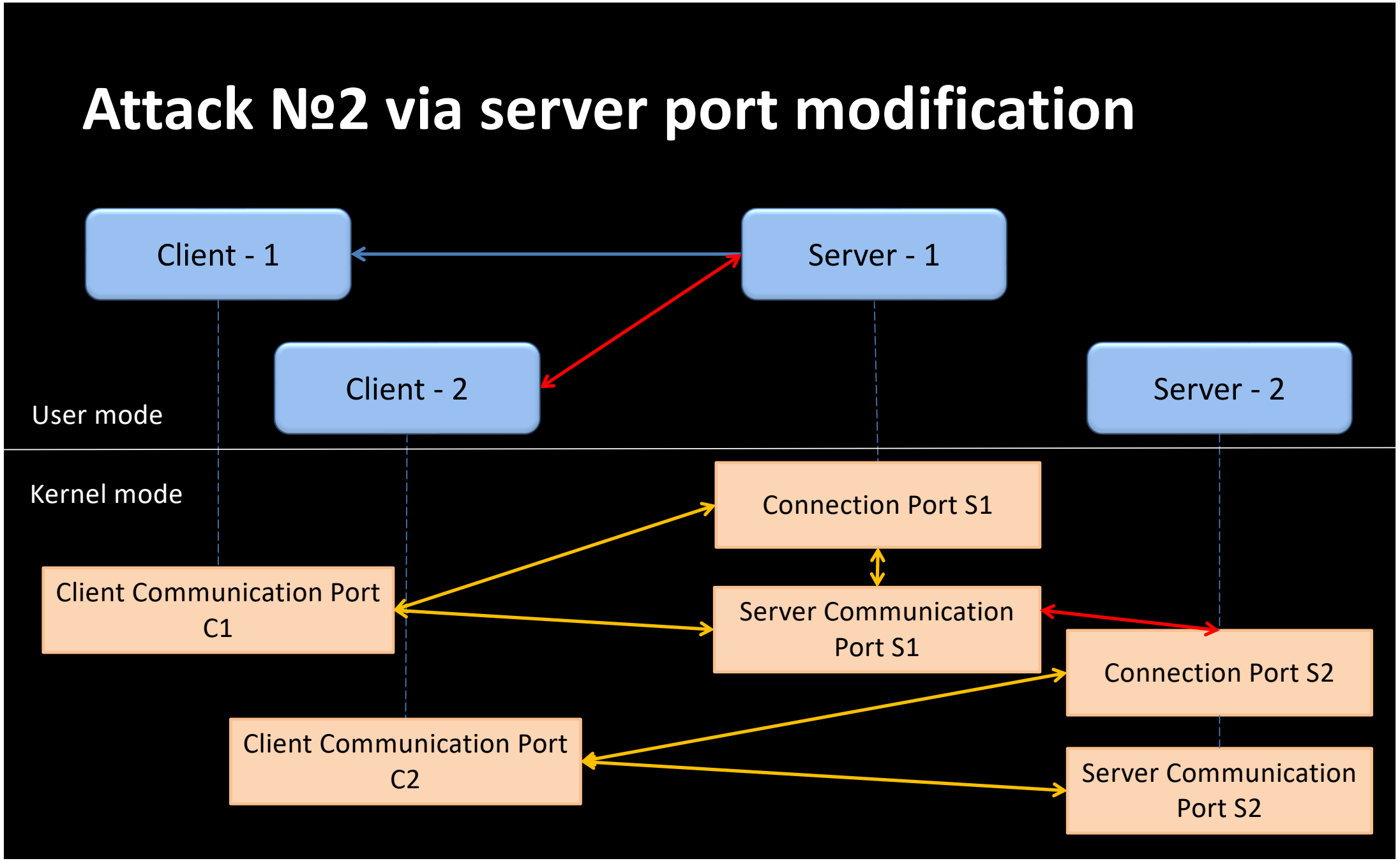
Test bench – 2 client apps and 2 server apps interacting via ALPC



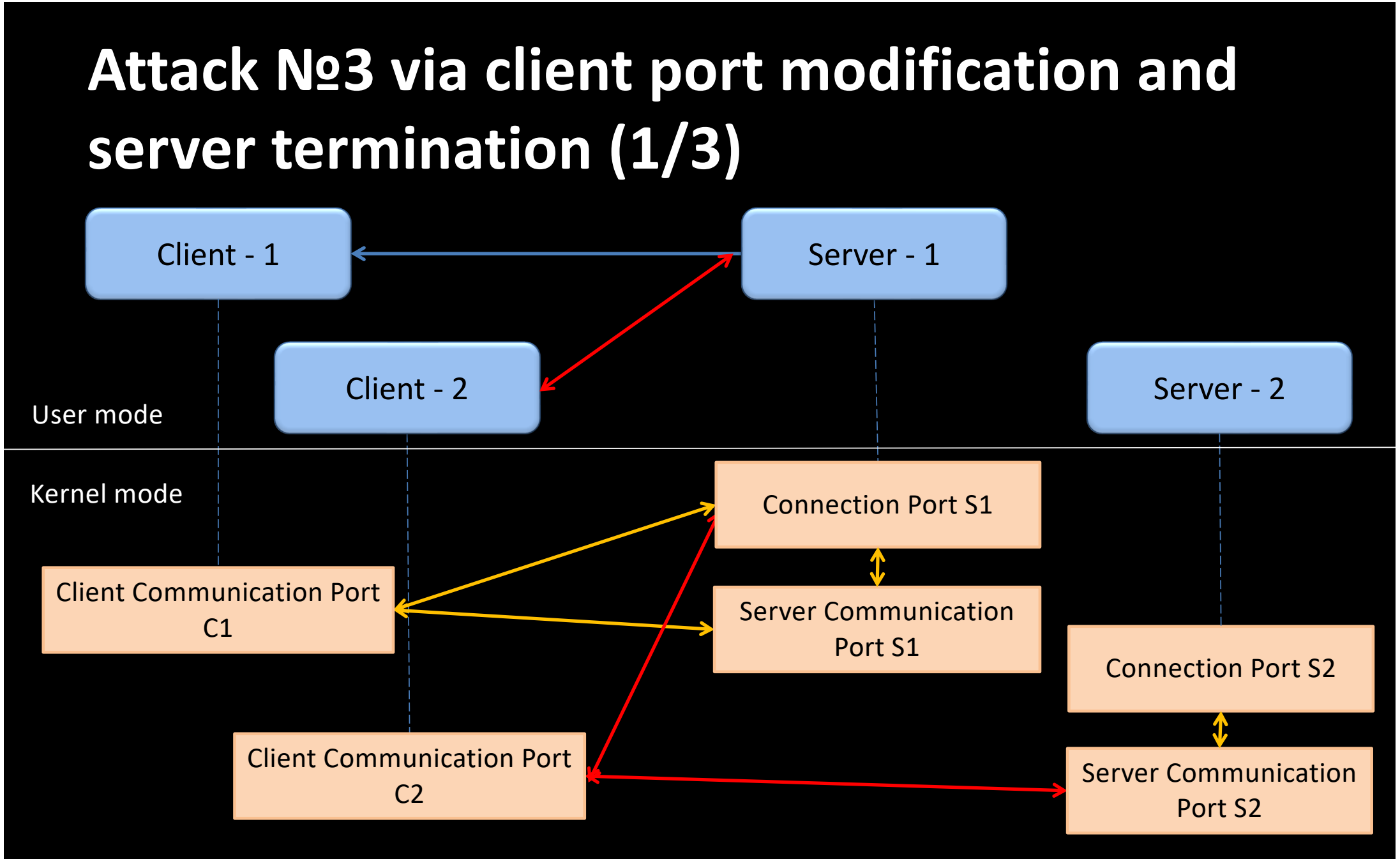
Attack №1 via client port modification



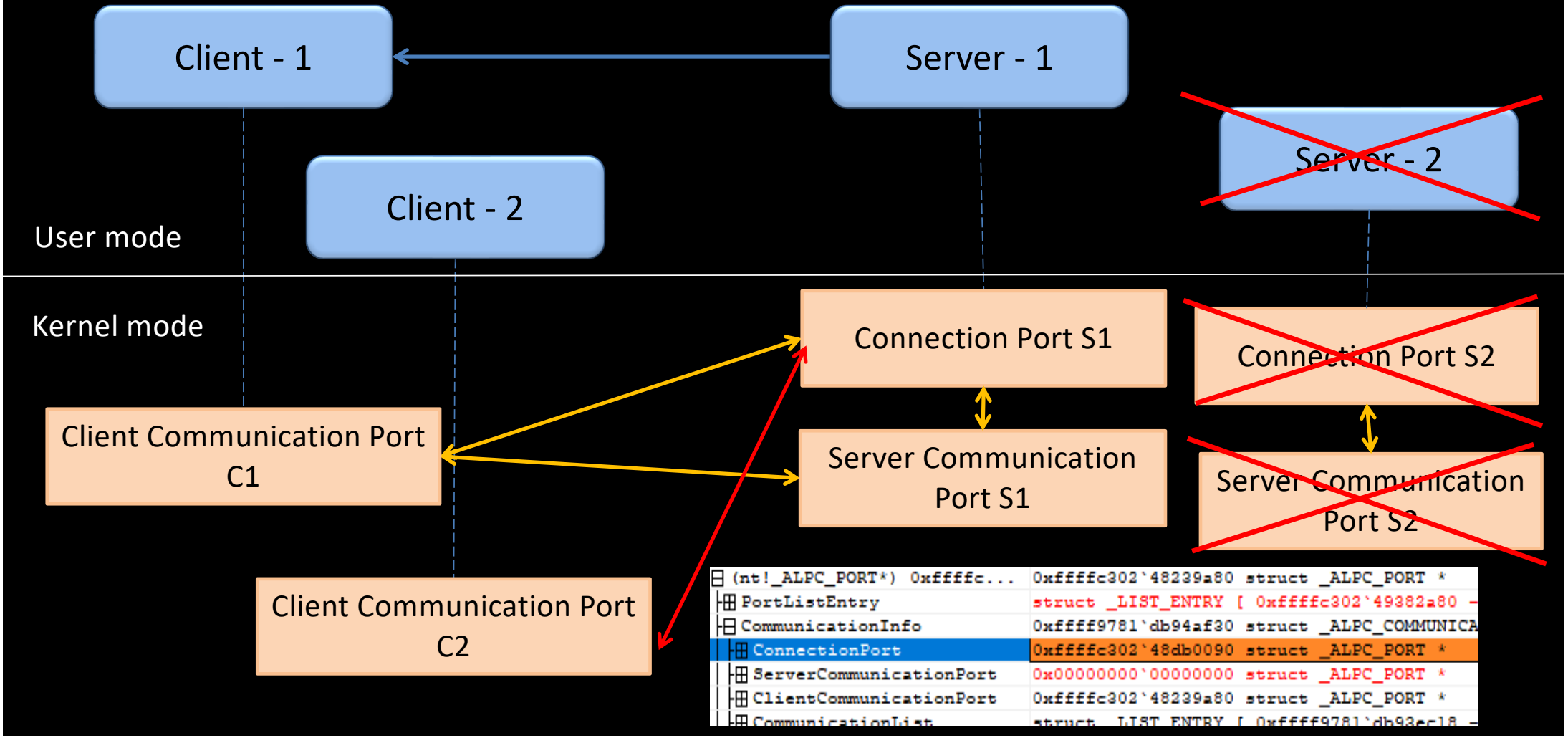
Attack №2 via server port modification



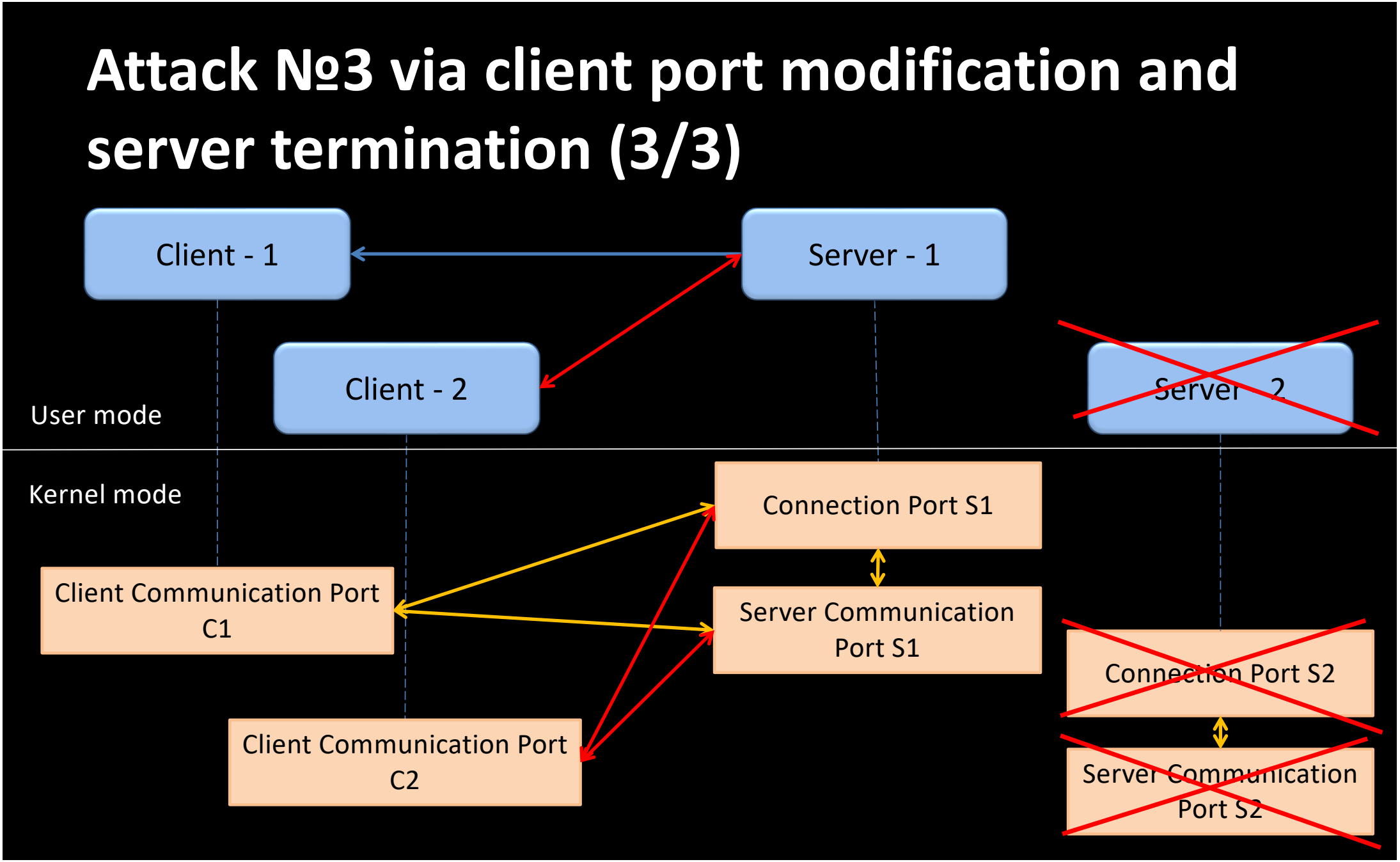
Attack №3 via client port modification and server termination (1/3)



Attack №3 via client port modification and server termination (2/3)



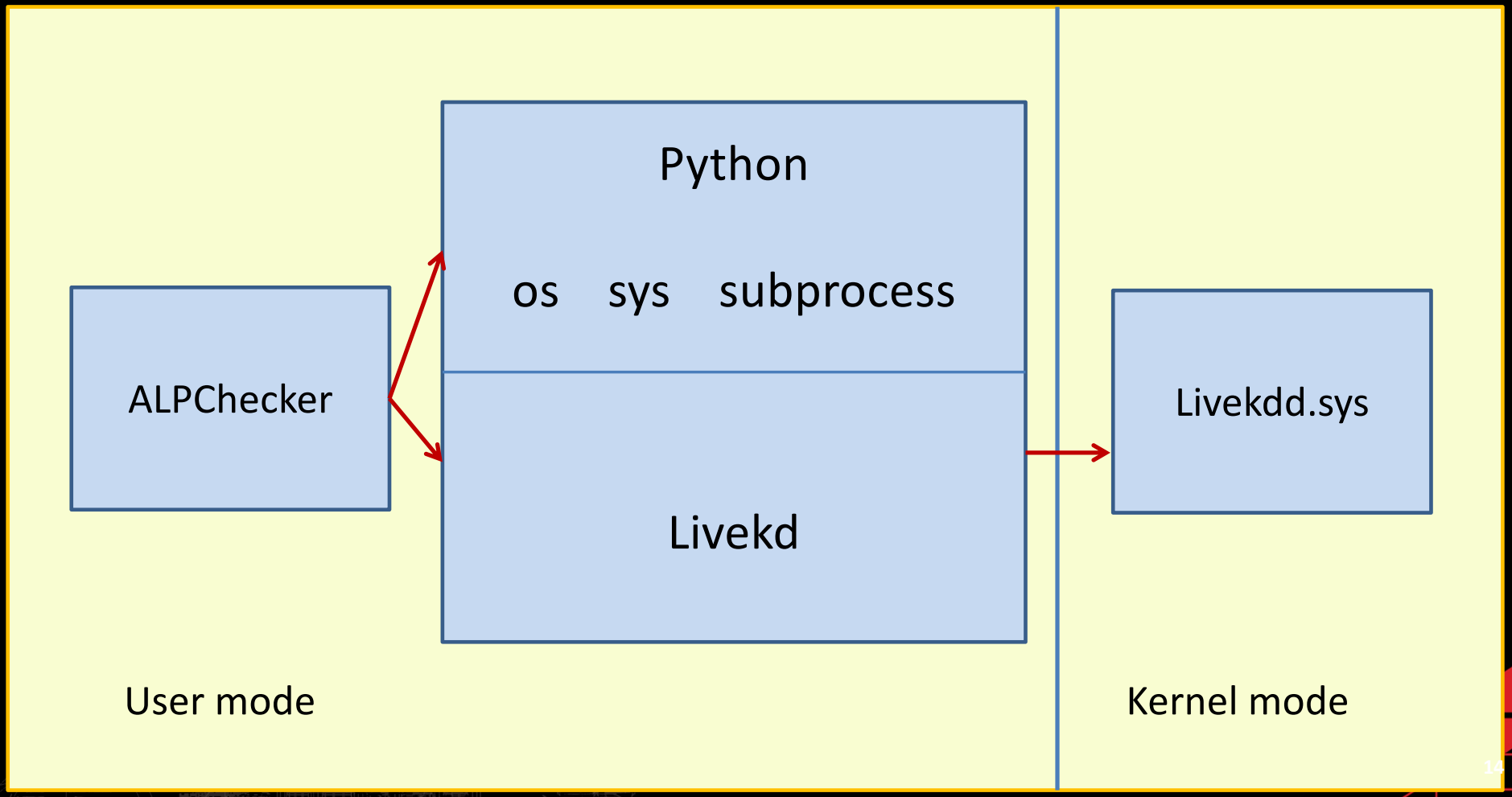
Attack №3 via client port modification and server termination (3/3)



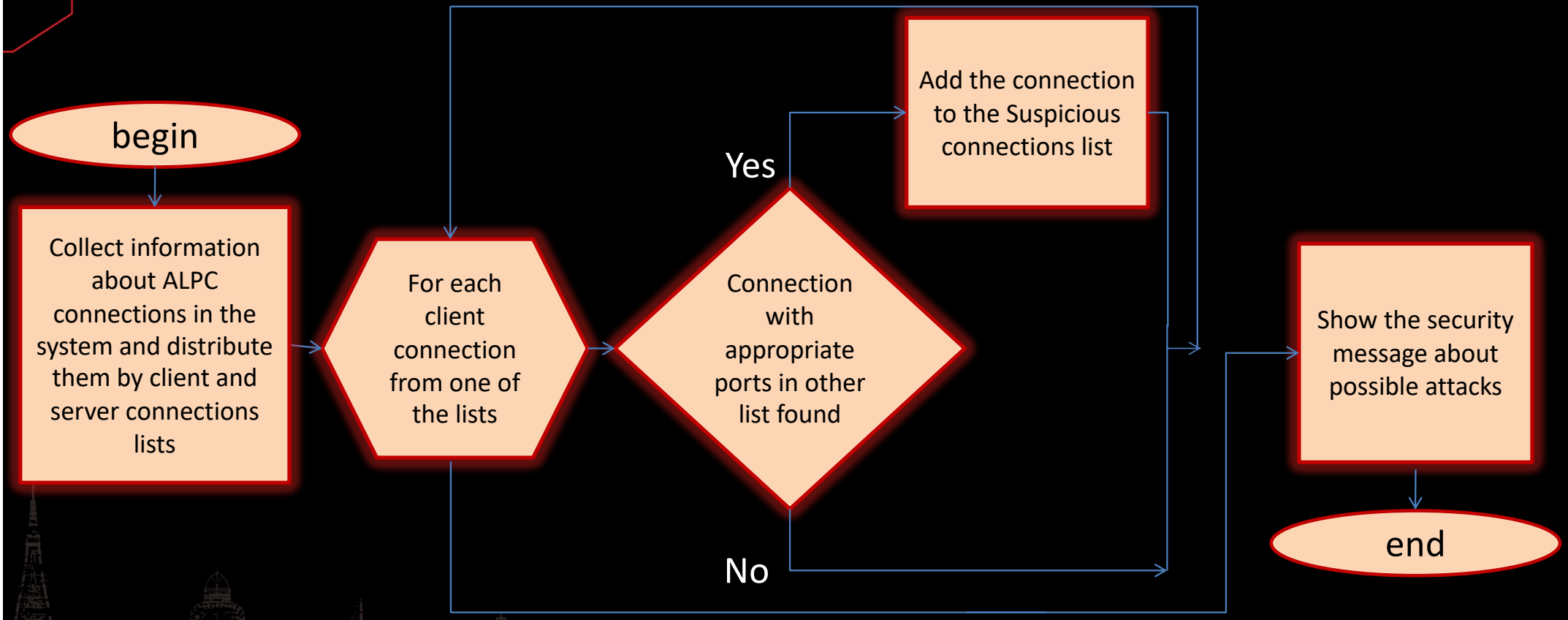
Attacks results

Attack	Processes with modified structures	Modified fields	Result
via client port modification	Client C2	ClientCommunicationPort ->CommunicationInfo-> ConnectionPort	Illegal connection C2-S1 has been established, S2 lost connection with C2
via server port modification	Server S2	ServerCommunicationPort ->CommunicationInfo-> ConnectionPort	Illegal connection C2-S1 has been established, S2 lost connection with C2
via client port modification and server termination	Client C2	ClientCommunicationPort -> CommunicationInfo-> ConnectionPort, ClientCommunicationPort -> CommunicationInfo-> ServerCommunicationPort	Illegal connection C2-S1 has been established, after terminating S2 connection was restored

ALPChecker - a tool for detecting attacks on ALPC interaction

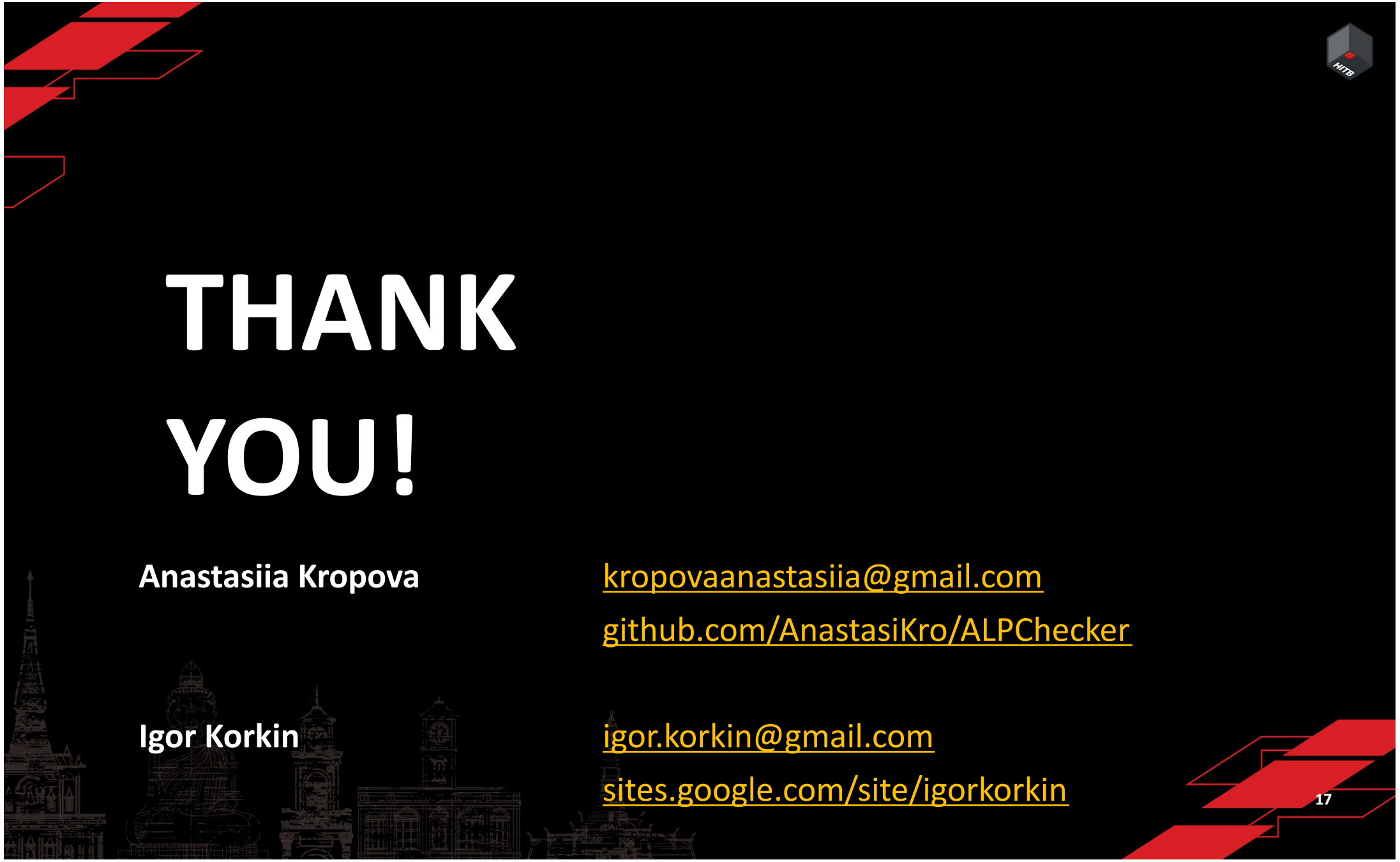


ALPChecker algorithm



ALPChecker results: all the attacks were detected

Attack	Result
via client port modification	Detected
via server port modification	Detected
via client port modification and server termination	Detected



Anastasiia Kropova

kropovaanastasiia@gmail.com

github.com/AnastasiKro/ALPChecker

Igor Korkin

igor.korkin@gmail.com

sites.google.com/site/igorkorkin