Take-home Exam 1

- Exam questions are made available on CANVAS on **February 17, 2023 (Friday)**.
- Please "type" answers and submit **a PDF file** by **11:59pm on March 3, 2023 (Friday)**.
- Late submission suffers from **20% reduction** from the total score.
- **Open book. No discussion or collaboration is allowed.**
- Any clarification question should be posted on **CANVAS Forum** for the sake of sharing (and fairness). No private inquiry is answered.

CS5321 Network Security
Week6: Honeypot and Threat Intelligence

Daisuke MASHIMA

http://www.mashima.us/daisuke/index.html

2022/23 Sem 2

Agenda

- What is Honeypot?
  - How would they help us?
  - Types of honeypots
- Threat Intelligence Analysis Using Low-interaction Honeypot Data
- Automated Utilization of Honeypot Data for Securing Large-scale System

What is Honeypot?

According to Google:

honeypot

/ˈhʌnɪpɒt/

noun

noun: **honeypot**; plural noun: **honeypots**; noun: **honey-pot**; plural noun: **honey-pots**

1. a container for honey.
   "an earthenware honeypot"
   - an enticing source of pleasure or reward.
     "massive increases in government purchases became a honeypot for the unscrupulous"
   - a place to which many people are attracted.
     "the tourist honeypot of St Ives"

In cyber security domain, "honeypot" is a dummy system or device for attracting cyber attackers
- Should look like a valuable, real system
- Intentionally exposed to attackers and made vulnerable

How Honeypots help us

- Mislead and trap attackers to detect indication of upcoming attacks and buy time before they mount real attacks
- Collect data (e.g., system logs and network traces) while attackers are scanning and attacking the system
  - Derive intelligence about attackers
    - Where are they coming from?
    - What tool / artifact they are using?
    - How the attacks progress?
    - Any pattern / trend?
  - Collected data can be used to evaluate the security
- Help us defend the system
  - E.g., Tuning firewall and intrusion detection systems

Types of Honeypot

- Low-interaction
  - Produce minimal responses for some protocols/services
  - Mainly used for statistical evaluation
  - Easy to implement and deploy
  - Less resource demanding

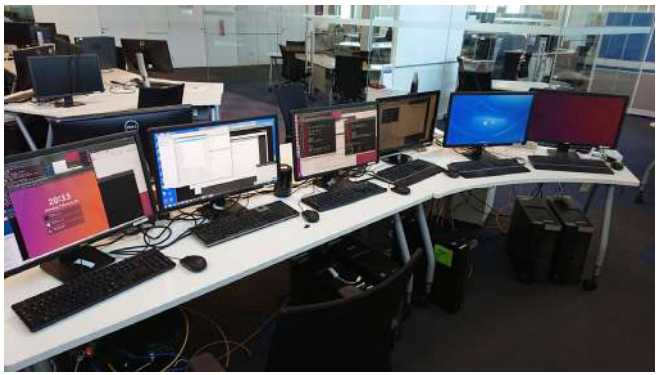
- High-interaction
  - Emulate realistic system to attack
  - Consisting of dummy/decoy devices as well as topology
  - Can collect more data, and enables observation for longer time period because of better realism
  - Difficult to implement
  - Requires more resource

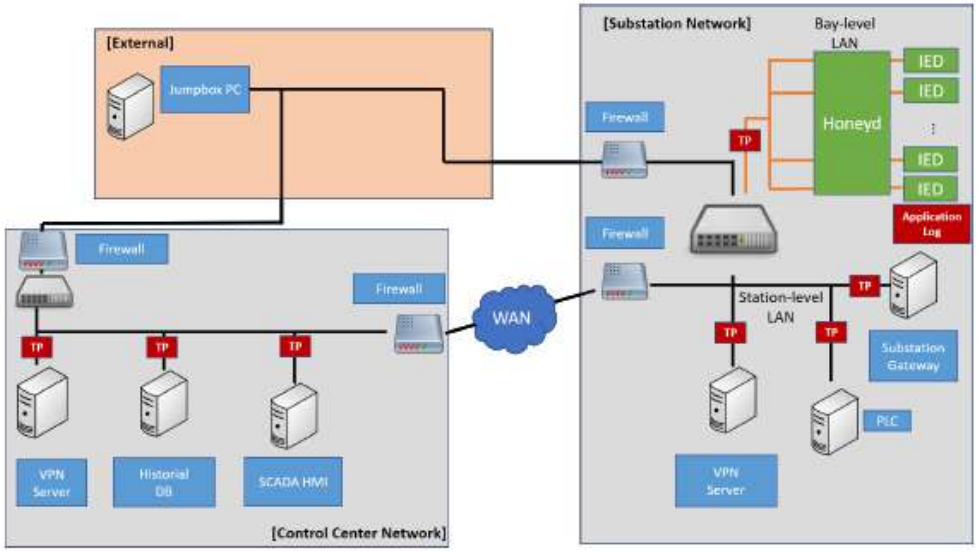
Example of Low-interaction Honeypot

- Industrial Control Systems (ICS) honeypot discussed in IEEE Globecom 2019 paper
  - TCP listeners for popular smart grid related ports and dummy servers
    - Open popular ICS protocol ports
    - IEC 61850 MMS or Siemens S7 (port 102), Modbus TCP (port 502), Niagara Fox (port 1911 and 4911), ENIP (port 2222 and 44818), IEC 60870-5-104 (port 2404), DNP3 (port 19999 and 20000), and BACnet (port 47808)
    - Runs simple server modules for IEC 104 and IEC 61850 MMS
    - Also opens SSH port

Example of High-interaction Honeypot

- Honeypot emulating whole smart grid monitoring and control infrastructure
  - Including virtualized workstations, servers, and standard-compliant industrial control system devices
  - VPN interface as an entry point for attackers
  - Deception by emulating device behaviours and characteristics
  - Secure logging
  - Can be used as **cyber range**





(URL: https://www.illinois.adsc.com.sg/spotify/index.html)

Open-source implementations

- Cowrie
  - High-interaction, SSH honeypot
- CONPOT
  - Low-interaction industrial control systems honeypot
- Honeyd
  - Framework to creates virtual honeypots
  - Can spoof OS fingerprinting
- Many others!
  - https://github.com/paralax/awesome-honeypots

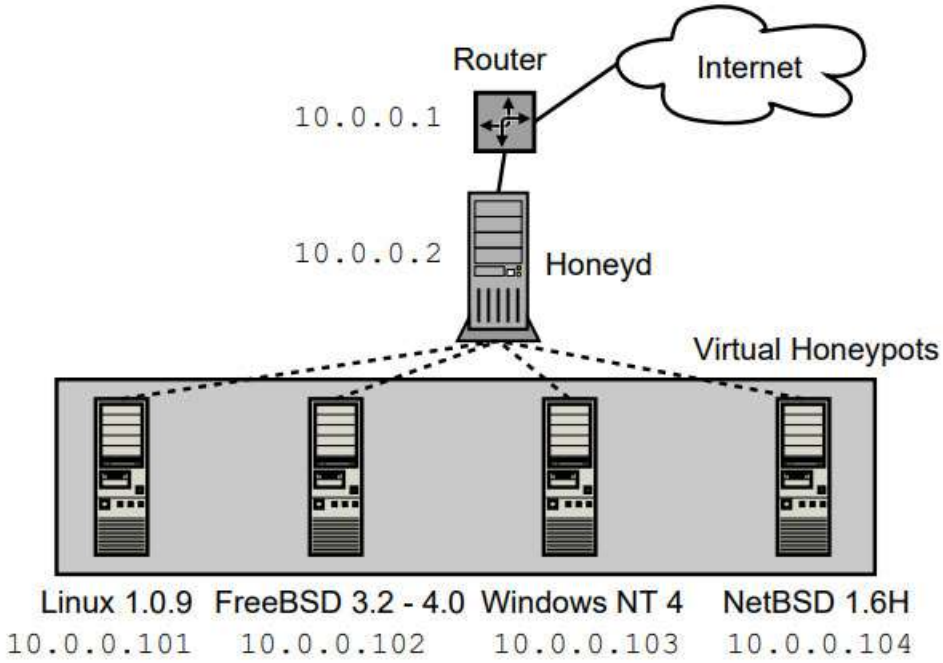
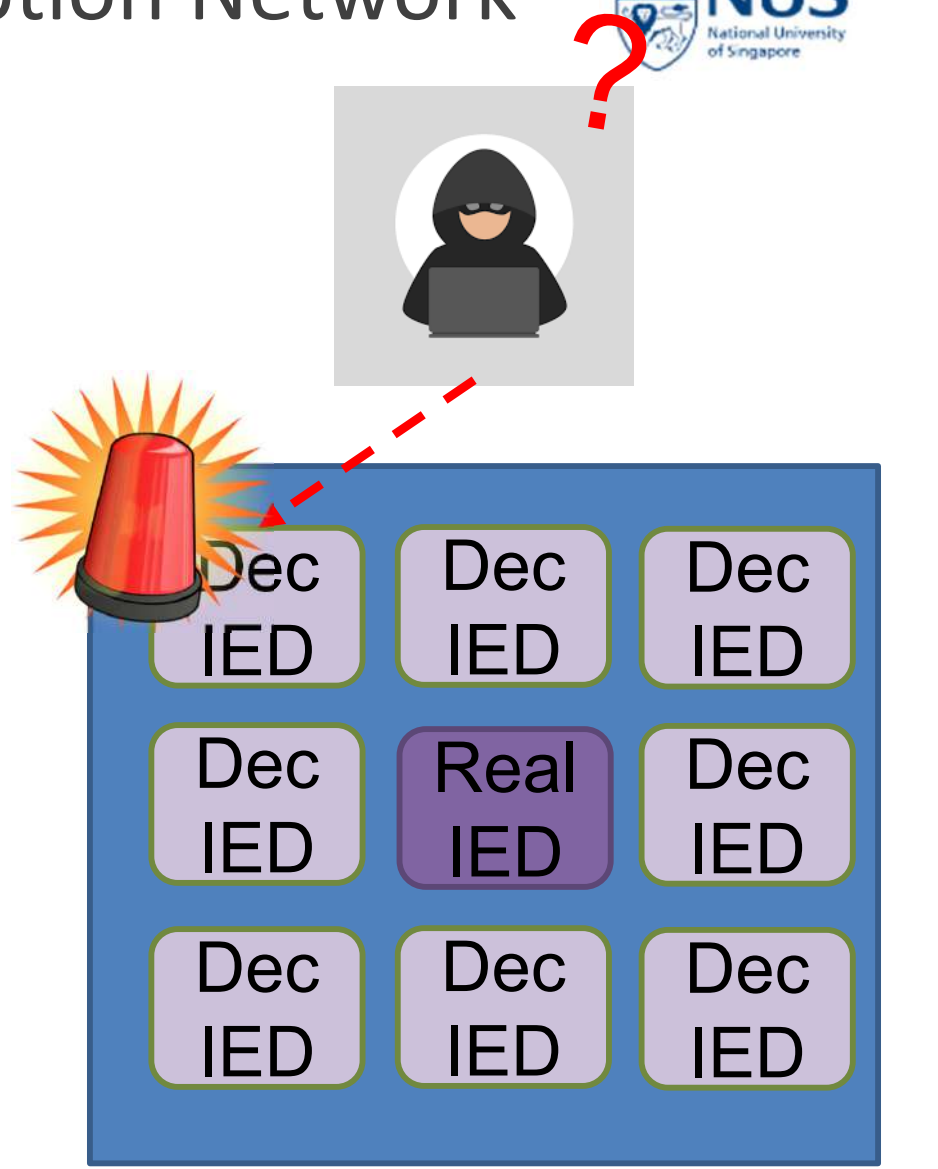


Figure 1: Honeyd receives traffic for its virtual honeypots via a router or Proxy ARP. For each honeypot, Honeyd can simulate the network stack behavior of a different operating system.

Honeypot vs Decoy / Deception Network

- Deploy indentically-looking “decoy” (virtual) devices to confuse attackers
- Unlike honeypot, decoy network is deployed **in the real system**
- Works as “smoke screen” and “tripwire”
- Example: “DecIED: Scalable decoy network technology for IEC 61850 based substations” in Proc. of ACM CPSS 2020



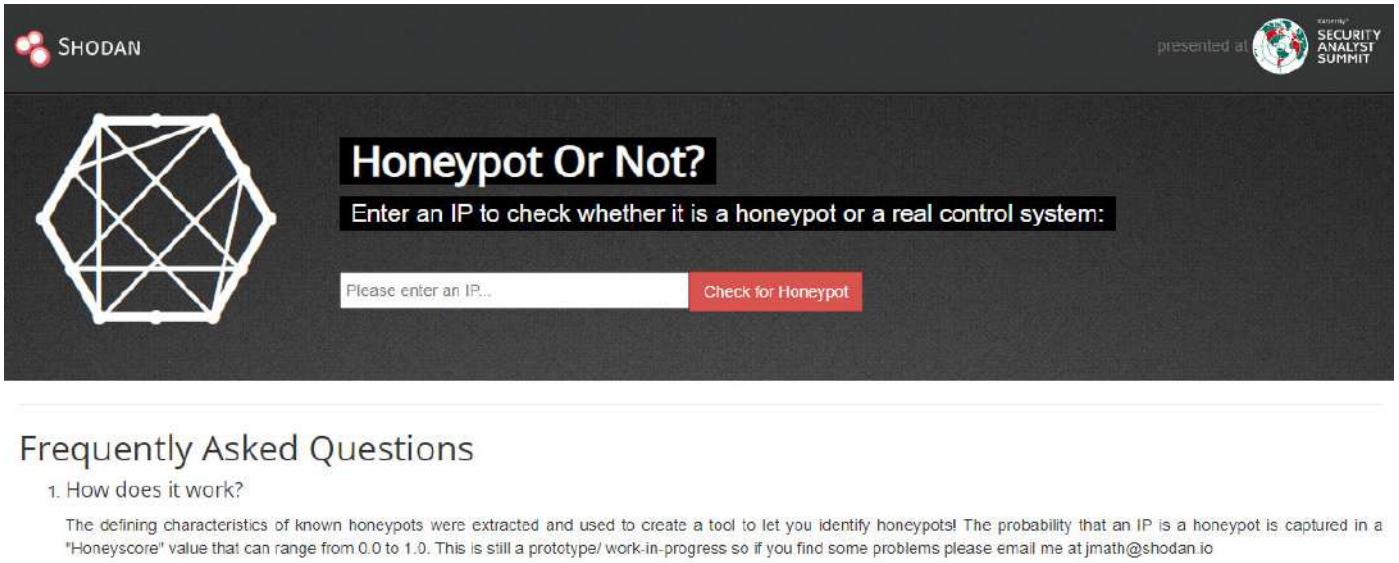
Deception with 9-anonymity

Threat intelligence analysis using low-interaction honeypot data (IEEE Globecom 2019)

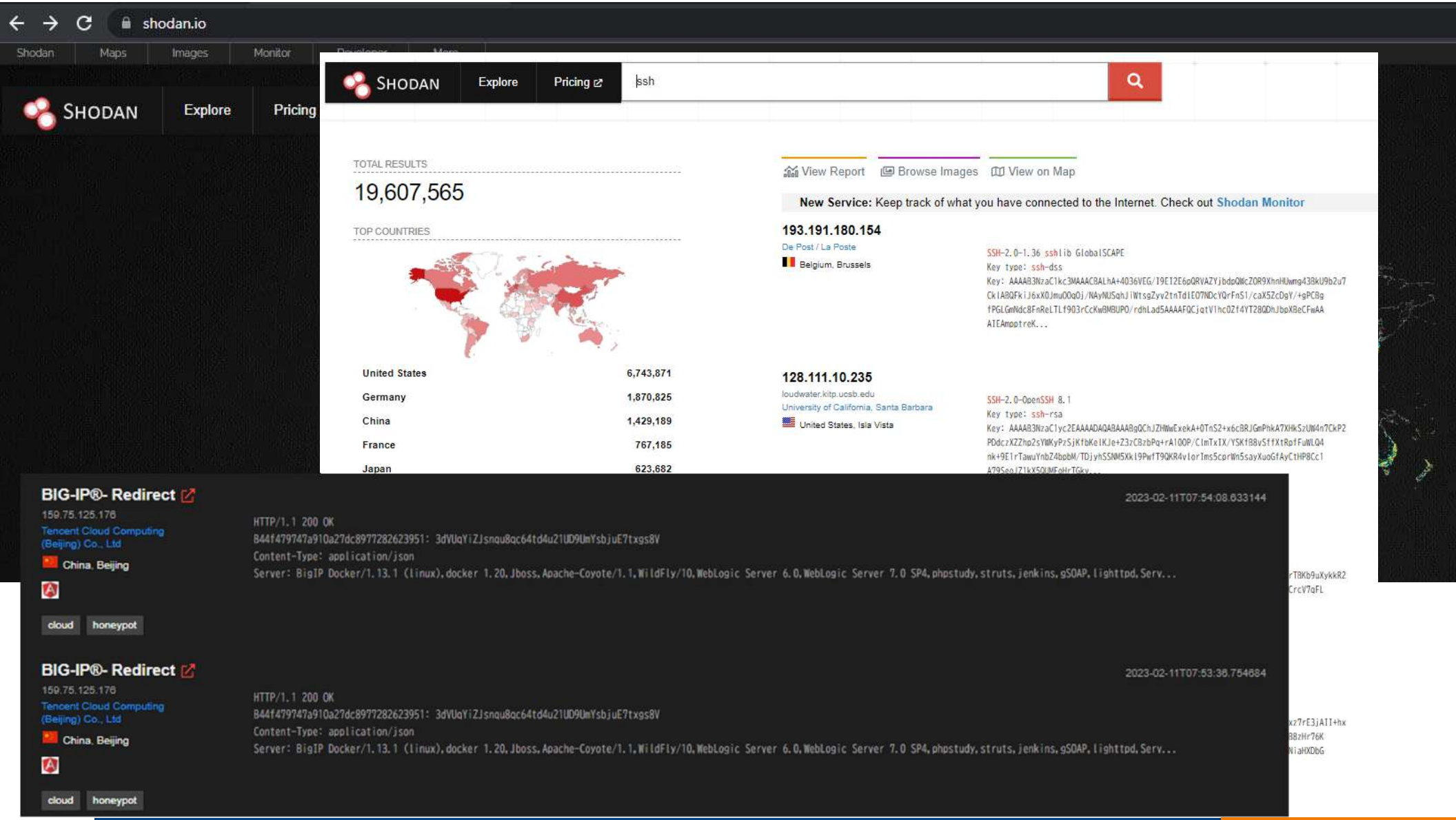
Industrial Control Systems Honeypot

- TCP listeners for popular smart grid related ports and dummy servers that are deployed on Amazon Cloud.
- Simple smart grid honeypot instances are deployed in multiple geographic locations
  - Singapore, US (Ohio), Canada, Germany, and Brazil

- **Shodan.io** indexed our honeypots as ICS devices, not as honeypot.

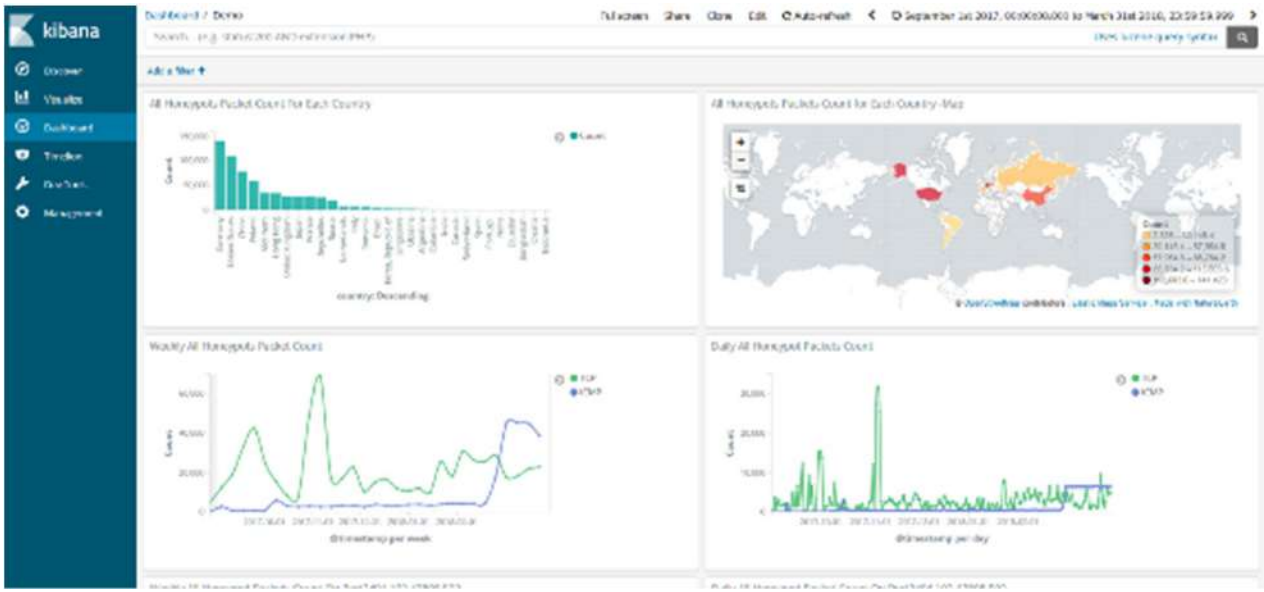


Shodan.io



Network Traces Collected

- Runs Wireshark for capturing network traffic
- Collection period so far is 6+ months
  - Sep., 2017 – Mar., 2018
  - Total file size: 6GB
- For each source IP address, Maxmind's GeoLite library is used for deriving country and (if available) city names.



Findings from Collected Data

- Protocol specific accesses: Siemens S7

No.	Time	Source	Destination	Protocol	Length	Info
48	239.869182425	118.193.31.181	172.31.13.26	TCP	66	52484 → 102 [RST, ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2359811058 TSecr=2242123772
49	239.893803719	118.193.31.181	172.31.13.26	TCP	74	53155 → 102 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2359811064 TSecr=0 WS=128
50	239.893825945	172.31.13.26	118.193.31.181	TCP	74	102 → 53155 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=2242124598 TSec
51	240.168082090	118.193.31.181	172.31.13.26	TCP	66	53155 → 102 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2359811132 TSecr=2242124598
52	240.174844196	118.193.31.181	172.31.13.26	COTP	88	CR TPDU src-ref: 0x0004 dst-ref: 0x0000
53	240.174858058	172.31.13.26	118.193.31.181	TCP	66	102 → 53155 [ACK] Seq=1 Ack=23 Win=26880 Len=0 TSval=2242124668 TSecr=2359811134
54	240.174911550	172.31.13.26	118.193.31.181	COTP	88	CC TPDU src-ref: 0x0025 dst-ref: 0x0004
55	240.449259779	118.193.31.181	172.31.13.26	TCP	66	53155 → 102 [ACK] Seq=23 Ack=23 Win=29312 Len=0 TSval=2359811203 TSecr=2242124668
56	240.452986825	118.193.31.181	172.31.13.26	S7COMM	91	ROSCTR:[Job] Function:[Setup communication]
57	240.453107000	172.31.13.26	118.193.31.181	TCP	66	102 → 53155 [FIN, ACK] Seq=23 Ack=48 Win=26880 Len=0 TSval=2242124737 TSecr=2359811204
58	240.737221375	118.193.31.181	172.31.13.26	S7COMM	99	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL] ID=0x0011 Index=0x0001
59	240.737252152	172.31.13.26	118.193.31.181	TCP	54	102 → 53155 [RST] Seq=24 Win=0 Len=0
60	240.737264498	118.193.31.181	172.31.13.26	S7COMM	99	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL] ID=0x001c Index=0x0001
61	240.737268782	172.31.13.26	118.193.31.181	TCP	54	102 → 53155 [RST] Seq=24 Win=0 Len=0
62	240.764532932	118.193.31.181	172.31.13.26	TCP	74	36017 → 102 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2359811280 TSecr=0 WS=128
63	240.764550531	172.31.13.26	118.193.31.181	TCP	74	102 → 36017 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=2242124815 TSec

```
▷ Frame 56: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
▷ Ethernet II, Src: 02:85:b5:68:62:bf (02:85:b5:68:62:bf), Dst: 02:d0:76:89:ba:1b (02:d0:76:89:ba:1b)
▷ Internet Protocol Version 4, Src: 118.193.31.181, Dst: 172.31.13.26
▷ Transmission Control Protocol, Src Port: 53155, Dst Port: 102, Seq: 23, Ack: 23, Len: 25
▷ TPKT, Version: 3, Length: 25
▷ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
◢ S7 Communication
  ◢ Header: (Job)
      Protocol Id: 0x32
      ROSCTR: Job (1)
      Redundancy Identification (Reserved): 0x0000
      Protocol Data Unit Reference: 0
      Parameter length: 8
      Data length: 0
  ◢ Parameter: (Setup communication)
      Function: Setup communication (0xf0)
      Reserved: 0x00
      Max AmQ (parallel jobs with ack) calling: 1
      Max AmQ (parallel jobs with ack) called: 1
      PDU length: 480
```

Findings from Collected Data

- Protocol specific accesses: IEC 60870-5-104

No.	Time	Source	Destination	Protocol	Length	Info
430	2649.5953792…	125.212.217.214	172.31.27.32	TCP	54	24366 → 2404 [SYN] Seq=0 Win=28460 Len=0
431	2649.5954113…	172.31.27.32	125.212.217.214	TCP	58	2404 → 24366 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
432	2649.8392873…	125.212.217.214	172.31.27.32	TCP	54	24366 → 2404 [RST] Seq=1 Win=0 Len=0
433	2651.2909413…	125.212.217.214	172.31.27.32	TCP	74	60446 → 2404 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=93908726 TSecr
434	2651.2909821…	172.31.27.32	125.212.217.214	TCP	74	2404 → 60446 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=8961 SACK_PERM=1 TSval=364
435	2651.5405742…	125.212.217.214	172.31.27.32	TCP	66	60446 → 2404 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=93908788 TSecr=3646049877
436	2651.7401186…	125.212.217.214	172.31.27.32	104apci	72	<- U (TESTFR act)
437	2651.7401567…	172.31.27.32	125.212.217.214	TCP	66	2404 → 60446 [ACK] Seq=1 Ack=7 Win=26880 Len=0 TSval=3646049989 TSecr=93908838
438	2651.7402785…	172.31.27.32	125.212.217.214	104apci	72	-> U (TESTFR con)
439	2651.9908703…	125.212.217.214	172.31.27.32	TCP	66	60446 → 2404 [ACK] Seq=7 Ack=7 Win=29312 Len=0 TSval=93908901 TSecr=3646049989
443	2655.2901590…	125.212.217.214	172.31.27.32	104apci	72	<- U (STARTDT act)
444	2655.2905703…	172.31.27.32	125.212.217.214	104apci	72	-> U (STARTDT con)
445	2655.5388083…	125.212.217.214	172.31.27.32	TCP	66	60446 → 2404 [ACK] Seq=13 Ack=13 Win=29312 Len=0 TSval=93909788 TSecr=3646050877
446	2659.1600522…	125.212.217.214	172.31.27.32	104asdu	82	<- I (0,0) ASDU=65535 C_IC_NA_1 Act IOA=0
447	2659.1632676…	172.31.27.32	125.212.217.214	104asdu	82	-> I (0,1) ASDU=65535 C_IC_NA_1 ActCon IOA=0
448	2659.4132175…	125.212.217.214	172.31.27.32	TCP	66	60446 → 2404 [ACK] Seq=29 Ack=29 Win=29312 Len=0 TSval=93910757 TSecr=3646051845
449	2659.4132515…	172.31.27.32	125.212.217.214	104asdu	90	-> I (1,1) ASDU=65535 M_ME_NB_1 Spont IOA[3]=1-3
450	2659.6622959…	125.212.217.214	172.31.27.32	TCP	66	60446 → 2404 [ACK] Seq=29 Ack=53 Win=29312 Len=0 TSval=93910819 TSecr=3646051908

Activate connection and send interrogation, then close.

```
▷ Frame 449: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▷ Ethernet II, Src: 02:cf:4e:7b:d8:47 (02:cf:4e:7b:d8:47), Dst: 02:87:35:92:69:b9 (02:87:35:92:69:b9)
▷ Internet Protocol Version 4, Src: 172.31.27.32, Dst: 125.212.217.214
▷ Transmission Control Protocol, Src Port: 2404, Dst Port: 60446, Seq: 29, Ack: 29, Len: 24
▷ IEC 60870-5-104-Apci: -> I (1,1)
◢ IEC 60870-5-104-Asdu: ASDU=65535 M_ME_NB_1 Spont   IOA[3]=1-3 'measured value, scaled value'
    TypeId: M_ME_NB_1 (11)
    1... .... = SQ: True
    .000 0011 = NumIx: 3
    ..00 0011 = CauseTx: Spont (3)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 65535
  ◢ IOA: 1
      IOA: 1
      Value: -32768
    ▷ QDS: 0xf1
  ▷ IOA: 2
  ▷ IOA: 3
```

Observed Attack Attempts

- Modbus scanning

modbus

No.	Time	Source	Destination	Protocol	Length	Info
813	3255.5487985…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 0, Func: 17: Report Slave ID
822	3257.2705397…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 1, Func: 17: Report Slave ID
829	3259.3186702…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 2, Func: 17: Report Slave ID
838	3259.8358055…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 3, Func: 17: Report Slave ID
845	3260.3358514…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 4, Func: 17: Report Slave ID
858	3261.8684841…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 5, Func: 17: Report Slave ID
865	3262.2046933…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 6, Func: 17: Report Slave ID
872	3262.4927479…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 7, Func: 17: Report Slave ID
881	3262.6866683…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 8, Func: 17: Report Slave ID
889	3262.8781531…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 9, Func: 17: Report Slave ID
896	3263.2850778…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 10, Func: 17: Report Slave ID
905	3263.6244282…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 11, Func: 17: Report Slave ID
916	3264.1816419…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 12, Func: 17: Report Slave ID
924	3264.3790454…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 13, Func: 17: Report Slave ID
932	3264.5555804…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 14, Func: 17: Report Slave ID
940	3264.7493250…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 15, Func: 17: Report Slave ID
948	3264.9451120…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 16, Func: 17: Report Slave ID
958	3265.2351353…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 17, Func: 17: Report Slave ID
967	3265.9503253…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 18, Func: 17: Report Slave ID
976	3266.3125343…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 19, Func: 17: Report Slave ID
983	3266.5718321…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 20, Func: 17: Report Slave ID
994	3266.7485506…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 21, Func: 17: Report Slave ID
1001	3266.9329093…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 22, Func: 17: Report Slave ID
1013	3267.1272940…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 23, Func: 17: Report Slave ID
1022	3267.3356327…	80.82.77.33	172.31.27.32	Modbus/TCP	74	Query: Trans: 0; Unit: 24, Func: 17: Report Slave ID

Observed Attack Attempts

- DNP3 scanning

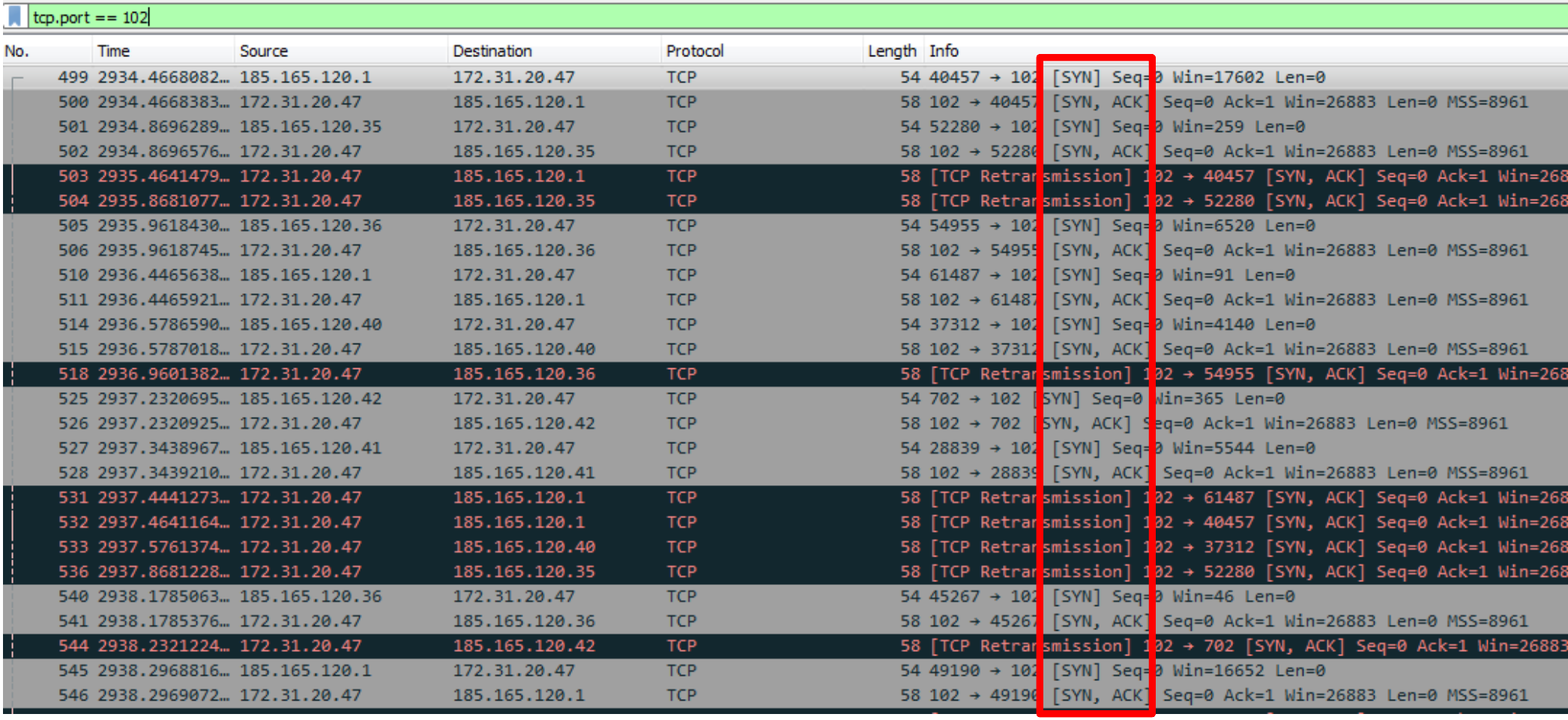
No.	Time	Source	Destination	Protocol	Length	Info
142	351.298393454	123.59.78.122	172.31.1.17	TCP	74	55744 → 20000 [SYN] Seq=0 Win=29200 Len=0 MSS
143	351.298459947	172.31.1.17	123.59.78.122	TCP	74	20000 → 55744 [SYN, ACK] Seq=0 Ack=1 Win=2684
144	351.536824224	123.59.78.122	172.31.1.17	TCP	66	55744 → 20000 [ACK] Seq=1 Ack=1 Win=29312 Len
145	351.541803621	123.59.78.122	172.31.1.17	DNP 3.0	1076	from 0 to 100, len=5, Request Link Status
146	351.541830111	172.31.1.17	123.59.78.122	TCP	66	20000 → 55744 [ACK] Seq=1 Ack=1011 Win=28928
147	351.541873462	172.31.1.17	123.59.78.122	TCP	66	20000 → 55744 [FIN, ACK] Seq=1 Ack=1011 Win=2
148	351.780693639	123.59.78.122	172.31.1.17	TCP	66	55744 → 20000 [ACK] Seq=1011 Ack=2 Win=29312
149	351.782912996	123.59.78.122	172.31.1.17	TCP	66	55744 → 20000 [FIN, ACK] Seq=1011 Ack=2 Win=2
150	351.782941628	172.31.1.17	123.59.78.122	TCP	66	20000 → 55744 [ACK] Seq=2 Ack=1012 Win=28928

```
▷ Frame 145: 1076 bytes on wire (8608 bits), 1076 bytes captured (8608 bits) on interface 0
▷ Ethernet II, Src: 02:9e:f5:4d:10:dd (02:9e:f5:4d:10:dd), Dst: 02:9b:b3:7d:e7:4e (02:9b:b3:7d:e7:4e)
▷ Internet Protocol Version 4, Src: 123.59.78.122, Dst: 172.31.1.17
▷ Transmission Control Protocol, Src Port: 55744, Dst Port: 20000, Seq: 1, Ack: 1, Len: 1010
◢ Distributed Network Protocol 3.0
  ◢ Data Link Layer, Len: 5, From: 0, To: 0, DIR, PRM, Request Link Status
      Start Bytes: 0x0564
      Length: 5
    ◢ Control: 0xc9 (DIR, PRM, Request Link Status)
        1... .... = Direction: Set
        .1.. .... = Primary: Set
        ..0. .... = Frame Count Bit: Not set
        ...0 .... = Frame Count Valid: Not set
        .... 1001 = Control Function Code: Request Link Status (9)
      Destination: 0
      Source: 0
      CRC: 0x4c36 [correct]
◢ Distributed Network Protocol 3.0
  ◢ Data Link Layer, Len: 5, From: 0, To: 1, DIR, PRM, Request Link Status
      Start Bytes: 0x0564
      Length: 5
    ◢ Control: 0xc9 (DIR, PRM, Request Link Status)
        1... .... = Direction: Set
        .1.. .... = Primary: Set
        ..0. .... = Frame Count Bit: Not set
        ...0 .... = Frame Count Valid: Not set
        .... 1001 = Control Function Code: Request Link Status (9)
      Destination: 1
      Source: 0
      CRC: 0x8ede [correct]
▷ Distributed Network Protocol 3.0
▷ Distributed Network Protocol 3.0
```

Multiple query requests in a single message

Observed Attack Attempts

- TCP SYN flooding attack against port 102



tcp.port == 102

No.	Time	Source	Destination	Protocol	Length	Info
499	2934.4668082…	185.165.120.1	172.31.20.47	TCP	54	40457 → 102 [SYN] Seq=0 Win=17602 Len=0
500	2934.4668383…	172.31.20.47	185.165.120.1	TCP	58	102 → 40457 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
501	2934.8696289…	185.165.120.35	172.31.20.47	TCP	54	52280 → 102 [SYN] Seq=0 Win=259 Len=0
502	2934.8696576…	172.31.20.47	185.165.120.35	TCP	58	102 → 52280 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
503	2935.4641479…	172.31.20.47	185.165.120.1	TCP	58	[TCP Retransmission] 102 → 40457 [SYN, ACK] Seq=0 Ack=1 Win=268
504	2935.8681077…	172.31.20.47	185.165.120.35	TCP	58	[TCP Retransmission] 102 → 52280 [SYN, ACK] Seq=0 Ack=1 Win=268
505	2935.9618430…	185.165.120.36	172.31.20.47	TCP	54	54955 → 102 [SYN] Seq=0 Win=6520 Len=0
506	2935.9618745…	172.31.20.47	185.165.120.36	TCP	58	102 → 54955 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
510	2936.4465638…	185.165.120.1	172.31.20.47	TCP	54	61487 → 102 [SYN] Seq=0 Win=91 Len=0
511	2936.4465921…	172.31.20.47	185.165.120.1	TCP	58	102 → 61487 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
514	2936.5786590…	185.165.120.40	172.31.20.47	TCP	54	37312 → 102 [SYN] Seq=0 Win=4140 Len=0
515	2936.5787018…	172.31.20.47	185.165.120.40	TCP	58	102 → 37312 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
518	2936.9601382…	172.31.20.47	185.165.120.36	TCP	58	[TCP Retransmission] 102 → 54955 [SYN, ACK] Seq=0 Ack=1 Win=268
525	2937.2320695…	185.165.120.42	172.31.20.47	TCP	54	702 → 102 [SYN] Seq=0 Win=365 Len=0
526	2937.2320925…	172.31.20.47	185.165.120.42	TCP	58	102 → 702 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
527	2937.3438967…	185.165.120.41	172.31.20.47	TCP	54	28839 → 102 [SYN] Seq=0 Win=5544 Len=0
528	2937.3439210…	172.31.20.47	185.165.120.41	TCP	58	102 → 28839 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
531	2937.4441273…	172.31.20.47	185.165.120.1	TCP	58	[TCP Retransmission] 102 → 61487 [SYN, ACK] Seq=0 Ack=1 Win=268
532	2937.4641164…	172.31.20.47	185.165.120.1	TCP	58	[TCP Retransmission] 102 → 40457 [SYN, ACK] Seq=0 Ack=1 Win=268
533	2937.5761374…	172.31.20.47	185.165.120.40	TCP	58	[TCP Retransmission] 102 → 37312 [SYN, ACK] Seq=0 Ack=1 Win=268
536	2937.8681228…	172.31.20.47	185.165.120.35	TCP	58	[TCP Retransmission] 102 → 52280 [SYN, ACK] Seq=0 Ack=1 Win=268
540	2938.1785063…	185.165.120.36	172.31.20.47	TCP	54	45267 → 102 [SYN] Seq=0 Win=46 Len=0
541	2938.1785376…	172.31.20.47	185.165.120.36	TCP	58	102 → 45267 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961
544	2938.2321224…	172.31.20.47	185.165.120.42	TCP	58	[TCP Retransmission] 102 → 702 [SYN, ACK] Seq=0 Ack=1 Win=26883
545	2938.2968816…	185.165.120.1	172.31.20.47	TCP	54	49190 → 102 [SYN] Seq=0 Win=16652 Len=0
546	2938.2969072…	172.31.20.47	185.165.120.1	TCP	58	102 → 49190 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=8961

Correlation among Honeypots

- Germany honeypot and Brazil honeypot have strong correlation.

	Weekly1	Weekly2	Weekly3	Weekly4	Weekly5
Weekly1	1.00000000	0.017591051	0.475467508	0.03721859	0.02724399
Weekly2	0.01759105	1.000000000	0.004500041	-0.14459185	0.98452942
Weekly3	0.47546751	0.004500041	1.000000000	0.39781618	0.03532604
Weekly4	0.03721859	-0.144591846	0.397816185	1.00000000	-0.09336888
Weekly5	0.02724399	0.984529423	0.035326041	-0.09336888	1.00000000

	Daily1	Daily2	Daily3	Daily4	Daily5
Daily1	1.000000000	0.008163411	0.57858745	0.04998651	0.01576193
Daily2	0.008163411	1.000000000	-0.02130427	-0.04224472	0.96779859
Daily3	0.578587449	-0.021304271	1.00000000	-0.04991620	-0.01918324
Daily4	0.049986508	-0.042244716	-0.04991620	1.00000000	-0.05519358
Daily5	0.015761928	0.967798589	-0.01918324	-0.05519358	1.00000000

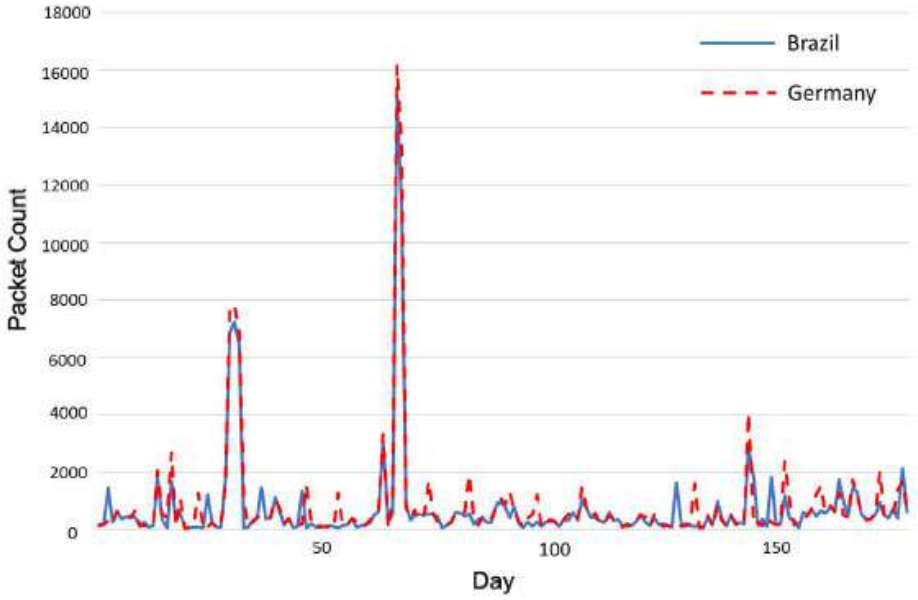


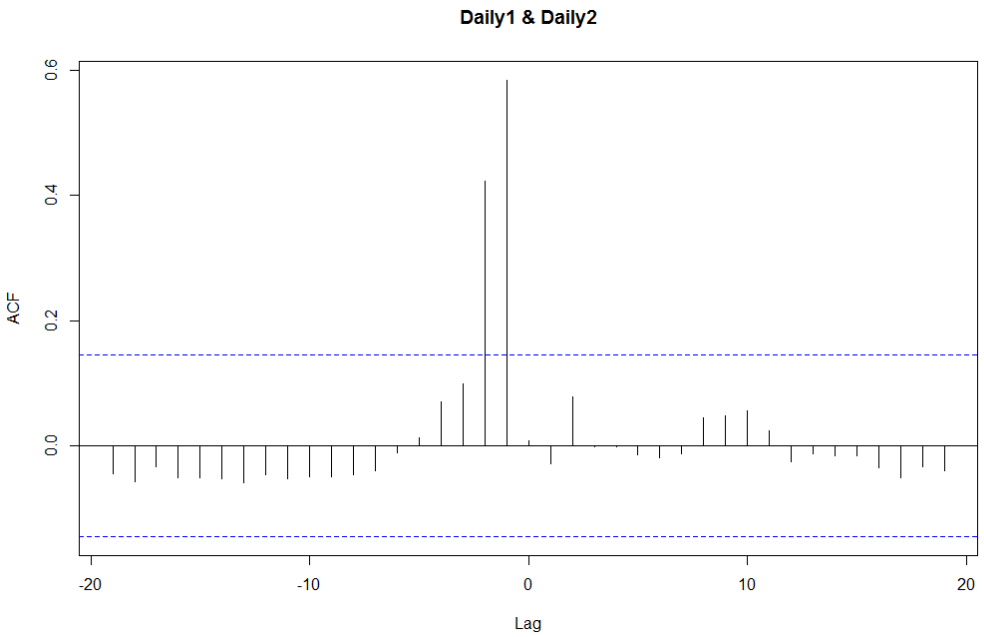
Fig. 7. Correlation in Packet Counts (Germany and Brazil)

Source IP Address	Country	Type
88.198.50.113	Germany	Web hosting
217.20.112.139	Germany	Web hosting
212.22.93.83	Russia	rental server
78.46.247.60	Germany	???
179.188.38.251	Brazil	Cloud hosting
210.245.90.23	Vietnam	ISP?
80.82.77.33	Netherlands	Server hosting
71.6.146.185	USA	Cloud
80.82.77.139	Netherlands	Server hosting
122.114.160.220	China	Server hosting

Majority of access sources are shared between the two.

Correlation among Honeypots

- For some pairs of honeypots, correlation can be observed with lag (Brazil and Canada)



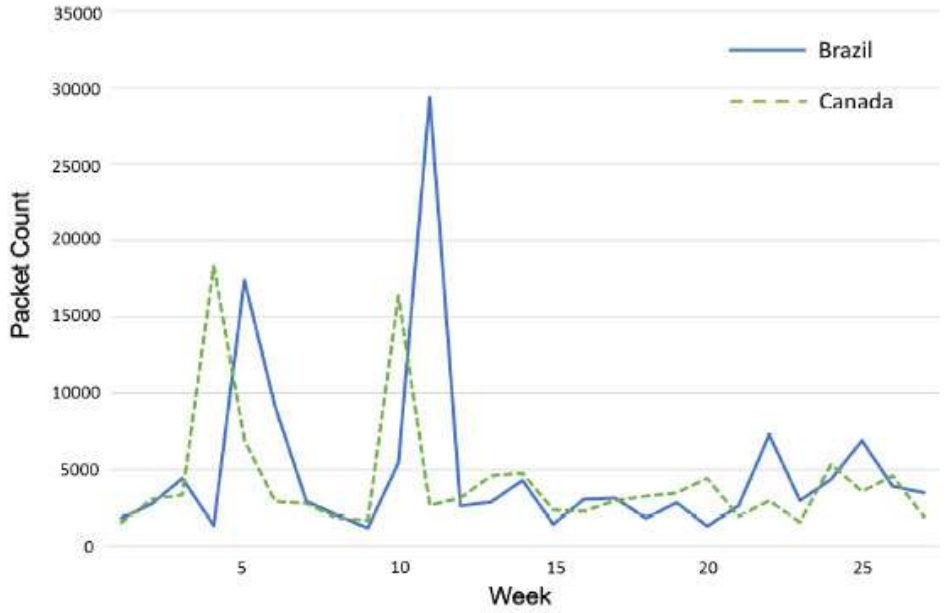
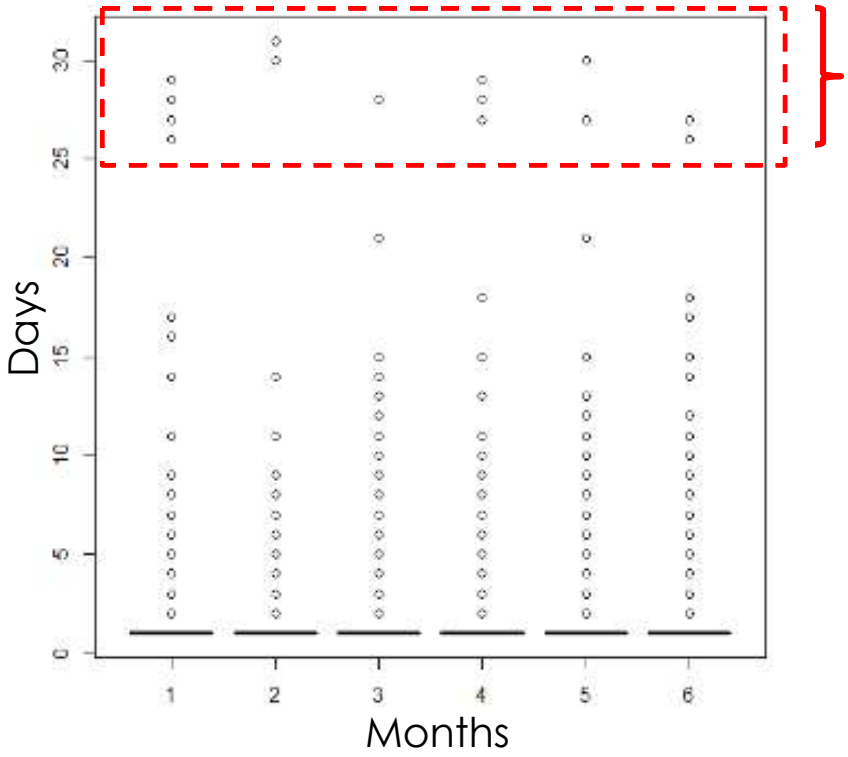


Fig. 8. Correlation in Weekly Packet Counts with Lag (Brazil and Canada)

- No significant auto-correlation is found.
  - I.e., no periodic pattern is found

Dynamics of Sources

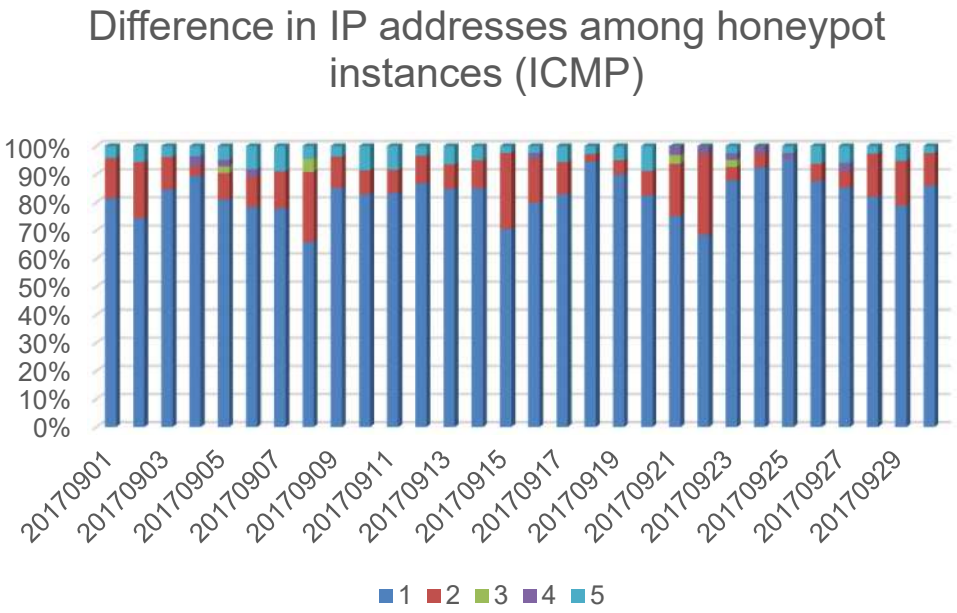
- Difference/Similarity over time
  - Some source IP addresses are observed throughout the data collection period

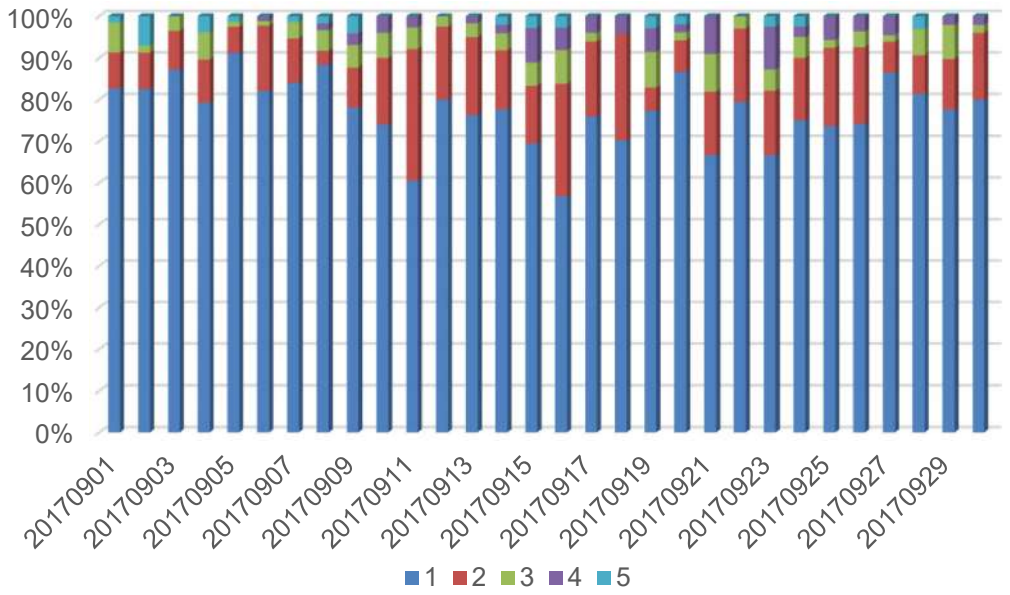


Access from Japan (Linode LLC), attempting port 102 (IEC 61850 MMS or Siemens S7) and 47808 (BACnet)

Dynamics of Sources

- Difference/Similarity among honeypots
  - Some IP addresses are observed by multiple honeypot instances





Automated utilization of Honeypot data

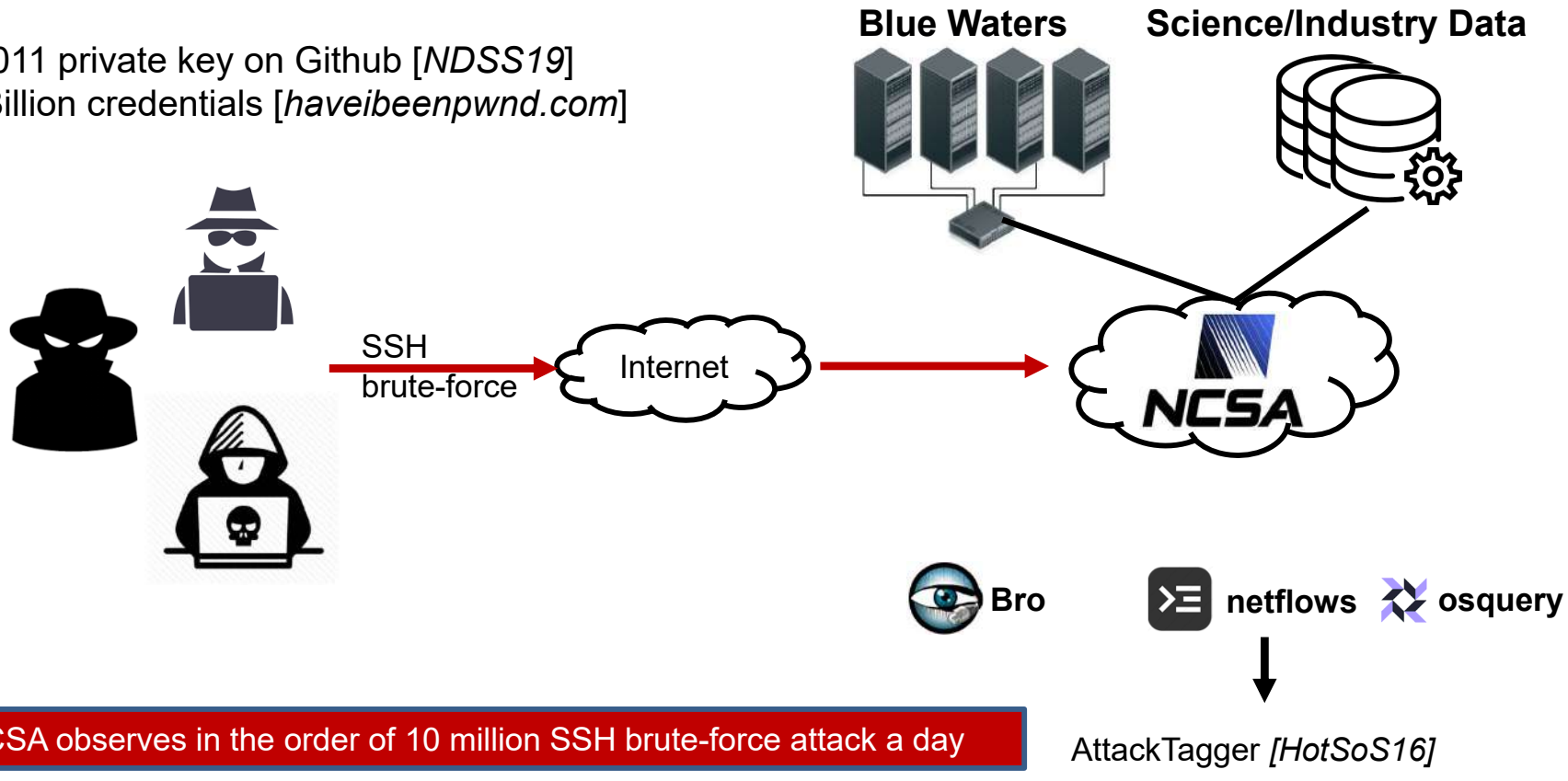
https://www.usenix.org/conference/nsdi19/presentation/cao

CAUDIT: Continuous Auditing of SSH Servers at Large Scale

- Addresses challenge in auditing and monitoring of SSH access to super computer center

Security for NCSA

158,011 private key on Github [*NDSS19*]
6.5 Billion credentials [*haveibeenpwnd.com*]



NCSA observes in the order of 10 million SSH brute-force attack a day

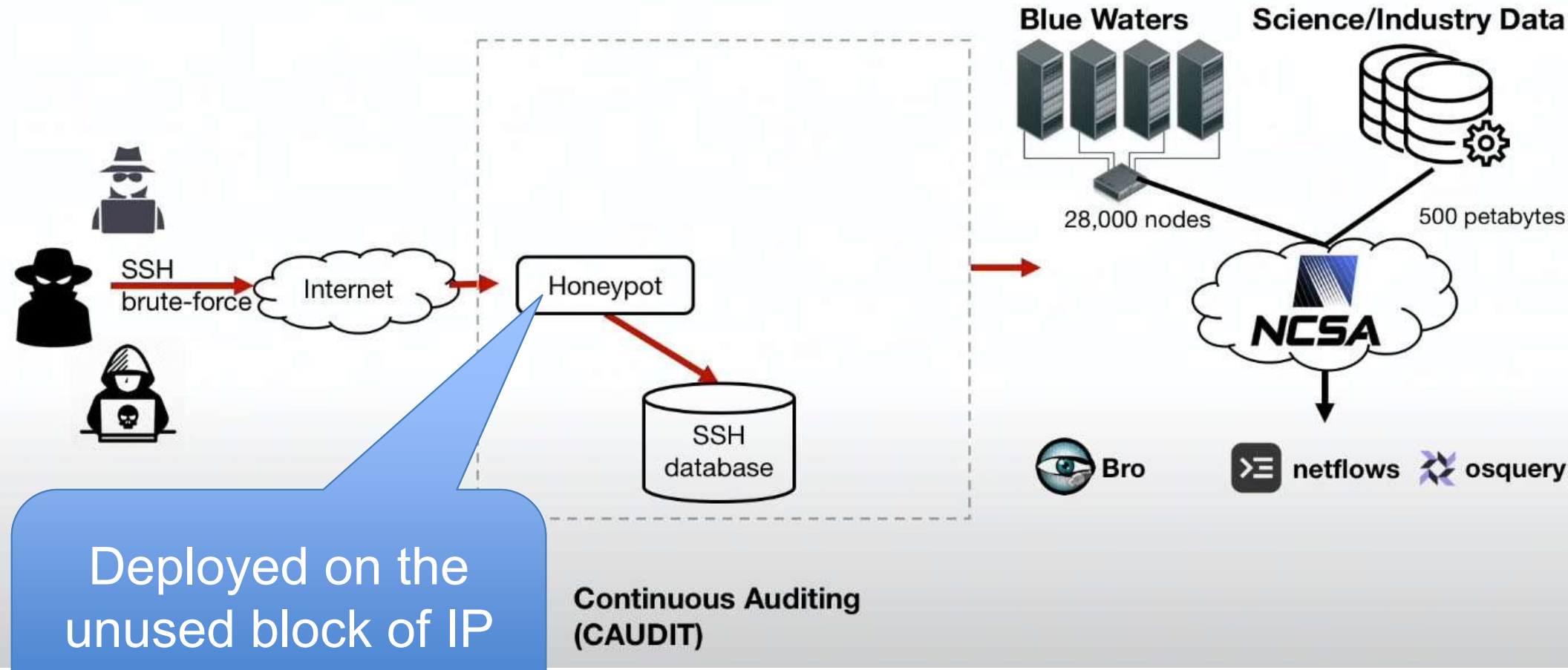
Problem Statement

- NCSA observes 10 million SSH brute-force attack a day!
- How could we avoid overwhelming network monitors / intrusion detection systems?
  - How could we do **traffic shaping**?

- How could we **audit** internal hosts against SSH brute-force attacks?
  - What are the attack vectors?
  - Can we automate the audit in a non-intrusive way?

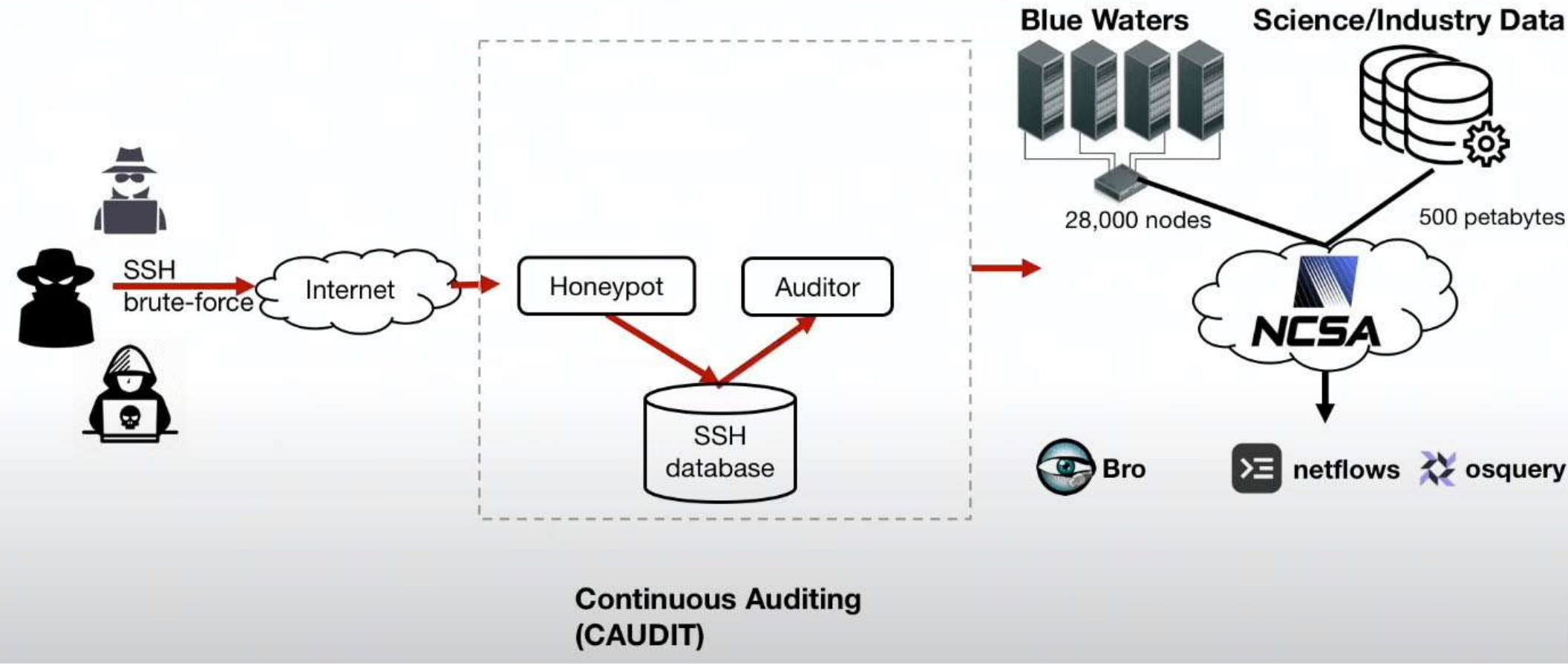
- **Honeypot!**

CAUDIT Framework



Deployed on the unused block of IP addresses in NCSA

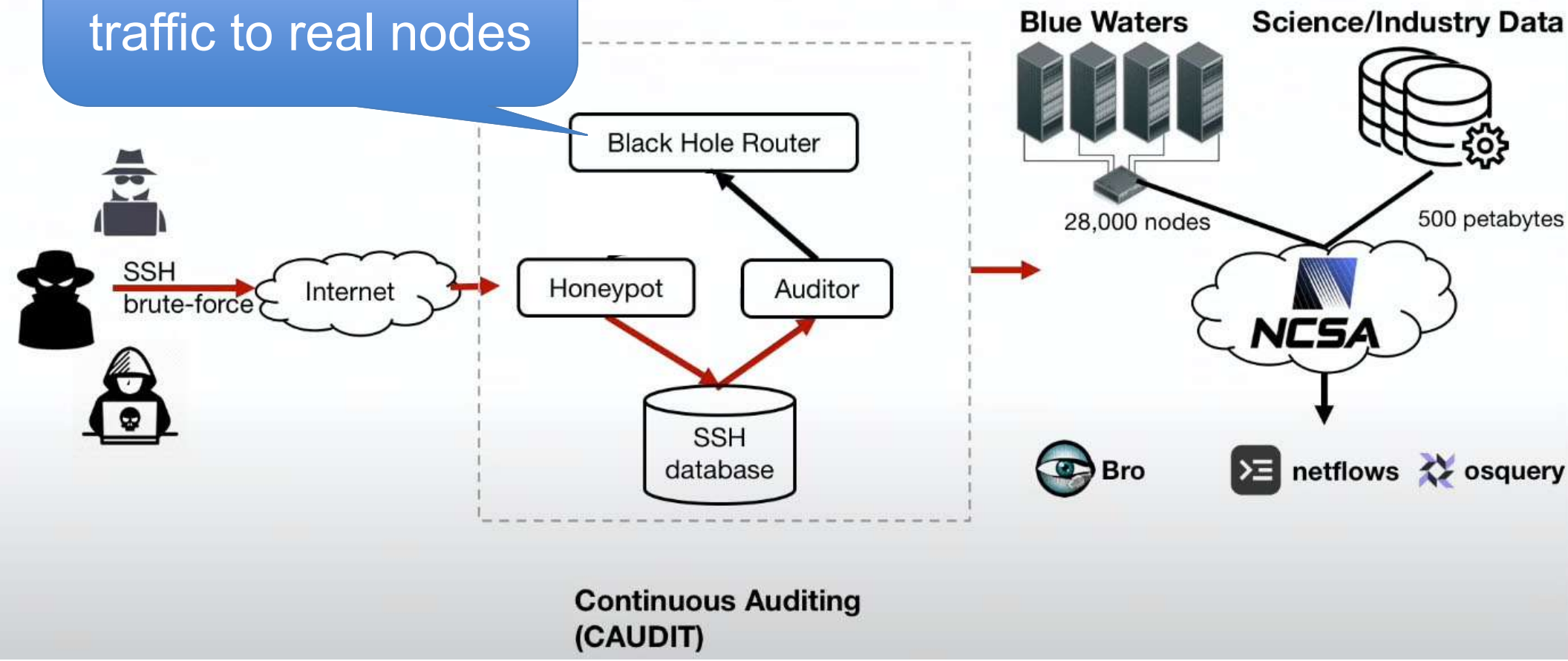
CAUDIT Framework



Continuous Auditing (CAUDIT)

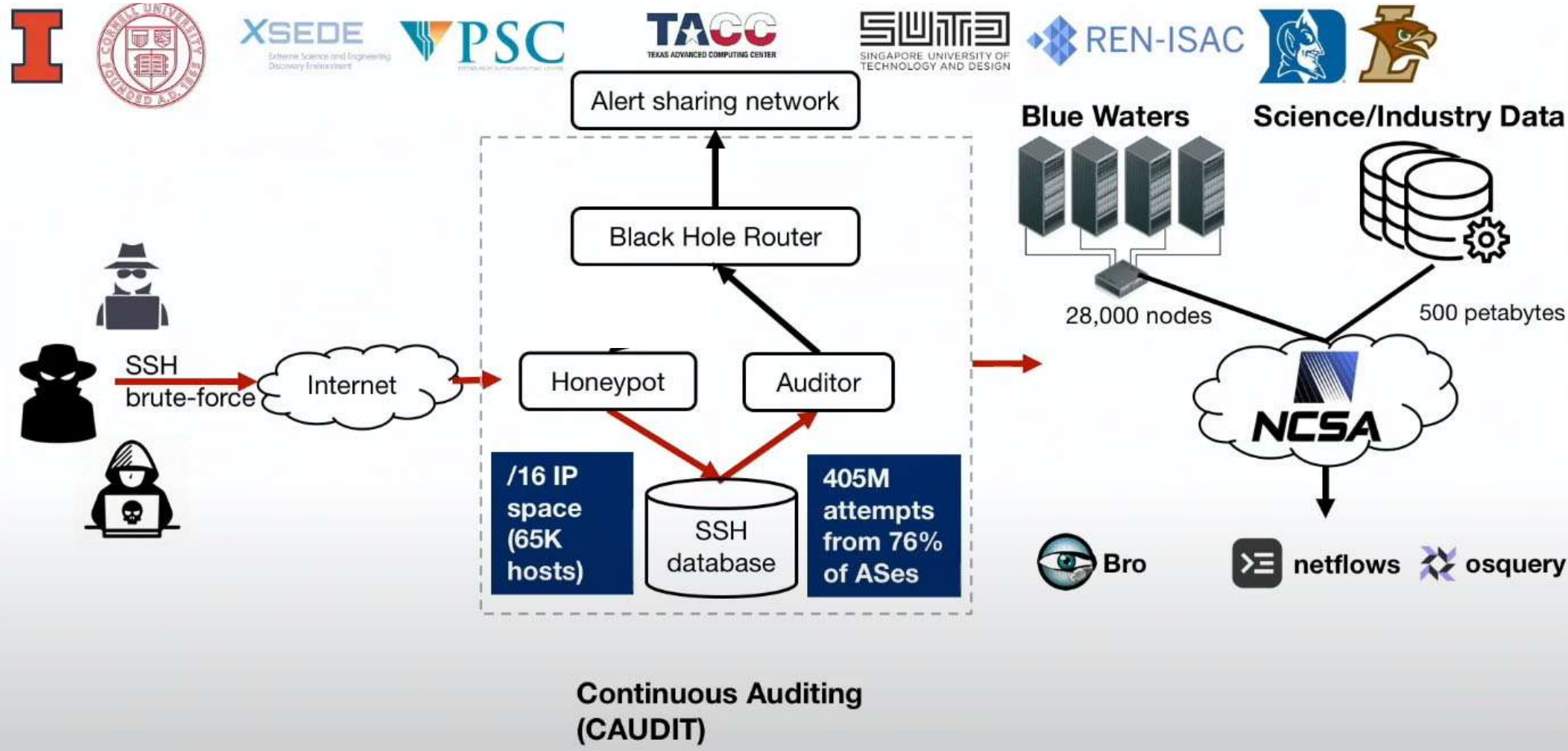
CAUDIT Framework

Implement traffic shaping for SSH traffic to real nodes

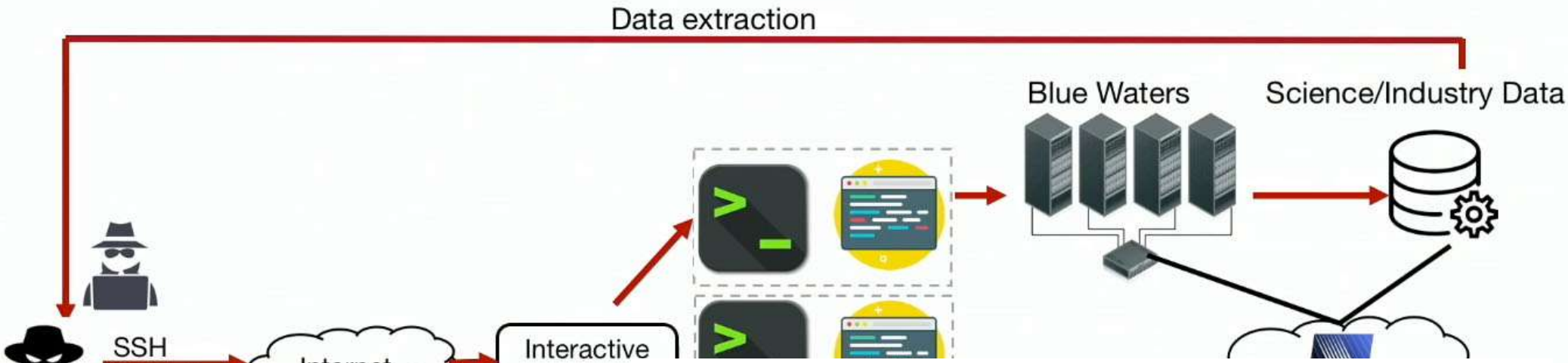


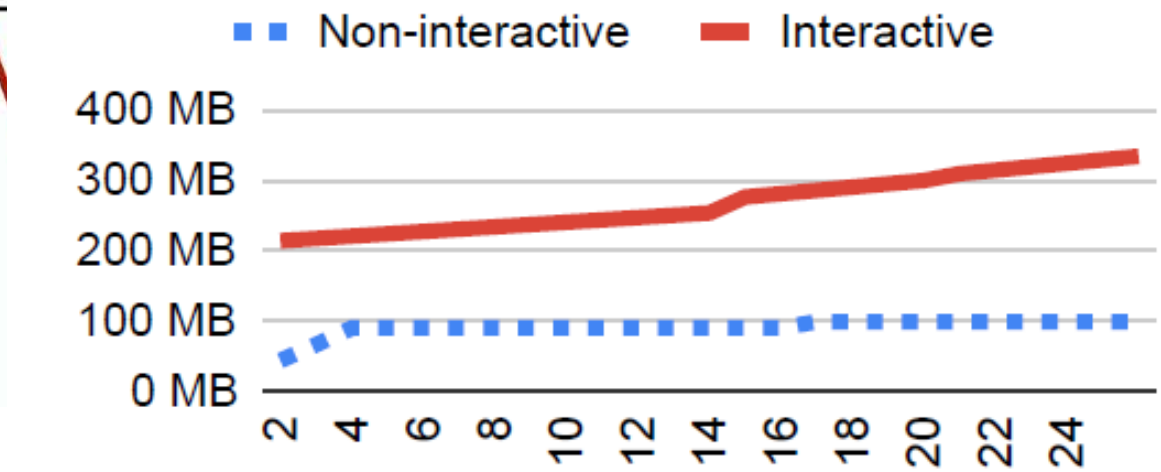
Continuous Auditing (CAUDIT)

CAUDIT Framework



Honeypot at Scale

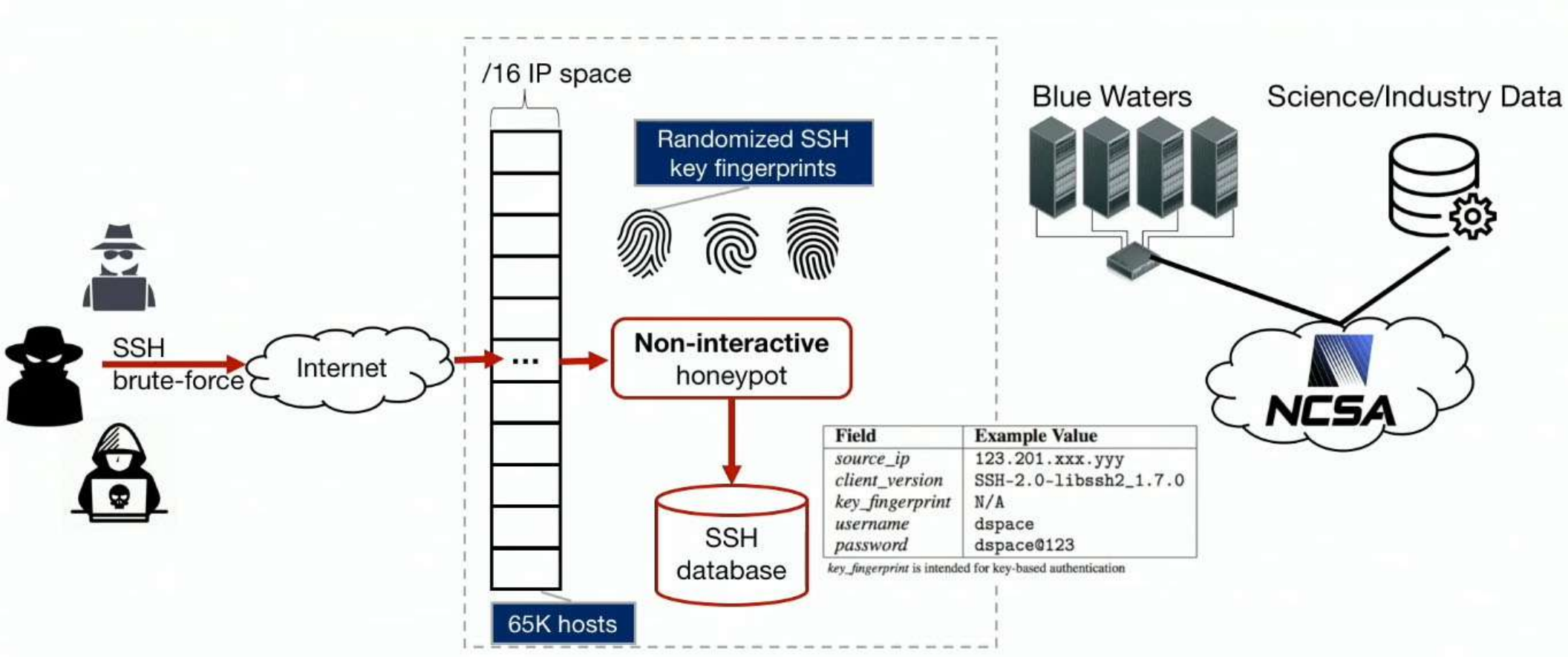




Resource consumption is an issue.
Could be used as stepping stone!

Honeypot at Scale

- Use low-interaction honeypot
  - Reject all login attempt by default, and thus, attackers cannot access to NCSA via honeypot



Field	Example Value
source_ip	123.201.xxx.yyy
client_version	SSH-2.0-libssh2_1.7.0
key_fingerprint	N/A
username	dspace
password	dspace@123

key_fingerprint is intended for key-based authentication

Attack Sources

Top 5 ISP	%
China Telecom	22.36
Indonesia Comnets	5.85
China Unicom	3.19
MCI Comm	0.13
Infonet Comm	0.12

Others: 63.12%

Top 5 Cloud/VPN	%
Microsoft Azure	4.60
OVH	0.28
Linode	0.20
21vianet	0.12
FrootVPN	0.03

China owns 7.7% of IPv4, but China ISPs are conduits for one fourth of attack attempts

Particular cloud providers are conduits for a high percentage of attacks

SSH Client Tools

Client	Version	Count	Release Year
sshlib	0.1	76.7M	2010
	0.5.2	1.8M	2011
libssh2	1.7.0	26.8M	2016
paramiko	2.4.0	25.1K	2017
Go	N/A	19.4M	–
PUTTY	N/A	20.4M	–

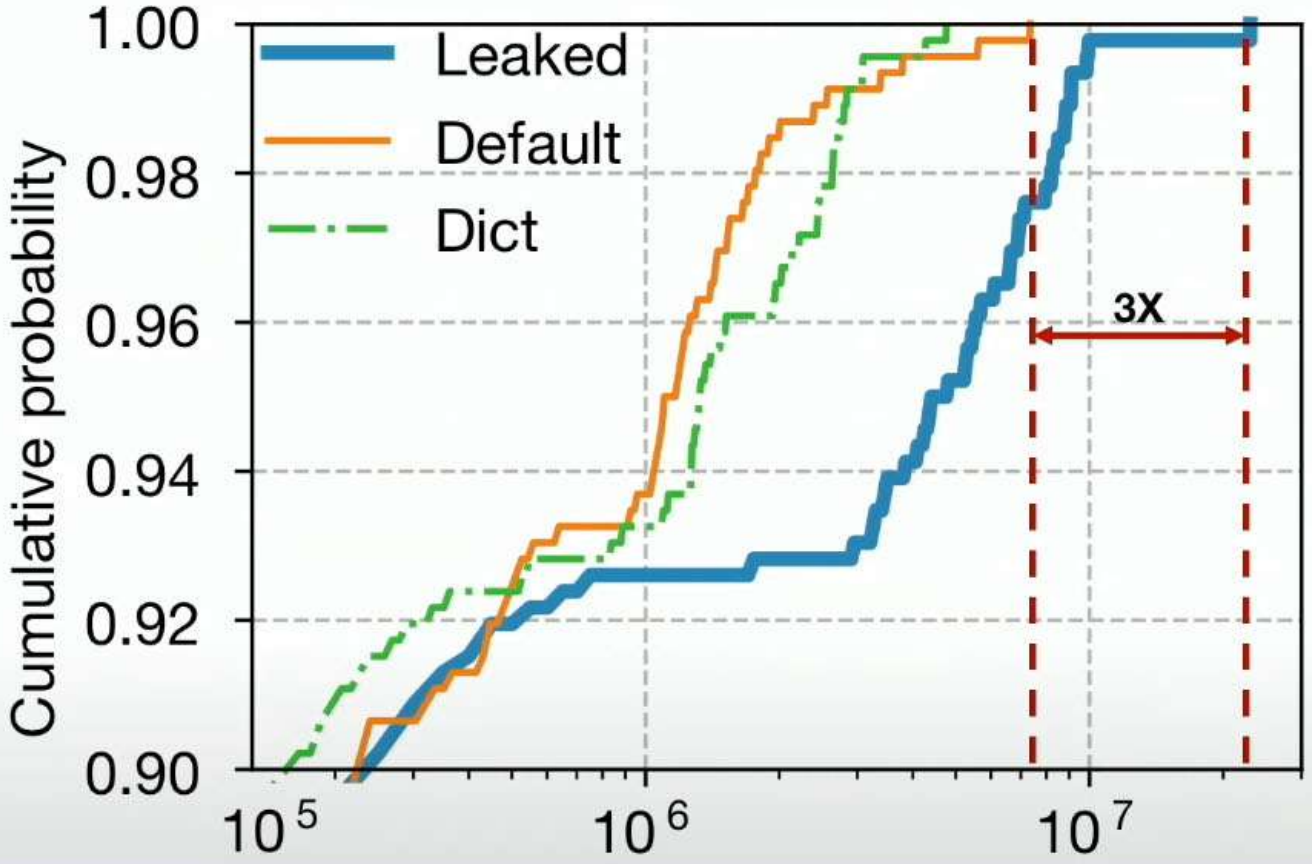
Top 5 SSH client libraries

CVE-2018-10933 (auth bypass)

Old routers or IoT devices

47% attack attempts used outdated SSH libraries released in 2010–2011.

Password Attempted



Leaked passwords are 3X more frequent than default/dictionary-based passwords

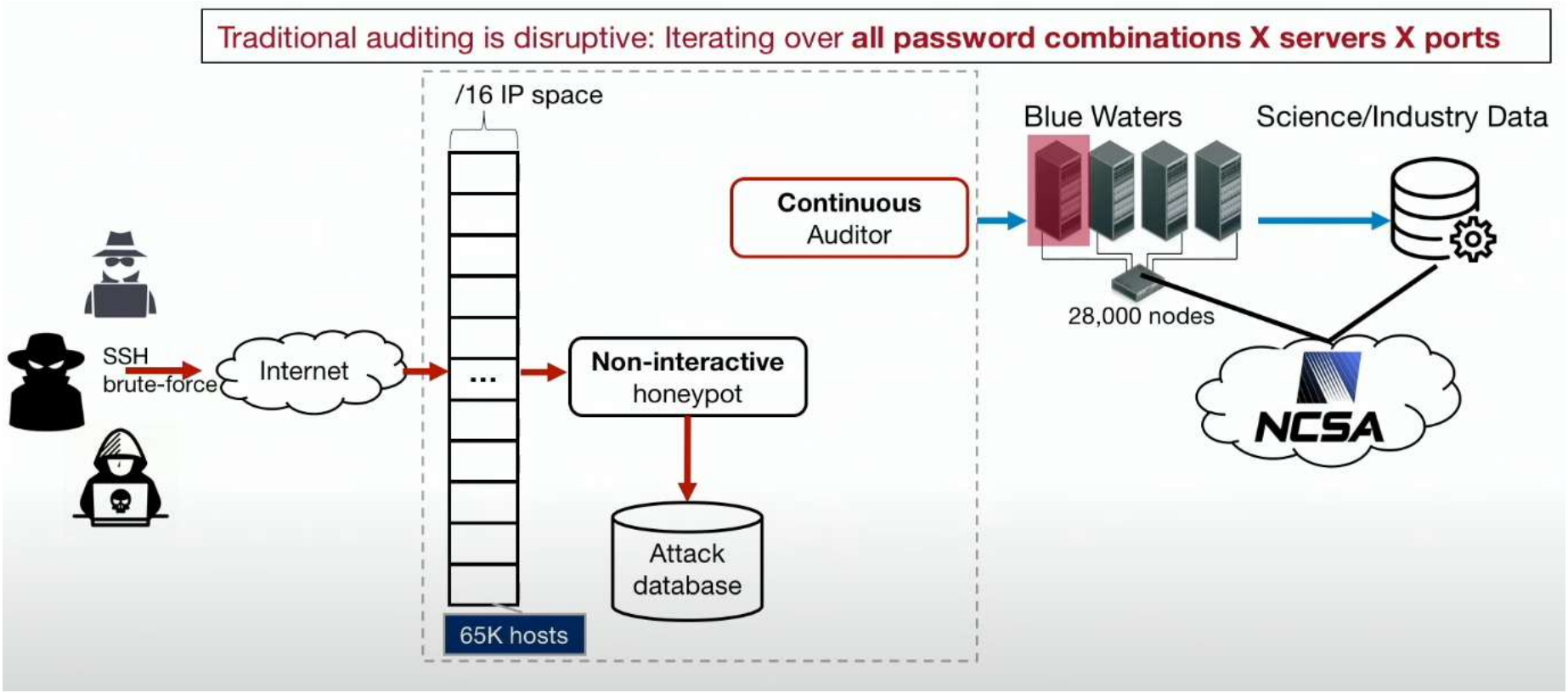
Keys Attempted

Key Fingerprint (SHA256) (Top 5)	Count
oHhjwxYH9v+ChV4Vr...Pk6KHla6P7g443w	20,307
qOd/Gr8bWftEu8HDU...aNCXA3Q/OzWMCdo	17,026
YEYlq2GOCueBnJRoS...f7KzN5meQVVQFmA	9,542
+UJNIlXcTgv4BLeaZ...QH//L2cG5GRQJUE	8,199
oU4y6kZLH2kAdhwWU...1eBJCButjeEhIwo	7,870

None of the 159 observed keys belongs to known leaked SSH key db

May have come from underground market, data breaches that were not reported.

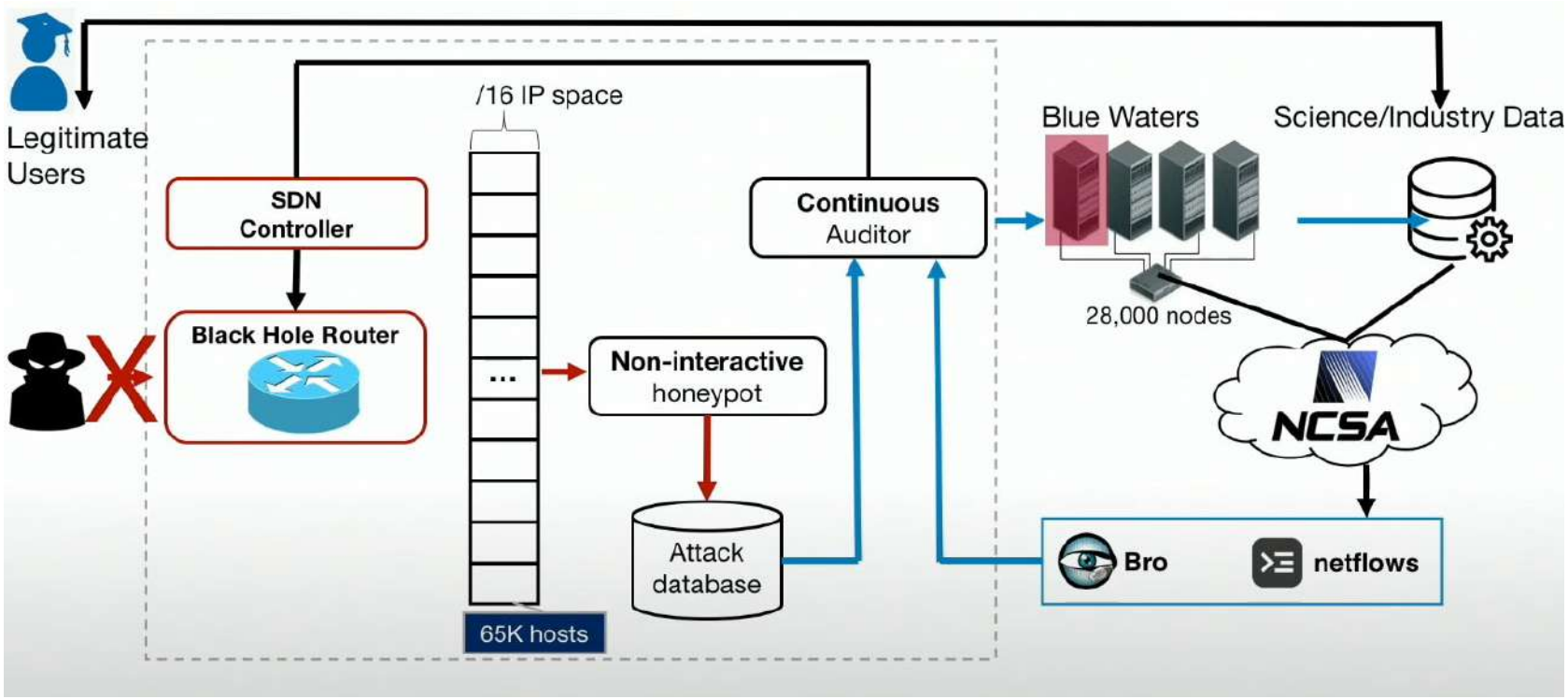
Continuous, Non-intrusive Auditing



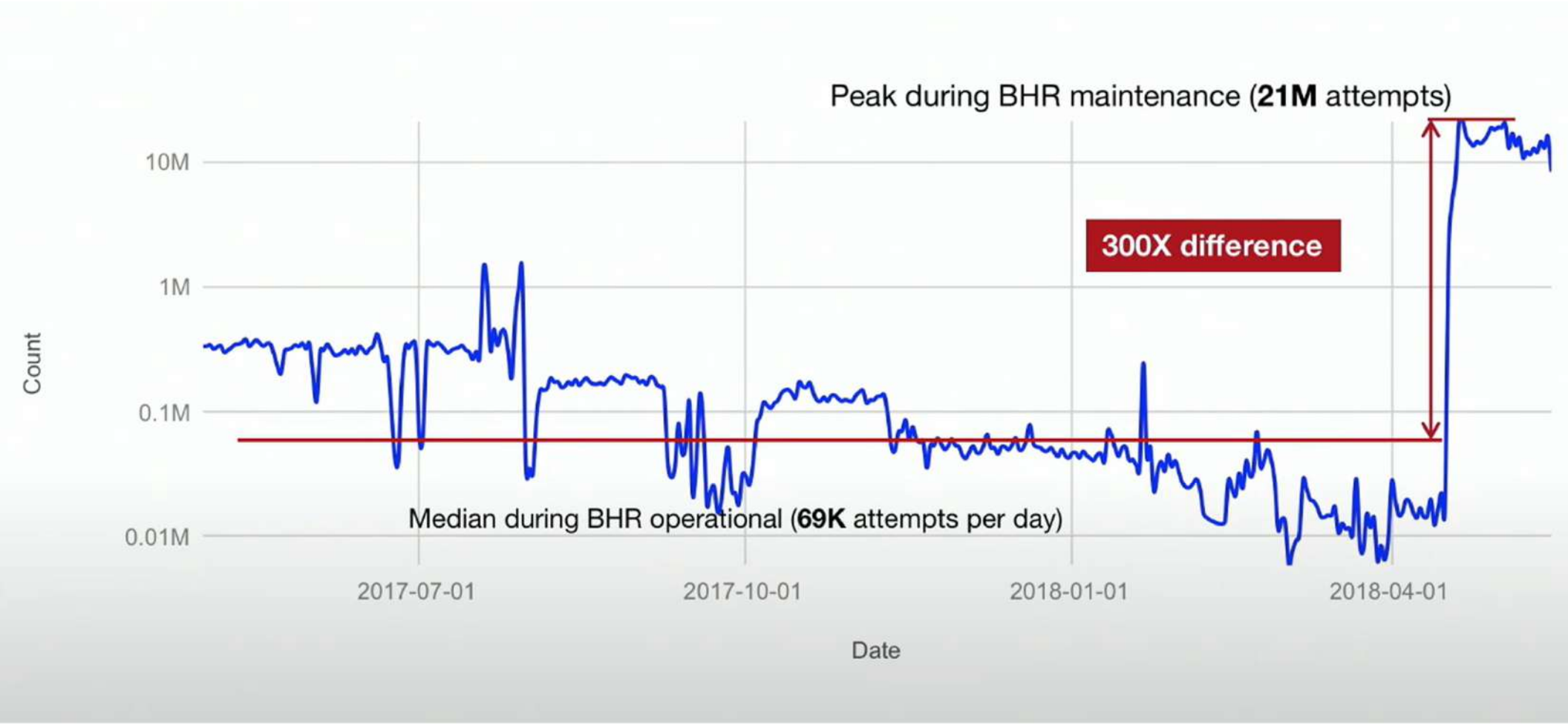
- Traditional auditing method is not feasible for large-scale system.
  - Utilize alert feed of IDS to identify SSH services
    - (e.g., Bro/Zeek IDS can detect SSH handshake activities)
  - Prioritize new attack vectors observed

Traffic Shaping using Black Hole Router

- Malicious IP that are **aggressively generating traffic** is provided to Black Hole Router
  - Avoid false positive while preventing IDS from being overwhelmed.



Benefit of Black Hole Router



Summary

- Honeypot is a tool for knowing attackers.
  - Where are they coming from?
  - How are they attacking the target?
  - Etc.
- Threat intelligence collected by honeypot can be used for fine-tuning our defence mechanisms
  - Firewall / IDS rules
  - Cybersecurity auditing
  - Traffic shaping mechanisms
- Analysis and utilization of high-interaction honeypot data is still in early stage
- Sharing of alerts and intelligence is still an open issue.

Questions?

NEXT LECTURE (WEEK 7): DNS SECURITY

Two papers

- The Hitchhiker's Guide to DNS Cache Poisoning (2010)
  - Read ***page 1—7***

- **An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? (IMC 2019)**