ILLINOIS
CSL | Coordinated Science Lab
COLLEGE OF ENGINEERING

Electrical and Computer Engineering, Computer Science,
National Center for Supercomputing Applications, Corelight

CAUDIT: Continuous Auditing of SSH Servers To Mitigate Brute-Force Attacks

Phuong Cao

Yuming Wu, Subho Banerjee, Justin Azoff, Alex Withers, Zbigniew Kalbarczyk, Ravishankar Iyer

National Center for Supercomputing Applications (NCSA)

1600 TB memory

28,000 nodes

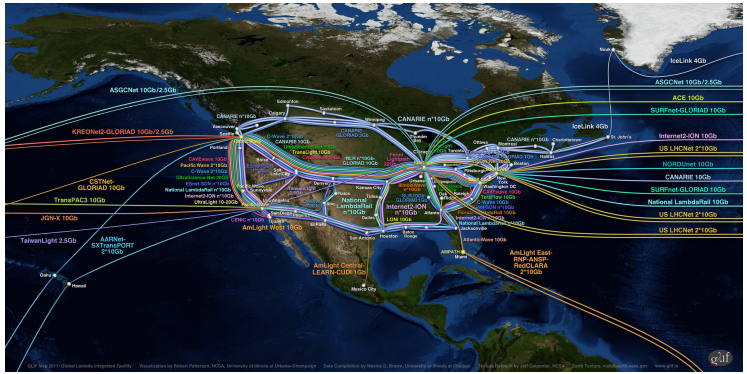
10/40/100 Gb Ethernet Switch

IB Switch

NCSA

National Center for Supercomputing Applications

300 Gbps WAN



NSF International Research Network Connections

500PB storage

NCSA hosts critical data and enables scientific research

1600 TB memory

28,000 nodes

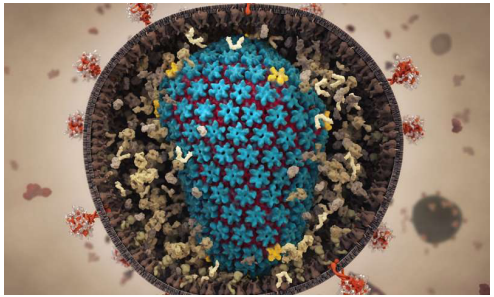
10/40/100 Gb Ethernet Switch

IB Switch

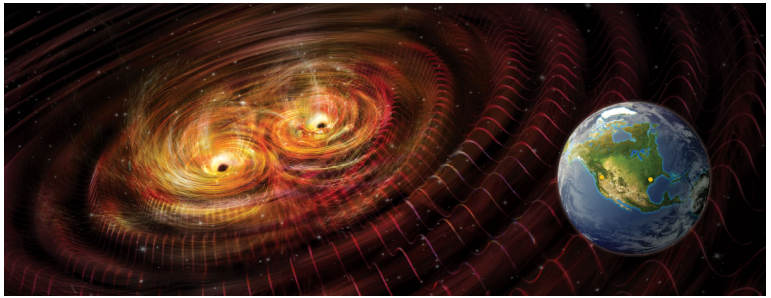
NCSA

National Center for Supercomputing Applications

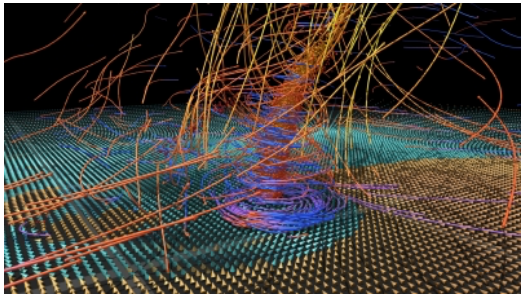
Enabling scientific discovery in genomics, astrophysics, and earth sciences.



HIV virus simulation



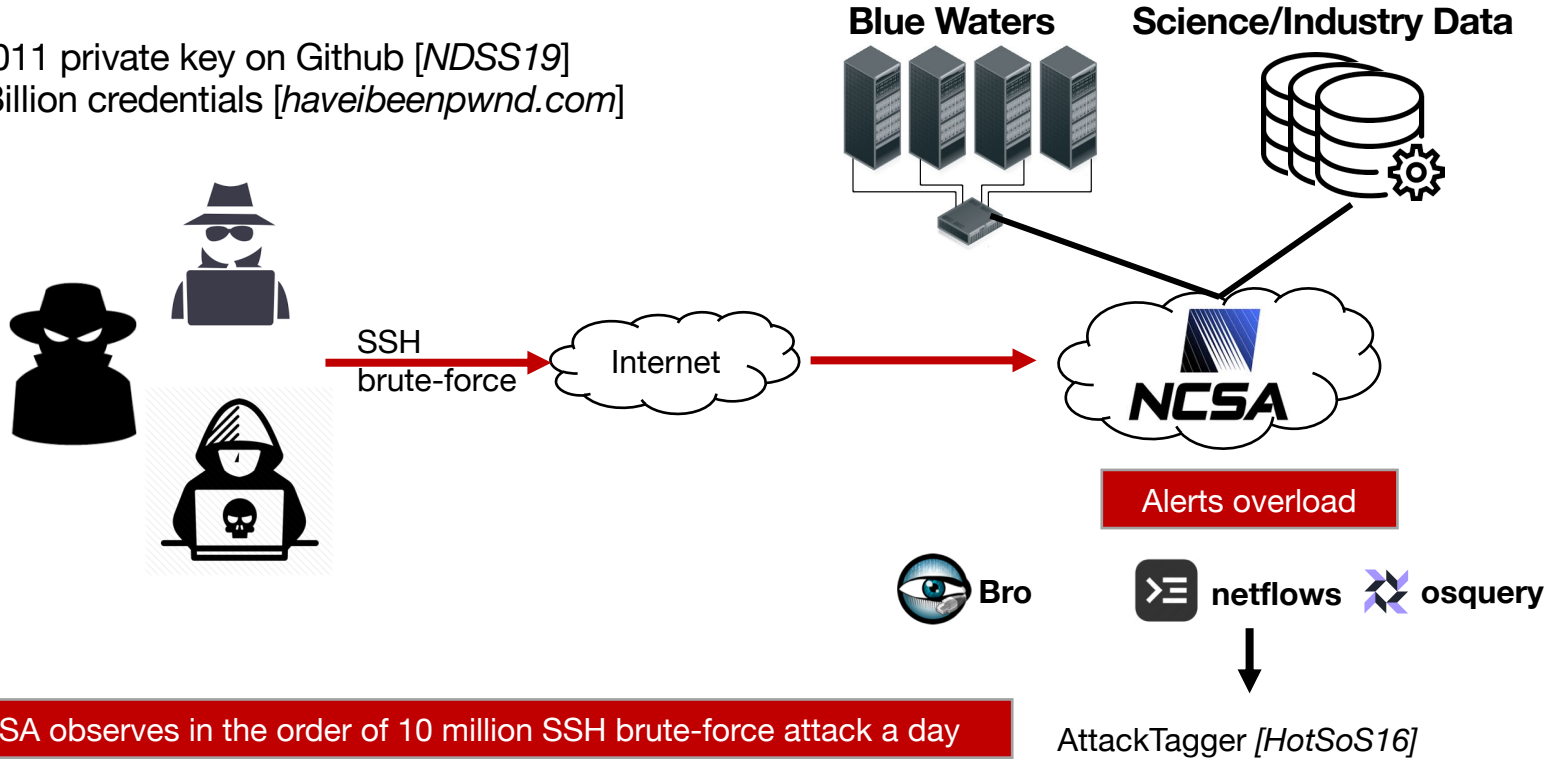
LIGO gravitational wave



Tornado simulation

SSH brute-force attacks affect internal hosts and monitors

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

SSH brute-force attacks affect internal hosts and monitors

Problem Statement:

"How to audit internal hosts against SSH brute-force attacks?"

Issues:

1: SSH brute-force attacks overwhelm existing monitors

2: Difficult to enforce password policies on individual hosts and devices

3: Limited visibility on SSH attack techniques at Internet scale

Putting SSH auditing in perspective

libssh Authentication Bypass Vulnerability Affecting Cisco Products 2018

Cisco Security Advisory

OpenSSH patches leak that could expose private SSH keys

COMPUTERWORLD

Marriott Hacking Exposes Data of Up to 500 Million Guests

The New York Times

Ashley Madison parent in $11.2 million settlement over data breach

CNBC

Failing to password-protect exposed SSH servers

How we protect #AzureAD and Microsoft Account from lists of leaked usernames and passwords

Who Are You? A Statistical Approach to Measuring User Authenticity *[NDSS16]*

David Mandell Freeman and Sakshi Jain
Markus Dürmuth, Ruhr-Universität Bochum
Battista Biggio and Giorgio Giacinto

Security of Interactive and Automated Access Management Using Secure Shell (SSH)

NISTIR 7966

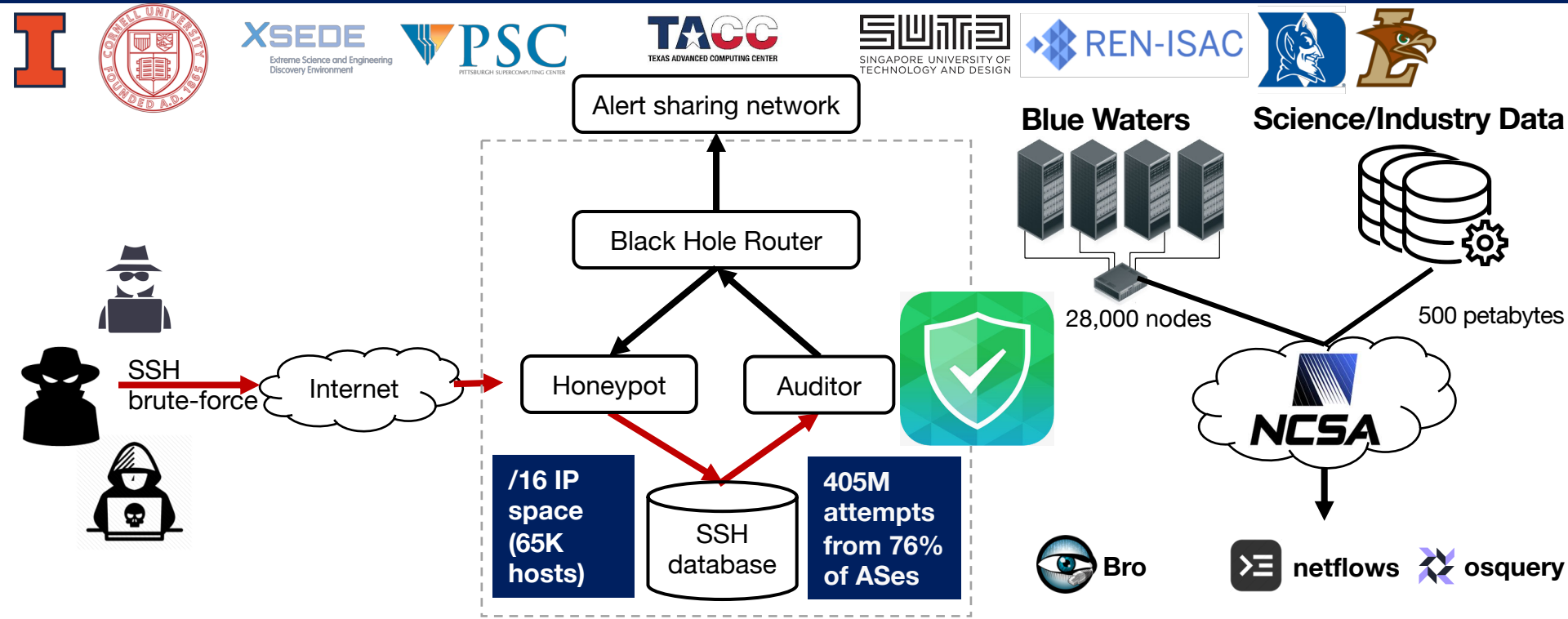
NIST National Institute of Standards and Technology U.S. Department of Commerce

Challenges in Managing SSH Keys – and a Call for Solutions

Tatu Ylonen
University of Helsinki
ylo@ssh.com

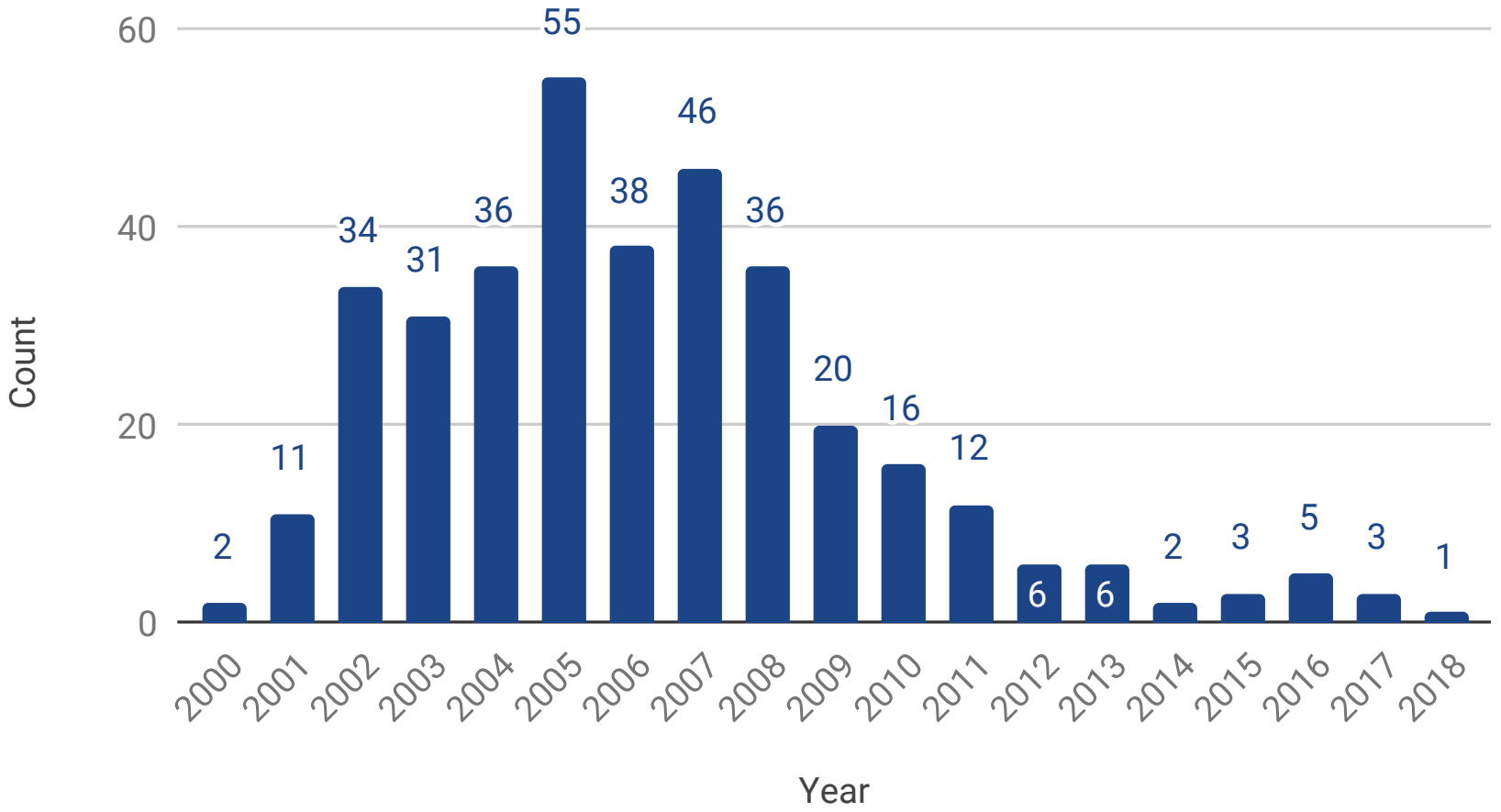
[SSH inventor]

CAUDIT: An operational system to audit internal servers



Continuous Auditing (CAUDIT)

Decreasing security incidents at NCSA



Outline

- **Internet-scale measurements of 405M SSH brute-force attacks**
- Key enabling techniques of CAUDIT
- Benefits of CAUDIT in operational network

Where are the attacks coming from?

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

IP -> ASN mapping using KeyCDN as of May 2018

What kind of SSH client libraries are brute-forcing NCSA?

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

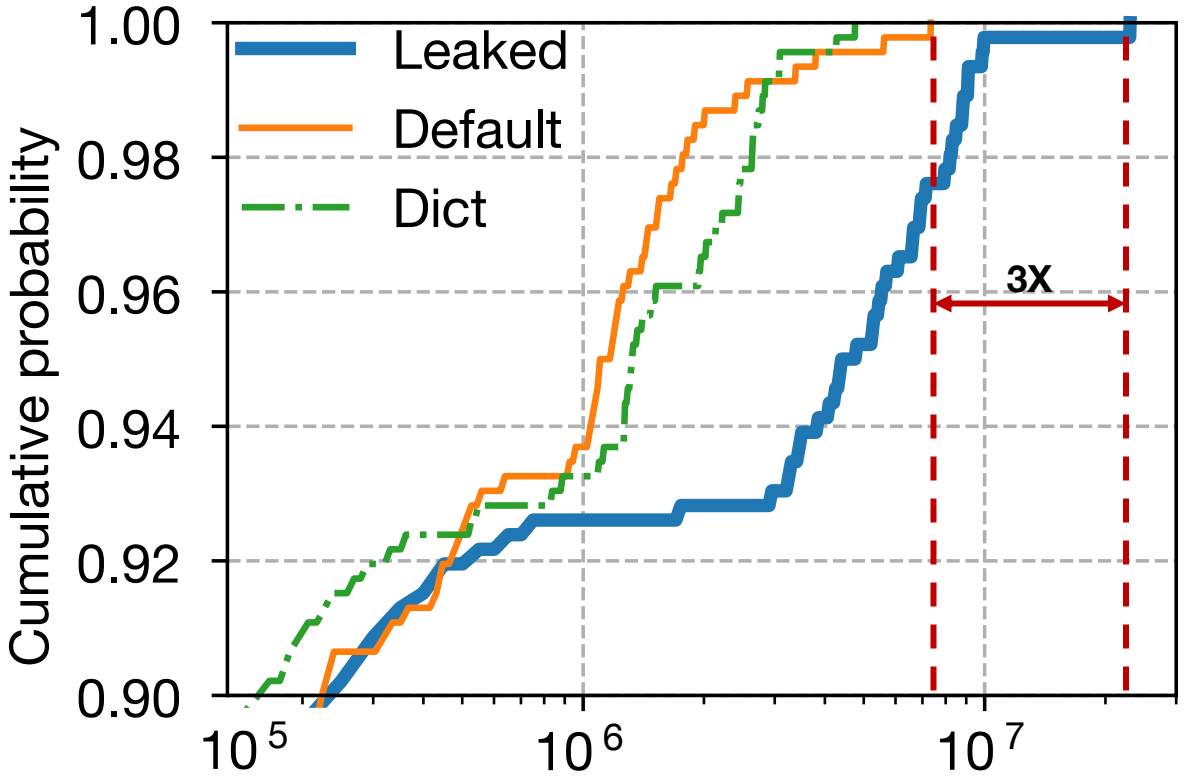
CVE-2018-10933 (auth bypass)

Old routers or IoT devices

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

Rethinking network security for the Internet-of-Things [HotNets' 15]

Leaked passwords could indicate targeted attacks



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

5B leaked passwords are from www.haveibeenpwned.com
excluding dictionary + default passwords

New and unknown SSH keys used in attack attempts

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

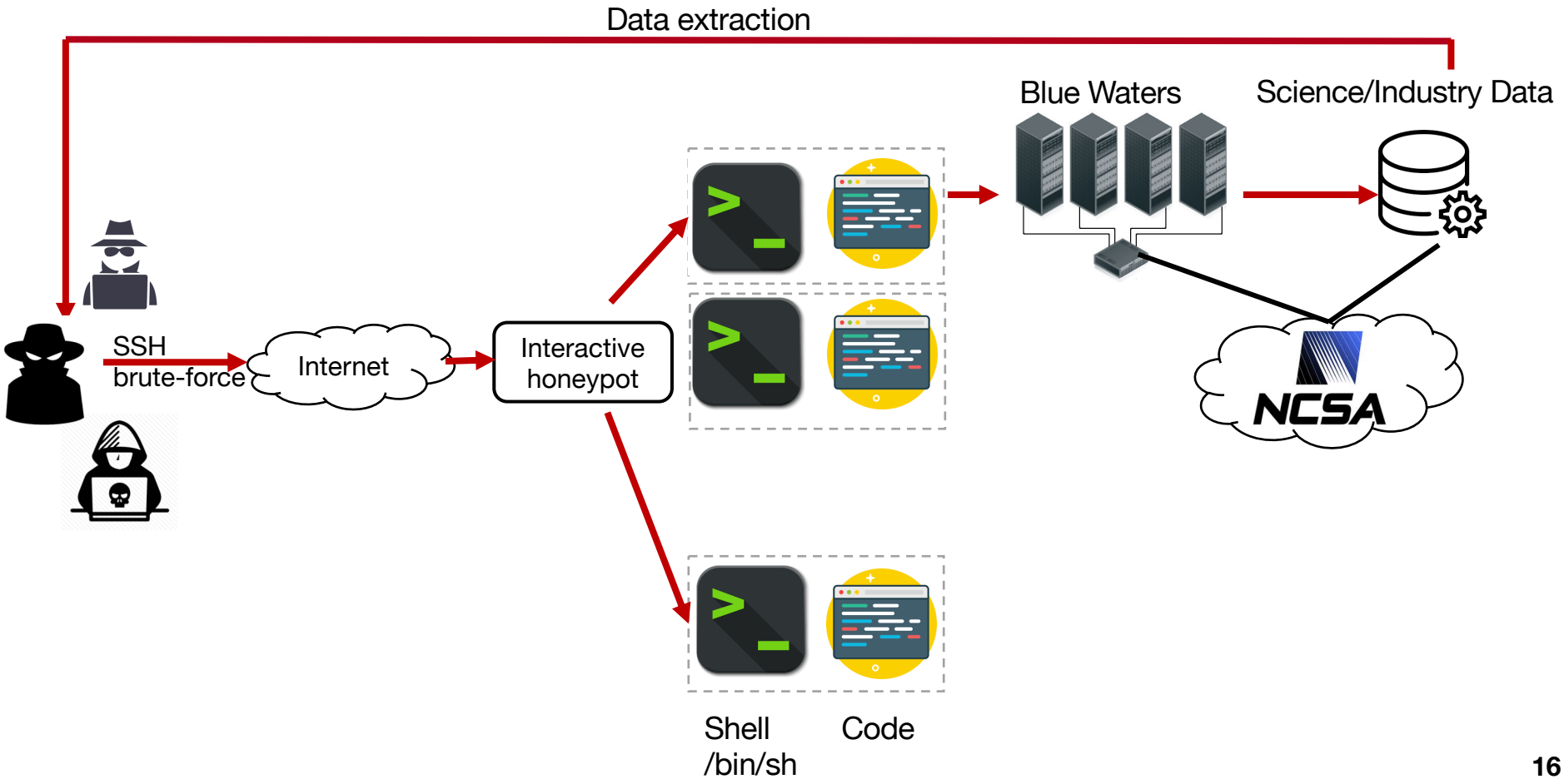
Those keys have led to the adoption of new security policies

- ✓ *Passphrase SSH private keys*
- ✓ *Hash of the recent host names in the known_host file*

Outline

- Internet-scale measurements of SSH brute-force attacks
- **Key enabling techniques of CAUDIT**
- Benefits of CAUDIT in operational network

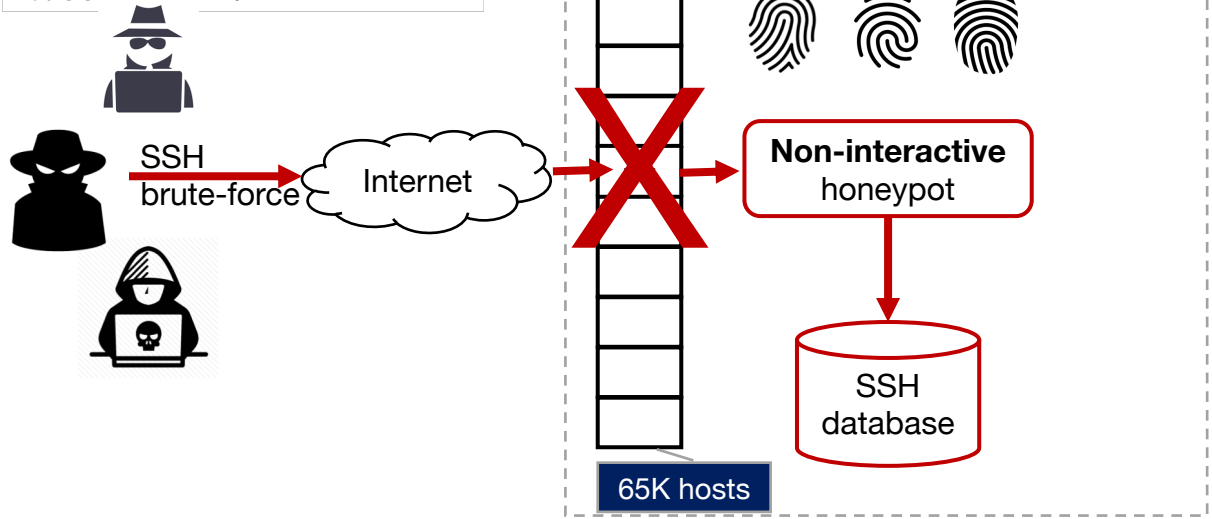
Interactive honeypots are difficult to operate at scale

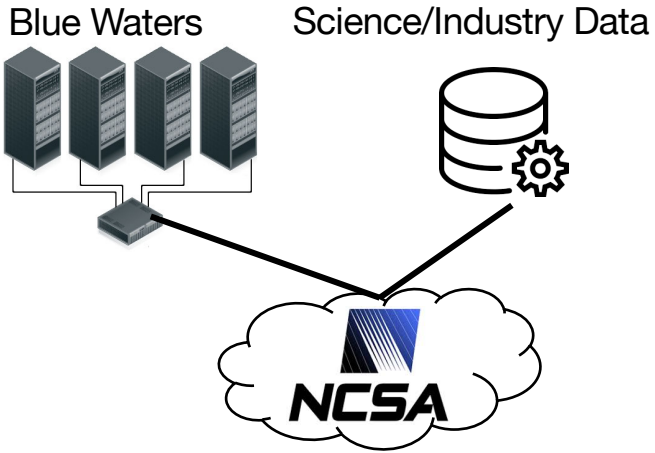


Non-interactive honeypots can scale to millions of attempts

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

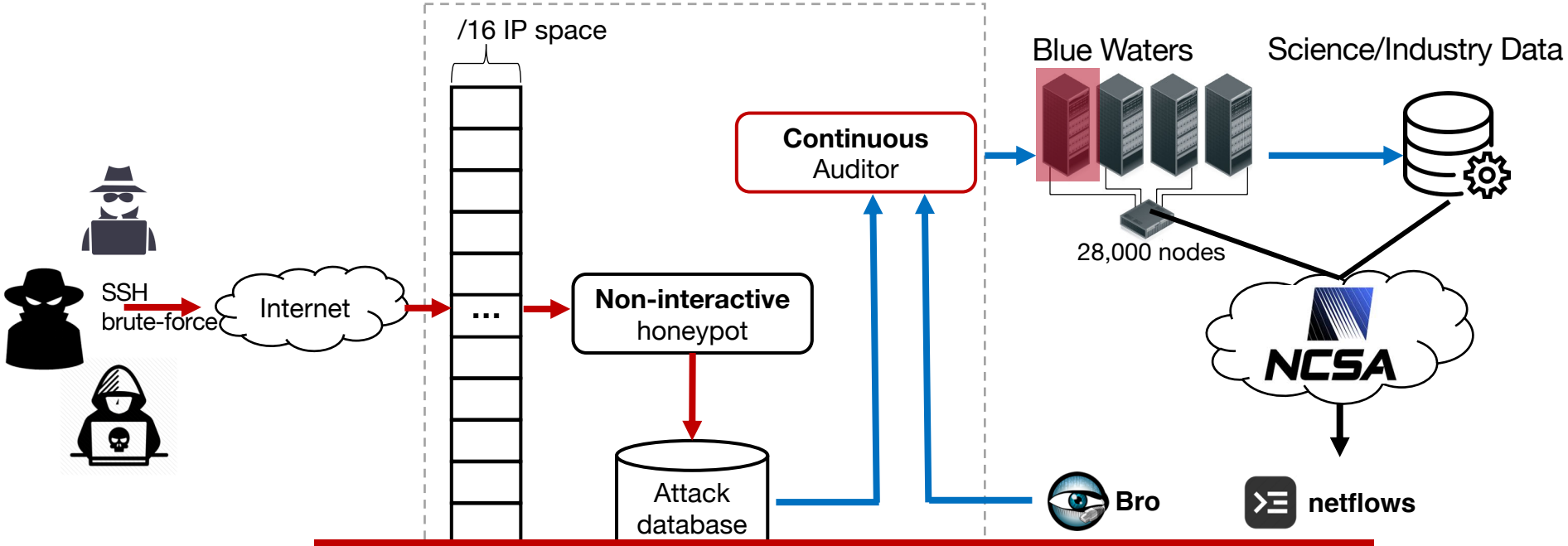




Non-interactive honeypots have a low memory footprint and are straightforward to operate.

Continuous audits are driven by external attack attempts

Traditional auditing is disruptive: Iterating over **all password combinations X servers X ports**

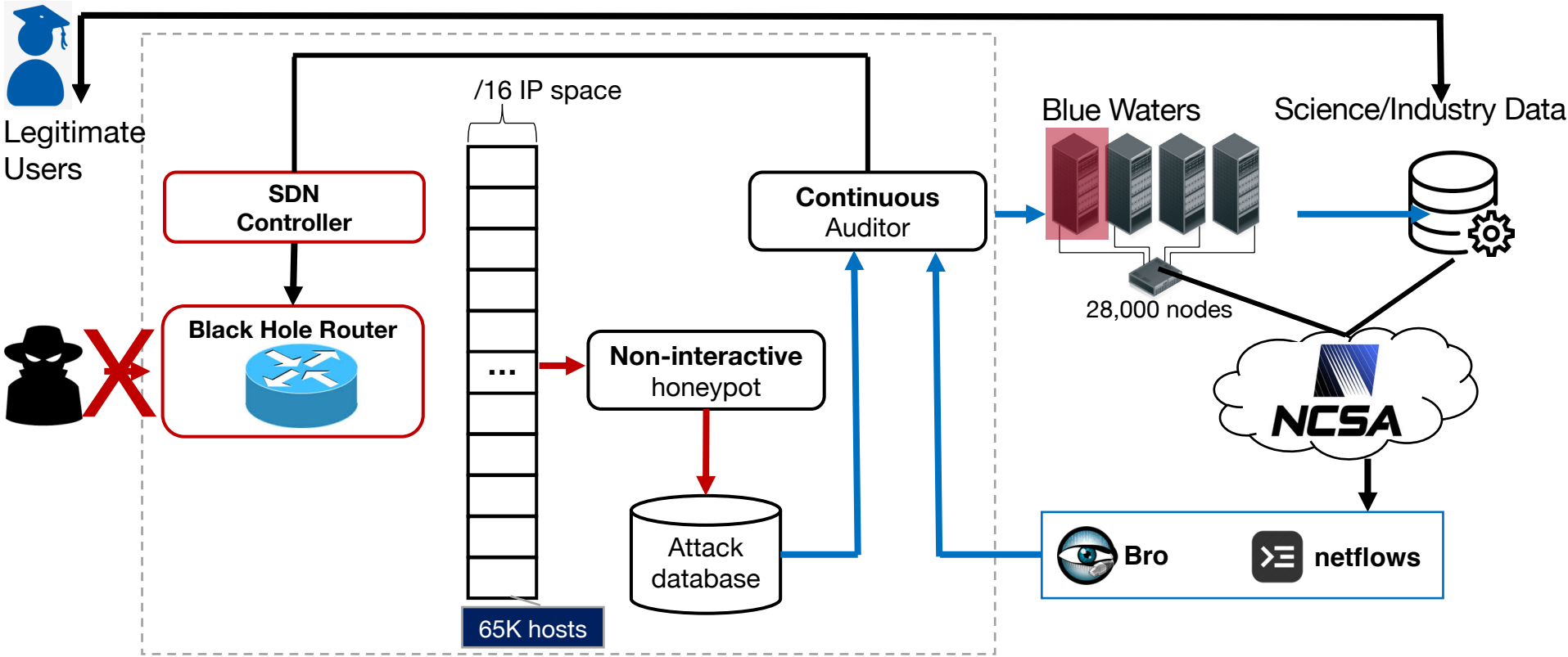


1: Audit target is driven by existing monitors

2: Audit credentials are driven by external attack attempts

Continuous auditing can be seamlessly integrated to existing network infrastructure.

BHR filters malicious connections from the network border



External attacker's attempts

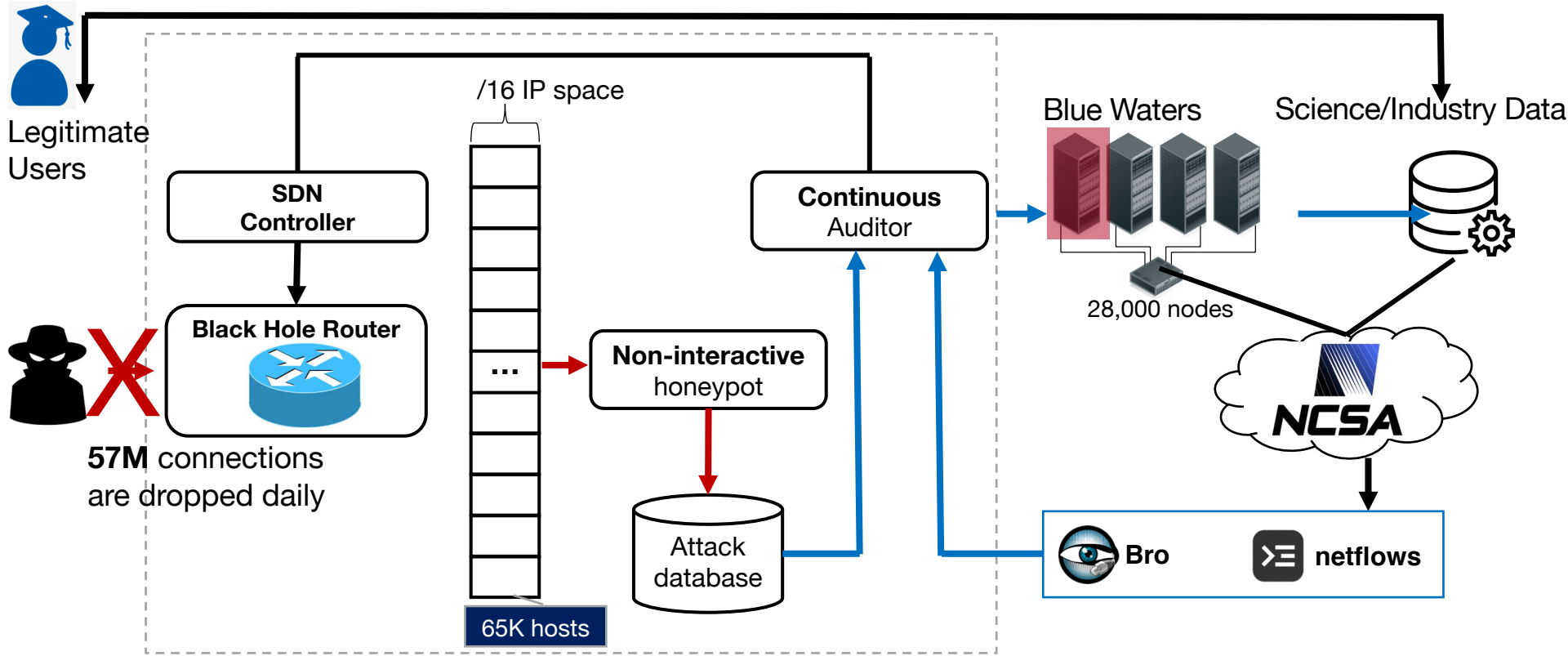
Continuous auditing

Continuous Auditing (CAUDIT)

Outline

- Internet-scale measurements of SSH brute-force attacks
- Key enabling techniques of CAUDIT
- **Benefits of CAUDIT in operational network**

BHR reduces attack traffic to internal monitors

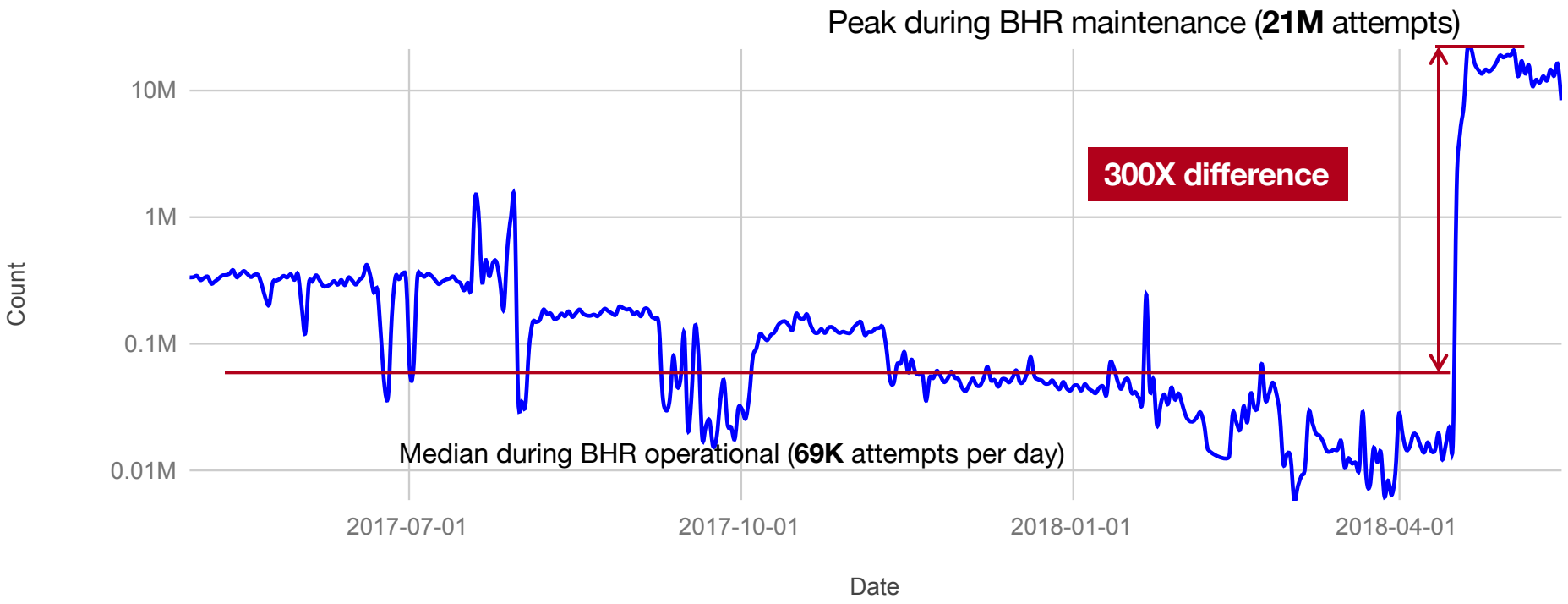


External attacker's attempts

Continuous auditing

Continuous Auditing (CAUDIT)

Attacks increased by 300x when the BHR is in maintenance



Continuous auditing preempted potential security incidents

One smart device that repeatedly scanned the internal network for 700 times

One unsecure DataDirect Network storage device for HPC research data

Six hosts with weak credentials in the NCSA internal network

Future Work

Extend the SSH honeypot to support other kinds of attacks, e.g., remote code execution

Evaluate effectiveness of the alert sharing network against attacks coordinated across sites

Conclusion

SSH brute-force attacks can have significant impact on network security infrastructure, however, existing solutions do not work with large-scale networks.

CAUDIT: Continuous auditing driven by attacker attempts

- Honeypot revealed the use of unknown SSH keys and leaked passwords
- Continuous auditing preempted several attacks from maturing to incidents
- Black hole router successfully blocks 57 million attack attempts on a daily basis
- Our data is being shared with partners in an alert sharing network

Open-sourced, compatible with standard tools, ready to deploy!

https://pmcao.github.io/caudit