Network Traffic Analysis

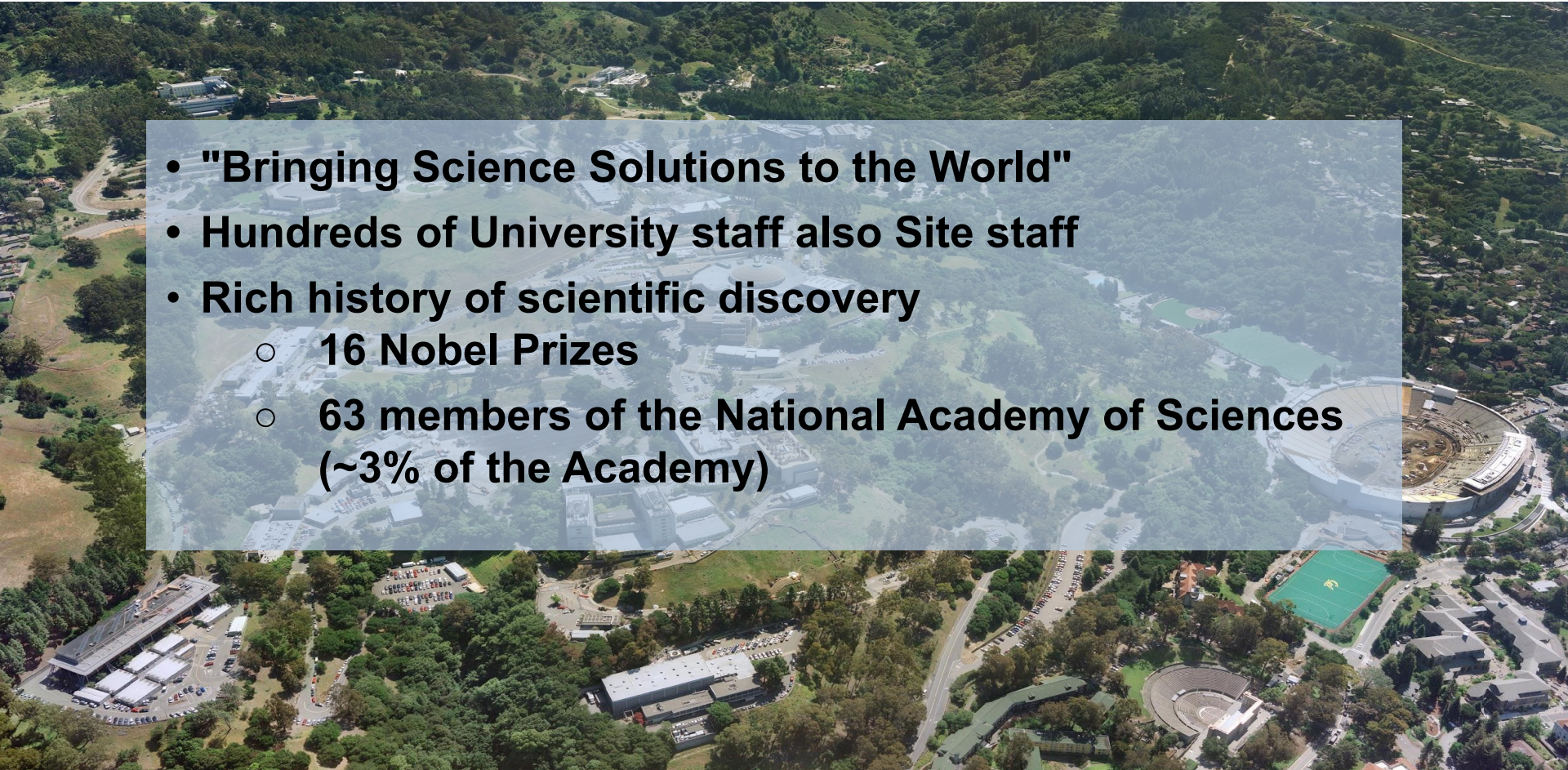
Aashish Sharma
LBNL

U.S. DEPARTMENT OF ENERGY

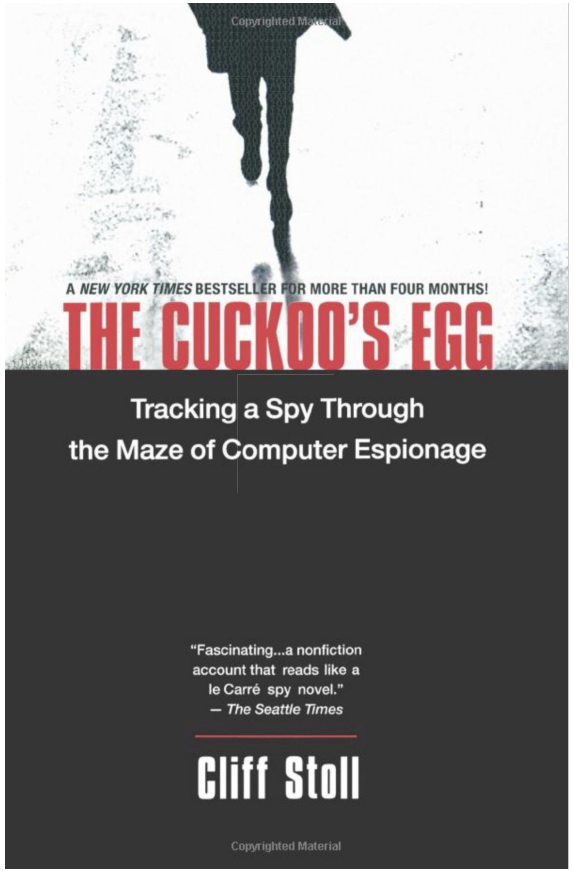
UNIVERSITY OF CALIFORNIA

BERKELEY LAB
Lawrence Berkeley National Laboratory

Lawrence Berkeley National Laboratory



- "Bringing Science Solutions to the World"
- Hundreds of University staff also Site staff
- Rich history of scientific discovery
  - 16 Nobel Prizes
  - 63 members of the National Academy of Sciences (~3% of the Academy)



Network utilities from Site

- traceroute
- libpcap
- tcpdump

Zeek Network Security Monitor

Agenda

1. How real world works - Some Incidents
2. Network monitoring Philosophy - underlying reasoning/thinking
3. Big picture - enterprise monitoring setup
4. Tools for network traffic analysis - Zeek
5. Scale of attacks / blocking and emergence of controls
6. A brief history of evolution of controls in network traffic analysis at the Berkeley Lab

---------- Forwarded message ----------
From: **IT Help Desk** <IThelp@lbl.gov>
Date: Fri, Dec 6, 2013 at 6:10 AM
Subject: New LBL Gmail account
To: iss-ia <iss-ia@lbl.gov>

Gmail@Berkeley Lab and Calendar service updated.
For instructions on how to access your email, sign in at http//gmail.lbl.gov with your Berkeley Lab Identity (LDAP) username (XXXxxxx) and password.
Access gmail at: http//gmail.lbl.gov/
Updated Gmail@Berkeley Lab includes a refreshed interface with tabs on top and a new inbox web-mail default theme.
The Laboratory's primary email service is Gmail@Berkeley Lab. Gmail supports access via the web interface, IMAP clients, and mobile devices. Gmail is fully integrated into the Google Apps Suite.
The new employee information page for Google Apps is https//commons.lbl.gov/x/SgveB

Thank you,

IT Division Help Desk, 510-486-4357, http://help.lbl.gov

lbnl.11r.us/http.gmail.lbl.gov.idp-Authn-UserPassword00000000wcltrh96UQb2W9rsJ9NowN42-LXrnNIj3ES46u4E9pfLOW8p

BERKELEY LAB

LAWRENCE BERKELEY NATIONAL LABORATORY

CENTRAL LOGIN FACILITY

Please login below with your LBNL LDAP username and pass

USERNAME:

Detection

- Reported by two users
- Stats
  - sent to 168 people
  - 2 clicked before blocked
  - 10 clicks after blocks

Subject: Message From University of California HR
Date: Thu, 16 Jan 2014 00:07:52 +0800
From: At Your Service <service@ucop.edu>

We received a notification fro m our date base system which require you to login your account in other to secure your profile .

You are require to **Click Here** and log-in in other to validate and secure your profile.

Sincerely,
At Your Service

uniqoom.ru/catalog/language/english/total/at/Aturservice.htm

At Your Service Online

Usage Tips:

- **Best viewed with Microsoft Internet Explorer 8.0, Mozilla Firefox, and Safari for the Mac.**
- Do not use your browser's Back button
- For confidentiality, always Log Off and close your browser when you have finished your online session.

Sign In

Username:

Password:

Date of Birth:

Sign In

- New to UC and have a temporary password?
- New User and don't have a password?
- Forgot your Username or Password?

uniqoom.ru/catalog/language/english/total/ks.gov.htm

Welcome to the [redacted] Employee Self Service

Problems signing in? Call the Help Desk at 296-1900 (Topeka) or toll-free 1-866-999-30
Help Desk hours are from 8:00 a.m. to 4:30 p.m. Monday through Frida

Employee ID:
Password:
Sign In

Forgot Your Password?

After signing in you can:

View
- Personal Data
- Benefits Confirmation Statement
- Training Summary
- Leave Balances
- Paycheck Information
- Total Compensation

Up
- Benefits Op
- General Pr
- W-4 Feders

Rec
- W-2 Reissu

uniqoom.ru/catalog/language/english/total/fgcu/fgcu.edu.htm

[redacted]

User Login

UIN: PIN: Date of Birth: Login

Forgot PIN?

Need classes to comple your degree in a timely manner?

Eagle Registration can help

Student Info and Alerts

- Graduate Candidates for Spring 2014 Graduation, please submit your application via GULFLINE by the deadline January 17, 2014
- Adjustments to your schedule cannot be made via Gulfline after the drop/add period. Click on link to Academic Calendar for exact date.
- Students should read the Campus Security and Safety Guide and FERPA Annual Notice to Students.
- If you need assistance or have questions about the use of Gulfline, contact the Office of the Registrar at 239-590-7980 or 1-888-373-2043. You can send an email to ORR@fgcu.edu. If you experience problems while registering via Gulfline, refer to Registration Troubleshooting.

Employee Info and Alerts

- If you need assistance or have HR questions, please contact the Office of Human Resources at 239-590-1400 or via email at hr@fgcu.edu.
- If you need assistance or have payroll questions, please contact Finance and Accounting at 239-590-1216 or via email at payrolloffice@fgcu.edu.

RELEASE: 8.2

powered by SUNGARD HIGHER EDUCATION

uniqoom.ru/catalog/language/english/total/ucf/ucf.edu.htm

[redacted] Quicklinks: UCF [redacted]

[redacted]

Sign on:

PID:

Password:

Sign on

By signing on, you agree to the terms of the UCF Information Technologies and Resources Policy

- What is my PID?
- What is my PID Password?
- What is Federated Identity?

Unspecified Service Provider

You have asked to login to Unspecified Service Provider

uniqoom.ru/catalog/language/english/total/at/Aturservice.htm

At Your Service Online

Usage Tips:
- Best viewed with Microsoft Internet Explorer 8.0, Mozilla Firefox, and Safari for the Mac.
- Do not use your browser's Back button.
- For confidentiality, always Log Off and close your browser when you have finished your online session.

Sign In

Username:
Password:
Date of Birth:
Sign In

- New to UC and have a temporary password?
- New User and don't have a password?
- Forgot your Username or Password?

uniqoom.ru/catalog/language/english/total/eku/eku.edu.htm

[redacted]

HELP EXIT

[redacted]

Please enter your user Identification Number (ID) and your Personal Identification Number (PIN). This password PIN is not your RAC Number given to you by your advisor. If you do not know your password PIN, please see the instructions. When finished, click Login.

When you are finished, please Exit and close your browser to protect your privacy.

After multiple UNSUCCESSFUL attempts to log in, the system will automatically disable your access.

User ID:

PIN:

Forgot your PIN?

Date of Birth:

Login

RELEASE: 8.5.2

About this phish

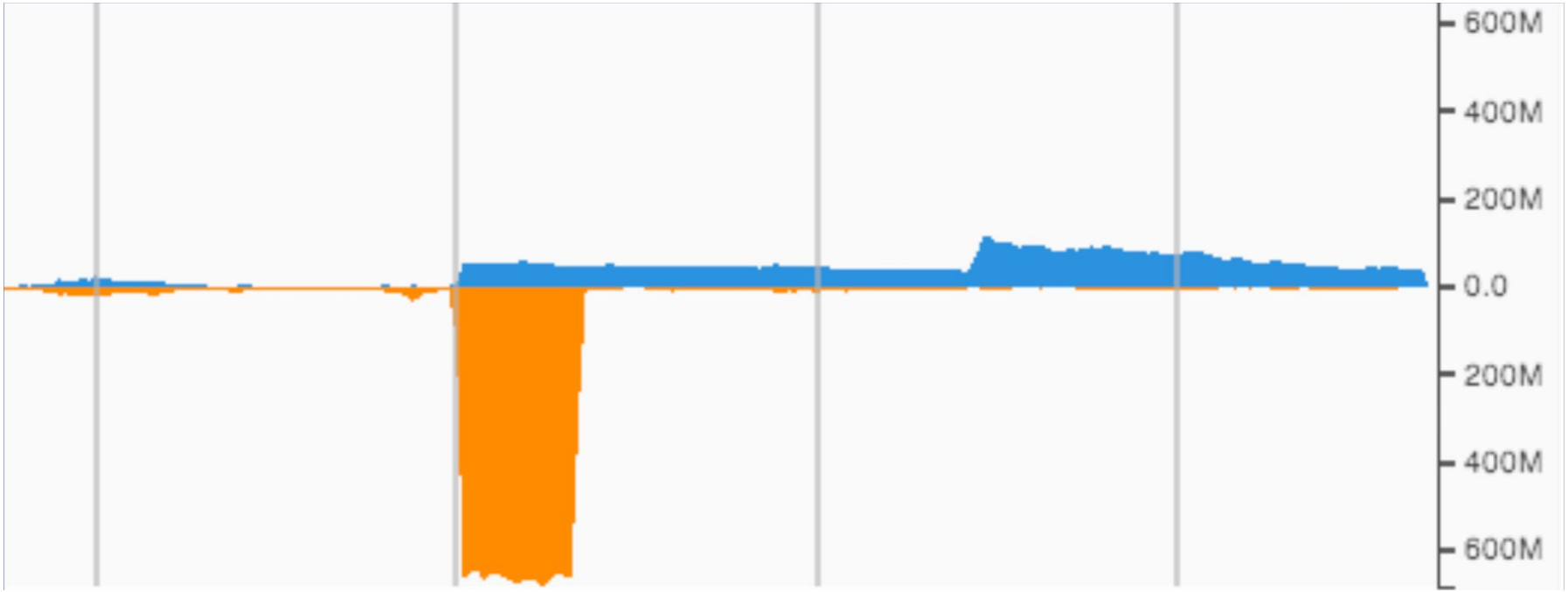
- Reported by 2 users
- Stats
  - 35 people visited AYSO phish
  - 4 entered passwords
  - other sites successfully phished as well

Christmas Day

53/udp outbound connections per second

```
18:03:44 69
18:03:45 75
18:03:46 100587
18:03:47 462718
18:03:48 462877
```

How does a DoS attack “looks” like ?



Network forensics

Zeek

```
Dec 25 18:06:22 CGtPdq4AI7c6eK8YMa      128.3.x.y    50275
111.74.239.11   8080    1       GET     111.74.239.11   /jave
-       Wget/1.15 (linux-gnu)   0       1223123 200     OK
-       -       -       (empty) -       -       -       -   -
FZlV9xKSmksOlMfHa       application/x-executable
```

Central Syslog

```
Dec 25 18:06:21 apexdir/128.3.x.y sshd[22544]: Accepted
publickey for root from 222.186.34.213 port 2349 ssh2: RSA
56:a9:4c:fc:b0:ba:52:ae:b3:f5:a1:53:00:24:95:92
```

Packet Capture

```
22:41:50.362755 IP 222.186.56.25.3516 > 128.3.x.y.6379:
Flags [P.], seq 1:425, ack 1, win 65535, length 424
$3
set
pwn
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDZSQUarS5hKhsXBEX1CAm5XN6mt7
ODEo4JXq8RUWNnimF087PNED0OmSy3bWlEozBxVJ1D/uKaQoubDveyq80R
XUPIM58WnEe4qQkPgUiK/3lOLpeMUnNwpCi1rQUqAc/kAFidSAJA2SktlS
srB7i9FdkRQ6L0idu9HSOEIEDZ1pFPPkVG7G9IWnhLIIPfK6YWLhQtROk5
6qc0EHBZ14cGtWIFaRRKSt1ecX86tVbsIUJDKVcJM941vtlqbBXjxKaRa9
1LMY3Hm+EAlH2AS8gR4D/GVuzinNICmMg5m5cCqROIOrGzYEIPZp9XhkxW
G3QuYnB6Z8sZQB8dC6q3kxzN redis
```

Google (translate)

- Chinese honeypot blog describes similar key
- Redis autop0wn tool
  - github.com/matiasinsaurralde/evilredis

```
== evilredis >:)

 Syntax:    evilredis [ target ] [ level = 0 ]
 Ex.        evilredis 192.168.0.0/24 1

 - Level 0: quick scan, dump server info & keys
 - Level 1: flushall
 - Level 2: flushall & shutdown
 - Level 3: root >:) (requires a pubkey)

   Specify your pubkey after evilness level
   Example: $ evilredis x.x.x.x 3 ~/.ssh/id_rsa.pub
```

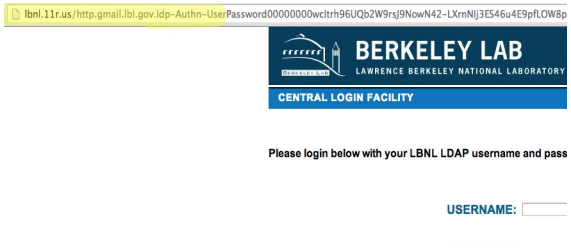
Host forensics

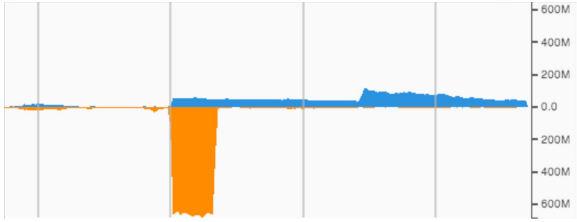
- lsof output

```
.sshd     22756    root  txt       REG                 8,5  1223123
1599198 /usr/bin/.sshd
```

- Strange authorized key

```
REDIS0006?pwnA?ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDZSQUarS5hKhsXBEX1CAm5XN6mt7ODEo4JXq8RUW
NnimF087PNED0OmSy3bWlEozBxVJ1D/uKaQoubDveyq80R6qc0EHBZ14cGtWIFaRRKSt1e
cX86tVbsIUJDKVcJM941vtlqbBXjxKaRa91LMY3Hm+EAlH2AS8gR4D/GVuzinNICmMg5m5
cCqROIOrGzYEIPZp9XhkxWG3QuYnB6Z8sZQB8dC6q3kxzN redis)
```



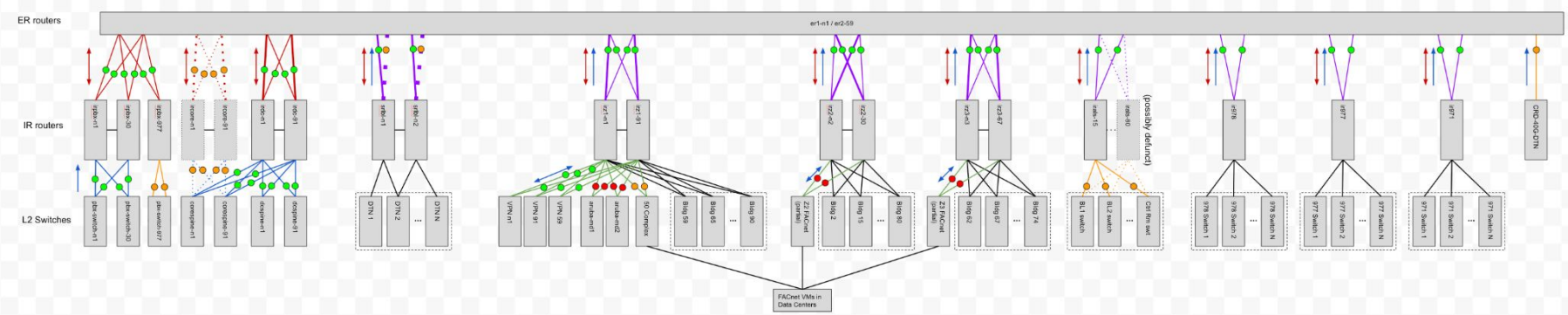


- Reported by two users
- Stats
  - sent to 168 people
  - 2 clicked before blocked
  - 10 clicks after blocks

- Reported by 2 users
- Stats
  - 35 people visited AYSO phish
  - 4 entered passwords
  - other sites successfully phished as well

53/udp outbound connections per second

```
18:03:44 69
18:03:45 75
18:03:46 100587
18:03:47 462718
18:03:48 462877
```



Incidents Happen	Study and Learn	New Controls
There is no perfect protection, incidents are going to happen. Architect to reduce the scope and severity, detect quickly.	Data driven cyber security. What exactly happened, bit by bit. How were controls bypassed? How best to defend in the future?	Take the lessons learned from study and consider new controls. Where to attack the kill chain?

Scientific Mission Needs Drive Cyber Strategy

- Mission
  - Open science, big data, high speed networking
  - Collaboration with guests as full participants
- Conventional cyber strategy can conflict with the mission
  - **No border firewall:** huge flows and worldwide collaborations
  - Centralized endpoint control is NOT reasonable, BYOD default
- LBNL Strategies
  - Pervasive visibility and risk based cyber security
  - Incidents happen: monitor, detect, and resolve

Our Cyber Security strategy for network monitoring

Design Principles

- Enable Science
- Open by default
- Platform neutral
- Risk Based
- Data and research based
- Active response and continuous monitoring
- Dynamic process that does not fit in compliance Wrapper

Design Considerations*

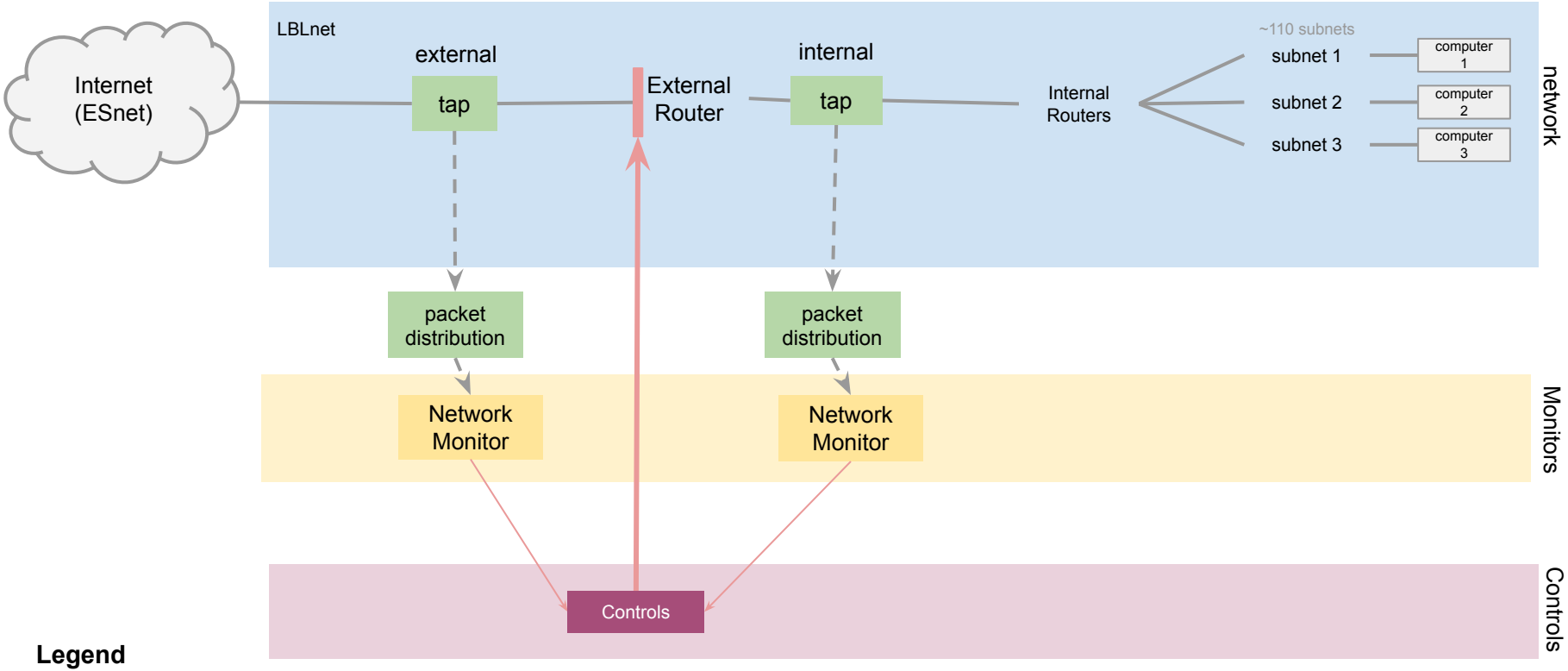
- Assume a hostile Environment
- Presume Breach
- Never Trust, Always Verify
- Scrutinize Explicitly
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

* Tenets of Zero Trust

Design Strategies

- **Pervasive Visibility without disruption**
- Be the attacker
- Resist temptation to centrally secure
- Avoid tight coupling and high consequence events
- Isolate higher risk activities from open science
- **Accept transient compromise: monitor, detect, resolve**
- **Spend the next dollar on detection/forensics**
- **Overall security evolves as attack landscape changes**

LBNL Cyber Security: Border Access Visibility and Controls



Legend

- network traffic
- copy of network traffic
- flow data
- block commands
- network equipment
- tapping equipment
- cyber security equipment
- Lab computers

Requirement of a network monitoring tool and Design Goals for Network Monitoring

- High-speed, large volume monitoring
- No packet filter drops
- Real-time notification
- **Extensible**
- **Avoid simple mistakes**
- **Mechanism separate from policy**
- **The monitor will be attacked**

From the very beginning …

Design goals and requirement of Zeek:

- High-speed, large volume monitoring
- No packet filter drops
- Real-time notification
- **Extensible**
- **Avoid simple mistakes**
- **Mechanism separate from policy**
- **The monitor will be attacked**

"... system clearly must be designed in order to make it easy to add to it knowledge of new types of attacks…"

From the very beginning …

Design goals and requirement of Zeek:

- High-speed, large volume monitoring
- No packet filter drops
- Real-time notification
- **Extensible**
- **Avoid simple mistakes**
- **Mechanism separate from policy**
- **The monitor will be attacked**

"We particularly desire that the way that a site defines its security policy be both clear and as error-free as possible"

From the very beginning …

Design goals and requirement of Zeek:

- High-speed, large volume monitoring
- No packet filter drops
- Real-time notification
- **Extensible**
- **Avoid simple mistakes**
- **Mechanism separate from policy**
- **The monitor will be attacked**

"....a clear separation between mechanism and policy…"

From the very beginning …

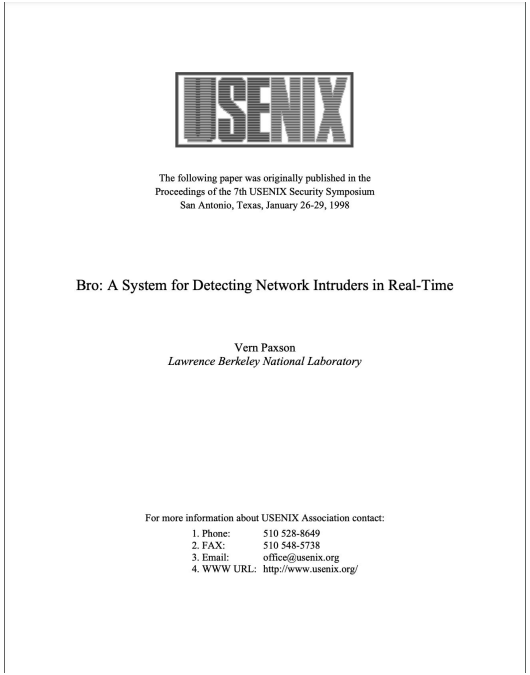
Design goals and requirement of Zeek:

- High-speed, large volume monitoring
- No packet filter drops
- Real-time notification
- **Extensible**
- **Avoid simple mistakes**
- **Mechanism separate from policy**
- **The monitor will be attacked**

Zeek:

Big Picture

- Zeek a continuous network monitoring tool
  - Network flight recorder
- The design goals written back in 1999 Usenix paper continue to be relevant in 2023 with new architectures / buzzwords / paradigms / Zero Trust …



The following paper was originally published in the
Proceedings of the 7th USENIX Security Symposium
San Antonio, Texas, January 26-29, 1998

Bro: A System for Detecting Network Intruders in Real-Time

Vern Paxson
Lawrence Berkeley National Laboratory

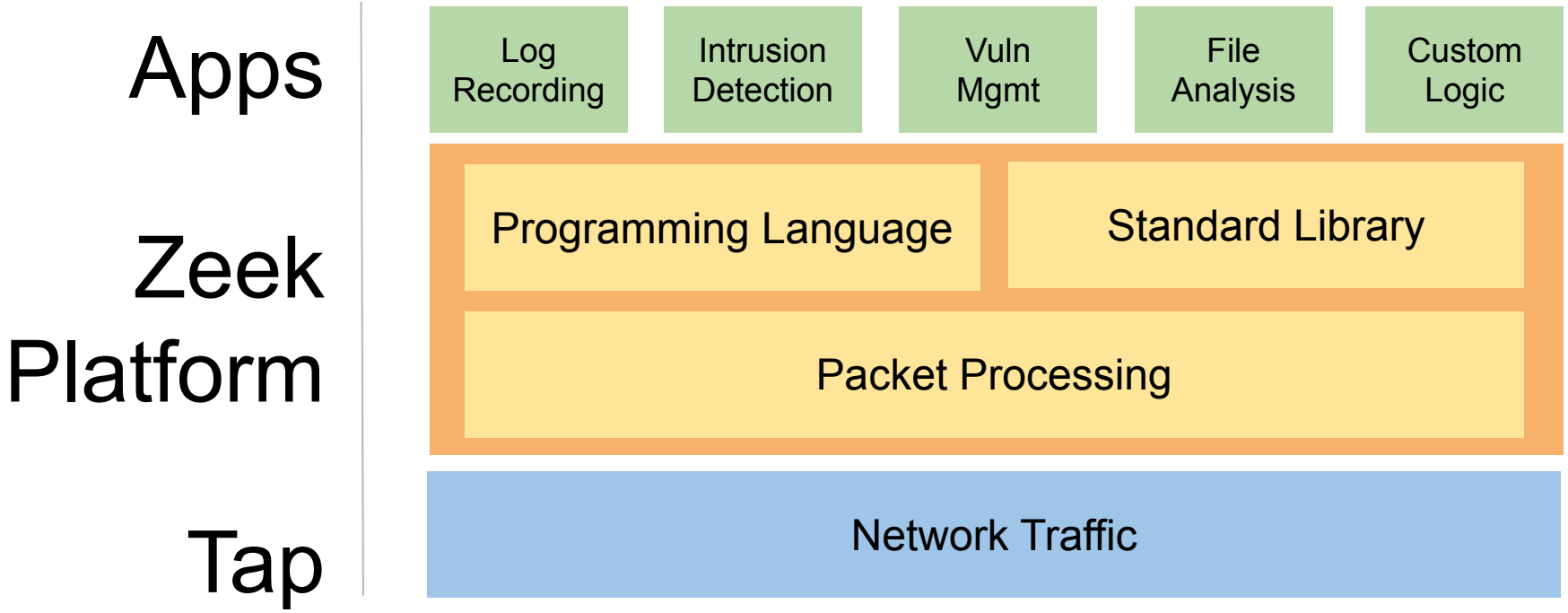
For more information about USENIX Association contact:
1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: http://www.usenix.org/

What is Zeek?

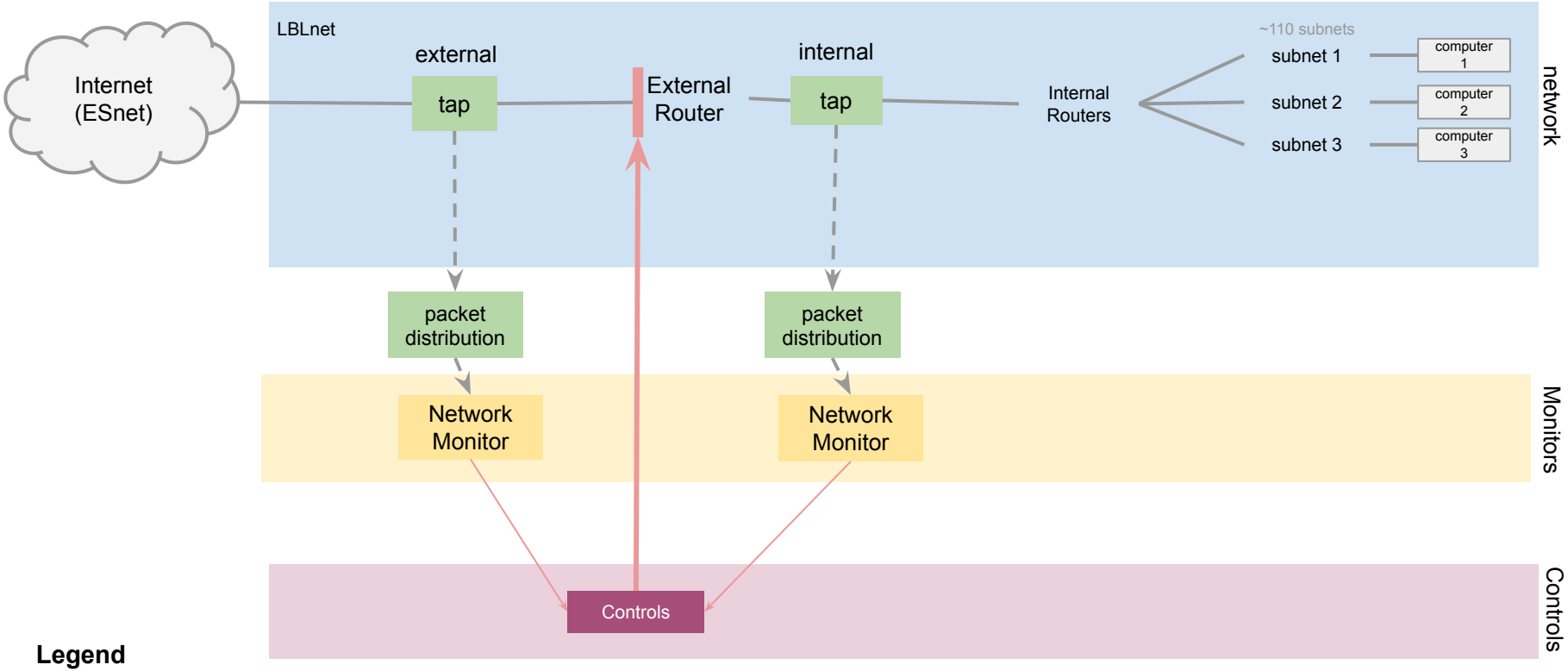
Not your typical IDS/IPS - but rather a monitoring platform

- A standalone network monitor
- A programmable framework
- An ecosystem

Zeek platform



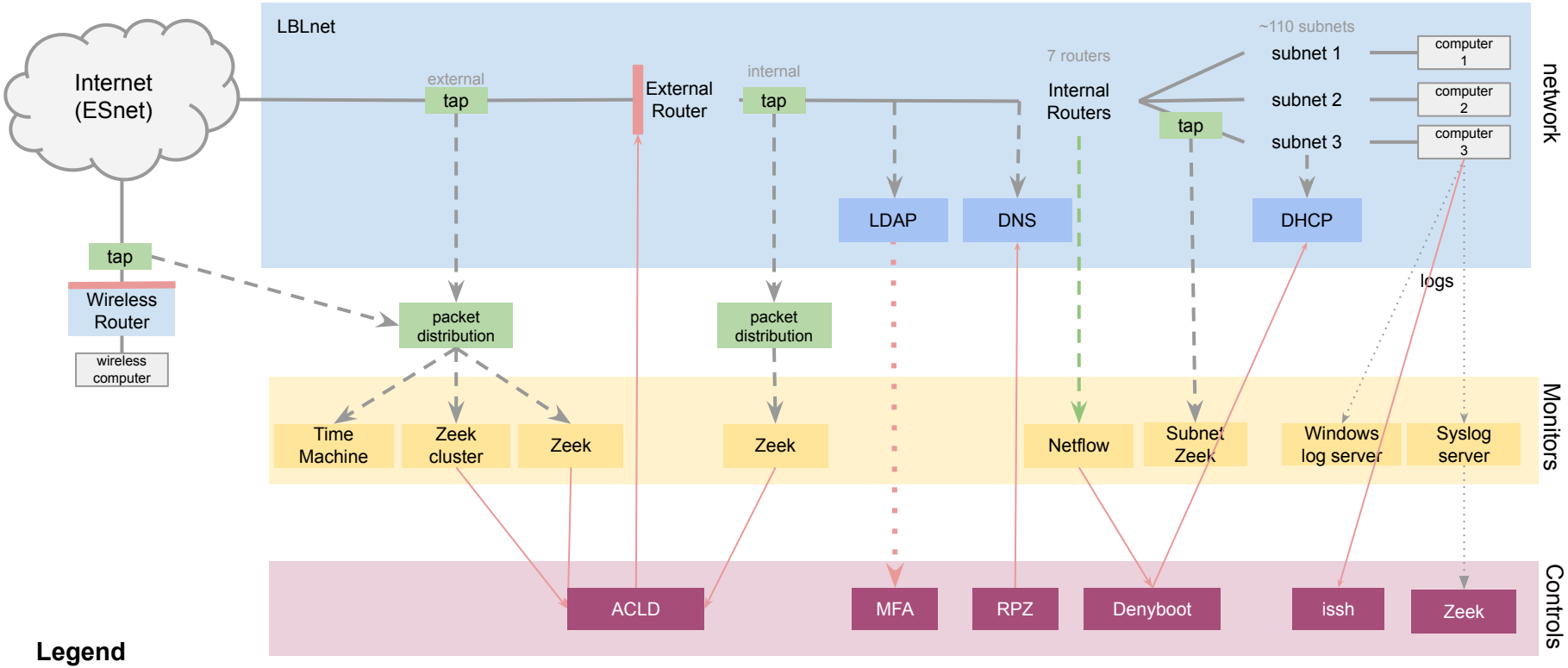
LBNL Cyber Security: Border Access Visibility and Controls



Legend

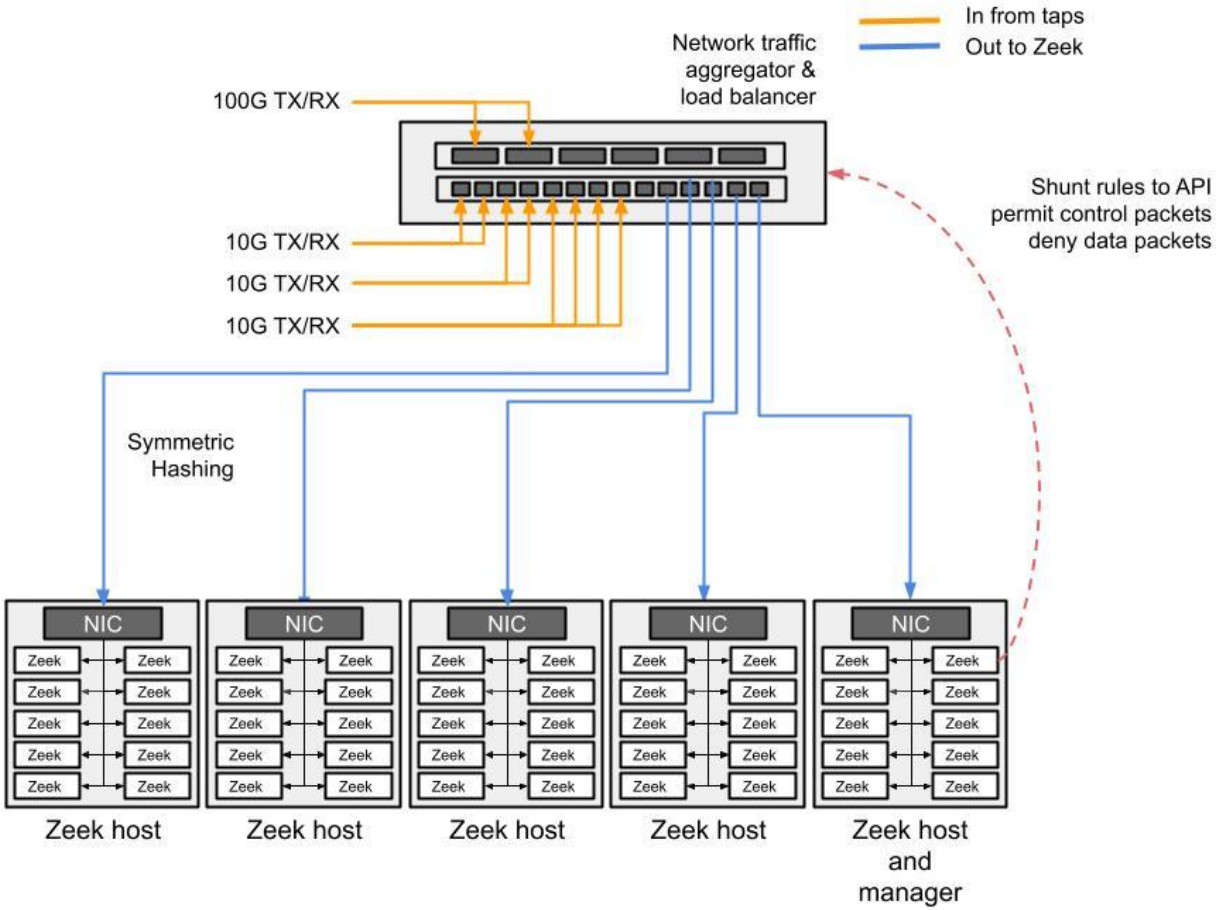
- network traffic
- copy of network traffic
- flow data
- block commands
- network equipment
- tapping equipment
- cyber security equipment
- Lab computers

LBNL Cyber Security: Border Access Visibility and Controls



Legend

- network traffic
- copy of network traffic
- flow data
- block commands
- network equipment
- tapping equipment
- cyber security equipment
- Lab computers


In from taps
Out to Zeek
Network traffic aggregator & load balancer
100G TX/RX
10G TX/RX
10G TX/RX
10G TX/RX
Shunt rules to API permit control packets deny data packets
Symmetric Hashing
NIC
Zeek
Zeek host
Zeek host
Zeek host
Zeek host
Zeek host and manager

Zeek logs

Don't defend alone. Nothing is faster than a community-based approach to security.

conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of first packet
uid	string	Unique identifier of connection
id	record conn_id	Connection's 4-tuple of endpoint addresses
orig_h	addr	IP address of system initiating connection
orig_p	port	Port from which the connection is initiated
resp_h	addr	IP address of system responding to connection request
resp_p	port	Port on which connection response is sent
proto	enum	Transport layer protocol of connection
service	string	Application protocol ID sent over connection
duration	interval	How long connection lasted
orig_bytes	count	Number of payload bytes originator sent
resp_bytes	count	Number of payload bytes responder sent
conn_state	string	Connection state (see conn.log - conn_state)
local_orig	bool	Value=T if connection originated locally
local_resp	bool	Value=T if connection responded locally
missed_bytes	count	Number of bytes missed (packet loss)
history	string	Connection state history (see conn.log - history)
orig_pkts	count	Number of packets originator sent
orig_ip_bytes	count	Number of originator IP bytes (via IP total_length header field)
resp_pkts	count	Number of packets responder sent
resp_ip_bytes	count	Number of responder IP bytes (via IP total_length header field)
tunnel_parents	table	If tunneled, connection UID value of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of originator
resp_l2_addr	string	Link-layer address of responder
vlan	int	Outer VLAN for connection
inner_vlan	int	Inner VLAN for connection

conn_state

A summarized state for each connection

S0	Connection attempt seen, no reply
S1	Connection established, not terminated (0 byte counts)
SF	Normal establish & termination (>0 byte counts)
REJ	Connection attempt rejected
S2	Established, Orig attempts close, no reply from Resp
S3	Established, Resp attempts close, no reply from Orig
RSTO	Established, Orig aborted (RST)
RSTR	Established, Resp aborted (RST)
RSTOS0	Orig sent SYN then RST; no Resp SYN-ACK
RSTRH	Resp sent SYN-ACK then RST; no Orig SYN
SH	Orig sent SYN then FIN; no Resp SYN-ACK ("half-open")
SHR	Resp sent SYN-ACK then FIN; no Orig SYN
OTH	No SYN, not closed. Midstream traffic. Partial connection.

history

Orig UPPERCASE, Resp lowercase, compressed

S	A SYN without the ACK bit set
H	A SYN-ACK ("handshake")
A	A pure ACK
D	Packet with payload ("data")
F	Packet with FIN bit set
R	Packet with RST bit set
C	Packet with a bad checksum
I	Inconsistent packet (both SYN & RST)
Q	Multi-flag packet (SYN & FIN or SYN + RST)
T	Retransmitted packet
W	Packet with zero window advertisement
^	Flipped connection

dhcp.log | DHCP lease activity

FIELD	TYPE	DESCRIPTION
ts	time	Earliest time DHCP message observed
uids	table	Unique identifiers of DHCP connections
client_addr	addr	IP address of client
server_addr	addr	IP address of server handing out lease
mac	string	Client's hardware address
host_name	string	Name given by client in Hostname option 12
client_fqdn	string	FQDN given by client in Client FQDN option 81
domain	string	Domain given by server in option 15
requested_addr	addr	IP address requested by client
assigned_addr	addr	IP address assigned by server
lease_time	interval	IP address lease interval
client_message	string	Message with DHCP_DECLINE so client can tell server why address was rejected
server_message	string	Message with DHCP_NAK to let client know why request was rejected
msg_types	vector	DHCP message types seen by transaction
duration	interval	Duration of DHCP session
msg_orig	vector	Address originated from msg_types field
client_software	string	Software reported by client in vendor_class
server_software	string	Software reported by server in vendor_class

http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when request happened
uid & id		Underlying connection info - See conn.log
trans_depth	count	Pipelined depth into connection
method	string	Verb used in HTTP request (GET, POST, etc.)
host	string	Value of HOST header
uri	string	URI used in request
referrer	string	Value of referer header
version	string	Value of version portion of request
user_agent	string	Value of User-Agent header from client
origin	string	Value of Origin header from client
request_body_len	count	Uncompressed data size from client
response_body_len	count	Uncompressed data size from server
status_code	count	Status code returned by server
status_msg	string	Status message returned by server
info_code	count	Last seen 1xx info reply code from server
info_msg	string	Last seen 1xx info reply message from server
tags	table	Indicators of various attributes discovered
username	string	Username if basic auth performed for

radius.log | RADIUS authentication attempts

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid & id		Underlying connection info - See conn.log
username	string	Username, if present
mac	string	MAC address, if present
framed_addr	addr	Address given to network access server, if present
tunnel_client	string	Address (IPv4, IPv6, or FQDN) of initiator end of tunnel, if present
connect_info	string	Connect info, if present
reply_msg	string	Reply message from server challenge
result	string	Successful or failed authentication
ttl	interval	Duration between first request and either Access-Accept message or an error

sip.log | SIP analysis

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when request happened
uid & id		Underlying connection info - See conn.log
trans_depth	count	Pipelined depth into request/response transaction
method	string	Verb used in SIP request (INVITE, etc)
uri	string	URI used in request
date	string	Contents of Date header from client
request_from	string	Contents of request From: header
request_to	string	Contents of To: header
response_from	string	Contents of response From: header
response_to	string	Contents of response To: header
reply_to	string	Contents of Reply-To: header
call_id	string	Contents of Call-ID: header from client
seq	string	Contents of CSeq: header from client
subject	string	Contents of Subject: header from client
request_path	vector	Client message transmission path, extracted from headers
response_path	vector	Server message transmission path, extracted from headers
user_agent	string	Contents of User-Agent: header from client
status_code	count	Status code returned by server
status_msg	string	Status message returned by server
warning	string	Contents of Warning: header
request_body_len	count	Contents of Content-Length: header from client
response_body_len	count	Contents of Content-Length: header from server
content_type	string	Contents of Content-Type: header from server

This logs' value usually appended to the sender's original off and not logged

smtp.log | SMTP transactions

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when message was first seen
uid & id		Underlying connection info - See conn.log
trans_depth	count	Transaction depth if there are multiple msgs
helo	string	Contents of Helo header
mailfrom	string	Email addresses found in From header
rcptto	table	Email addresses found in Rcpt header
date	string	Contents of Date header
from	string	Contents of From header
to	table	Contents of To header

ssl.log | SSL handshakes

FIELD	TYPE	DESCRIPTION
ts	time	Time when SSL connection first detected
uid & id		Underlying connection info - See conn.log
version	string	SSL/TLS version server chose
cipher	string	SSL/TLS cipher suite server chose
curve	string	Elliptic curve server chose when using ECDH/ECDHE
server_name	string	Value of Server Name Indicator SSL/TLS extension
resumed	bool	Flag that indicates session was resumed
last_alert	string	Last alert seen during connection
next_protocol	string	Next protocol server chose using application layer next protocol extension, if present
established	bool	Flags if SSL session successfully established
cert_chain_fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by server
client_cert_chain_fuids	vector	Ordered vector of all certificate file unique IDs for certificates offered by client
subject	string	Subject of X.509 cert offered by server
issuer	string	Subject of signer of X.509 server cert
client_subject	string	Subject of X.509 cert offered by client
client_issuer	string	Subject of signer of client cert
validation_status	string	Certificate validation result for this connection
ocsp_status	string	OCSP validation result for this connection
valid_ct_logs	count	Number of different logs for which valid SCTs encountered in connection
valid_ct_operators	count	Number of different log operators for which valid SCTs encountered in connection
notary	record Cert Notary::Response	Response from the ICSI certificate notary

syslog.log | Syslog messages

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when syslog message was seen
uid & id		Underlying connection info - See conn.log
proto	enum	Protocol over which message was seen
facility	string	Syslog facility for message
severity	string	Syslog severity for message
message	string	Plain text message

tunnel.log | Details of encapsulating tunnels

FIELD	TYPE	DESCRIPTION
ts	time	Time at which tunnel activity occurred
uid & id		Underlying connection info - See conn.log
tunnel_type	enum	Tunnel type
action	enum	Type of activity that occurred

weird.log | Unexpected network/protocol activity

FIELD	TYPE	DESCRIPTION
ts	time	Time when weird occurred
uid & id		Underlying connection info - See conn.log
name	string	Name of weird that occurred
addl	string	Additional information accompanying weird, if any
notice	bool	If weird was turned into a notice
peer	string	Peer that originated weird

Alert logs

intel.log | Intelligence data matches

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when data discovered
uid & id		Underlying connection info - See conn.log
seen	record Intel::Seen	Where data was seen
matched	set [enum]	Which indicator types matched
sources	set [string]	Sources which supplied data that resulted in match
fuid	string	If file was associated with this intelligence hit, this is uid for file
file_mime_type	string	Mime type if intelligence hit is related to file
file_desc	string	Files 'described' to give more context
cif	record Intel::CIF	CIF

notice.log | Interesting events and activity

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when notice occurred
uid & id		Underlying connection info - See conn.log
fuid	string	File unique ID if notice related to a file
file_mime_type	string	Mime type if notice related to a file
file_desc	string	Files 'described' to give more context
proto	enum	Transport protocol
note	enum	Notice Type of notice
msg	string	Human readable message for notice
sub	string	Human readable sub-message
src	addr	Source address, if no conn_id
dst	addr	Destination address
p	port	Associated port, if no conn_id
n	count	Associated count or status code
peer_descr	string	Text description for peer that raised notice, including name, host address and port
actions	set[enum]	Actions applied to this notice
suppress_for	interval	Field indicates length of time that unique notice should be suppressed
remote_location	record geo_location	If GeoIP support is built in, notices have geographic information attached to them
dropped	bool	Indicates if Bro IP address was dropped and denied network access

SURICATA

AVAILABLE WITH CORELIGHT

Corelight's Suricata and Zeek logs link alerts and evidence to accelerate incident response

suricata_corelight.log

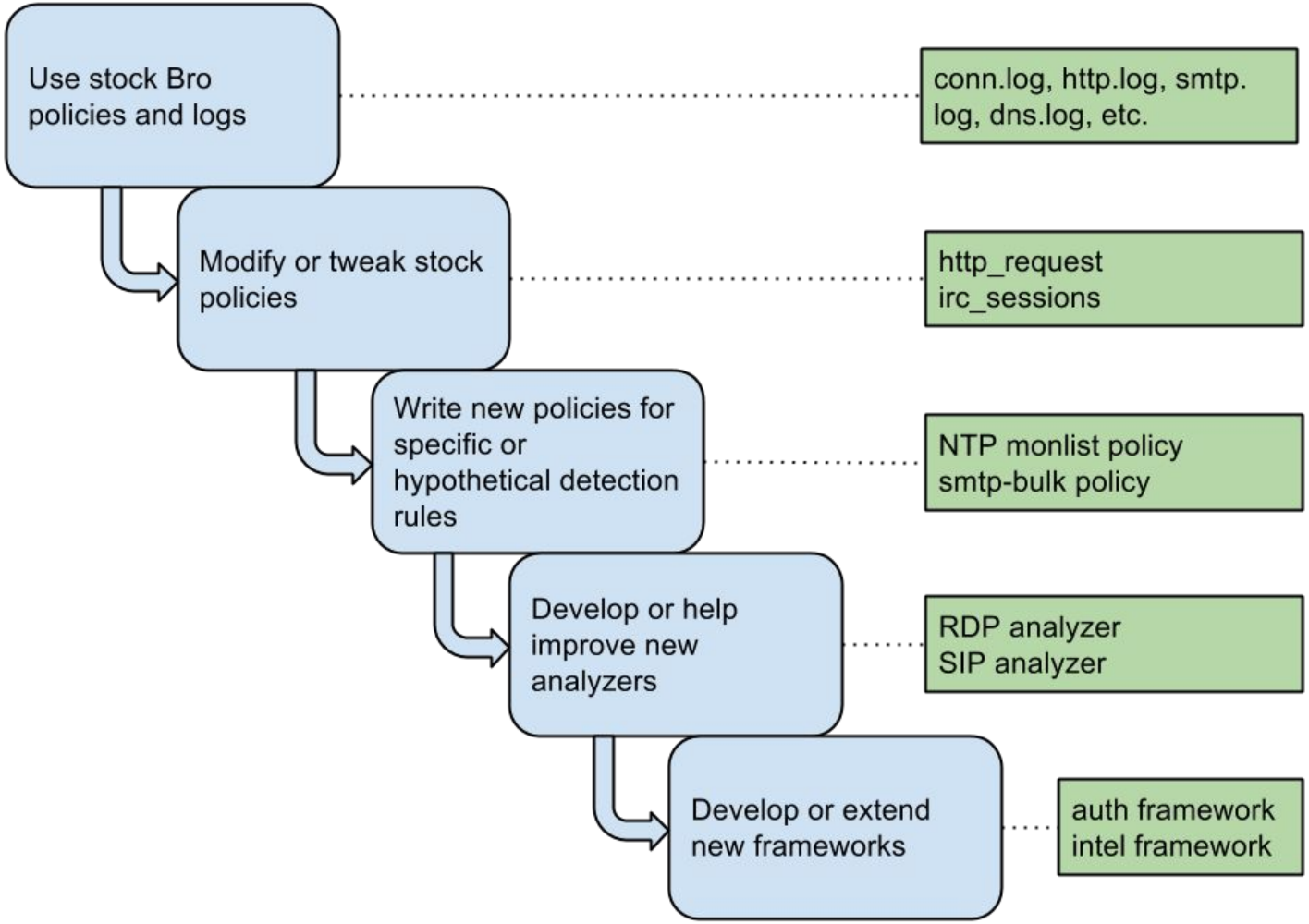
FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the Suricata alert
uid & id		Underlying connection info - See conn.log
alert.category	string	Type of attack being detected
alert.metadata	vector	All metadata keywords from signature in "name:value" format. Conveys info such as modification time, deployment location, etc.
alert.rev	integer	Revision number of signature
alert.severity	count	Seriousness of attack, with 1 being most severe
alert.signature	string	Human readable description of the attack type
alert.signature_id	count	Numeric signature identifier
community_id	string	The community ID generated by Suricata, if community ID is configured
flow_id	count	The Suricata-assigned flow ID in which the alert occurred
metadata	vector of strings	Application layer metadata, if any, associated with the alert (for example, Hostnames)
pcap_cnt	count	The PCAP record count, present when the packet that generated the alert originated from a PCAP file
rules	count	The number of rules performed to write this log entry. Used in diagnostic sessions.
service	string	The application protocol
uuid	string	The unique ID for the log record
tx_id	count	The Suricata-assigned transaction ID in which the alert occurred

Encrypted Traffic collection

AVAILABLE WITH CORELIGHT

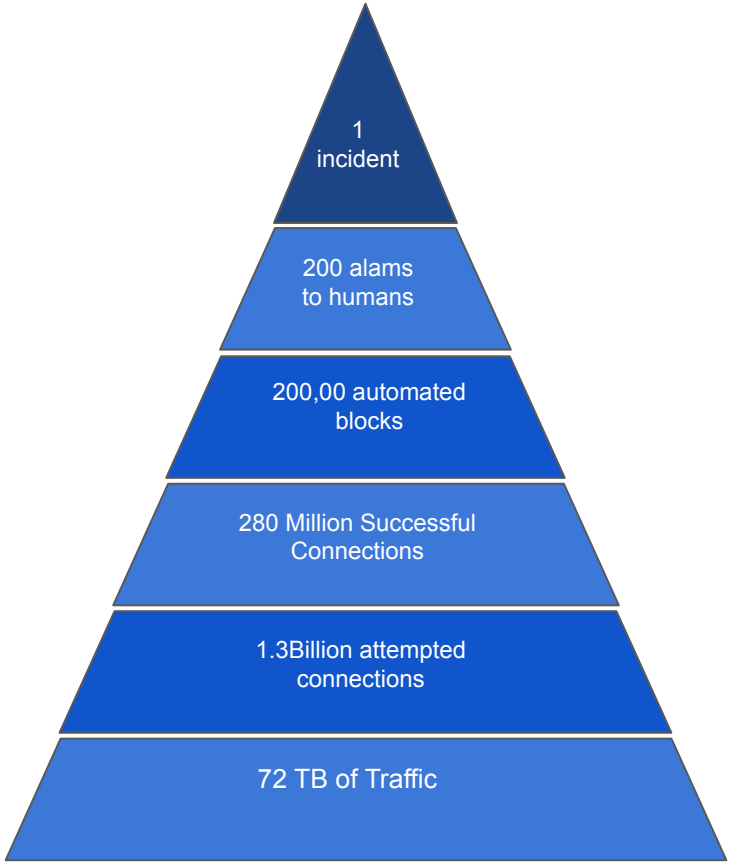
Packages

PACKAGE	DESCRIPTION
Cert Hygiene	Tracks risk indicators in TLS traffic, such as newly-minted certificates, expiring certificates, and weak encryption keys
Encrypted DNS	Flags known servers that use encrypted DNS traffic
Encryption Detection	Tracks and logs information regarding the visibility of transport flows


Use stock Bro policies and logs
conn.log, http.log, smtp.log, dns.log, etc.
Modify or tweak stock policies
http_request
irc_sessions
Write new policies for specific or hypothetical detection rules
NTP monlist policy
smtp-bulk policy
Develop or help improve new analyzers
RDP analyzer
SIP analyzer
Develop or extend new frameworks
auth framework
intel framework

Network and Monitoring Environment

Devices:	20,000+ (one of everything) A lot of "Cloud" usage
Users:	6000+
Network:	IPv4: 2 x Class B's IPv6: 3 x /64
Links:	100G and multiple 10G
Core Tools:	Zeek IDS (80G daily logs) Network Flow (35G) Central Syslog (15G)
Endpoints:	Most endpoints are unmanaged BYOD is standard



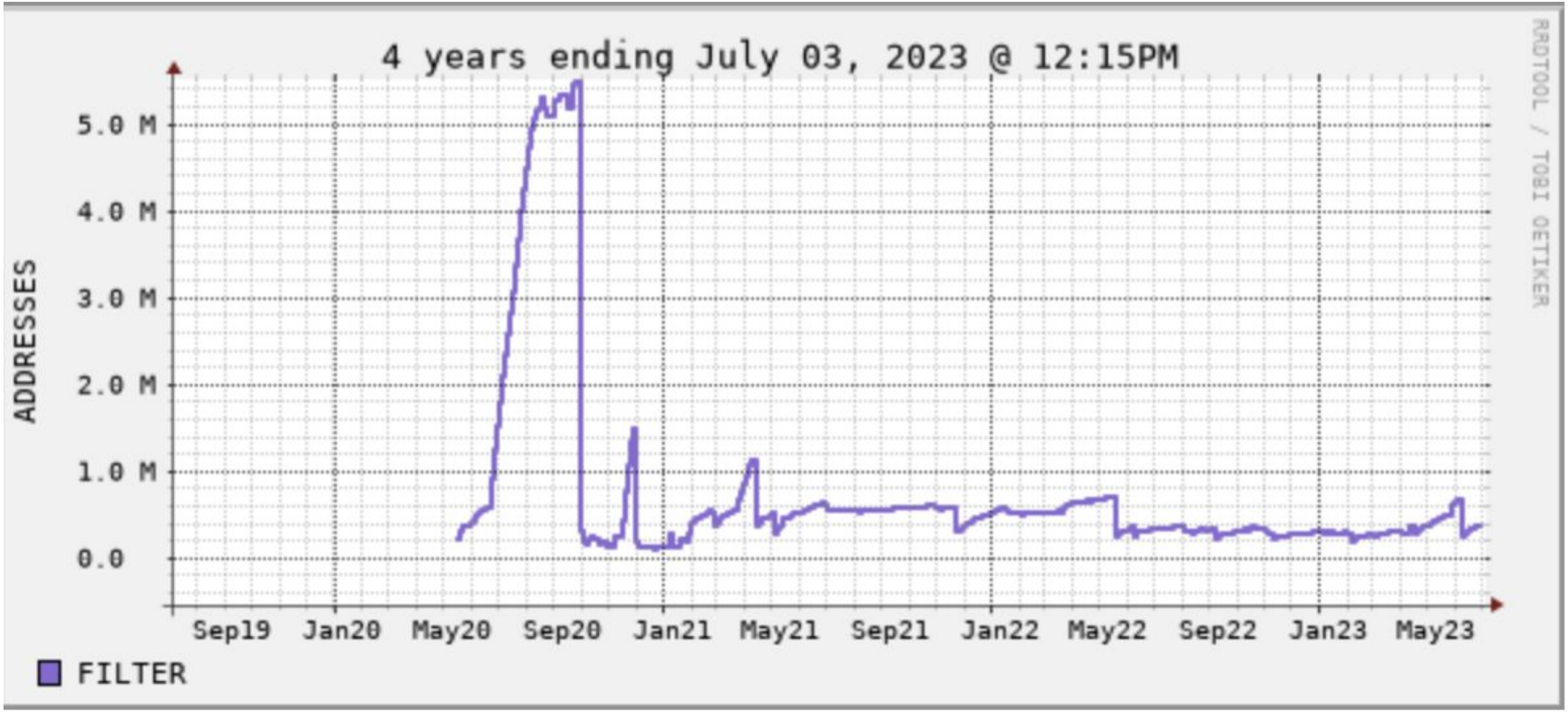
Strategies* for scan/reconnaissance detection

Heuristics	Descriptions
Summary statistics	Number of IPs in time OR Number of ports in time
Signature Based	Metasploit signature
Behavior Based	Nmap scans start with 80/TCP, 443/TCP, ICMP
Probabilistic models	Threshold Random Walk (Fast Portscan Detection Using Sequential Hypothesis Testing)
know_your_network_approach	● Knockknock ● Landmine (DarkNet Space) ● Blacklist Escalations

* https://github.com/initconf/scan-NG.git

Identifying and blocking “attacks”

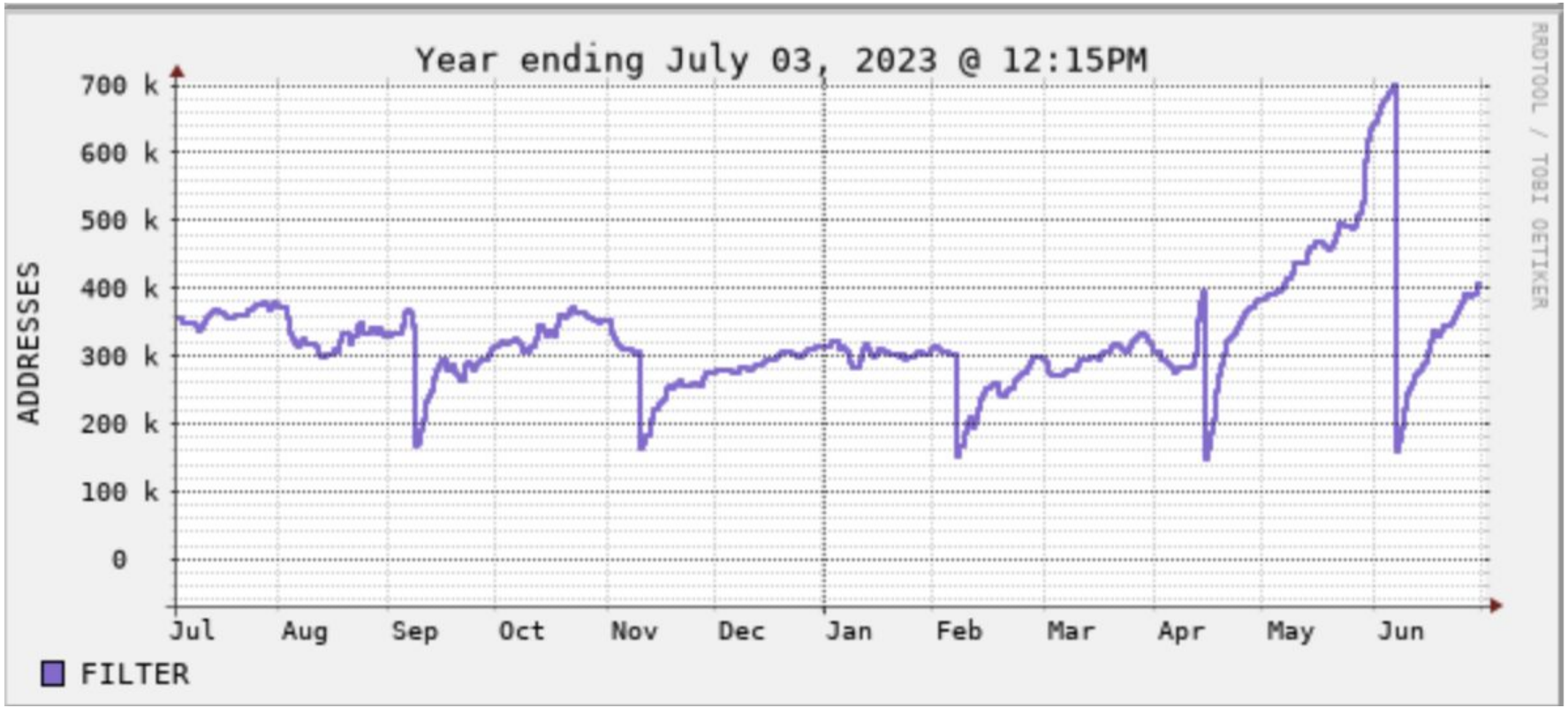
blocks

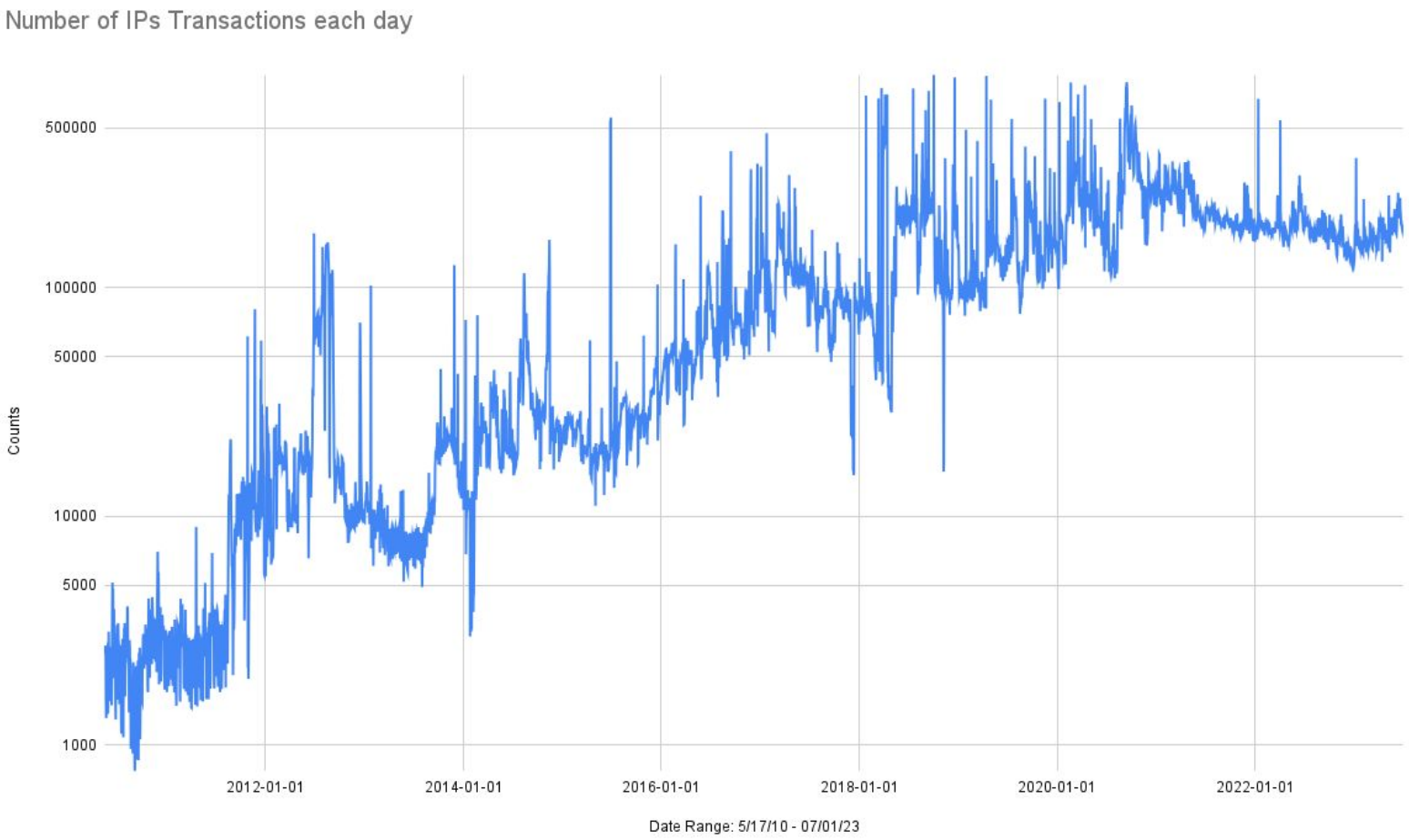


Strategies*

Strategy	Description	Effects
Catch-n-release	A home grown system of prioritizing block removals	10,000,000 (800K at any given time)
Subnet level blocks	Block entire subnets if meet certain criteria of badness	5,000
TCP Syn Flag blocks	Port specific blocks based on TCP flags	500,000 - 1,000,000
Corsa Filters	Ability to block entire IPv4 Space	4.2 Billion IPs

blocks


Year ending July 03, 2023 @ 12:15PM
ADDRESSES
700 k
600 k
500 k
400 k
300 k
200 k
100 k
0
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
FILTER
RRDTOOL / TOBI OETIKER


Number of IPs Transactions each day
500000
100000
50000
10000
5000
1000
Counts
2012-01-01
2014-01-01
2016-01-01
2018-01-01
2020-01-01
2022-01-01
Date Range: 5/17/10 - 07/01/23

Year Added	Era	Controls	Definition	Volume (as of 2023)	Primarily Subject to	driver/in response to
2022	clouds	Logs and shields	Ability to block entire IPv4 space	300-600K / day	Remote IPs	Huge reconnaissance Activity
2019	Monetization	Filters	Ability to block entire IPv4 space	300-600K / day	Remote IPs	Huge reconnaissance Activity
2017	IoT botnets	TCP syn port blocks	Block a port if syn originating from ext-dmz	300-600K / day	Remote IPs	Huge botnet activity
2017	SSH/Phishing	MFA/OTP	Two factor auth	~8-10K/day	Authentication	Compromised credentials
2016	Phishing	GAM removal	Delete emails on google server	~1 / 3-6 months	EMAIL	Phishing
2011	Drive-by-downloads	RPZ	Response Policy Zone	10-100’s / day	All LBNL hosts	Drive by downloads and phishing
2008	SSH credential theft	iSSHD	Instrumented SSH	~1 / month	HPC and Supercomputers	Compromised ssh credentials
2006 2013 operational	Worms/botnets	BGP Nullroutes	Block rule for dropping Packets that match	~ 200K / day	Remote IPs	Remote Scanners Malicious activity Blacklisted IPs Repeated offenders
2004	Worms/botnets	Denyboot	Stop giving out DHCP leases	3-10/day	Internal MAC	Malware Infections, Copyright
2004	Inflationary Period	DHCP Jail (isolation)	Redirections to a notification server	10+/day	Internal MAC	People not fixing vulnerabilities Nimda/code red
1994	Early Incidents	ACLD Drop	ACL at the border	Rare (may be 1/month)	Internet	Internet attacks

Uses of network monitoring at LBNL

1. Visibility - know your network
2. Dynamic firewall
3. Identifying vulnerable software
4. Forensics and reconstruction of events
5. Capacity planning
6. Policy enforcements
7. Instrumented SSH
8. Protecting VoIP systems
9. Detections and protection against Phishing attacks
10. Wireless monitoring

The Reality of Cyber Security Operations

- No perfect protection
  - Miscreants are always one step ahead
  - **Acknowledging this improves protection!**
- Know your network
- Hire good sysadmins (or train the bad ones)
- Credential stealing is not just an SSH problem
  - Windows, Facebook, Gmail, banks, etc.
- Mutual Cooperation is super beneficial

Questions

security@lbl.gov

asharma@lbl.gov