

Lawrence Berkeley National Laboratory

LBL Publications

Title

Zero Trust, and verify - Zeek

Permalink

<https://escholarship.org/uc/item/97n430p3>

Author

Sharma, Aashish

Publication Date

2022-10-12

Copyright Information

This work is made available under the terms of a Creative Commons Attribution License, available at

<https://creativecommons.org/licenses/by/4.0/>

Peer reviewed

Zero-Trust... before it was a Buzzword!

Aashish Sharma
Lawrence Berkeley National Lab

ZeekWeek - 2022, Austin, TX

"Zero-Trust, and verify" - Zeek

Aashish Sharma



U.S. DEPARTMENT OF
ENERGY



**UNIVERSITY OF
CALIFORNIA**



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 (2 this year)**
 - **63 members of the National Academy of Sciences (~3% of the Academy)**

LAWRENCE BERKELEY NATIONAL LABORATORY NOBEL LAUREATES



Founder,
Ernest Orlando
Lawrence
Physics, 1939

Honoring men and women from all corners of the globe for outstanding achievements in physics, chemistry, medicine, literature and peace...



Glenn T. Seaborg
Chemistry, 1951



Edwin M. McMillan
Chemistry, 1951



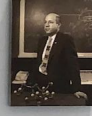
Owen Chamberlain
Physics, 1959



Emilio G. Segrè
Physics, 1959



Donald A. Glaser
Physics, 1962



Melvin Calvin
Chemistry, 1961



Luis W. Alvarez
Physics, 1980



Yuan T. Lee
Chemistry, 1986



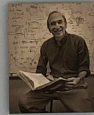
Steven Chu
Physics, 1997



George
F. Smoot III
Physics, 2006



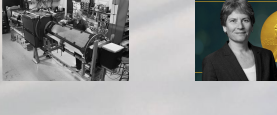
Intergovernmental Panel on
Climate Change
Peace, 2007

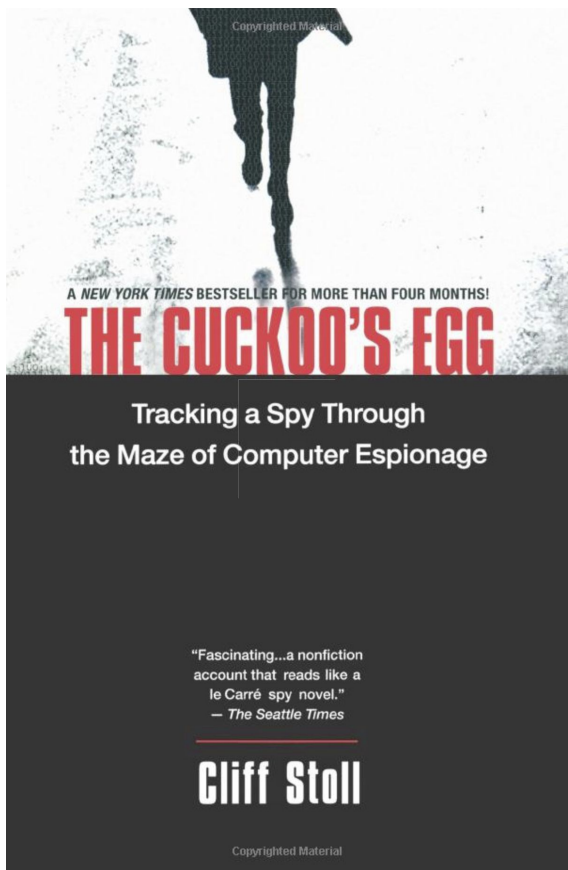


Saul Perlmutter
Physics, 2011



Jennifer Doudna
2020





Zeek Week 2022

Network utilities from Site

- traceroute
- libpcap
- tcpdump

Zeek Network Security Monitor



Zero Trust | BERKELEY LAB

About this talk

- What is Zero-Trust ?
- When Zero-trust was not even a buzzword
 - Looking at fundamental design goals of Zeek
 - Looking at LBL's Network Security Philosophy
 - How Zeek's usage naturally evolves into some aspects of Zero-Trust
- Zero Trust security models - specifically the Networking Pillar
- How Zeek can play a crucial role in enabling various tenets of Zero-Trust.
- At the end of this talk we focus on Zeek's challenges in optimal zero trust implementation and discuss possible workarounds.

What exactly is Zero-Trust ?

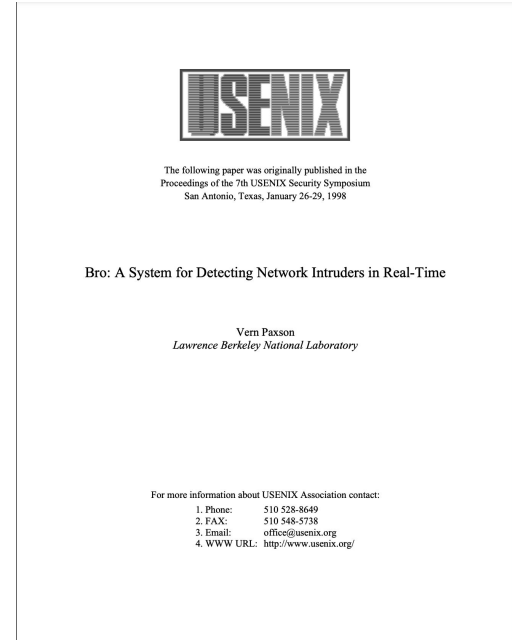
Lot of literature, lots of Reference Architectures documents, lots of material - Air Force definition* seems to resonate more with us:

Zero Trust is data/application access strategy that assumes all resource request originates from untrusted sources. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.

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**



From the very beginning ...

Design goals and requirement of Zeek:

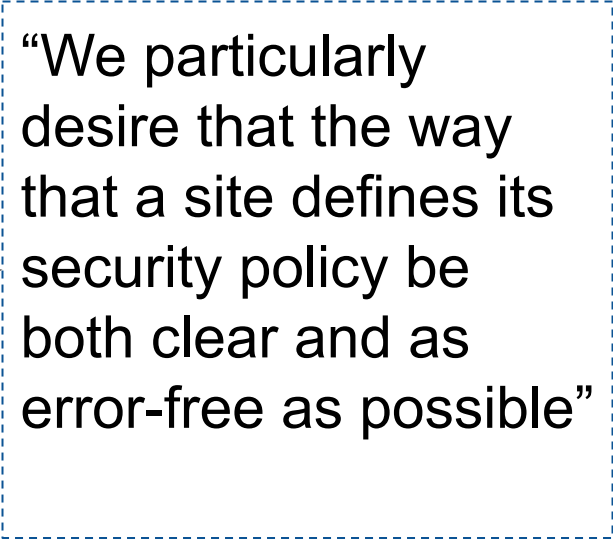
- High-speed, large volume monitoring
- No packet filter drops
- Real-time notification
- **Extensible**
- **Avoid simple mistakes**
- **Mechanism separate from policy**
- **The monitor will be attacked**

“... 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**

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**

Big Picture

- Zeek a continuous network monitoring tool
 - Network flight recorder
- The design goals weren't written back in 1999 Usenix paper keeping Zero-Trust in mind but now in 2022 one cannot help but realize that these goals continue to be relevant with (new?) architectures/buzzwords/paradigms

1993 Berkeley Lab Cyber Security*

Design Principles

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

*Slide 2, Krous, Jay, "Zero Trust at Berkeley Lab", July 2021

1993 Berkeley Lab Cyber Security*

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 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 and not configuration mgmt.

Tenets of Zero trust + Our Cyber Security

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 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 and not configuration mgmt.

Tenets of Zero Trust

- **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.**

Zeek comes into play ...

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 Strategies

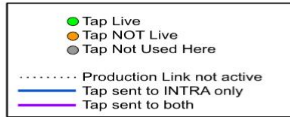
- **Pervasive Visibility without disruption**
- Be the attacker
- Resist temptation to centrally secure
- Avoid tight coupling and high consequence events
- Isolate higher risk activities from open science
- **Accept transient compromise: monitor, detect, resolve**
- **Spend the next dollar on detection/forensics and not configuration mgmt.**

Tenets of Zero Trust

- **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.**
- **All data sources and computing services are considered resources.**

Zeek?

Pervasive Visibility::Internal Taps



INTRA Tap Agg Tapped Production Links

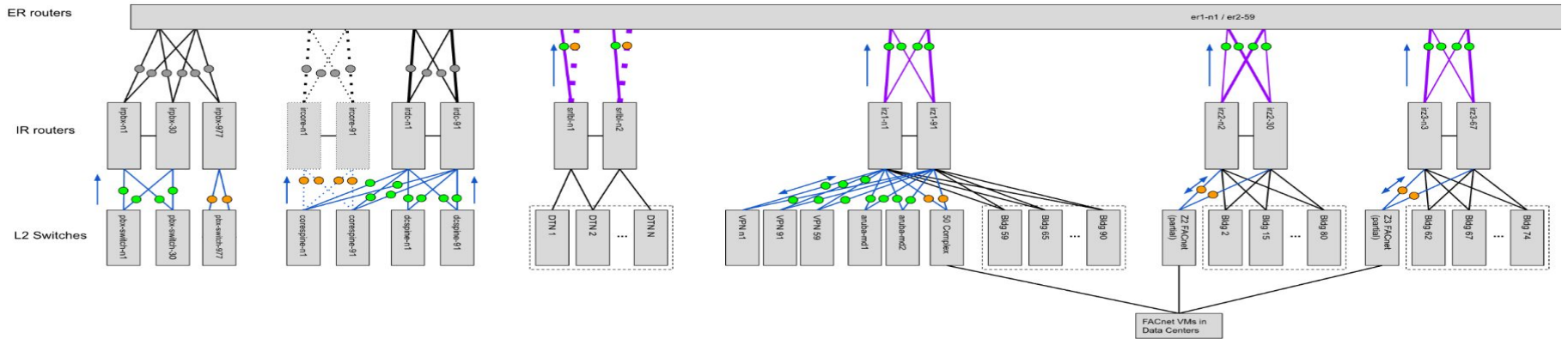


Diagram by Michael Smitasin, LBNL

We are not there yet ... Can Zeek be a tool for (i) implementation (ii) enforcement of Zero-Trust ?

For implementation of Zero Trust Capabilities

1. Know your network ← Zeek is very good at this

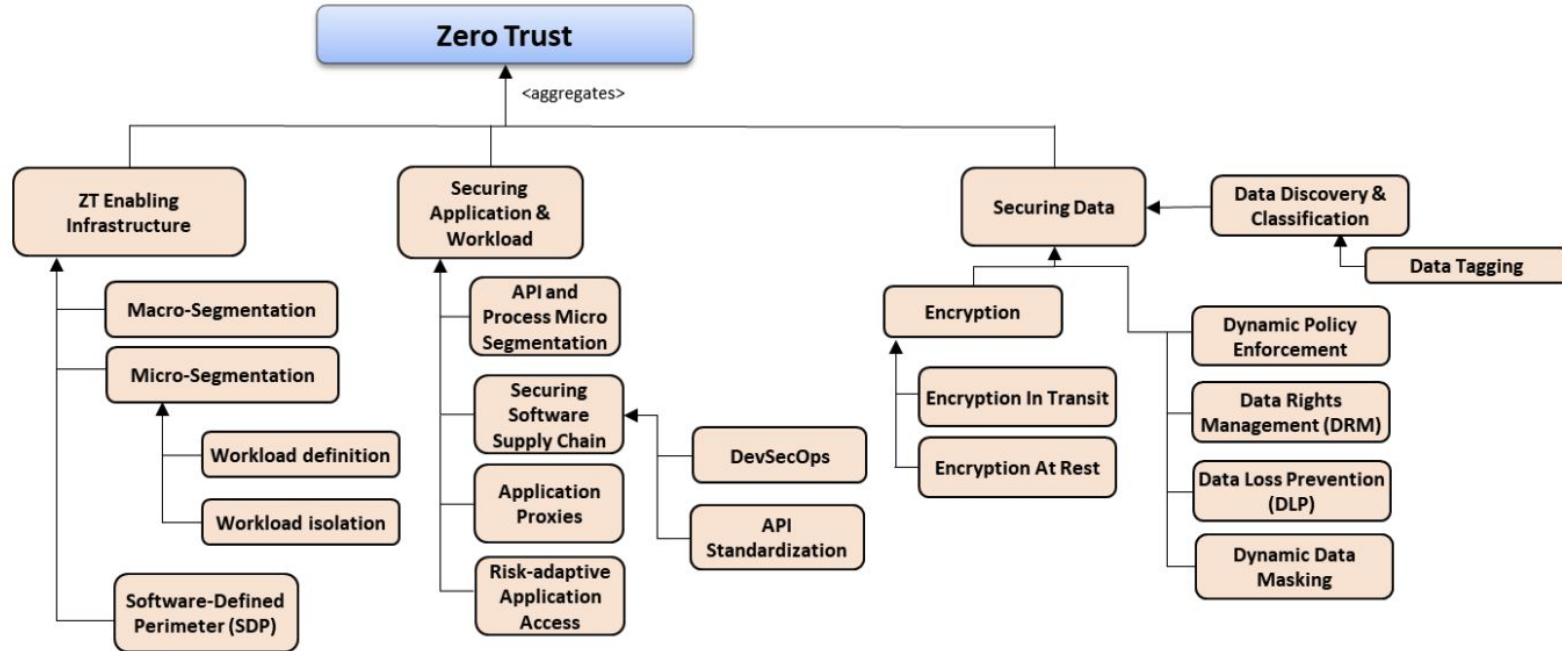
- a. Visibility of who, when, what and how:
 - i. Data - file analysis framework, SMB analyzer, ?
 - ii. Applications - software.log
 - iii. Computational resources - ??
 - iv. Users - auth framework ?
 - v. Privileges - ??

2. Quality of information

- a. Zeek can be instrumental in guaranteeing that quality
- b. Achieve comprehensive inventory of devices, applications, access methods and data flows

Zero Trust Infrastructure, Workload and Data Capability Taxonomy

Image: Page 28 DoD Zero trust Reference Architecture [1]



How Zeek can be relevant

- Encryption in transit
 - Zeek cannot see inside but zeek can definitely tell if its a Cipher, weak cipher or what is the state of encryption - Policy enforcement
- Data discovery and classification
 - Data tagging and identification
 - Not much available but we can definitely explore here
- Data loss prevention

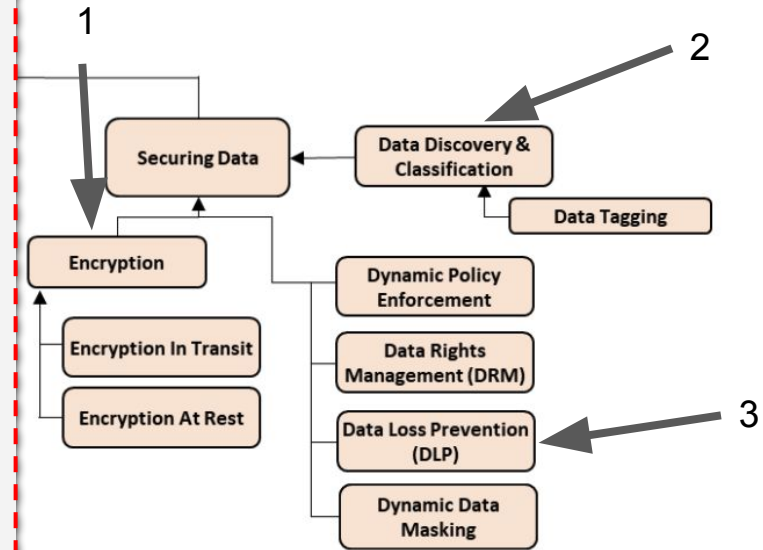


Image: Page 28 DoD Zero trust Reference Architecture [1]

Data Loss Prevention(DLP)

- Zeek used to detect and Prevent unwanted presence of sensitive data by use of certain policies to categorize and identify specific information
 - CUI / OOU in our case - Emails are over TLS
 - Question: How do you get visibility then ?
- One can use zeek to
 - Categorize data
 - DoD guidance on data marking is: visible, accessible, understandable, linked, Trustworthy, Interoperable, Secure, Extensible
 - Understand how your data is moving around and/or if at risk
 - Internal cluster : SMB protocol analyzer
 - Monitor data movements
 - Byte sizes ?
 - Develop controls to keep enforcement checks

Visibility in Zero Trust Era

According to **NIST 800-207** Zero-Trust tenet:

All communication is secured regardless of network location

NIST-800-207 also notes as Zero-Trust tenet:

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.

Yes Both are doable ... at least in some cases

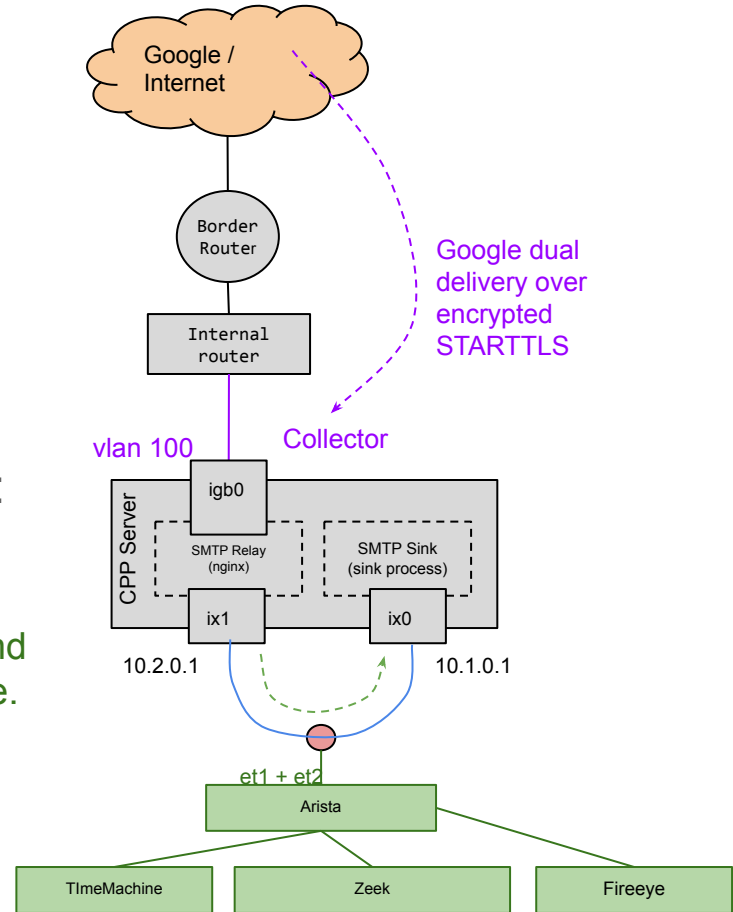
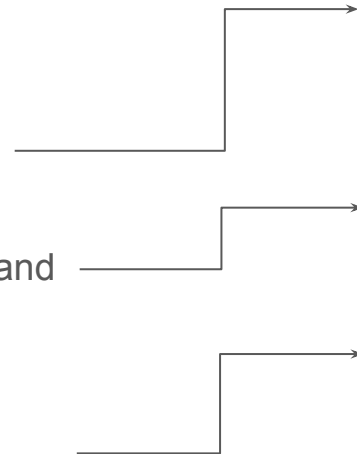


Diagram by Michael Smitasin, LBNL

Zero Trust

- Attribute Based Access Control
- Behavioral based
 - User and Entity Behavior Analytics
- Device Hygiene
 - Continuous, Automated, Inventory and Telemetry
 - Status Scans & Dynamic Instrumentation
 - Dynamic Device Service Updates
- Just-in-time Authorization
- Privileged Access Management



Zeek

- Authentication Framework
- Monitor / profile user activity

- known-hosts, known-services,
- conn.log
- software.log

- Institutional Services
- Host profiling

Visibility & Analytics + Automation & Orchestration

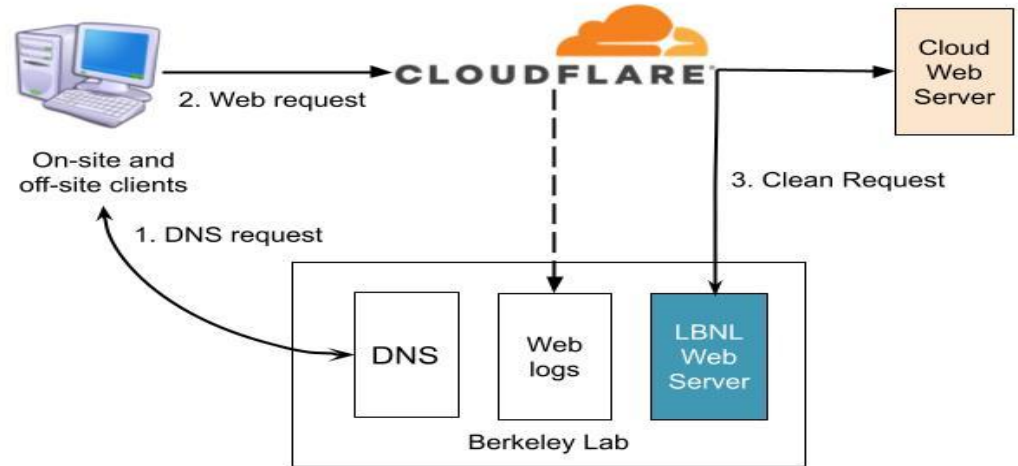
- Advance visibility - we've talked about this
- Proactive response
 - Deployment Automate defences
 - Eg. Dynamic firewall, Just-in-time blocking capability
 - May be Just-in-time whitelisting ?
- Solid data -> robust analytics
- Anomaly detections
 - Capability for advanced heuristic development
 - ML?

Adapting to the new world of Zero-Trust

- “Pillars of Zero Trust”
 - Identity, Device, Data, Network, Applications
 - Visibility ? Logs ? Input-framework ?
- Visibility into and enforcing attributes based authentication and access controls
- No concept of “approved” characteristics to distinguish between authorized and unauthorized users/data/systems/resources etc for enforcement and/or monitoring
- No defined perimeter anymore - hosting on premises and/or cloud - software defined perimeter ?

When the Network isn't even "Network"

- Zero Trust: Software Defined Perimeter (SDP)
 - Cloudflare front-ends on-site and Cloud web servers



Adapting to the new world of Zero-Trust ...

- Endpoints aren't on the network in the traditional sense
- Transit communications are encrypted
 - DHS requirements of : DoT (DNS over TLS), DoH (DNS over HTTPS)
- User activity analytics not straightforward
- Current monitoring won't detect a compromised system until it connects on the network/VPN
- Data discovery, data access, modifications
- Network devices security

Thoughts?

security@lbl.gov

asharma@lbl.gov

References:

1. Department of Defense (DoD) Zero Trust Reference Architecture
[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v2.0\(U\)_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)
2. Zero Trust Reference Architecture Overview, US Air Force
3. Krous, Jay, “Zero Trust at Berkeley Lab”, July 2021
4. Zero Trust Architecture, NIST Special Publication 800-207

Visibility::Logs






- Collect any and all logs
 - keep them forever, because we can
 - multiple uses: operations, learning, forensics, research, etc.
- Examples:
 - syslog (from thousands of computers)
 - arp data from switches (every 10 minutes)
 - web servers logs (thousands from Cloudflare)
 - mail logs from Google Workplace
 - dns queries (every query ever done, forever)
 - centralized authentication logs
 - VOIP system logs
 - firewall logs
 - domain controller logs

Visibility::Know your network

- We know what internal flows look like
 - flag what is not normal (anomaly detection)
 - internal developed detection is better than vendor offerings
 - demonstrably successful detection internal scanning
- Cyber security incidents are inevitable
 - working assumption: there is a compromised computer
 - detect quickly, remediate, move along (no mission impact)
 - spend the next dollar on detection, not configuration management
- Analytics examples
 - script to correlate authentications to MAC address over time
 - "live" open services and vulnerability data

Maturity of **networkZERO**
DAF Zero Trust

Governance
Automation & Orchestration
Visibility & Analytics

Zero Trust Maturity <i>How advanced are the capabilities within each pillar?</i>	Application & Workloads 	Data 	Identity (ICAM) 	Device 	Network & Environment 
Basic Security & Access	<ul style="list-style-type: none"> Data Center Segmentation Cloaked applications Application Visibility & Access (Anytime, Anywhere) 	<ul style="list-style-type: none"> Critical Data Tagging Cloaked data RBAC 	<ul style="list-style-type: none"> Basic Cybersecurity Access Policy CAC MFA Privilege Access Management 	<ul style="list-style-type: none"> Cloud-based baseline enforcement HW & SW Inventory Compliance enforcement 	<ul style="list-style-type: none"> Software Defined Perimeter (Access to Applications and Data) On premise and off premise Mutual TLS
Intermediate Automated Management	<ul style="list-style-type: none"> Application/host Micro-Segmentation 	<ul style="list-style-type: none"> Semi-automated Data Tagging Data Loss Prevention 	<ul style="list-style-type: none"> Enhanced Cybersecurity Access Policy Single Identity Platform Alt. MFA RBAC for policy creation 	<ul style="list-style-type: none"> Domain-less environment Cloud-based automatic detection and response (SOAR/EDR/XRD) Cloud-based Software deployment & management 	<ul style="list-style-type: none"> Cloud Migrations API Integration Common service access Cloud Management & Control (CASB)
Advanced Cyber Ops Integration	<ul style="list-style-type: none"> Service-layer Segmentation Nano-Segmentation IoT Segmentation 	<ul style="list-style-type: none"> Fully-automated Data Tagging via ML/AI DLP encryption and tracking ABAC 	<ul style="list-style-type: none"> Continuous and adaptive authentication and authorization In-session monitoring Transparent authentication to all services 	<ul style="list-style-type: none"> Fused multi-source intelligence for endpoint response 	<ul style="list-style-type: none"> Cloud hosted & Globally Fully encrypted traffic

Network And Environment: Current

- Micro-segmentation
 - many small VLANs, /29 is common
 - not for security boundaries, to force a Layer 2
 - netflow and across a tap
 - examples: bastions different than resources, VMware management different than guests, each FMCS vendor
- Isolate higher risk activities
 - enclave for business systems with PII
 - no direct access: privileged via bastions, users via Cloudflare
- Cloud migrations completed
 - Email and office productivity (Google Workspace)
 - HR system and Recruitment (UCPath and Taleo)
 - Ticketing (Service-now)

34

Automation aspects of zeek

Network And Environment: Future

- Pockets of immaturity
 - we still have a VPN
 - firewalls all around the Lab
 - trusted IPs and networks defined
 - many on-site only resources (SMB, NFS, etc.)
- The Northstar: no difference if you're inside or outside our network
 - reduce on-site as an access control
 - VPN still used to protect remote clients
- Continue to expand existing strategies
 - Cloudflare for web Software Defined Perimeter
 - Cloudflare Access for other protocols

1993 Berkeley Lab Cyber Security*

Design Principles

- Enable science
 - Open by default
 - Platform neutral
- Risk based
- Data and research based
- Active, responsive, and continuous
- This is a dynamic process that doesn't fit in compliance wrapper

Design Strategies

- Pervasive visibility without disruption
- Be the attacker
- Resist the temptation to centrally secure, avoid tight coupling and high consequence events
 - Isolate higher risk activities from open science
- Accept transient compromise: monitor, detect, and resolve
- Spend the next dollar on detection/forensics, not config mgt.

DOD

- Assume a Hostile Environment. There are malicious personas both inside and outside the network.
- Presume Breach. Consciously operate and defend resources with the assumption that an adversary has presence within your environment.
- Never Trust, Always Verify. Deny access by default. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.
- Scrutinize Explicitly. All resources are consistently accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources

800-207

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- 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.



2022: Where are we now

Design Strategies

- Pervasive visibility without disruption
 - Be the attacker
 - Resist the temptation to centrally secure, avoid tight coupling and high consequence events
Isolate higher risk activities from open science
 - Accept transient compromise: monitor, detect, and resolve
 - Spend the next dollar on detection/forensics, not config mgt.
- Zeek used for pervasive visibility (*Continuous monitoring*)
 - Vulnerability Scanning and pen-testing
 - Risk acceptance/mitigation
 - Limit the spread / containment

Zeek in the Zero Trust Era:

Zeek environment and capabilities aligns with the goals of Zero-Trust

- **Data and research based**
- **Active response and continuous monitoring**
- **Dynamic process that does not fit in compliance Wrapper**

- **Pervasive Visibility without disruption**
- **Accept transient compromise: monitor, detect, resolve**
- **Spend the next dollar on detection/forensics and not configuration mgmt.**

- **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.**

Designing the zeek road map for future -think of these angles here

How zero trust - makes it hard for zeek

Challenge people in the group - zeek becoming less effective

Protocol analyzers make it hard when all is encrypted.

Encrypt everything but how we get visibility
ZEEK SMTP logs - google dual delivery

End points are remote

EDR -

Users are remote

Cloud is remote

DHS - encouraging DoT and DoH - what will zeek do there