Symmetric Key Intercept
for TLS1.3 (and Legacy) Decrypted Visibility

Steve Perkins
CMO and Head of Product

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

NUBEVA
www.nubeva.com

WHAT WE DO

Develop and License Software for

SYMMETRIC KEY INTERCEPT

A New Approach for TLS Decrypted Visibility

IMPROVED/RESTORED FUNCTIONALITY
Unlock ALL Traffic
TLS 1.3 (and Legacy) Inline and Passive

HIGHER PERFORMANCE
>10X Performance Throughput & Latency

SIMPLIFICATION
Architectural and **Operational**

INCREASED CAPABILITY

LOWER CAPEX and OPEX

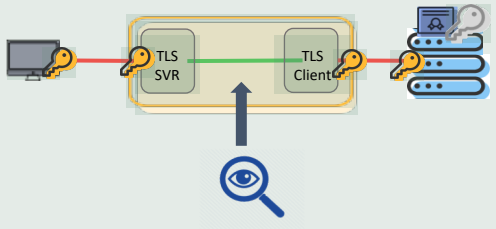
PROBLEM WE ADDRESS

ORGANIZATIONS NEED VISIBILITY INTO TLS

BUT **TRADITIONAL METHODS HAVE <u>GROWING</u> ISSUES**

Limited Capability – Price/Performance/Scaling - Complexity

Man-in-the-Middle

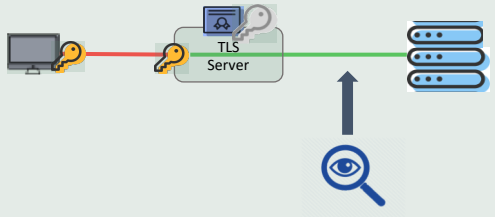


Blind Spots
- Pinned Certificates
- "Difficult" Protocols/Apps

Performance / Cost
- Throughput + Latency

Industry Moves To Thwart

Termination

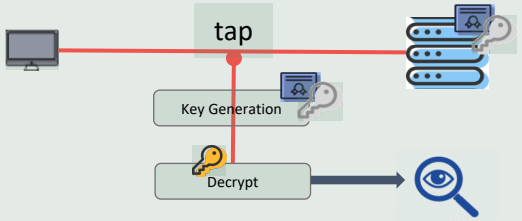


Security / Regulatory
- Exposes cleartext

Certificate Management/Security

Limited Use
- Not for Client-Side Connections
- Not Ideal Microservices/Service Mesh/Cloud

Handshake Replay



Does Not Work with Diffie-Hellman/PFS!!
- In TLS 1.3 and 1.2 (~90% of all traffic)

Limited Use - Requires Server Keys
- Not For Traffic To 3rd Party Servers e.g. Cloud, Internet, Suppliers

Certificate Management/Security

RETHINKING THE PROBLEM

Decryption is Easy and Efficient…

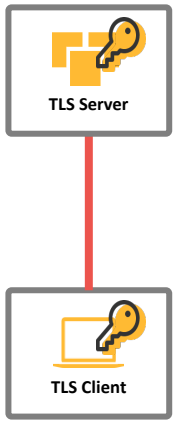
IF You Have the Session Keys!

WHAT IF…

YOU COULD GET THE SESSION KEYS **ANOTHER WAY?**

FACT

Symmetric Keys Exist
In Servers' and Clients' Memory
During The Session



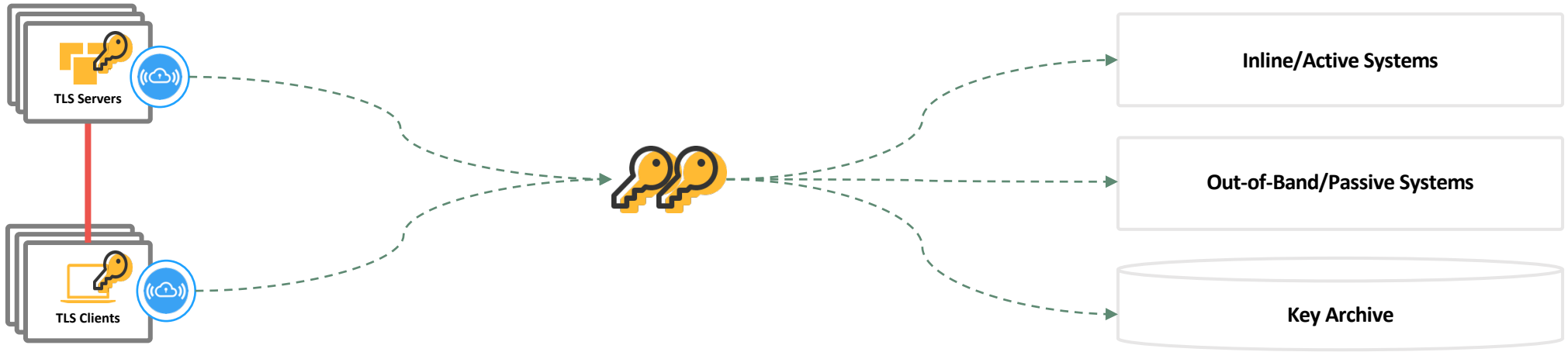
IDEA

Capture and **Re-Use**
Symmetric Keys
To Fuel Visibility Systems

And Make It
Commercially Viable
Reliable – Secure – Scalable
Non-Disruptive – Easy - Economic

THE NEW SOLUTION

SYMMETRIC KEY INTERCEPT (SKI)



Capture and Re-Use TLS Symmetric Session Keys

from **TLS SERVER and/or TLS CLIENT Memory** in during sessions

via **Suite of Nextgen Endpoint Agents**

To Enable Decryption and Visibility Systems

KEY SENSOR TECHNOLOGY

LEARN AND EXTRACT SYMMETRIC KEYS

- From TLS Processes and Libraries In Memory
- Nubeva Patented Algorithms = Core IP

A READ-ONLY MEMORY TRACER ON TLS SERVER AND/OR CLIENT

- Cannot Change System or Alter Memory
- Requires No Changes to Application or TLS Code/Libraries

HOW IT WORKS

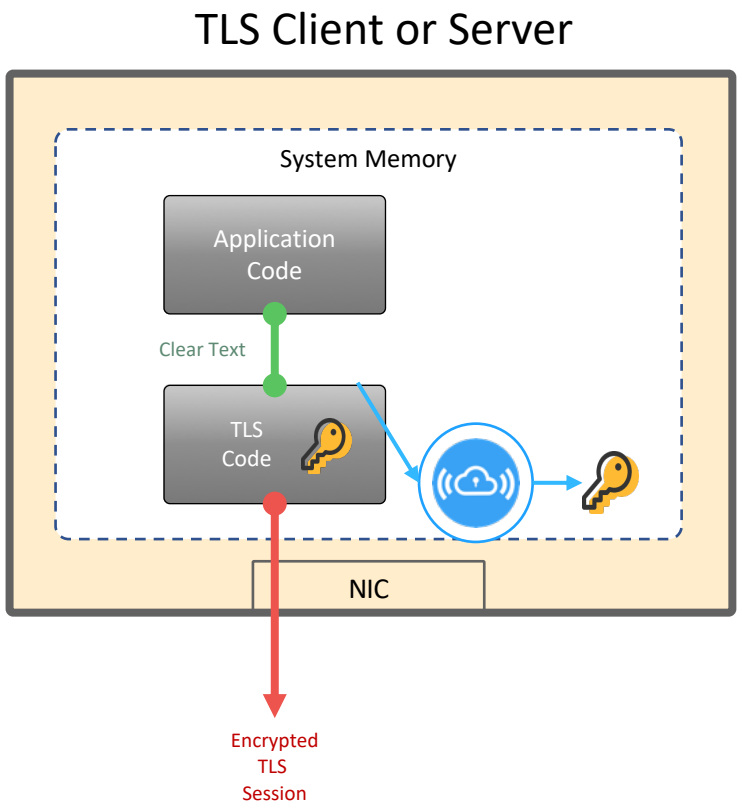
- Scan's System To Discover TLS Processes
- Loads Signatures with Discovery Algorithms
- Triggers on "Client Hello"
- Knows where Symmetric Key will be Set
- Copies and Exports It

ARCHITECTURAL ADVANTAGES

- Works for All / Independent of Protocol, Cipher, Handshake
- Easily Extensible to New Apps/Libraries/Protocols
- Only needed on 1 "side" of session (keys are Symmetric!)

HIGH PERFORMANCE + SMALL FOOTPRINT

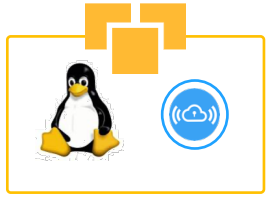
- <200 µsec extraction time
- Reference Benchmark
  - 600 keys/second, AWS C5a.XLARGE
  - <28MB Memory, <0.5% CPU Core



SUPPORTED PLATFORMS

Works With Modern Environments in Private, Public and Hybrid Clouds

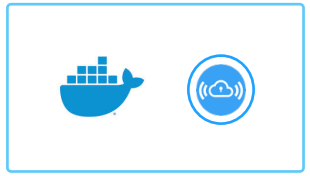
LINUX



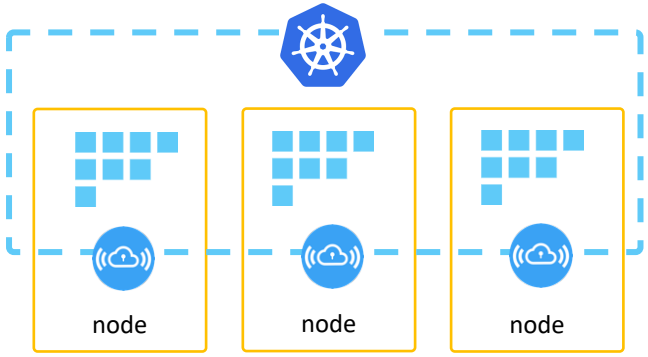
WINDOWS SERVER

WINDOWS DESKTOP

CONTAINER



KUBERNETES DAEMONSET



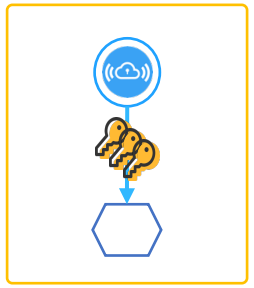
*OSX, Android, IOS In Development

KEY HANDLING

Multiple Secure Options For Key Re-Use

WRITE TO
LOCAL FILE

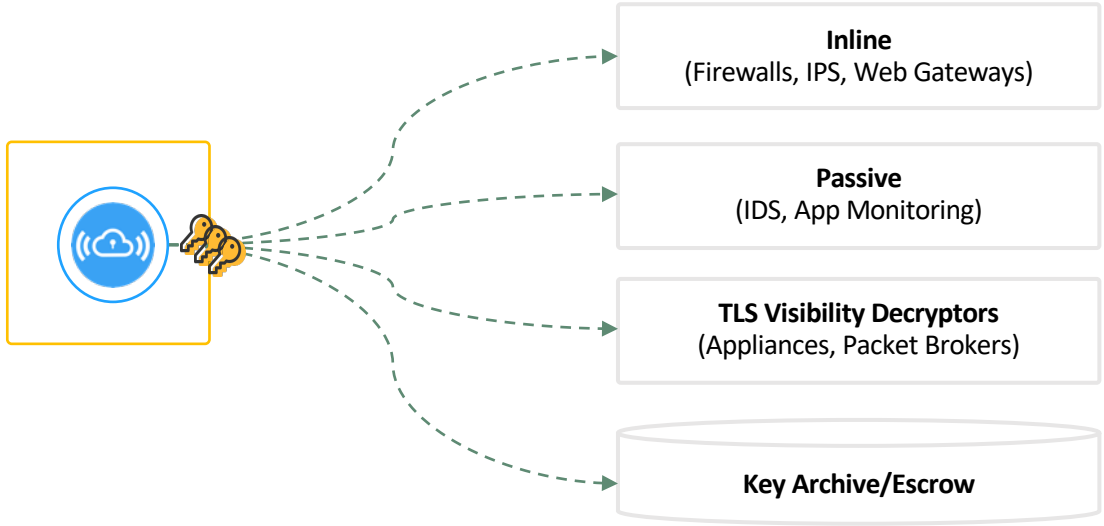
PIPE TO
LOCAL APP
Or AGENT



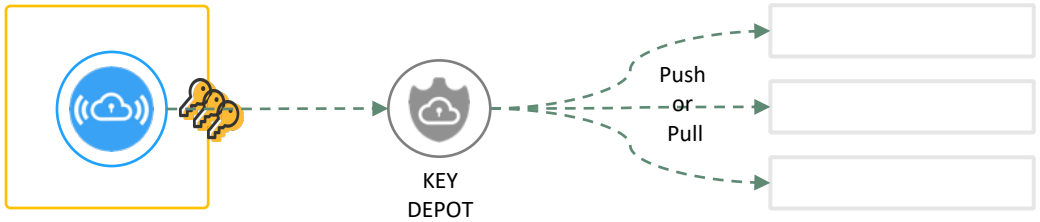
Or.. Export via

HTTP or DTLS

EXPORT TO
DECRYPTION
SYSTEMS



EXPORT TO
"KEY DEPOT"
TO AGGREGATE,
BUFFER/DISTRIBUTE
and SCALE-OUT



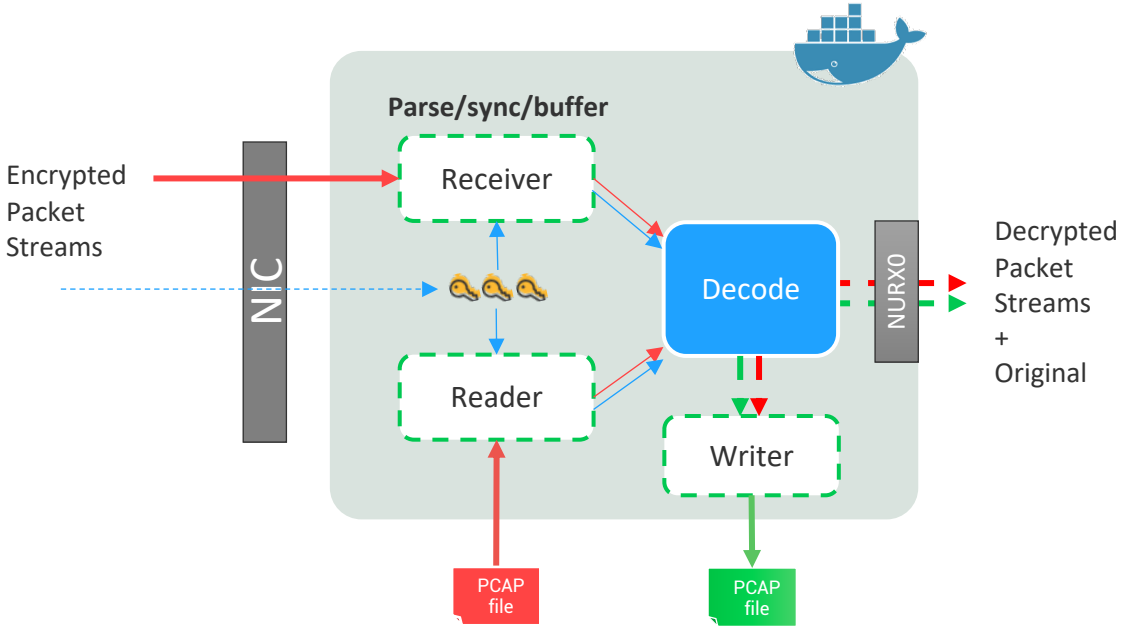
SYMMETRIC DECRYPTORS

FORM
- Container (Docker)

CORE FUNCTION
- Reads Inbound Encrypted Streams
- Buffers and Queries Key via Client Random
- Syncs and Passes to Decryption Function
- Efficient Decrypt of all Modern Protocols

OUTPUT
- Established output Interface: NURX0
- Output Original Packet, and..
- Outputs Matching Decrypted Packets
- CLI based File Reader/Decrypt Function

BENEFITS/ADVANTAGES
- Reference Solution for Symmetric Key Decryption
- Run Anywhere – Embedded or Standalone
- Scale up/down – With Parallel Operation



SWEEPING APPLICATION

SYMMETRIC KEY INTERCEPT CAN ENABLE MOST SYSTEMS AND USE-CASES

ENHANCE AND BOOST

INLINE SYSTEMS

Web GW's, NGFW, IPS/APT,
Visibility Appliances, ADCs

10x Performance Boost
See all Traffic – Including Pinned
Operational Simplicity

RESTORE AND EXPAND

PASSIVE SYSTEMS

Security and App Monitoring Tools
Visibility Appliances and NPBs

See PFS Traffic – TLS1.3, 1.2
See Into 3rd Party Traffic
Eliminate Cert/Key Complexities

CREATE AND ENABLE

GREENFIELD

Container-Container/Kubernetes,
Cloud Platforms, High Speed Links

Now Functionally Possible
Now Economically Viable
OpenSource and Commercial

WHAT WE DO

Develop and License Software for

SYMMETRIC KEY INTERCEPT

A New Approach for TLS Decrypted Visibility

IMPROVED/RESTORED FUNCTIONALITY
Unlock ALL Traffic
TLS 1.3 (and Legacy) Inline and Passive

HIGHER PERFORMANCE
>10X Performance Throughput & Latency

SIMPLIFICATION
Architectural and **Operational**

INCREASED CAPABILITY

LOWER CAPEX and OPEX