

EPICS Security Technical Plan



 A presentation of the implementation plan for EPIC Security, being carried out by SLAC, Osprey DCS and ORNL

Agenda

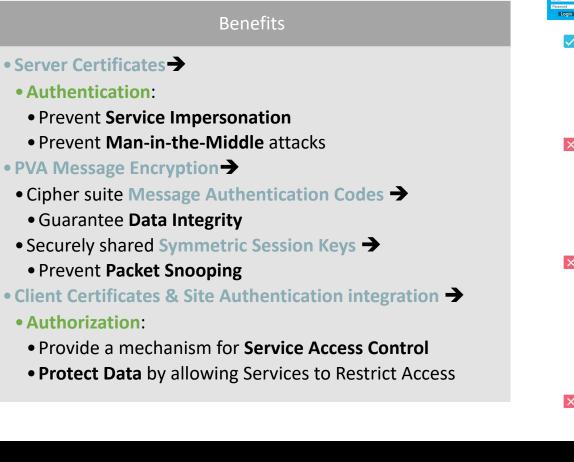
• Planned Features

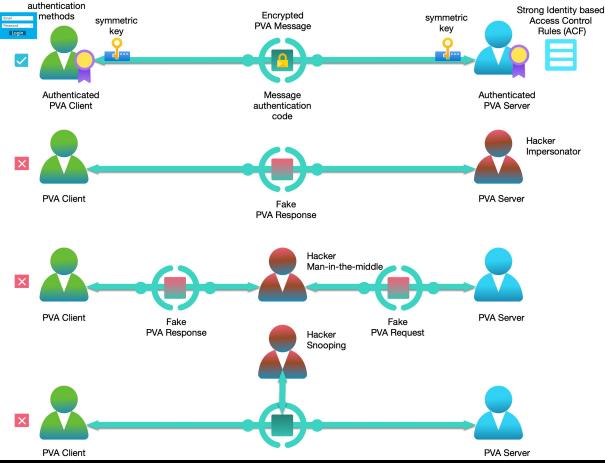
- Implementation of basic TLS
- Certificate Management
- TLS Session Status & Management
- Enhanced Client Authorization

TLS Demo

- Manually Create Certificates
- Configure Wireshark
- Non-secure PVA communications
- Configure secure PVA communications
- Demo Secure PVA communications

What this implementation will get us?







What this implementation will get us?

Benefits

- Server Certificates ->
- Authentication:
- Prevent Service Impersonation
- Prevent Man-in-the-Middle attacks
- PVA Message Encryption
- Cipher suite Message Authentication Codes →
 - Guarantee Data Integrity
- Securely shared Symmetric Session Keys →
- Prevent Packet Snooping
- Client Certificates & Site Authentication integration 🚽
- Authorization:
- Provide a mechanism for Service Access Control
- Protect Data by allowing Services to Restrict Access

Will Not

- Prevent **PV Impersonation** in a mixed TLS/TCP network
- Prevent discovery of Service Endpoint or PV name
- Prevent discovery of Encryption Type
- Prevent discovery of Data Transmission Frequency
- Prevent discovery of approximate Amount of data transmitted
- Change Site Security Policies you need to implement these on top of the technical solution presented here

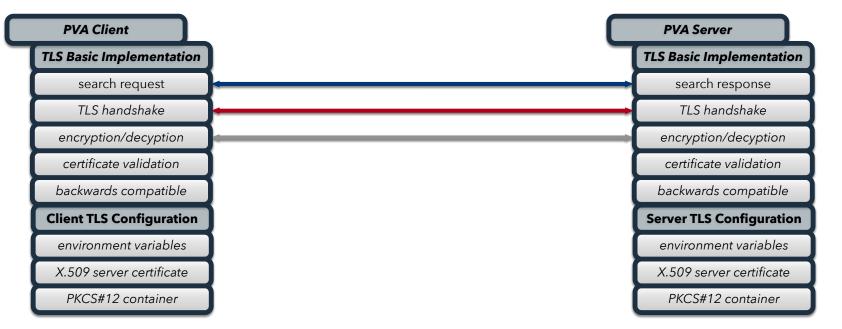


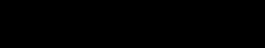
Basic TLS Implementation

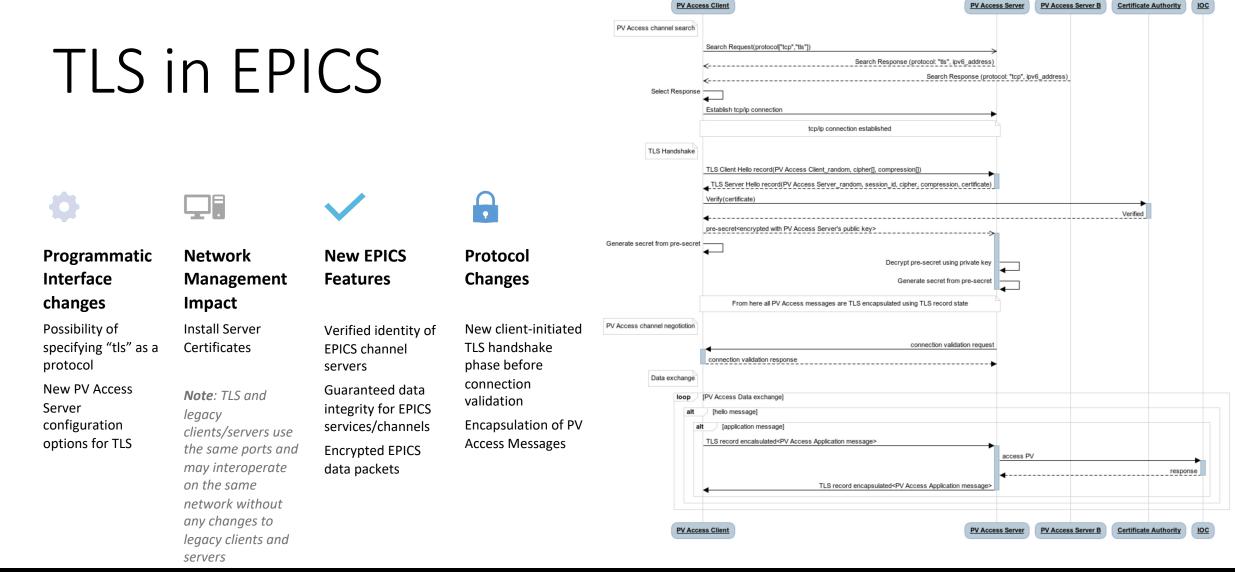
EPICS Collaboration Meeting, ICALEPCS23, Cape Town, South Africa

Basic TLS Implementation

- Allow "tls" in search request
- Allow "tls" in search response
- Initiate TLS handshake if server certificate is configured
- Pass client certificate in handshake if client certificate is configured
- Encapsulate and encrypt PVA protocol messages
- Maintain backwards compatibility









Implementation repositories

Java implementation — maintainer Kay Kasemir

<u>https://github.com/ControlSystemStudio/phoebus/tree/master/core/pva</u>

C++ implementation — maintainer Michael Davidsaver

<u>https://mdavidsaver.github.io/pvxs</u> branch TLS

Documentation

<u>https://github.com/epics-base/pvAccessCPP/wiki/protocol</u>



Out of scope

Features

Add TLS to Channel Access

UDP Broadcast search

UDP response

Beacon messages

Add additional TLS beacon messages for servers supporting both TLS and TCP

Any changes to support TLS in Gateways

Any changes to support TLS in EPICS Python (pvaPy)

Any changes to support TLS in PV Database

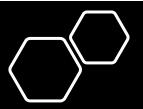
Repositories

EPICS base Java

- <u>https://github.com/epics-base/epicsCoreJava</u>
- https://github.com/epics-base/pvaClientJava

EPICS base C++

- https://github.com/epics-base/pvAccessCPP
- https://github.com/epics-base/pvaClientCPP



EPICS Collaboration Meeting, ICALEPCS23, Cape Town, South Africa

Certificate Management

Certificate Management

- Update PVA Name Server to issue client and server certificates
- Manage Site Certificate
 Authorities

PVA Client		PVA Server
S Basic Implementation		TLS Basic Implementation
search request		search response
TLS handshake		TLS handshake
encryption/decyption		encryption/decyption
certificate validation		certificate validation
backwards compatible		backwards compatible
Client TLS Configuration		Server TLS Configuration
environment variables		environment variables
X.509 server certificate	PVA Name Server	X.509 server certificate
PKCS#12 container	Certificate Management	PKCS#12 container
	issue certificates	
	PVA NS Configuration	
	environment variables	
	CA certificate	
	PKCS#12 container	





Certificate Management



Manage Site Certificate Authority

Secure Storage for Site CA Management of Private Key



Issue and Distribute Server and Client Certificates Create Certificate Key Pairs Create Signing Request Sign Certificates with CA Deliver server and client certificates

Session Status and Management

EPICS Collaboration Meeting, ICALEPCS23, Cape Town, South Africa

Session Status and Management

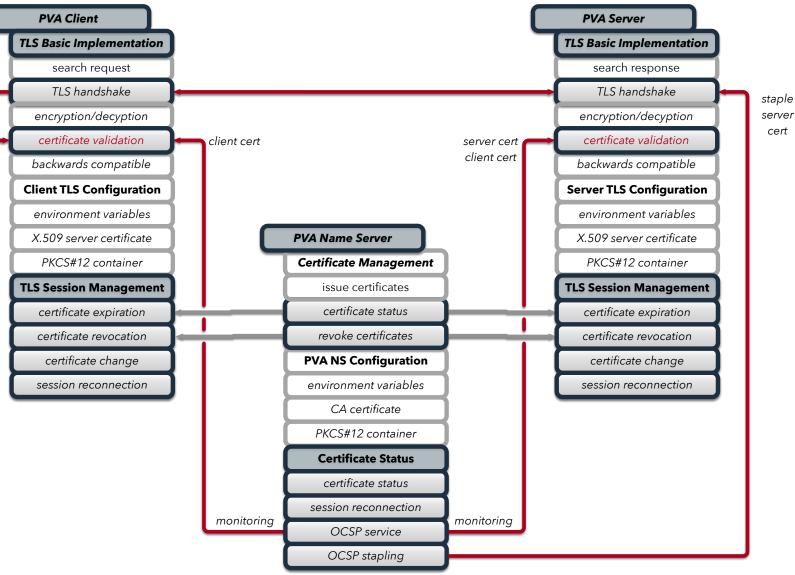
stapled *(*

server

cert

status

- Update Client and Server to handle reconnections after session disconnections
- Update PVA Name Server to provide certificate status via OCSP for Server and Client's certificate validation
- Update server TLS handshake to include server certificate status with OCSP stapling and update client certificate validation to use this server certificate status
- Update Client and Server to handle certificate expiration, revocation, and change





cert

EPICS Collaboration Meeting, ICALEPCS23, Cape Town, South Africa

Session Status & Management



Certificate Status

Implement OCSP server to deliver certificate status

Allow pub/sub event model for server status monitoring

Client and Server use this service to monitor for their own status changes

Revocation

Implements a function that revokes a certificate by setting the appropriate status

Clients and servers respond appropriately to revoked status



Expiration

Recognizes certificate expiration

Alerts listeners to upcoming expirations

Clients and Servers respond appropriately when certificates expire



Rotation

Allow orderly rotation of valid certificates with new valid certificates



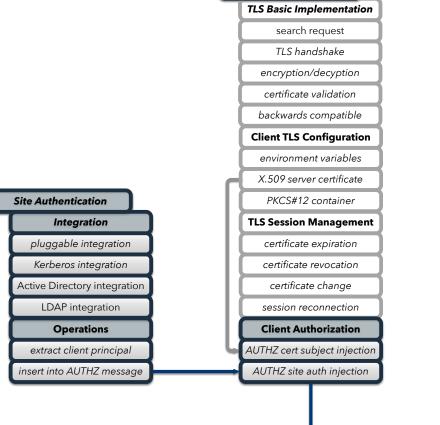
Stapling

Append server certificate status to TLS handshake with the OCSP stapling extension so that clients don't have to verify the status Enhanced Client Authorization

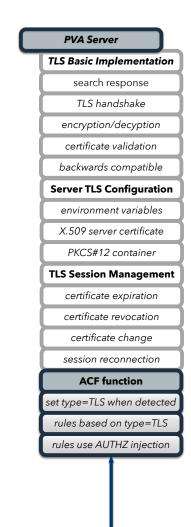


Enhanced Client Authorization

- Integrate with common site authentication methods
 - Kerberos
 - LDAP
 - Active Directory
- In PVA Connection validation message inject into the AUTHZ name field either the certificate subject or principal from site authentication integration
- Update ACF function that controls authorization so that it can use TLS status to control access



PVA Client



PVA Name Server

Certificate Management

issue certificates

revoke certificates

PVA NS Configuration

environment variables

CA certificate

PKCS#12 container

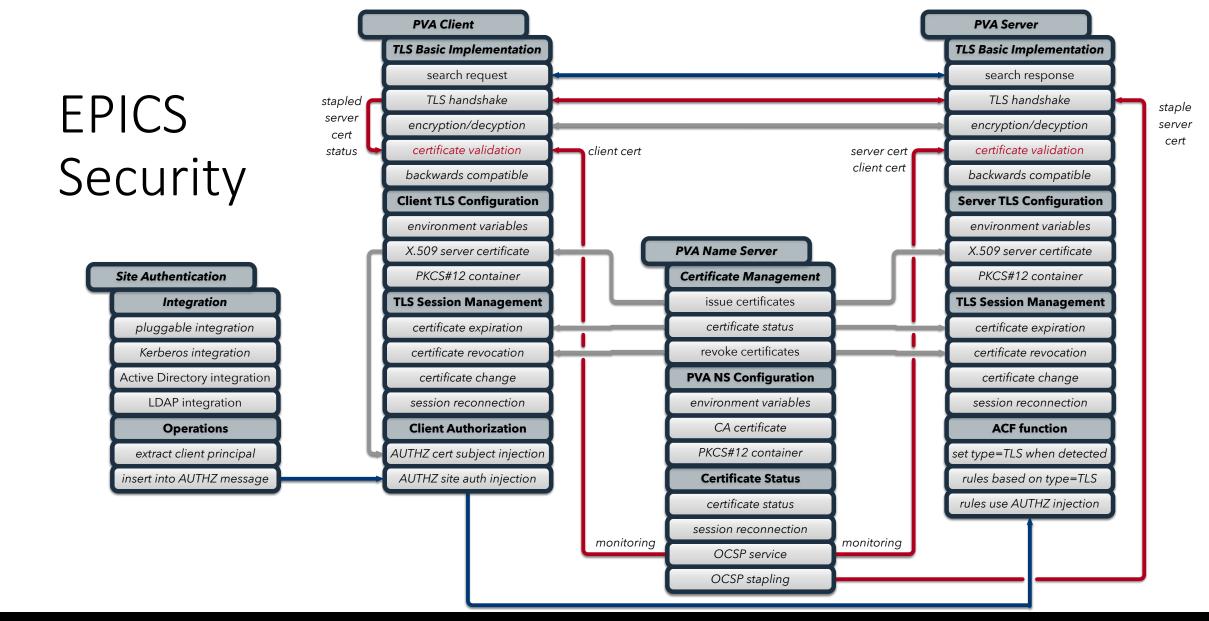
Certificate Status

certificate status

session reconnection

OCSP service





- 1. Basic TLS to authenticate and encrypt
- 2. Certificate Management to issue and distribute certificates
- 3. Session Management to handle expiration, revocation, recycling, and reconnection
- 4. Authorization using site authentication or client certificates

EPICS Collaboration Meeting, ICALEPCS23, Cape Town, South Africa

Recap

TLS Demo

......

...................

...............

..............

Manually create certificates

CA Certificate

openssl genpkey -algorithm RSA -out ca.key

create ca_config.cnf

openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt -config ca_config.cnf

Server Certificate

openssl genpkey -algorithm RSA -out server.key

create server_config.cnf

openssl req -new -key server.key -out server.csr -config server_config.cnf

openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 365 -sha256 -extfile server_config.cnf -extensions v3_req

openssl pkcs12 -export -out server.p12 -inkey server.key -in server.crt -certfile ca.crt

Client Certificate

openssl genpkey -algorithm RSA -out client.key

create client_config.cnf

openssl req -new -key client.key -out client.csr -config client_config.cnf

```
openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt -days 365 -sha256
-extfile client_config.cnf -extensions v3_req
```

openssl pkcs12 -export -out client.p12 -inkey client.key -in client.crt -certfile ca.crt

ca_config.cnf ...
keyUsage = digitalSignature, cRLSign, keyCertSign
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = CA:TRUE

server_config.cnf ...
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

client_config.cnf ...
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth

			client.p12 - KeyStore B	xplorer 5.5.2			
		🎗 🏗 🚥 🕕 🖻 🕅	0				
	client.p12 * server.p12 *						
	T E Entry Name		Algorithm	Key Size	Certificate Expiry	Last Modified	
lse	🃅 🗎 🥥 1		RSA	2048	07/09/2024, 14:54:36 CES	т -	
Jse KeyStore explorer to			Certificate	Details for En	try '1'		
ovnlorar to							
		Certificate Hierarchy:	<pre> level-n.com</pre>	m			
view				5111			
certificates		Version:	3				
centificates		Subject:		ire I – I vdnev O	=Level N Ltd,CN=mcinpro.lev	el-n.cc	
				ine, L=Lydney, O			
		Issuer:	CN=level-n.com				
		Serial Number (hex.):	0x1F0EC7D5434FD9420	65C58431AB88	B3B801F74FA		
		Serial Number (dec.):	17730833224283590210	7509237383924	524607269205242		
		Valid From:	08/09/2023, 14:54:36 CE	EST			
		Valid Until:	07/09/2024, 14:54:36 CE	EST			
		Public Key:	RSA 2048 bits			7	
	KeyStore Type: PKCS #12, Size: 1 entry, Selecte	ed Signature Algorithm:	SHA-256 with RSA				
		Fingerprint:	SHA-1 V DB:	40:E4:62:CB:32	:3D:D4:41:B3:8A:A6:86:A3:4A:	:D0:C6:	
			Export	Extensions	PEM Verify	ASN.1	
					_		
						ок	

Configure Wireshark

Set up LUA scripts

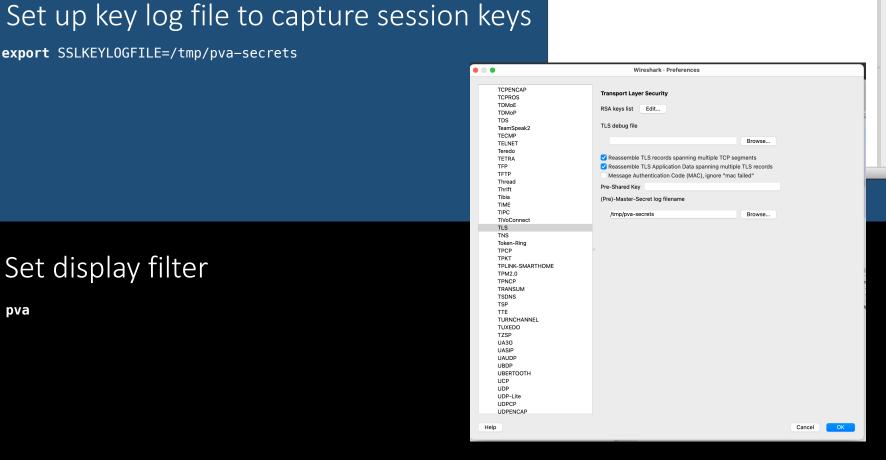
cd ~/.config/wireshark/plugins/

export SSLKEYLOGFILE=/tmp/pva-secrets

ln -s ~/Projects/com/osprey-dcs/cashark/*.lua

Set display filter

pva

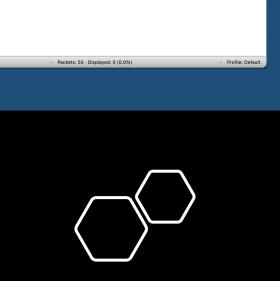


🛅 🗋 🕅 🙆 🍳 👄 🌧 🖭 🏹 🛃 🧊

. . .

13 ۲

pva



🗙 🔜 🝷 🕂 🛛 PVA

Loopback: Io0

Non-Secure PVA Communications

Start IOC server

softIocPVX -v -m user=test,N=tst,P=tst -d test/testioc.db -d test/testiocg.db -a test/testioc.acf dbLoadDatabase("/Users/george/Projects/com/osprey-dcs/pvxs/bin/darwin-aarch64/../../dbd/softIocPVX.dbd") softIocPVX_registerRecordDeviceDriver(pdbbase) dbLoadRecords("test/testioc.db", "user=test,N=tst,P=tst") dbLoadRecords("test/testiocg.db", "user=test,N=tst,P=tst") asSetSubstitutions("user=test,N=tst,P=tst") asSetFilename("test/testioc.acf") asSetFilename: Warning - relative paths won't usually work iocInit() INFO: PVXS QSRV2 is loaded and ENABLED. Starting iocInit ************* ## EPICS R7.0.7.1-DEV ## Rev. R7.0.7-56-g718da5c9be96b7eccd7c ## Rev. Date Git: 2023-02-04 22:56:19 -0600

epics>



Non-Secure PVA Communications

Get a PV

pvxget test:calcExample test:calcExample value double = 4alarm.severity int32_t = 1 alarm.status int32 t = 1 alarm.message string = "LOW" timeStamp.secondsPastEpoch int64 t = 1695756172timeStamp.nanoseconds int32_t = 258063000 timeStamp.userTag int32_t = 0 display.limitLow double = 0 display.limitHigh double = 10 display.description string = "Counter" display.units string = "Counts" display.form.index int32_t = 0 display.form.choices string[] = {7}["Default", "String", "Binary", "Decimal", "Hex", "Exponential", "Engineering"] control.limitLow double = 0control.limitHigh double = 10valueAlarm.lowAlarmLimit double = 2 valueAlarm.lowWarningLimit double = 4 valueAlarm.highWarningLimit double = 6

EPICS Collaboration Meeting, ICALEPCS23, Cape Town, South Africa

valueAlarm.highAlarmLimit double = 8

	_									
••	The second s				ng from Loopback: IoO					
1		N N N	🔍 🍋 🧉 🔁 🕻	r 🕹 📃						
pva	1.001									
No.	Time 1 0.000000	Source 192.168.2.3	Destination 192.168.2.255	Protocol PVA	Length Info 94 60009 -> 5076 Client SEARCH(1, 270544961:'test:calcExam					
	2 0.000974	192.168.2.3	192.168.2.3	PVA	85 5076 -> 60009 Server SEARCH(1, 270544961; Cestructerall	pre /,				
	7 0.001956	192.168.2.3	192.168.2.3	PVA	92 5075 -> 63068 Server SET_BYTE_ORDER, CONNECTION_VALIDAT	TON				
	9 0.003790	192.168.2.3	192.168.2.3	PVA	114 63068 -> 5075 Client CONNECTION_VALIDATION,	ION,				
	11 0.003880	192.168.2.3	192.168.2.3	PVA	65 5075 -> 63068 Server CONNECTION_VALIDATED,					
	13 0.003945	192.168.2.3	192.168.2.3	PVA	87 63068 -> 5075 Client CREATE_CHANNEL('test:calcExample')					
	15 0.004042	192.168.2.3	192.168.2.3	PVA	73 5075 -> 63068 Server CREATE_CHANNEL(cid=270544961, sid=				Capturing	g from Loopback: Io0
	17 0.004118	192.168.2.3	192.168.2.3	PVA	79 63068 -> 5075 Client GET(sid=117768961, ioid=2154848333					
	19 0.004208	192.168.2.3	192.168.2.3	PVA	515 5075 -> 63068 Server GET(inid=2154848337 sub=08)			Q 🍋 🔿 🖭	T 🔸 🔳	
	21 0.004375	192.168.2.3	192.168.2.3	PVA	73 63068 -> 5075 Client GET(sid=117768961, ioid=215484833;			• • • • •		
	23 0.004518	192.168.2.3	192.168.2.3	PVA	254 5075 -> 63068 Server GET(ioid=2154848337, sub=00),	pva 📃				🗙 🚬 🔹 🕇 🕹 PVA
	29 0.267694	192.168.2.3	192.168.2.3	PVA	85 5076 -> 60009 Server SEARCH_RESPONSE(1, 270544961)	No. Time	Source	Destination	Protocol	Length Info
	50 21.045525	192.168.2.3	192.168.2.255	PVA	79 50803 -> 5075 Server BEACON(0x734deb58ba42096376b0ee66	1 0.000000	192.168.2.3	192.168.2.255	PVA	<pre>94 60009 -> 5076 Client SEARCH(1, 270544961:'test:calcExample'),</pre>
						2 0.000974	192.168.2.3	192.168.2.3	PVA	85 5076 -> 60009 Server SEARCH_RESPONSE(1, 270544961)
100000000000000000000000000000000000000		on wire (752 bits)	, 94 bytes captured (75			7 0.001956	192.168.2.3	192.168.2.3	PVA	92 5075 -> 63068 Server SET_BYTE_ORDER, CONNECTION_VALIDATION,
	l/Loopback			0010		9 0.003790	192.168.2.3	192.168.2.3	PVA	<pre>114 63068 -> 5075 Client CONNECTION_VALIDATION,</pre>
			2.168.2.3, Dst: 192.168	2.255 0030	0 00 00 00 00 00 00 00 00 00 00 00 00 0	11 0.003880	192.168.2.3	192.168.2.3	PVA	65 5075 -> 63068 Server CONNECTION_VALIDATED,
			009, Dst Port: 5076	0040	69 ea 01 03 74 63 70 01 00 41 30 20 10 10 74 65 i···tcp· A0 ··te	13 0.003945	192.168.2.3	192.168.2.3	PVA	87 63068 -> 5075 Client CREATE_CHANNEL('test:calcExample'),
	cess Variable A	ccess		0050	73 74 3a 63 61 6c 63 45 78 61 6d 70 6c 65 st:calcE xample	15 0.004042	192.168.2.3	192.168.2.3	PVA	73 5075 -> 63068 Server CREATE_CHANNEL(cid=270544961, sid=117768961)…
	1agic: 0xca					17 0.004118	192.168.2.3	192.168.2.3	PVA	79 63068 -> 5075 Client GET(sid=117768961, ioid=2154848337, sub=08),
	/ersion: 2					19 0.004208	192.168.2.3	192.168.2.3	PVA	515 5075 -> 63068 Server GET(ioid=2154848337, sub=08),
	lags: 0x00					21 0.004375	192.168.2.3	192.168.2.3	PVA	73 63068 -> 5075 Client GET(sid=117768961, ioid=2154848337, sub=00),
	Command: SEARCH	(0x03)				23 0.004518	192.168.2.3	192.168.2.3	PVA	254 5075 -> 63068 Server GET(ioid=2154848337, sub=00),
	Size: 54			0		29 0.267694	192.168.2.3	192.168.2.3	PVA	85 5076 -> 60009 Server SEARCH_RESPONSE(1, 270544961)
	Search Sequence	#: 1				50 21.045525	192.168.2.3	192.168.2.255	PVA	79 50803 -> 5075 Server BEACON(0x734deb58ba42096376b0ee66, 16, 2)
	1ask: 0×00					Eromo 2: 05 hutos	an wire (600 bits)	85 bytes captured (6	80 bits 0000	02 00 00 00 45 00 00 51 ac 63 00 00 40 11 00 00 ····E··O ·c··@···
		00000000000000ffff	0000000			> Null/Loopback	UN WITE (000 DICS),	os bytes captureu (o	0010	C0 a8 02 03 c0 a8 02 03 13 d4 ea 69 00 3d 85 a5
	Port: 60009						Version 4 Erci 102	.168.2.3, Dst: 192.16	0020	ca 02 c0 04 00 00 00 2d 73 4d eb 58 ba 42 09 63 ·····- sM·X·B·c
	Transport Proto	col: tcp					tocol, Src Port: 507		0030	76 b0 ee 66 00 00 01 00 00 00 00 00 00 00 00 00 v··f····
	PV Count: 1					 Process Variable 		o, bat rolt. 00009		00 00 ff ff 00 00 00 00 13 d3 03 74 63 70 01 00 ······························
	CID: 270544961					Magic: 0xca	necess		0050	01 10 20 30 41 ··· 0A
	ame: test:calc	Example				Version: 2				
0.7						> Flags: 0xc0				
	Loopback: Io0: <li< td=""><td>ve capture in progress></td><td></td><td></td><td>Packets: 94 · Displayed: 13 (13.8%)</td><td></td><td>RESPONSE (0×04)</td><td></td><td></td><td></td></li<>	ve capture in progress>			Packets: 94 · Displayed: 13 (13.8%)		RESPONSE (0×04)			
						Size: 45				
							a42096376b0ee66			
						Search Sequence #: 1				
							Address: 00000000000000000000000000000000000			
						Port: 5075				

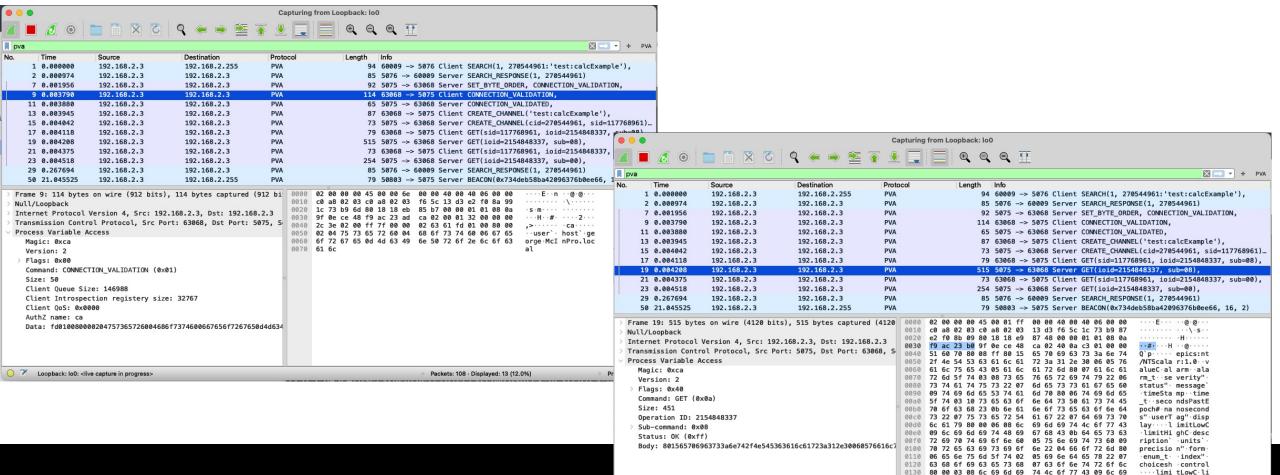
View Non-Secure Results in Wireshark



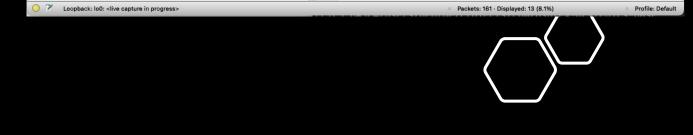
• Only tcp is included in search message

Transport Protocol: tcp Found: True

• No TLS Handshake takes place



View Non-Secure Results in Wireshark



6d 69 74 48 69 67 68 43 07 6d 69 6e 53 74 65 70

0150 43 0a 76 61 6c 75 65 41 6c 61 72 6d 80 00 0a 06

mitHighC ·minStep

C.valueA larm

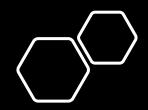
0140

- Only tcp is included in search message
- No TLS Handshake takes place

Secure PVA Communications

Configure TLS Client and Server environments

export EPICS_PVAS_TLS_KEYCHAIN="~/Projects/com/osprey-dcs/certificates/server.p12"
export EPICS_PVA_TLS_KEYCHAIN="~/Projects/com/osprey-dcs/certificates/client.p12"



Secure PVA Communications

Start IOC server

softlocPVX -v -m user=test,N=tst,P=tst -d test/testioc.db -d test/testiocg.db -a test/testioc.acf

dbLoadDatabase("/Users/george/Projects/com/osprey-dcs/pvxs/bin/darwin-aarch64/../../dbd/softIocPVX.dbd")

softIocPVX_registerRecordDeviceDriver(pdbbase)

NOTICE: debug logging TLS SECRETS to SSLKEYLOGFILE=/tmp/pva-secrets

dbLoadRecords("test/testioc.db", "user=test,N=tst,P=tst")

dbLoadRecords("test/testiocg.db", "user=test,N=tst,P=tst")

asSetSubstitutions("user=test,N=tst,P=tst")

asSetFilename("test/testioc.acf")

asSetFilename: Warning - relative paths won't usually work

iocInit()

INFO: PVXS QSRV2 is loaded and ENABLED.

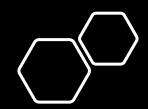
Starting iocInit

EPICS R7.0.7.1-DEV

Rev. R7.0.7-56-g718da5c9be96b7eccd7c

Rev. Date Git: 2023-02-04 22:56:19 -0600

epics>



Secure PVA Communications

Get a PV

```
pvxget test:calcExample
NOTICE: debug logging TLS SECRETS to SSLKEYLOGFILE=/tmp/pva-secrets
test:calcExample
   value double = 4
    alarm.severity int32_t = 1
    alarm.status int32 t = 1
    alarm.message string = "LOW"
    timeStamp.secondsPastEpoch int64 t = 1695756172
    timeStamp.nanoseconds int32_t = 258063000
    timeStamp.userTag int32_t = 0
    display.limitLow double = 0
    display.limitHigh double = 10
    display.description string = "Counter"
    display.units string = "Counts"
    display.form.index int32_t = 0
    display.form.choices string[] = {7}["Default", "String", "Binary", "Decimal", "Hex", "Exponential", "Engineering"]
    control.limitLow double = 0
    control.limitHigh double = 10
    valueAlarm.lowAlarmLimit double = 2
    valueAlarm.lowWarningLimit double = 4
    valueAlarm.highWarningLimit double = 6
    valueAlarm.highAlarmLimit double = 8
```

					g from Loopback: lo0						
	1 0		Q 🧀 🛋 👀 🛣		📃 @, @, @, II						
				<u> </u>		_					
pva						• + PVA					
No.	Time	Source		Protocol	Length Info						
	0.000000	192.168.2.3		PVA	98 51760 -> 5076 Client SEARCH(1718185572, 305419896:'test:c						
	0.000167	192.168.2.3		PVA	85 5076 -> 51760 Server SEARCH_RESPONSE(1718185572, 30541989						
	0.005053	192.168.2.3		PVA	2485 5076 -> 63108 Server SET_BYTE_ORDER, CONNECTION_VALIDATIO	N,					
	0.005183	192.168.2.3		PVA	92 63108 -> 5076 Client CONNECTION_VALIDATION,				Capturi	ing from Loopback: lo0	
1000	0.005220	192.168.2.3 192.168.2.3		PVA PVA	109 5076 -> 63108 Server CONNECTION_VALIDATED,				~ • -		
10.25	0.005422	192.168.2.3		PVA	<pre>101 63108 -> 5076 Client CREATE_CHANNEL('test:calcExample'), 117 5076 -> 63108 Server CREATE CHANNEL(cid=305419896, sid=11</pre>			🍳 🦛 🌩 👱 🧌	} 👱 🔦	. E. Q. Q. T.	
1000	0.005624	192.168.2.3		PVA	<pre>99 63108 -> 5076 Client GET(sid=117768961, ioid=268443648, s</pre>						1 514
	0.005678	192.168.2.3		PVA	559 5076 -> 63108 Server GET(ioid=268443648, sub=08),						T PVA
215.55	0.005770	192.168.2.3		PVA	87 63108 -> 5076 Client GET(sid=117768961, ioid=268443648, sub=08),	No. Time ub= 1 0.000000	Source	Destination	Protocol	Length Info	I - France C
	0.005833	192.168.2.3		PVA	298 5076 -> 63108 Server GET(ioid=268443648, sub=00),		192.168.2.3 192.168.2.3	192.168.2.255 192.168.2.3	PVA PVA	98 51760 -> 5076 Client SEARCH(1718185572, 305419896:'test:cal	
	0.005955	192.168.2.3		PVA	86 63108 -> 5076 Client DESTROY REQUEST(sid=117768961, ioid=	2 0.000167	192.168.2.3	192.168.2.3	PVA	85 5076 -> 51760 Server SEARCH_RESPONSE(1718185572, 305419896)	
	0.033334	192.168.2.3		PVA	85 5076 -> 51760 Server SEARCH_RESPONSE(1718185572, 30541989	10 0100000	192.168.2.3	192.168.2.3	PVA	2485 5076 -> 63108 Server SET_BYTE_ORDER, CONNECTION_VALIDATION, 92 63108 -> 5076 Client CONNECTION VALIDATION,	1
	4.640150	192.168.2.3		PVA	79 53904 -> 5075 Server BEACON(0x501536078ea537da3c521a3a, 8		192.168.2.3	192.168.2.3	PVA	109 5076 -> 63108 Server CONNECTION_VALIDATION,	
						23 0.005315	192.168.2.3	192.168.2.3	PVA	101 63108 -> 5076 Client CREATE CHANNEL('test:calcExample'),	
		on wire (784 bits), 9	8 bytes captured (784 b			25 0.005422	192.168.2.3	192.168.2.3	PVA	101 05108 -> 5070 CTERTC CREATE_CHANNEL(test.catteRampte), 117 5076 -> 63108 Server CREATE CHANNEL(cid=305419896. sid=1177	768961)
	Loopback			0010		29 0.005624	192.168.2.3	192.168.2.3	PVA	99 63108 -> 5076 Client GET(sid=117768961, ioid=268443648, sub	
			68.2.3, Dst: 192.168.2.	255 0030	00 00 00 00 00 00 00 00 00 00 00 00 00	31 0.005678	192.168.2.3	192.168.2.3	PVA	559 5076 -> 63108 Server GET(ioid=268443648, sub=08),	
		col, Src Port: 51760	, Dst Port: 5076		ca 30 02 03 74 6c 73 03 74 63 70 00 01 12 34 56 0tls.tcp4V	35 0.005770	192.168.2.3	192.168.2.3	PVA	87 63108 -> 5076 Client GET(sid=117768961, ioid=268443648, sub	p=00).
	ss Variable Ac	cess			78 10 74 65 73 74 3a 63 61 6c 63 45 78 61 6d 70 x test:c alcExamp	37 0.005833	192.168.2.3	192.168.2.3	PVA	298 5076 -> 63108 Server GET(ioid=268443648, sub=00),	
	ic: 0xca sion: 2			0000	6c 65 le	41 0.005955	192.168.2.3	192.168.2.3	PVA	86 63108 -> 5076 Client DESTROY_REQUEST(sid=117768961, ioid=26	5844364
	sion: 2 lgs: 0x80					47 0.033334	192.168.2.3	192.168.2.3	PVA	85 5076 -> 51760 Server SEARCH RESPONSE(1718185572, 305419896)	
	mand: SEARCH	(0-02)				69 4.640150	192.168.2.3	192.168.2.255	PVA	79 53904 -> 5075 Server BEACON(0x501536078ea537da3c521a3a, 8,	2)
	e: 58	(0,03)				France Dr. Of Lute	(COO	05 but a sectored (600	- Lit- 000	0 02 00 00 00 45 00 00 51 3b 6b 00 00 40 11 00 00 ····E··O ;k··@···	
	rch Sequence a	#: 1718185572		0		<pre>> Frame 2: 85 byte > Null/Loopback</pre>	s on wire (680 Dits)	, 85 bytes captured (680	DITS 0001	0 c0 a8 02 03 c0 a8 02 03 13 d4 ca 30 00 3d 85 a5	
	k: 0x00						Version 4 Erci 10	2.168.2.3, Dst: 192.168.	3 002	0 ca 02 c0 04 00 00 00 2d 50 15 36 07 8e a5 37 da P.67	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		000000000000000000000000000000000000000	0000				otocol, Src Port: 50		003	0 3c 52 1a 3a 66 69 6e 64 00 00 00 00 00 00 00 00 <r :="" find<="" td=""><td></td></r>	
Po	t: 51760					Process Variable		, bit for the silves		0 00 00 ff ff 00 00 00 00 13 d4 03 <mark>74 6c 73</mark> 01 00 ···········tls···	
	insport Protoc	ol: tls				Magic: 0xca	Access		005	0 01 12 54 50 78 ··· 4vx	
	insport Protoc					Version: 2					
PV	Count: 1	And				> Flags: 0xc0					
CI	: 305419896						H RESPONSE (0×04)				
Na	e: test:calcE	xample				Size: 45	-				
				100		GUID: 50153607	/8ea537da3c521a3a		0		
0 7	Transport Protocol ((pva.proto), 3 bytes			 Packets: 114 · Displayed: 16 (14.0%) Provide the second seco	ofile Search Sequence	e #: 1718185572				
						Address: 00000	000000000000000ffff0	0000000			
						Port: 5076					
						Transport Prot	ocol: tls				
						Found: True					
						CID: 305419896					
											/

View Secure Results in Wireshark

• Both tcp and tls are included in search message

Transport Protocol (pva.proto), 3 bytes

- TLS Handshake takes place
- PVA session is encrypted, and we see the decrypted message thanks to the key log.



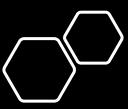
Profile: Default

ckets: 121 · Displayed: 16 (13.2%

•••			Capturing fr	rom Loopback: Io0						
	o x a =	ې 🐳 🔶 🦉	🛪 🐥 💳 🛙							
		• • • =	• ~ - !		_					
pva					+ PVA					
No. Time	Source	Destination	Protocol	Length Info						
1 0.000000	192.168.2.3	192.168.2.255	PVA PVA	98 51760 -> 5076 Client SEARCH(1718185572, 305419896:'test:ca						
2 0.000167 13 0.005053	192.168.2.3 192.168.2.3	192.168.2.3	PVA	85 5076 -> 51760 Server SEARCH_RESPONSE(1718185572, 305419896						
13 0.005053	192.168.2.3	192.168.2.3	PVA	<pre>2485 5076 -> 63108 Server SET_BYTE_ORDER, CONNECTION_VALIDATION 92 63108 -> 5076 Client CONNECTION VALIDATION,</pre>				Capturing	from Loopback: Io0	
19 0.005220	192.168.2.3	192.168.2.3	PVA	109 5076 -> 63108 Server CONNECTION VALIDATION,						
23 0.005315	192.168.2.3	192.168.2.3	PVA	101 63108 -> 5076 Client CREATE CHANNEL('test:calcExample'),			🗣 👄 警	1	📃 🔍 Q, Q, 🎹	
25 0.005422	192.168.2.3	192.168.2.3	PVA	117 5076 -> 63108 Server CREATE_CHANNEL(cid=305419896, sid=11)	Dva					
29 0.005624	192.168.2.3	192.168.2.3	PVA	99 63108 -> 5076 Client GET(sid=117768961, ioid=268443648, s		Source	Destination	Protocol	Length Info	
31 0.005678	192.168.2.3	192.168.2.3	PVA	559 5076 -> 63108 Server GET(ioid=268443648, sub=08),	1 0.000000	192.168.2.3	192.168.2.255	PVA		ARCH(1718185572, 305419896:'test:calcExamp
35 0.005770	192.168.2.3	192.168.2.3	PVA	87 63108 -> 5076 Client GET(sid=117768961, ioid=268443648, su		192.168.2.3	192.168.2.3	PVA		ARCH_RESPONSE(1718185572, 305419896)
37 0.005833	192.168.2.3	192.168.2.3	PVA	298 5076 -> 63108 Server GET(ioid=268443648, sub=00),	13 0.005053	192.168.2.3	192.168.2.3	PVA		T BYTE ORDER, CONNECTION VALIDATION,
41 0.005955	192.168.2.3	192.168.2.3	PVA	86 63108 -> 5076 Client DESTROY_REQUEST(sid=117768961, ioid=:		192.168.2.3	192.168.2.3	PVA	92 63108 -> 5076 Client CO	
47 0.033334	192.168.2.3	192.168.2.3	PVA	85 5076 -> 51760 Server SEARCH_RESPONSE(1718185572, 30541989)		192.168.2.3	192.168.2.3	PVA	109 5076 -> 63108 Server CO	
69 4.640150	192.168.2.3	192.168.2.255	PVA	79 53904 -> 5075 Server BEACON(0x501536078ea537da3c521a3a, 8	23 0.005315	192.168.2.3	192.168.2.3	PVA		EATE_CHANNEL('test:calcExample'),
Erame 17: 02 bytes	on wire (726 hits)	92 bytes captured (7	26 bit 0000 0	22 00 00 00 45 00 00 58 00 00 40 00 40 06 00 00 ····E··X ··@·@····	25 0.005422	192.168.2.3	192.168.2.3	PVA		EATE_CHANNEL(cid=305419896, sid=117768961)
> Null/Loopback	on wrie (750 brts),	92 bytes captured (7		c0 a8 02 03 c0 a8 02 03 f6 84 13 d4 93 eb e6 74	29 0.005624	192.168.2.3	192.168.2.3	PVA	99 63108 -> 5076 Client GE	T(sid=117768961, ioid=268443648, sub=08),
	Version 4 Src: 192	168.2.3, Dst: 192.168		38 01 da 66 80 18 18 a0 85 a1 00 00 01 01 08 0a 8 f · · · · · · · · · · ·	31 0.005678	192.168.2.3	192.168.2.3	PVA	559 5076 -> 63108 Server GE	T(ioid=268443648, sub=08),
		t: 63108, Dst Port: 5	076 C 0030 0	52 cf 26 f2 30 ee 47 43 17 03 03 00 1f 49 31 f9 b & 0 GC ·····I1	35 0.005770	192.168.2.3	192.168.2.3	PVA	87 63108 -> 5076 Client GE	T(sid=117768961, ioid=268443648, sub=00),
> Transport Layer Se			. 0040 2	26 a8 c3 d0 0d da 1f ad 3b 15 e9 b8 25 75 d3 64 &	37 0.005833	192.168.2.3	192.168.2.3	PVA	298 5076 -> 63108 Server GE	T(ioid=268443648, sub=00),
	segments (22 bytes)	: #15(8), #17(14)]	0050 0		41 0.005955	192.168.2.3	192.168.2.3	PVA	86 63108 -> 5076 Client DE	STROY_REQUEST(sid=117768961, ioid=26844364
Process Variable A					47 0.033334	192.168.2.3	192.168.2.3	PVA		ARCH_RESPONSE(1718185572, 305419896)
Magic: 0xca					69 4.640150	192.168.2.3	192.168.2.255	PVA	79 53904 -> 5075 Server BE	ACON(0x501536078ea537da3c521a3a, 8, 2)
Version: 2					> Frame 37: 298 bvt	es on wire (2384 bit	s), 298 bytes capture	d (2384 0000	ca 02 40 0a be 00 00 00 00 20 00 10 00	ff 04 ba ···@······
> Flags: 0x00					> Null/Loopback			0010	7b 36 1e 00 00 00 00 00 00 00 40 02 00	00 00 01 {6·····
Command: CONNEC	TION_VALIDATION (0×0	1)	1			Version 4, Src: 192	.168.2.3, Dst: 192.16	B.2.3 0020 0030	00 00 00 04 4c 4f 4c 4f f6 e6 13 65 00	00 00 00 ····LOLO ···e···· 00 00 00 ····LOLO ···e····
Size: 14					> Transmission Cont	rol Protocol, Src Po	rt: 5076, Dst Port: 63	3108, S 0040	00 00 00 00 00 00 24 40 07 43 6f 75 6e	
Client Queue Si	ze: 65536				> Transport Layer S	ecurity		0050	06 43 6f 75 6e 74 73 00 00 00 00 07 07	44 65 66 ·Counts· ····Def
	ction registery size	: 32767			> [2 Reassembled TL	S segments (198 byte:	s): #37(8), #37(190)]		61 75 6c 74 06 53 74 72 69 6e 67 06 42	
Client QoS: 0x0					> Process Variable	Access		0070	72 79 07 44 65 63 69 6d 61 6c 03 48 65	78 Øb 45 ry.Decim al.Hex.E 67 69 6e xponenti al.Engin
AuthZ name: x50	9				Magic: 0xca			0000	65 65 72 69 6e 67 00 00 00 00 00 00 00 00	00 00 00 eering.
Data: ff					Version: 2			00a0	00 00 00 00 24 40 00 00 00 00 00 00 00	40 00 00\$@@
					> Flags: 0x40	2		00b0	00 00 00 00 10 40 00 00 00 00 00 00 18	
			Frame (9	22 bytes) Decrypted TLS (14 bytes) Reassembled TLS (22 bytes)	Command: GET (0x0a)		00c0	00 00 00 00 20 40	···· @
○ [™]			calife (o		Size: 190					
😑 🍸 Loopback: Io0: <li< td=""><td>ve capture in progress></td><td></td><td></td><td>Packets: 165 · Displayed: 16 (9.7%) Pro</td><td></td><td></td><td></td><td></td><td></td><td></td></li<>	ve capture in progress>			Packets: 165 · Displayed: 16 (9.7%) Pro						
					> Sub-command: 0: Status: OK (0x)					
				, i			0000001000000044c4f4c	4ff5051		
				· · · · · · · · · · · · · · · · · · ·	Body: 04037036	120000000000000000040020	10000001000000044C414C	4110601		
					2			Frame		TLS (190 bytes) Reassembled TLS (198 bytes)
					😑 🎽 Body (pva.body)	, 184 bytes			Packets: 299 · D	isplayed: 16 (5.4%) Profile: Default

View Secure Results in Wireshark

- Both tcp and tls are included in search message
- TLS Handshake takes place
- PVA session is encrypted, and we see the decrypted message thanks to the key log.



EPICS Security Technical Plan Osprey DCS

• Thank You

George McIntyre george@level-n.com