SECURE CHANNEL ESTABLISHMENT & ATTESTATION

(CCC ATTESTATION SIG, 2022-05-10)

- **RA-TLS** (DMITRII)
- **STET** (KEITH)
- **OE SDK** (ANDY)
- **EKEP** (TOM)
- **VERACRUZ** (DEREK)
- **CLOUDPROXY** (TOM)
- **HTTPA** (HANS)
- **TLS+CWT** (HANNES)

COMPARE AND CONTRAST

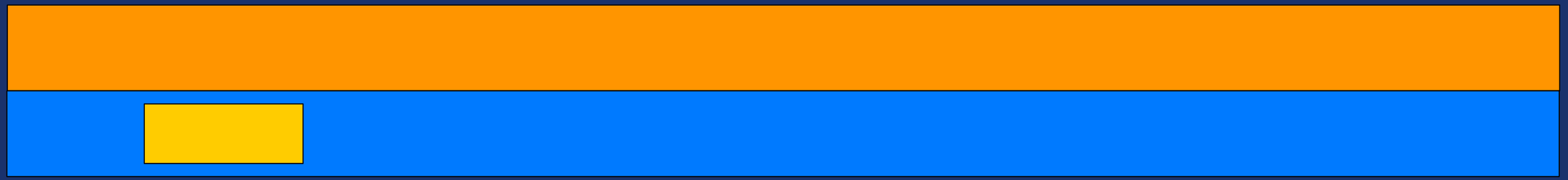
COLOR CODING

App chan

TLS chan

Attestation Chan

(A) EXTEND TLS/ALTS TO MAKE ATTESTATION NATIVE



- EXAMPLES: TLS+CWT, EKEP

(B) RUN ATTESTATION A TOP AN EXISTING TLS SESSION

- EXAMPLES: STET, HTTPA/1

(C.1) TUNNEL ATTESTATION INSIDE X.509

- EXAMPLES: RA-TLS, ATTESTED TLS

(C.2) MINT ATTESTED IDENTITIES INTO X.509 CERTS

- EXAMPLES: VERACRUZ, CLOUDPROXY(?)
- (DICE ALSO, EXCEPT MORE RADICALLY)

DISCUSSION

- WHAT STANDARDISATION NEEDS TO HAPPEN?
- OPPORTUNITIES FOR PROTOTYPING & COLLABORATION?
- HOW ARE THE PROTOCOL ELEMENTS EFFECTIVELY GOING TO BE CONSUMED BY RELYING PARTIES?

DISCUSSION (STD)

- (A) NEEDS EXTENDING THE TLS HANDSHAKE (IETF TLS WG)
- (B.HTTPA) NEEDS EXTENDING HTTP (IETF HTTPBIS WG)
- (C.1) NEW "ATTESTATION MESSAGE" X.509 EXTENSION FORMAT AND THE ASSOCIATED OID (IETF LAMPS WG)
- (C.2) NEW "ATTESTED IDENTITY" SUBJECT ALTERNATIVE NAME TYPE (IETF LAMPS WG)
- OTHER?

DISCUSSION (PROTO)

- HANNES: PROTOTYPE (A) IN MBEDTLS
- HARMONISING SOLUTIONS IN (C.1)
- DEREK: INTEGRATE VERAISON W/ VERACRUZ'S PROXY ATTESTATION SERVICE
- OTHER?

DISCUSSION {DAN@SLACK}

ONE PATTERN I'D LIKE TO DRAW FROM EACH OF THESE PROPOSALS IS:

- **HOW TO PRACTICALLY USE THE IDENTITY / MEASUREMENT OF THE ATTESTING WORKLOAD**

OR, WORDED DIFFERENTLY:

- **HOW THE RELYING PARTY END OF THE PROTOCOL KNOWS WHAT WORKLOAD IDENTITY OR MEASUREMENT VALUES IT EXPECTS?**

NEXT STEPS?

REFRESHER

RA-TLS

- GOAL IS TO BIND A PRIVATE KEY TO AN ENCLAVE RUNNING ON GENUINE SGX HARDWARE
- CREATE A SELF-SIGNED CERT ASSOCIATED TO THE EPHEMERAL KEY
- PUT THE SGX QUOTE OF THE ENCLAVE IN AN EXTENSION OF THE CERT
- BIND QUOTE AND KEY VIA USER DATA

RA-TLS (CONT.)

- FRESHNESS: NOT BOUND TO THE SESSION
- ATTESTATION FORMATS: SGX
- API ANGLE: RP AND ATTESTER APP HOOK INTO THE CERT VERIFICATION PHASE OF THE TLS HANDSHAKE
- STD ANGLE: SHOULD AN X.509 EXTENSION (OID AND FORMAT) BE STANDARDISED TO CARRY ATTESTATION INFORMATION IN CERTS?

STET

- ATTESTED TLS OVER GRPC OVER "TRADITIONAL" TLS
- THE TLS-IN-TLS CONSTRUCTION ALLOWS HOPPING THROUGH TLS PROXIES WHILE ACHIEVING END-TO-END SECURITY
- FRESHNESS: USE EXPORTED KEY MATERIAL (EKM) FROM THE FULLY ESTABLISHED TLS SESSION TO CREATE THE ATTESTATION NONCE (BIND ATTESTATION TO THE SESSION)
- ATTESTATION FORMAT: TPM BUT EXTENSIBLE

OE SDK

- CONCEPTUALLY IDENTICAL TO RA-TLS: SELF-SIGNED CERT OF THE ENCLAVE'S EPHEMERAL KEY, WHICH INCLUDES THE SGX ATTESTATION TUNNELLED INTO AN X.509 EXTENSION
- API ANGLE: SAME AS RA-TLS, BUT ALSO ADD ABILITY FOR APPLICATIONS TO ADD ADDITIONAL CLAIMS
- STD ANGLE: SHOULD AN X.509 EXTENSION (OID AND FORMAT) BE STANDARDISED TO CARRY ATTESTATION INFORMATION IN CERTS?

EKEP

- BASED ON ALTS
  - MUTUAL AUTH SEC CHAN ESTABLISHMENT (SIMILAR TO TLS)
  - IDENTITIES ARE BASED ON THE CONCEPT OF ENTITY (I.E., USERS, MACHINES, SERVICES, WORKLOADS) – CMP TO THE TLS/HTTPS TRUST MODEL WITH THE SERVER NAME AS THE ONLY IDENTITY

EKEP (CONT.)

- DIFFERENCES W/ ALTS:
  - ALWAYS USES DHE (AND GETS PFS)
  - NO SESSION RESUMPTION (KEEP IT SIMPLE, FOR NOW)
  - ALLOW EACH PARTICIPANT TO ATTEST TO MULTIPLE IDENTITIES
    - EXPRESS POLICIES INVOLVING MULTIPLE LEVELS OF IDENTITY (E.G., PLATFORM + WORKLOAD)
  - EXTEND ALTS TO NEGOTIATE ATTESTATION PARAMETERS

EKEP (CONT.)

- GOAL OF THE K-E PART: TO ATTEST TO IDENTITIES AND THE KEYS USED TO ESTABLISH THE CHANNEL
- NOTE THAT BOTH CLIENT AND SERVER CREATE THEIR VERIFIABLE IDENTITY SO THAT THEY ARE BOUND TO THE PREVIOUS HS MSGS (CANNOT BE REUSED OUTSIDE THE CURRENT SESSION)
- MAY PROVIDE A GOOD CONCEPTUAL FRAMEWORK BOTH IN TERMS OF END GOALS, BASE MECHANISMS, AS WELL AS FORMAL VERIFICATION FOR EXTENDING TLS

VERACRUZ

- GOAL: ASSURE CLIENT (EITHER PROGRAM / DATA PROVIDER, OR THE RESULT CONSUMER) THAT THE PROCESS IT'S COMMUNICATING TO IS THE VERACRUZ RUNTIME EXECUTING INSIDE ONE OF THE SUPPORTED ENCLAVES (E.G., AWS NITRO, ARM TZ, INTEL SGX)
  - FOR THAT REASON (I.E., MULTIPLE PLATFORM SUPPORT) VC LOOKS LIKE AN EXCELLENT PILOT FOR HARMONISATION

VERACRUZ (CONT.)

- A PROXY ATTESTATION SERVICE ACTS AS A CA / ATTESTED IDENTITY PROVIDER THAT HAS VERIFICATION BACKENDS FOR EACH OF THE SUPPORTED EVIDENCE FORMATS
  - IF ATTESTATION EVIDENCE IS VERIFIED, THE CA ISSUES A SHORT-TERM X.509 CERT FOR THE REQUESTOR ATTESTER (I.E., THE ENCLAVE RUNNING VERACRUZ RUNTIME) WITH THE WORKLOAD IDENTITY STASHED IN AN X.509 EXTENSION.

VERACRUZ (CONT.)

- STD ANGLE: ISN'T THIS A KIND OF "NAME" OF THE WORKLOAD? SHOULD A SUBJALTNAME TYPE BE DEFINED TO CARRY THESE KINDS OF NAMES?
  - (SEE ALSO CLOUDPROXY)

CLOUDPROXY

- DEFINES A NAMING SCHEME FOR EXPRESSING A RECURSIVE VIEW OF THE TRUST CHAIN IN AN EXECUTION ENVIRONMENT
- THE NAMING SCHEME ALLOWS A POLICY TO BE DEFINED AND EVALUATED TO DETERMINE AUTHENTICATION & AUTHORISATION PROPERTIES FOR A GIVEN CHANNEL

CLOUDPROXY (CONT.)

- USES DATALOG [1]
  - STD ANGLE: THIS MAY BE A FORMAT THAT CAN BE REUSED FOR NAMING IN X.509 SAN (SEE VERACRUZ)

[1] REGO (OPEN POLICY AGENT) IS DERIVED FROM DATALOG

HTTPA/1

- THE GOAL IS TO ESTABLISH TRUST IN THE WEB SERVICE (WS) ENDPOINT (L7) BEING RUN INSIDE AN ENCLAVE.
- EXTEND HTTP WITH NEW METHOD (ATTEST) THAT ADDS AN ATTESTATION HANDSHAKE

HTTPA/1

- A WS USES THE APPLICATION LAYER ATTESTATION PROTOCOL TO SHOW THE CLIENT THAT IT RUNS INSIDE A SECURE ENCLAVE, AND TO NEGOTIATE SESSION KEYS TO ESTABLISH AN END-TO-END SECURE TUNNEL
- NOTE THAT THE SECURE TUNNEL IS LIMITED TO HTTP REQUEST AND RESPONSE BODIES ONLY (HEADERS/TRAILERS ARE OUTSIDE THE SECURE ENVELOPE)

TLS+CWT

- EXTEND TLS TO ALLOW EAT-BASED EVIDENCE AND ATTESTATION RESULTS TO BE A NEW KIND OF CERTIFICATE CREDENTIAL
  - WHY ONLY EAT-BASED? MAYBE WE ARE MISSING THE OPPORTUNITY TO PROVIDE A MORE GENERIC CONTAINER FOR EVIDENCE AND ATTESTATION RESULTS WHATEVER FORMAT THEY MAY HAVE?
- THE APPROACH IS SIMILAR TO EKEP EXCEPT IT'S FOR TLS RATHER THEN ALTS

TLS+CWT (CONT.)

- REQUIRES MODIFICATION TO THE API FOR EXPLICIT FRESHNESS
- COULD RE-USE THE CERTIFICATE CHECKING CALLBACK LOGICS USED BY RA-TLS AND ATTESTED TLS?
  - STD ANGLE: THIS NEEDS WORK IN THE TLS WG BEFORE IT CAN BECOME GENERALLY AVAILABLE
  - LOOKS LIKE A GOOD PROTOTYPING CANDIDATE