redhat.

THE IETF SECURITY AREA

Connections, Bangalore, India
November 8, 2017

Paul Wouters,
RHEL Security

IETF: SECURITY AREA

- Security Area Advisory Group (SAAG)
  - Area Directors: Kathleen Moriarty, Eric Rescorla
- Security Area Directorate (SecDir)
  - Mostly WG chairs, security veterans
- Security Considerations Section in RFCs

- Working Groups:
  - ace, acme, curdle, dots, i2nsf, ipsecme, kitten
  - lamps, mile, oauth, openpgp, sacm, secevent, tls
  - tokbind, trans, [tcpme, tcpinc, cfrg]

TLS UPDATE: TSL 1.3

- TLS 1.3 almost-nearly-truly ready for RFC
  - algorithm update, move to AEAD algorithms
  - 0RTT (send application data in first packet, on resumption)
  - Only ephemeral (perfect forward security) Key Exchanges
  - Only ServerHelo message not encrypted
  - Certificate message now encrypted
  - No Server Name Information (SNI) encryption
    (but see draft-ietf-tls-sni-encryption)
  - Version negotiation changed, accommodating bad middleware
  - Session resumption with and without server state
- TLS 1.3 shows about 3.5% failure rate
  - Due to broken middleware boxes
- See also QUIC, HTTP/2, tcpcrypt, Opportunistic IPsec

TLS MIDNIGHT UPDATE BY EKR FOR IETF100

- Changes to provide middlebox robustness
  - https://github.com/tlswg/tls13-spec/pull/1091
- Move version negotiation entirely into "supported_versions", and hence ServerHello.version == 0x0303 (TLS 1.2)
- Restore the missing session_id and compression fields in ServerHello
- The client sends a fake session_id and the server echoes it
- The server sends ChangeCipherSpec messages after ServerHello/ HelloRetryRequest
- The client sends ChangeCipherSpec after ClientHello.
- Merge HRR and ServerHello into a single message with the semantics distinguished by a special ServerHello.Random value.
- Switch the record layer version to 0x0303 for post-ClientHello messages to match ServerHello.

TLS: MIDDLEWARE BOXES AND ENTERPRISE DECRYPTION

- The "TLS 1.3 backdoor" proposal (draft-green-tls-static-dh-in-tls13)
- The "TLS 1.3 is hard" document (draft-camwinget-tls-use-cases)
- Surprisingly, about a 50/50 split at IETF#99
- IMHO: Any Enterprise decryption requirement should not require an Internet-wide protocol change

ACME: AUTOMATED CERTIFICATE MANAGEMENT ENVIRONMENT

- Protocol that powers LetsEncrypt
- Hugely successful: 50M certs, 25% increase of https
- Problem with Certificate Transparency due to speed of issuance
- Race to bottom for commercial CA's ?
- ACME relies on DNS for authentication, authorization of Challenge Token.
- Why not skip CA infrastructure and use DNSSEC?
  - draft-ietf-tls-dnssec-chain-extension
  - RFC 7901: Chain Query requests in DNS

TCPCRYPT: OPPORTUNISTICALLY ENCRYPT ALL TCP

- WG advancement has been extremely slow (years)
- Finally all proposals merged into a few documents
- Running code (tcpcryptd, linux, freebsd)

- Anonymous encryption
- Possible upgrade to authenticated encryption
- Biggest problem: middleware boxes of course
- See also: QUIC, HTTP/2, TLS

IPSEC DEVELOPMENTS

- Algorithm Updates for IKEv2 (RFC 8247)
  - kills DH 1024, DH 1536, RFC 5114 groups
  - Demote 3DES, SHA1, promote AES_GCM, AES_CCM (IoT)
  - Promotes Digital Signatures (RFC 7427)
  - RSA-PKCS1.5 vs RSA-PSS interop issue
- Algorithm Updates for ESP/AH (RFC 8221)
  - Similar to above
  - Warn SHA2_256 is tainted due to Linux truncation bug
  - Manual Keying mostly banned (IKEv2 vs SDN controller)
- New algos: chacha20poly1305 AEAD, eddsa, QuantumSecure algo's ?

IPSEC DEVELOPMENTS

- IKE and ESP over TCP support (RFC 822)
  - Vendors had their own, now standardized
  - Hidden feature: ESPinTLS to bypass VPN blocking
- IKEv2 DNS and DNSSEC update
  - VPN server can send list of domains and nameservers
- PostQuantum Preshared Key (PPK)
  - A bandaid until we have quantum secure algorithms
- IoT savings (dietESP, implicit-IV)

THE WEB: DNSSEC VERSUS CAB/FORUM

- Browsers don't want DNSSEC TLSA record (latency, reliability)
- The Certificate Agency ecosystem cannot be trusted (500+ trust roots)
  - CRLs, OneCRL, OCSP, et all
  - Pinning with HPKP (RFC 7469)
  - Pinning with TACK (draft-perrin-tls-tack)
  - Pinning with HSTS (RFC 6797)
  - Certificate Transparency (RFC 6269bis)
  - Preloading HSTS blobs in browsers
    - Google asked at ICANN#60 for TLD's to start mandating HTTPS (!!!)
  - OCSP stapling (RFC 6961)
  - OCSP over DNS (ODIN, draft-pala-odin)
  - Certificate Transparency over DNS

  - ACME (LetsEncrypt) reduced CA Industry to DNS security
  - draft-ietf-tls-dnssec-chain-extension seems logical solution

CERTIFICATE TRANSPARENCY (RFC 6269BIS)

- Reduce the attack surface of 600+ (sub) CA's
  - Issue and Pre-publish certificates (as SCT's)
  - Publish on an append-only public audit logs
  - Browsers regularly download the Signed Tree Heads (STH's)
  - Monitors gossip the logs among many
  - Monitors the audit logs
  - Operators monitor the log for their own domains
  - clients trust CERT when pre-CERT on multiple audit logs
  - Submit old CERTs to webserver on CERT change (gossip)
  - Industry wants "certificate redaction" (secret certs)
  - Transparency for binaries, DNSSEC, other things?

DNS SECURITY:

- DNSSEC – DNS data integrity
  - Authenticity of DNS data
  - DNSSEC as a PKI
  - No encryption of data
- DPRIVE – DNS query privacy
  - Reduce sending privacy sensitive data
- DNSOPS - Making it all work

See apps track later today for detailed overview

OPENPGP (RFC 4880BIS)

- Update core specification
- Obsolete old algorithms
- Introduce new algorithms

- Progress is slow
- OCB / patent discussion

QUESTIONS?