Introduction to the Security Area

(the one area to rule them all)

Alexey Melnikov & Sean Turner

2014-11-09

Purpose

- Provide a high level overview of the Security Area:
  - Why you want security services and what they are
  - What are some of IETF’s foundational security-related RFCs
  - Summarize the active Security Area working groups as well as Security-related working groups in other Areas

Security Quotes

- The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.
  - Gene Spaffor

Security Quotes

- The design of security protocols is a subtle and difficult art. … Security protocols are very hard to design; rolling out a new one will require extensive theoretical and practical work to confirm its security properties and will incur both delay and uncertainty.
  - Steve Bellovin

Who’s at fault?

- Mallory and Eve – that’s who!
- Mallory and Eve want:
  - Alice and Bob’s data,
  - Alice to think they’re Bob,
  - Bob to think they’re Alice,
  - Etc.
- Need to ensure protocols continue to operate in a given threat environment.

Security Services: Authentication

- Data Origin Authentication:
  - The corroboration that the source of data received is as claimed.
- Peer Entity Authentication:
  - The corroboration that a peer entity in an association is the one claimed.

Security Services: Data Integrity

- The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Security Services: Data Confidentiality

- The property that data is not disclosed (AM: not readable by unauthorized...???) to system entities unless they have been authorized to know the data.

Security Services: Access Control

- Protection of system resources against unauthorized access.

Security Services: Non-Repudiation

- A security service that provides protection against false denial of involvement in an association.

Some Foundational Security-Related RFCs

- IAB and IESG Statement on Cryptographic Technology and the Internet (RFC 1984)
- Security Considerations Required (as per RFC 2223)
- Strong Security Requirements for Internet Engineering Task Force Standard Protocols (RFC 3365)
- IETF Policy on Wiretapping (RFC 2804)
- Pervasive Monitoring Is an Attack (RFC 7258)
- How to write Security & Privacy Considerations:
  - Guidelines for Writing RFC Text on Security Considerations (RFC 3552)
  - Privacy Considerations for Internet Protocols (RFC 6973)

Some Building Blocks

- IPSec (Internet Protocol Security): IKE (Internet Key Exchange), ESP (Encapsulating Security Payload, AH (Authentication Header)
- TLS (Transport Layer Security) & DTLS (Datagram TLS)
- SSH (Secure Shell)
- Frameworks for application protocol authentication (and more)
  - SASL (Simple Authentication, Security Layer)
  - GSSAPI (Generic Security Service Application Program Interface)
- Kerberos
- PKIX (Pubic Key Infrastructure X.509)
- DNSSEC (Domain Name Security Extensions)
- Object (end-to-end) security:
- S/MIME (Security Multi-purpose Internet Mail Extensions)
- PGP (Pretty-Good Privacy)

DANE

DNS-based Authentication of Named Entities

- Use DNSSEC (Domain Name System Security Extension) protected RRs (resource records) applications.
- RFC 6698 - The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
- SMTP security via opportunistic DANE TLS: draft-ietf-dane-smtp-with-dane
- Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records: draft-ietf-dane-srv-08
- Using Secure DNS to Associate Certificates with Domain Names For S/MIME: draft-ietf-dane-smime-07
- Using DANE to Associate OpenPGP public keys with email addresses: draft-ietf-dane-openpgpkey-01; Best Common Practise for using OPENPGPKEY records: draft-ietf-dane-openpgpkey-usage-01
- Authenticating Raw Public Keys with DANE TLSA: draft-ietf-dane-rawkeys-00

HTTPAUTH

Hypertext Transfer Protocol Authentication

- Update HTTP’s Basic and Digest Authentication mechanisms and work on additional user authentication schemes.
- Password based:
  - The 'Basic' HTTP Authentication Scheme: draft-ietf-httpauth-basicauth-update-02
  - HTTP Digest Access Authentication: draft-ietf-httpauth-digest-08 - WGLC finished
  - Salted Challenge Response (SCRAM) HTTP Authentication Mechanism: draft-ietf-httpauth-scram-auth-03
  - Mutual Authentication Protocol for HTTP: draft-ietf-httpauth-mutual-03
- HTTP Origin-Bound Authentication (HOBA): draft-ietf-httpauth-hoba-05 - WGLC finished
  - Replaces password with a bare key

Kitten

- Kerberos Authorization Data Container Authenticated by Multiple MACs: draft-ietf-krb-wg-cammac-11 - submitted to IESG
- A set of SASL Mechanisms for Oauth: draft-ietf-kitten-sasl-oauth-16 - in WGLC
- SAML Enhanced Client SASL and GSS-API Mechanisms: draft-ietf-kitten-sasl-saml-ec-11 - currently expired
- Namespace Considerations and Registries for GSS-API Extensions: draft-ietf-kitten-gssapi-extensions-iana-08 - currently expired
- AES Encryption with HMAC-SHA2 for Kerberos 5: draft-ietf-kitten-aes-cts-hmac-sha2-05
- Structure of the GSS Negotiation Loop: draft-ietf-kitten-gss-loop-00- in WGLC
- Initial and Pass Through Authentication Using Kerberos V5 and the GSS-API (IAKERB): draft-ietf-kitten-iakerb-02

MILE

Managed Incident Lightweight Exchange

- Develops IODEF (Incident Object Description Exchange Format) to support computer and network security incident management.
- The Incident Object Description Exchange Format v2: draft-ietf-mile-rfc5070-bis-09
- IODEF Enumeration Reference Format: draft-ietf-mile-enum-reference-format-09 - in IESG review
- IODEF Usage Guidance: draft-ietf-mile-iodef-guidance-03

SACM

Security Automation and Continuous Monitoring

- Is tasked to produced standardized protocols to collect, verify, and update system security configurations in order to automate what is frequently done manually.
- This work is related to MILE and a now complete NEA (Network Endpoint Assessment) WGs.
- Documents:
  - draft-ietf-sacm-architecture-00
  - draft-ietf-sacm-information-model-00
  - draft-ietf-sacm-requirements-02
  - draft-ietf-sacm-terminology-05
  - Endpoint Security Posture Assessment - Enterprise Use Cases (draft-ietf-sacm-use-cases-07)

TRANS

Public Notary Transparency

- Certificate Transparency (draft-ietf-trans-rfc6962-bis-04)
- Possible new work?
  - Gossiping in CT (draft-linus-trans-gossip-ct-00) - detecting malicious logs showing different views to different clients
  - CT for Binary Codes (draft-zhang-trans-ct-binary-codes-00)

WebSec (APPS)

Web Security

- Public Key Pinning Extension for HTTP (draft-ietf-websec-key-pinning-21) - approved for publication
  - Defines a new HTTP header that allows web host operators to instruct user agents to remember ("pin") the hosts' cryptographic identities over a period of time.
  - Helps to deal with compromised Certificate Authorities (CAs)
- The WG will close after publication, rechartering looks unlikely

TLS

Transport Layer Security

- Prohibiting RC4 Cipher Suites: draft-ietf-tls-prohibiting-rc4-01 – resolving WGLC comments
- TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks: draft-ietf-tls-downgrade-scsv-00 – just about read for WGLC
- TLS Session Hash and Extended Master Secret Extension: draft-ietf-tls-session-hash-02 – just about ready for WGLC
- Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for TLS: draft-ietf-tls-negotiated-ff-dhe-02 – probably ready for WGLC after this meeting
- TLS 1.3: draft-ietf-tls-tls13-03 – lively discussions

ACE

Authentication and Authorization for Constrained Environments

- No WG drafts yet but they’re getting close
- DTLS based proposal is being worked on initially

DICE

DTLS In Constrained Environments

- Profiling DTLS for CoAP:
  - A Datagram Transport Layer Security (DTLS) 1.2 Profile for the Internet of Things: draft-ietf-dice-profile-05
- Use of DTLS with multicast is in scope, but no official WG document yet

UTA (APPS)

Using TLS in Applications

- Summarizing Known Attacks on TLS and DTLS (draft-ietf-uta-tls-attacks-05) - should be approved by IESG shortly
- Recommendations for Secure Use of TLS and DTLS (draft-ietf-uta-tls-bcp-06) - in WGLC
- Updated TLS Server Identity Check Procedure for Email Related Protocols (draft-ietf-uta-email-tls-certs-00)
- Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP) (draft-ietf-uta-xmpp-02)
- A document describing use of TLS in IMAP/POP/SMTP submission is discussed, but not yet a WG document

IPSECME

Internet Protocol Security Maintenance and Extensions

- Currently re-chartering (normal for them)
- The NULL Authentication Method in IKEv2 Protocol: draft-ietf-ipsecme-ikev2-null-auth-01 – recently adopted
- Protecting Internet Key Exchange (IKE) Implementations from Distributed Denial of Service Attacks: draft-ietf-ipsecme-ddos-protection-00 – recently adopted

JOSE

Javascript Object Signing and Encryption

- “cookbook” (draft-ietf-jose-cookbook-05) – IETF LC soon
- JWA (JSON Web Algorithms): draft-ietf-jose-json-web-algorithms-36 – Almost through IESG
- JWE (JSON Web Encryption): draft-ietf-jose-json-web-encryption-36 – Almost through IESG
- JWK (JSON Web Key): draft-ietf-jose-json-web-key-36 – Almost through IESG
- JWS (JSON Web Signature): draft-ietf-jose-json-web-signature-36 – Almost through IESG

OAUTH

Web Authorization Protocol

- OAUTH allows a user to grant a third-party Web site or application access to the user's protected resources, without necessarily revealing their long-term credentials, or even their identity.
- Too many drafts to list …
  - OAuth 2.0 Dynamic Client Registration Protocol (draft-ietf-oauth-dyn-reg-20)
  - SAML, JSON token types, …

STIR (RAI)

Secure Telephone Identity Revisted

- Specify Internet-based mechanisms that allow verification of the calling party's authorization to use a particular telephone number for an incoming call.
- Authenticated Identity Management in the Session Initiation Protocol (SIP): draft-ietf-stir-rfc4474bis-02
- Secure Telephone Identity Credentials: Certificates: draft-ietf-stir-certificates-00

TCPINC (TRANS)

TCP Increased Security

- Develop the TCP extensions and a key management scheme to support unauthenticated encryption and integrity protection of TCP streams.
- No WG drafts yet …

DMARC (APPS)

Domain-based Message Authentication, Reporting & Conformance

- Just formed, no official documents.
- DMARC allows mail sending organization to express in DNS domain-level policies and preferences for message validation, disposition, and reporting.
- Is using SPF and DKIM underneath, but in theory other authorization mechanism can be added.

DPRIVE (INT)

DNS PRIVate Exchange

- Develop mechanisms to provide confidentiality to DNS transactions, to address concerns surrounding pervasive monitoring.
- Just started!
- DNS privacy considerations: draft-ietf-dprive-problem-statement-00

SIDR (RTG)

Secure Inter-Domain Routing

- Reduce vulnerabilities in the inter-domain routing system: address address blocks being inappropriately announced by an originating autonomous system and reachability information inserted inappropriately.
- RFCs and drafts too many to list.

OPSEC (OPS)

Operational Security Capabilities for IP Network Infrastructure

- Document operational issues and best current practices with regard to network security.
- BGP operations and security: draft-ietf-opsec-bgp-security-06
- Operational Security Considerations for IPv6 Networks: draft-ietf-opsec-v6-05
- DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers: draft-ietf-opsec-dhcpv6-shield-04

CFRG (IRTF)

Crypto Forum Research Group

- Works on cryptographic primitives used by all of IETF protocols, such as:
  - Ciphers
  - Hash Functions
  - PAKE (Password-authenticated key agreement)
  - Elliptic curve (EC) recommendations