COMSEC 1 – How can we increase usage of current COMSEC tools?

Hannes Tschofenig

Why aren't people using them? In what situations are / aren't they used?

ON PAPER EVERYTHING LOOKS GREAT

HTTP

- Story in a nutshell:
  - HTTPS is a core piece in the complex Web security story.
  - HTTPS also key for mobile apps although there are additional challenges with cert verification (see #48)
- Eckersley argues in #38 that part of the problem is the CA infrastructure, slow update cycles, and captive portals.
- While the % of websites using HTTPS is increasing it is still rather low.

Session Initiation Protocol (SIP)

- Story in a nutshell:
  - TLS and IPsec for hop-by-hop security
  - SIP Identity for caller identity assurance (see also STIR)
  - Long list of end-to-end media security: RFC 5479 (including DTLS-SRTP)
- Peterson argues in #10
  - “SIP’s susceptibility to mass surveillance was essential to its success.”
  - Is there an attribute problem in the telecommunication industry?
- Does RTCWeb suffer from the same problem?
  - “For the most part, no. The constituencies behind RTCWeb are radically different than those who drove SIP. ”

XMPP

- Story in a nutshell:
  - Hop-by-hop security using TLS
  - End-to-end security (various solutions, including OTR)
- In #22 Saint-Andre highlights the ongoing community effort with the “IM Observatory“ to mandate encryption on all hops under their control.
- Still, many normal users utilize proprietary IM tools like Skype, Whatsapp, etc. with unknown or questionable security properties.
  - End user awareness problem? Lack of usable software?

AAA: RADIUS & Diameter

- Story in a nutshell:
  - Hop-by-hop authentication standardized for RADIUS and Diameter.
  - Products sometimes implement security techniques but deployments rarely use them.
- Aboba observes (in #53) that
  - Operational cost (and impact on network reliability) of key management, troubleshooting, etc. is a major factor.
  - Developing best practice guidelines could help to result in pressure to enable.
- Solutions for lowering operational costs proposed in #19 and #34.

How can we (IETF / W3C / Internet community) encourage more/better use?

WHAT SHOULD BE DONE?

Solution Strategies

- The toolbox is incomplete
  → New specifications
  - Alternatives to CA system (e.g., hosts file - #38)
  - Opportunistic Keying (see #66)
- Operational Cost
  → Reducing complexity
  - Via Profiles (see #34)
  - Via new key management techniques (see #19)
- Lack of awareness / insufficient knowledge
  → Education and outreach (see #5)
- There is something wrong with the deployment / vendor community
  → Focus on different communities (see #10)

Questions

- What are the low hanging fruits?
- What are the stumbling blocks for deployment?
- How can we encourage deployment?
- Is running (D)TLS / SSH going to solve the problem? (e.g., in the AAA/syslog/snmp) context?
- Are there problems with implementations?