TCP Increased Security (tcpinc) WG

IETF 91
Honolulu, HI, USA
2014-11-14 09:00-11:30

Chairs: Tero Kivinen
Marcelo Bagnulo

Area Director: Martin Stiemerling
Tech Advisor: Stephen Farrel

Mailing list: tcpinc@ietf.org

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Administrativia (chairs, 5 minutes)
  - Blue sheets, Jabber scribe, Minute-taker
- Agenda Bashing (chairs, 5 minutes)
- Summary of Related Drafts (chairs, 5 minutes)
- Protect or not the TCP header fields (chairs, 15 minutes)
- Inner space (Bob Briscoe, 15 minutes)
- Discussion

Summary of Related Drafts

- Draft-bittau-tcpinc-tcpcrypt-00
- Draft-rescorla-tcpinc-tls-option-01
- Draft-thomson-tcpinc-dtls-00
- Draft-touch-tcp-ao-encrypt-02

Draft-bittau-tcpinc-tcpcrypt

- Continued deployment.
  - Official Debian and Fedora packages released.
- Biggest uncertainty: tcpinc stance on header protection:
  - If we want header protection: tcpcrypt solves problem as is.
  - If not: have contingency plan to update draft with cumulative MAC more robust to middleboxes.

Draft-rescorla-tcpinc-tls-option

- Removed the tiebreaker from the default SYN (saving options space)
- Added support for explicit simultaneous open
- Explicitly discussed channel bindings
- Expanded security considerations

Draft-thomson-tcpinc-dtls

- Nothing to report.

Draft-touch-tcp-ao-encrypt

- New version this week
- Allows use of a 128-bit DH key in legacy TCP
- Allows use of larger keys given any of the SYN option space extensions under discussion in TCPM

Protect or not the TCP header fields

Tero Kivinen

Protect or not the TCP header fields

- Summary posted by Marcelo 2014-10-06
- Trade-offs:
  - Security
    - Protecting headers might offer better security
  - Deployability
    - Protecting headers would most likely be less deployable
  - Complexity
    - Protecting headers would most likely be more complex

Header fields

- IP and ports
- Sequence and ACK numbers
- Flags
- URG pointer, RCV Window

TCP Header

Offsets Octet		0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																	Urgent pointer (if URG set)														
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Options

1. Protect only payload
   - Don't include any of the TCP header fields in the MAC calculations
2. Protect the payload plus some fields of the TCP header

   a) MAC in TCP option

   b) MAC in TCP payload

   c) MAC for TCP header fields in TCP option, and MAC for payload in payload

Consensus on the list

- There were only few answers to the which option to pick, and for those who clearly selected one option, majority supported option 1, i.e. that there is no need to protect TCP headers.

Inner Space

Bob Briscoe

Discussion