SecSH WG Core IDs

Chris Lonvick
clonvick@cisco.com

Core IDs

- draft-ietf-secsh-architecture-18.txt
  - [SSH-ARCH]
- draft-ietf-secsh-assignednumbers-07.txt
  - [SSH-NUMBERS]
- draft-ietf-secsh-connect-20.txt
  - [SSH-CONNECT]
- draft-ietf-secsh-transport-19.txt
  - [SSH-TRANS]
- draft-ietf-secsh-userauth-22.txt
  - [SSH-AUTH]

Tickets

- http://rt.psg.com/
- Userid: ietf
- Passwd: ietf
- Select tickets from the SecSH WG.

Ticket 440 - registries

- There were instructions to the IANA in [SSH-ARCH].
- A statement was added to specify that only [SSH-NUMBERS] contained the instructions to the IANA for all IDs.
- Recommend to CLOSE this ticket.

Ticket 441 – “at sign”

- The IESG felt that the “@” in the local namespace would be confused with email addresses and should be allocated by mail administrators.
- Additional text was inserted to state that the local namespace was using the “@” character to differentiate PRIVATE USE namespace from IANA assigned namespace.
- Additionl text was inserted to say that the use of “@” had nothing to do with RFC0822.
- Recommend to CLOSE this ticket.

Ticket 450 - “example”

- The IESG noted that there were several cases where real IP address ranges and real DNS names were used in the IDs.
- RFC1918 addresses were inserted (except cases where 127.0.0.1 are needed), and “example.com” replaced other DNS names.
- Recommend to CLOSE this ticket.

Ticket 453 - “sshv1”

- The IESG wants a reference to SSHv1.
- Some textual changes were made but we're still looking for a stable reference to the source code.
- Recommend to find a reference.

Ticket 454 - Algorithm

- [SSH-TRANS]19 Section 6.3, second paragraph. The document says: "...effective key length of 128 bits or more". Yet, Triple-DES is the REQUIRED algorithm, and it does not meet this goal. Suggestion: "...effective key length of 96 bits or more".
- Is this suggestion acceptable?

Ticket 461 - implicit

- The IESG notes that [SSH-TRANS]19 Section 10 contains, “Note that after a key exchange with implicit server authentication, the client MUST wait for response to its service request message before sending any further data.” Which is “unclear”; what is “implicit authentication”?
- Recommend that we take this to the mailing list.

Ticket 462 - “different”

- [SSH-TRANS]19 Section 6.3. SSH allows the client and server to employ different algorithms for the data that they encrypt. This practice should be discouraged somewhere in the document. It is likely to cause interoperability problems, and it offers no security advantage.
- The same is done for compression in Section 6.2.
- Recommend to take this to the mailing list.

Ticket 463 - “timeout”

- [SSH-USERAUTH]22 Section 4, last paragraph. Setting the SHOULD for the timeout to 10 minutes seems very long. Doesn't it open up some denial-of-service attacks. The SHOULD for the timeout ought to be for interoperability.
- Recommend we quickly discuss and resolve, or take it to the mailing list.

Ticket 464 - utf8

- [SSH-USERAUTH]22 Section 8 - “Saying that UTF-8 is the encoding for passwords means that implementations need to check for valid UTF-8 encoding. This could lead to unexpected failures. It would be much better to say that passwords are arbitrary binary strings with no specified encoding. Exact match of the binary strings ought to be sufficient.”
- This seems to be similar to the current discussion on the mailing list.
- Any quick resolution, or keep it on the mailing list?

Ticket 465 – new proto

- “I have been reading these drafts for the past several weeks attempting to figure out how another protocol (netconf) could run over ssh. As a newcomer to these specifications, it was difficult for me to figure out how the different ssh protocols and services relate to each other. In particular, how the ssh-userauth and ssh-connection services are related.
- Although the architecture document discusses the fact that ssh-connection runs "over" ssh-userauth, it isn't entire clear to me what that means. If I understand correctly, it means that the ssh-userauth service needs to be invoked and result in a successful authentication before the ssh-connection service can be invoked?
- If so, I think it would be helpful for the ssh-connect document to explicitly say that.”
- Discussion?

Ticket 474 - x509

- X509 certs is specified in [SSH-TRANS]19 Section 6.6. Comments received have been that either this needs to be described better, or removed.
- Discussion?

Ticket 460 and 601 - Oakley

- We started by updating the diffie-hellman-group1-sha1 group. We arrived at
  - diffie-hellman-group2-sha1
  - diffie-hellman-group14-sha1
- Both of these are now in use and mean the same thing.
- Discussion?