Report of the 34rd meeting of ISO/IEC JTC1/SC27 in Russia

Erik Zenner

Danmarks Tekniske Universitet
e.zenner@mat.dtu.dk

København, 20. juni 2007

Preliminaries

Special circumstances:

- Unusual location
- Low participation
- Many editors and important experts missing (U.S., Canada, U.K., France,...)
- Very little progress

WG 2 current issues

Working items:

- Normal cryptographic standardization (Encryption, Authentication, Signatures,...)
- Study periods:
  - Road map
  - Low-power encryption
  - Signcryption
  - Merge 9796 and 14888
  - Formal proof and verification of security of cryptographic mechanisms
  - OIDs and ASN.1 syntax
- Liaison statement ISO/TC 68/SC 2

Hash functions status

What happened?

- Recent results:
  - De Cannière, Rechberger: Collision for 64-round SHA-1.
  - Preneel: Expects collision for full SHA-1 before the end of the year.
- ISO: No update of hash standard at the moment (await development).
- NIST: Starts selection of new hash standard (similar to AES).

A footnote in 18033-3

Original footnote:

The keying Option 2 (2-key Triple DES) is approved only through the year 2010 by NIST.

What happened?

- Banking industry protests through ISO / TC 68 / SC 2.
- WG 2 had many discussions about this issue in 2006 and 2007.
- WG 2 decides to change text: "keying option 2 is approved [...] by NIST *for the protection of US federal government information*."
- SC 27 plenary overrules WG 2 decision and deletes footnote.
- A liaison officer for ISO / TC 68 / SC 2 is requested.

Stream cipher amendment

What happened?

- In December, the editor (i.e., me) submitted a 2nd working draft.
- Three days before the meeting, Japanese experts submit a new algorithm which is very new (first proposed in February 2007).
- In the editing session, only 5 national bodies are present: Denmark, South Africa, UK, Korea, Japan
- No agreement $\Rightarrow$ Call for comments (N5804).
- In the next days, I will propose a Danish comment.

WG 5 comments

What happened?

- I did not participate in any of the WG 5 meetings, and will not be able to do so in the future, either. $\Rightarrow$ Anyone interested?
- Dick Brackney was not present at the meeting.
- Convenor issue is still somewhat difficult.

Upcoming meetings

Next meetings:

- October 1-5, 2007; Luzern (Switzerland)
- April 14-18, 2008; Kyoto (Japan)