Preventing type flaw attacks

Type flaw attacks can be prevented by tagging each field—atomic values, concatenations, encrypted components, etc.—with some information giving their claimed type.

(The tag for concatenations should include enough information to allow the concatenation to be split into components correctly; and the tag for encryptions should include the type of the encryption key and of the body.)

Principle 11

The protocol designer should know which trust relations his protocol depends on, and why the dependence is necessary. The reasons for particular trust relations being acceptable should be explicit though they will be founded on judgement and policy rather than on logic.

Examples of Principle 11

The Kerberos protocol depends upon Kerberos and the ticket granting servers being trustworthy.

Protocols that use random values (e.g. nonces and session keys) depend upon the random number generators being trustworthy.

Protocols that use public key cryptography depend upon the certificates that authenticate those public keys being accurate, so these protocols depend upon the certification authorities being trustworthy.

Predictable RNG useless in security protocols!
Must not predict last/next.
Seeding?
- Simple semi-rand noise on comm. channels.
- random keyboard character junk.
-