Report on Present State of DSA Signature Evaluation (full evaluation)

January 28, 2002

Seiichi Susaki, Member

Public-Key Cryptography Subcommittee

DSA signature

(one of the signature systems included in guidelines for electronic signature law)

- Category: Signature
- Security basis: Discrete logarithm problem on a finite field
- Provable security: Provable security has not been shown.
- Characteristics: This signature uses Schnorr's technique to improve upon the deficiencies in the ElGamal signature (in which the signature is twice as long as the original message).

Full evaluation

- Four evaluators were requested to evaluate the scheme based on the following perspectives:
  - Cryptographic primitives
  - Cryptographic scheme
  - Random number generating method provided in FIPS 186-2 Appendix 3.

Evaluation comments

– Parameter selection –

- Attack methods for a number of special parameters have been reported. Therefore, suitable parameters must be selected.
- The same random number k must not be applied to multiple messages (messages with signatures).
- An evaluator commented that the parameter size should be set to a higher value.

Evaluation comments

– Provable security –

- As of the present time, provable security based on a suitable model or assumption has not been reported. (It is possible to show provable security on par with the difficulty of discrete logarithm problems if slight changes are made to the DSA signature.)

Evaluation comments
– Random number generation –

- With the random number generation method in Appendix 3, the output random numbers show a bias. Therefore, it is recommended that random numbers be generated using the procedure presented as Change Notice 1 (the detailed attack method is not disclosed).
- It was reported that if a certain number of bits in random number k are known, the secret key could be known.
- Systems using SHA-1 and DES are specified as the random number generation methods. However, an evaluator noted that SHA-1 should be used because systems using DES have special properties.

Evaluation comments

– Other issues –

- Efficient attack methods have not been reported for SHA-1. Therefore, at the present time it can be regarded as a secure, one-way hash function.
- An evaluator noted that replay attacks could occur depending on the implementation method.