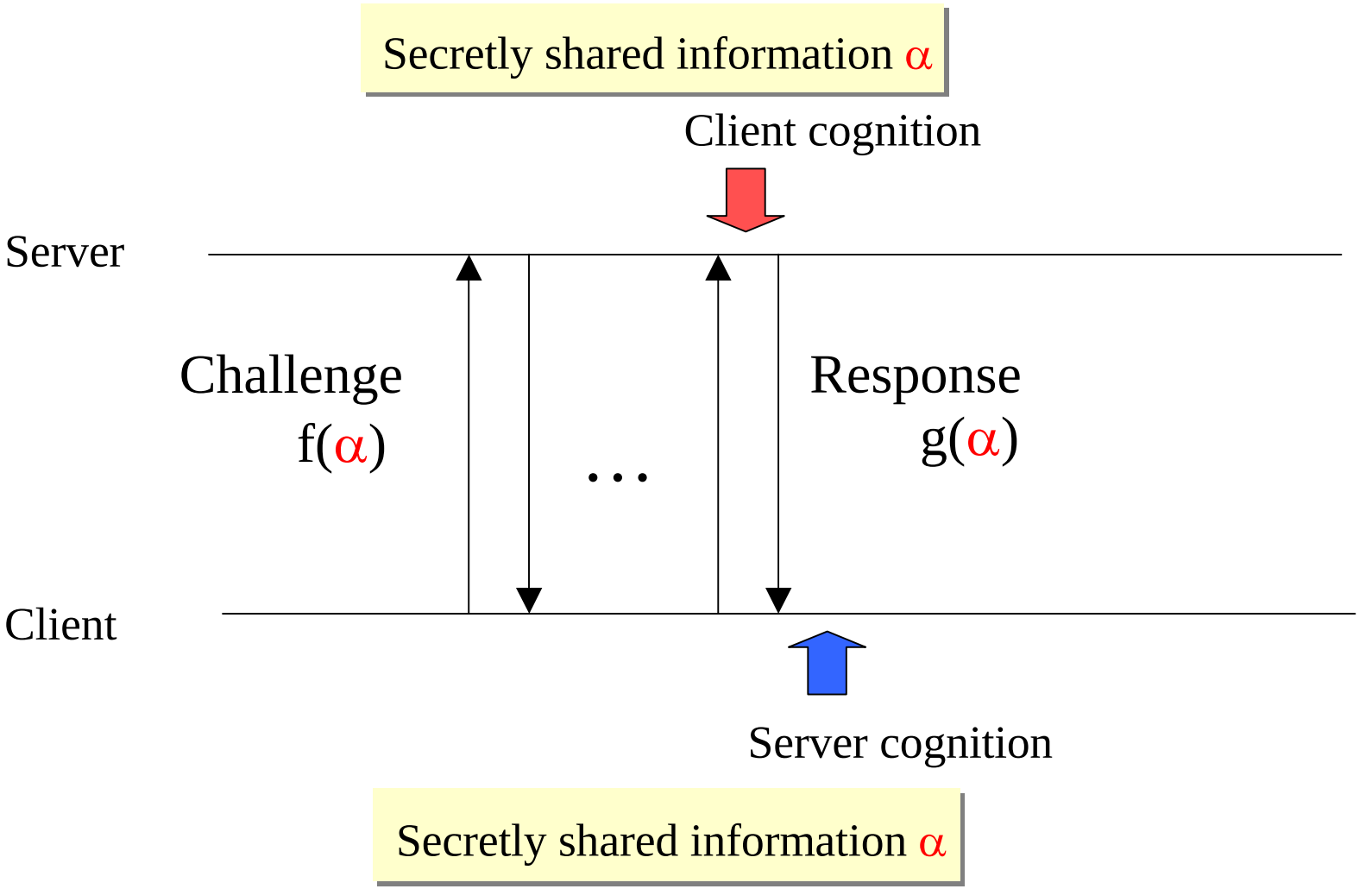
Report on Present State of TAO TIME Evaluation (screening evaluation)

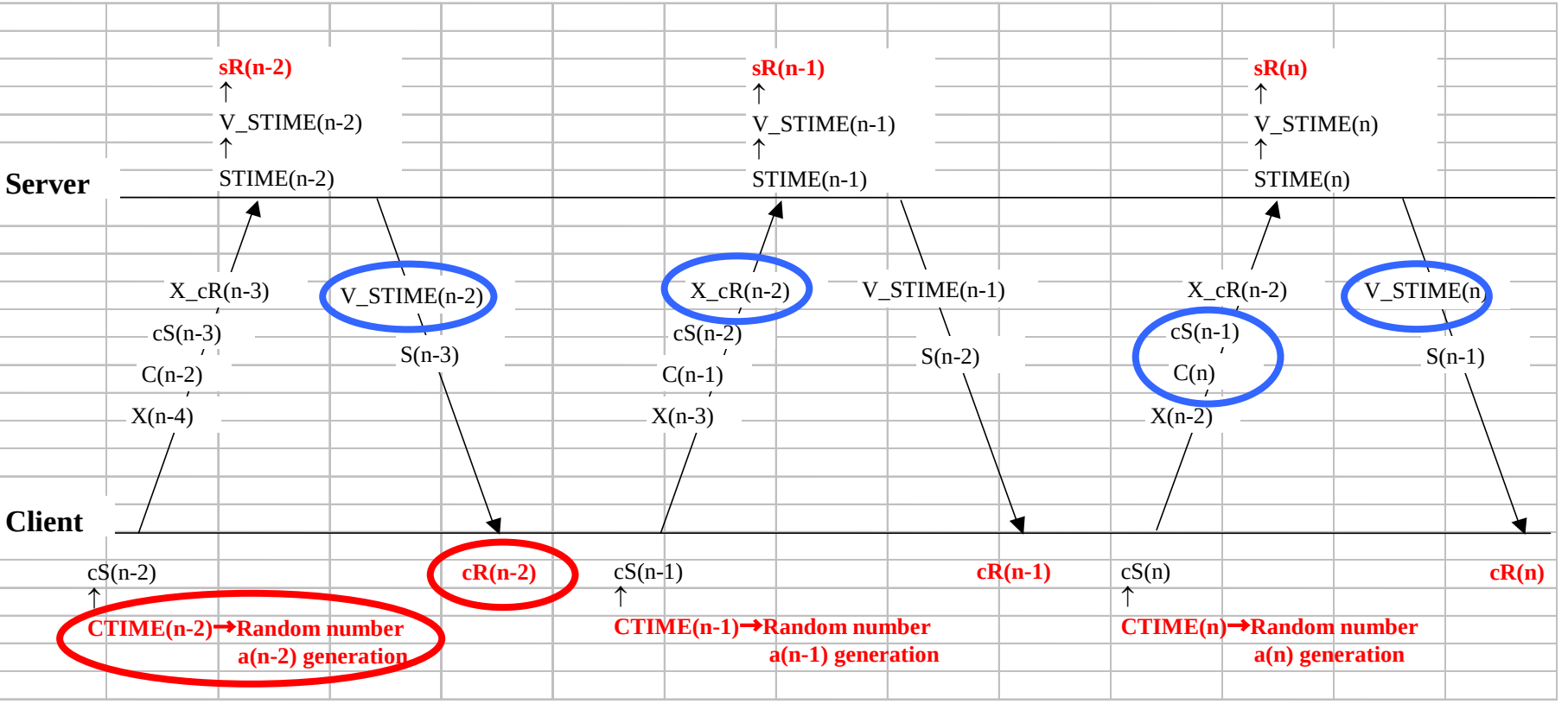
January 28, 2002

Kazuo Takaragi, Member
Symmetric-Key Cryptography Subcommittee

Basic flow of remote party authentication with TAO TIME



Overview of processing sequence



$$cR(n-2)=<V\_STIME(n-2)\ldots+\{cR(n-3)-cS(n-3)\} + \ldots + \mathbf{a}(n-2)> + 1$$

$$X\_cR(n-2) = cR(n-2) + \{\alpha(X(n-2)) + \beta(X(n-2))\}$$

– – – The red characters are TAO data which is not exposed to the network – – –

Pseudo-random number generating functions to be evaluated

Focus points for CRYPTREC

Is random number a(n) a pseudo-random number generator for the call?
→ Evaluated this way because it is not seen elsewhere.
→ Is a(n) recognized as a pseudo-random number generator?

a(n) calculation formulas to be evaluated:

[CTIME(n) calculation formula]: CTIME(n) = Client local clock sending event time (current time in milliseconds)

[rand() initial value calculation formula]: a(n-1) ∗ 1000 +CTIME(n) mod 1000
The above calculation is performed each time a(n-1) is generated.

a(n)=a(n-1)+{rand( )+1} ∗ 100000 +CTIME(n) mod 100000

Rand function in ANSI C

- The rand function generates random integers between 0 and RAND_MAX.
- The only requirement specified by the ANSI C standard is that RAND_MAX must be at least 32767.
- ANSI C standard permits that the calculation method may vary.
- However, pseudo-random numbers generated by rand() are in fact as shown below (example for Visual C++), as in the case of numbers based on the linear congruence method).

$x_1 = 1$ (This is the seed. It can be changed using srand().)

$x_n \equiv 214013 * x_{n-1} + 2531011 \bmod 2^{31}$

X = Integer portion of $(x_n/2^{16})$ $(0 < X < 2^{15})$

a(n) Series

- CTIME(n) is the current time (sending time) displayed in milliseconds; i.e., the physical time.
- Calculation formula
  $a(n)=a(n-1)+\{rand( )+1\}*100000 +CTIME(n) \bmod 100000$
  Thus, the last five digits, when a(n)-a(n-1) is given in decimal notation, are matched to the last five digits in CTIME(n) (decimal notation).

  This means that the last five digits of a(n)-a(n-1) are always the physical time.

Evaluation by Evaluator 1

Conclusion: There is no need for a full evaluation.

Comments
(excerpts):

- The specifications describe the primary objective as providing simple authentication functions between client and server.
- With minor modifications, it is possible to change the specifications so as to generate pseudo-random numbers.
- However, these specifications make absolutely no use of cryptographic functions (basic operations used in asymmetric-key cryptography (e.g., addition and multiplication in prime field, extension field, and rings and groups based thereon), hash functions, pseudo-random number generators (key stream generators), block ciphers). Thus regardless of the type of modification, it is not possible to expect random number generation for use in secure key generation and the like.

Evaluation by Evaluator 2

Conclusion: There is no need for a full evaluation.

Comments
(excerpts):

- In Section 1 (Introduction) of the cryptographic technique specifications, the submitter claims the following: “The TAO TIME cognition algorithm is a cognition algorithm whose purpose is to build a mutual cognition system between client and server, existing at any two points in the network”. The specifications describe this cognition algorithm.
- In my opinion, these cryptographic technique specifications do not describe a “deterministic algorithm that outputs a (pseudo-random) sequence with respect to a seed (input value)”, which is required for the specifications of a pseudo-random number generator.
- Therefore, the cryptographic technique is not considered to be a candidate for screening evaluation due to insufficiencies in the submitted documents. In conclusion, I believe a full evaluation is not needed.

Evaluation by Evaluator 3

Conclusion: There is no need for a full evaluation.

Comments
(excerpts):

- This proposal was submitted as a random number generating technique, but it is actually a proposal for a “cognition” system that uses random number generation. In addition, the random number generation consists of nothing more than using known methods. Even as a “cognition” system, it is not sufficiently described, and seems to have security problems as well.
- The introduction of random numbers seems to be important for “cognition”, but this is not discussed.

Evaluation by Evaluator 4

Conclusion: There is no need for a full evaluation.

Comments
(excerpts):

- The submitter claims the TAO TIME cognition algorithm is a pseudo-random number generator, but I see absolutely no grounds for this claim. I believe this method is not a pseudo-random number generator. Therefore, a full evaluation is not necessary.
- The submitter provides no grounds for the claim that the TAO TIME cognition algorithm is a pseudo-random number generator. If the submitter is to claim this, then it would be necessary to evaluate aspects such as the generated pseudo-random number sequence's period, linear complexity, and 0/1-balancedness, etc.

Evaluation by CRYPTREC Symmetric-Key Cryptography Subcommittee

Opinion: Full evaluation is not necessary.

Reasons:

- This proposal was submitted as a random number generating technique, but it is in fact a “cognition” system that uses random number generation.
- With minor modifications, it is possible to change the specifications to a proposal for a random number generating technique.
- However, we believe the submitter has weak grounds for claiming that the TAO TIME cognition algorithm is a pseudo-random number generator.