T-79.5502 Advanced Course in Cryptology

Lecture 4, Part 2

November 13 , 2007

Authentication Theory

Authentication Codes

This lecture is based on: Thomas Johansson. Authentication codes, see: http://www.selmer.uib.no/researchcourse2004/program/

An unconditionally secure solution to the authentication problem first appeared in 1974:

E.N. Gilbert, F.J. MacWilliams and N.J.A. Sloane, “Codes which detect deception”, *Bell System Technical Journal*, vol. 53, no. 3, 1974, pp. 405–424.

Gustavus Simmons was independently working on the same problems. In the beginning of the 80’s Simmons published several papers on the topic, and established the authentication model, see

G.J. Simmons, “A survey of Information Authentication”, in *Contemporary Cryptology, The science of information integrety*, G.J. Simmons, Ed., IEEE Press, New York, 1992. pp. 379–420.

Simmons work on authentication theory has a similar role as Shannon’s work on secrecy, see:

C.E. Shannon, “Communication Theory of Secrecy Systems”, *Bell Syst. Tech. J.*, vol. 28, Oct. 1949, pp. 269–279.

Authentication Model

- Three participants, *the transmitter*, *the receiver*, and *the opponent*.
- The transmission from the transmitter to the receiver takes place over an insecure channel.
- Opponent (enemy) has access to the channel in the sense that he can insert a message into the channel, or alternatively, observe a transmitted message and then replace it with another message.

Authentication code

s source message, $s \in S$, S is the set of possible source messages;

m (channel) message, $m \in M$, M is the set of possible channel messages;

e secret encoding rule (aka key), $e \in E$, E is the set of possible encoding rules. The key is secretly shared between the transmitter and the receiver.

Authentication code (A-code) is a mapping $f : S \times E \to M$, $(s, e) \to m$.

Injectivity property of f: if $f(s, e) = m$ and $f(s', e) = m$, then $s = s'$. (Otherwise the receiver would not be able to determine which source message was transmitted.)

When the receiver receives a message m, he must check whether a source message s exists, such that $f(s, e) = m$. If such an s exists, the message m is accepted as authentic (m is called valid). Otherwise, m is not authentic and thus rejected. We can assume that the receiver checks $f(s, e)$ for all $s \in S$, and if he finds $s \in S$ such that $f(s, e) = m$ he outputs s and otherwise he outputs a reject signal.

Deception

Two possible attacks:

(1) impersonation attack: the opponent inserts a message m and hoping for it to be accepted as authentic

(2) substitution attack: the opponent observes the message m and replaces this with another message m', $m \neq m'$, hoping for m' to be valid.

The opponent chooses the message to maximize success probability.

Impersonation probability: $P_I = \max_m \Pr[m \text{ is valid}]$

Substitution probability: $P_S = \max_{m,m',\, m \neq m'} \Pr[m' \text{ is valid} \mid m \text{ is valid}]$.

(Note that these definitions consider only transmission of a single message. For transmission of multiple messages, we must introduce a more general definition of the deception probabilities.)

Deception probability: $P_D = \max(P_I, P_S)$.

Denote: $E(m)$ the set of keys for which a message m is valid,

$E(m) = \{e \in E; \text{ there is } s \in S, f(s, e) = m\}$.

Basic properties

The number of authentic messages in M is at least |*S*| . Hence

$$P_I \geq |S| \,/\, |M|$$

Similarly for the substitution attack, after the observation of one legal message, at least $|S| - 1$ of the remaining $|M| - 1$ messages must be authentic. Thus

$$P_S \geq \, (|S| - 1) \,/\, (|M| - 1) \,.$$

It follows:

(1) In order to have good protection $|M|$ must be chosen much larger than $|S|$. This affects the message expansion of our authentication code. For a fixed source message space, an increase in the authentication protection implies an increased message expansion.

(2) Complete protection, i.e., $P_D = 0$, is not possible. We must be satisfied with a protection where P_D is small.

Example 1

$S = \{H, T\}$, $M = \{1, 2, 3, 4\}$ and $E = \{0, 1, 2, 3\}$

e \ m	1	2	3	4
0	H	T	-	-
1	T	-	H	-
2	-	H	-	T
3	-	-	T	H

It is easy to verify that $P_I = 1/2$ if the keys are uniformly distributed.

Simmons' Bounds

(Simmons' bounds) Let $\mathrm{H(X)}$ denote the entropy of the random variable X, and $\mathrm{I(X;\,Y)}$ denote the mutual information between X and Y, $\mathrm{I(X,Y)} = \mathrm{H(X)} - \mathrm{H(X|Y)}$. For any authentication code,

$$P_I \geq 2^{-\mathrm{I(M;E)}} \text{ , and } P_S \geq 2^{-\mathrm{H(E|M)}} \text{ , if } |S| \geq 2.$$

For the impersonation attack, we see that P_I is upper bounded by the mutual information between the message and the key. This means that in order to have a good protection, i.e., P_I small, we must give away a lot of information about the key. In the substitution attack, P_S is lower bounded by the uncertainty about the key when a message has been observed. Thus we cannot waste all the key entropy for protection against the impersonation attack, but some uncertainty about the key must remain for protection against the substitution attack.

It follows that

$$P_I P_S \geq 2^{-\mathrm{I(M;E)}-\mathrm{H(E|M)}} = 2^{-\mathrm{H(E)}} .$$

From the inequality $\mathrm{H(E)} \leq \log_2 |\mathrm{E}|$ we then obtain:

(Square root bound). For any authentication code, $P_D \geq \sqrt{|E|}$

Example 1 continued

- Keys are uniformly distributed, thus $H(E) = 2$. Then also M is uniformly distributed, and $H(M) = 2$, independently of the distribution of S. Similarly, as in Stinson, Thm 2.10 we get: $H(E|M) + H(M) = H(E,M) = H(E,S) = H(E) + H(S)$, from where it follows that $H(E|M) = H(E) + H(S) - H(M) = H(S)$. Thus $H(E|M) \leq 1$ with equality if the source messages H and T are equiprobable. Hence $I(M;E) = H(E) - H(E|M) \geq 1$. It follows that $P_I = ½ \geq 2^{-I(M;E)}$ with equality if the source messages are equiprobable.

- For the substitution probability we get $P_S \geq 2^{-H(E|M)} = 2^{-H(S)}$ if. In the case where the source messages are equally likely, we can easily verify that $P_S = ½$. On the other hand, then $H(S) = 1$, and thus the equality $P_S = 2^{-H(S)}$ holds.

Constructions based on Reed-Solomon codes

Let $\mathbb{F}_q$ be a field with q elements. We set

$S = \{s=(s_1,\ldots,s_k),\ s_i \in \mathbb{F}_q\}$

$s(x) = s_1x + s_2x^2 + s_3x^3 + \ldots + s_kx^k$

$E = \{(e_1,e_2)\}$

We define f: $f(s,e) = (s,\ e_1 + \mathrm{s}(e_2))$, where $\mathrm{s}(e_2)$ is the polynomial $s(x)$ evaluated at the point $x = e_2$.

Then the parameters of the A-code are:

$|S| = q^k,\ |E| = q^2,\ |M| = q^k + 1.$

The attack probabilities are $P_I = 1/q$ and $P_S = k/q$. The latter follows from the covering radius properties of the Reed-Solomon codes.

We see that the longer the source message, the easier the substitution attack becomes.

AU-hash families

Definition: Let $H = \{h_K \mid K, h_K : D \rightarrow T\}$ be a family of hash functions mapping elements of set D to set T. Then H is ε-Almost-Universal (ε-AU) if, for all $x, x' \in D, x \neq x'$, we have $\Pr[h_K(x) = h_K(x')] \leq \varepsilon$.

Known constructions of ε -AU hash families have the property that the value of ε depends on the length of message inputs, e.g., the construction given on the previous slide. Typically, the tag space T is relatively small and it is desired that $\varepsilon \approx 1/|T|$. The effect of message length can be eliminated using constructions based on concatenation of hash families. Towards this end the following theorem is useful.

Theorem: If there exists an ε_1 -AU hash family H_1 of hash functions from D to T_1 and an ε_2 -AU hash family H_2 of hash functions from T_1 to T_2, then there exist an ε -AU hash family H of hash functions from D to T_2, where $\varepsilon = \varepsilon_1 + \varepsilon_2 + \varepsilon_1 \varepsilon_2 \leq \varepsilon_1 + \varepsilon_2$

The hash functions in H are constructed as composed functions of hash function in H_1 and H_2.

Polynomial MAC (Example)

Suppose that the message to be authenticated (after appropriate formatting) consists of L 64-bit blocks $M_{L-1}, \ldots, M_1, M_0$. Given a 64-bit quantity k, a 64-bit authenticator (tag) t is computed using a $L \cdot 2^{-64}$-AU hash family as

$t = M_{L-1} k^{L-1} + \ldots + M_1 k + M_0$ over $\mathrm{GF}(2^{64})$.

Given a second 64-bit quantity λ the 32-bit message authentication tag is computed by computing first the product $\lambda \cdot t$ over $\mathrm{GF}(2^{64})$, and truncating the result to the least significant 32 bits. This is an instantiation of an 2^{-32}-AU hash family (secure truncation), see Lemma 10 of [BJKS93]. The authentication tag is obtained by xor-ing this result with a 32-bit one time pad. For this construction the forgery probability is bounded by $L \cdot 2^{-64} + 2^{-32} \approx 2^{-32}$ for messages with length up to 2^{38} bits.

[BJKS93]J. Bierbrauer, T. Johansson, G. Kabatianskii, and B. Smeets. On families of hash functions via geometric codes and concatenation. Proceedings of CRYPTO '93, LNCS 773, 331-342, Springer-Verlag, 1993.