A SECURE SUBLIMINAL CHANNEL (?)*

Gustavus J. Simmons
Sandia National Laboratories
Applied Mathematics Department
Albuquerque, New Mexico 87185

Introduction

At Crypto'83, the present author showed that a transmitter and chosen receiver(s) -- by secretly exchanging some side information -- could pervert an authentication without secrecy channel to allow them to convert a portion of the authentication information to a hidden (covert) communications channel [1]. It was also shown that under quite reasonable conditions even the detection of the existence of this covert channel could be made as difficult as the underlying authentication algorithm was "cryptosecure". In view of this open -- but indetectable -- existence, such a covert channel was called a "subliminal" channel. The examples constructed in [1] were more in the nature of existence proofs than of practical subliminal communications channels. At Eurocrypt'84 [2], however, it was shown how to use digital signature schemes as a way of realizing practical subliminal channels and, in particular, subliminal channels were devised using Ong and Schnorr's quadratic approximation scheme [3], Ong, Schnorr and Shamir's quadratic representation schemes [4] and Ong, Schnorr and Shamir's cubic signature scheme [5] as well as Gamal's discrete logarithm-based digital signature scheme [6]. Unfortunately, from the standpoint of providing a secure (and feasible) subliminal channel, all of these digital signature schemes were cryptanalyzed [7,8] shortly after being proposed. At Crypto'84, a fourth variant to the earlier digital signature schemes of Ong, Schnorr and Shamir was presented by Schnorr [9] which was also quickly cryptanalyzed [10]. At the 1985 IEEE Symposium on Security and Privacy, Okamoto and Shiraishi proposed yet another digital signature scheme based on quadratic inequalities [11] which had been designed to avoid the cryptanalytic weaknesses that had flawed the schemes of Schnorr, et al. The cryptanalysis of this scheme by Brickell and DeLaurentis is reported elsewhere in these Proceedings [12]. In view of the short-lived nature of all of these schemes, it has become a high risk venture to propose subliminal channels based on digital signatures. The motivation for doing so is that digital signatures can be much easier to calculate and verify than full-fledged two-key ciphers. As a result, the benefits (of a successful implementation) far outweigh

* This work performed at Sandia National Laboratories supported by the U.S. Department of Energy under contract no. DE-AC04-76DP00789.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 33-41, 1986.

the risks of perhaps having an insecure digital signature (or subliminal) channel slip by undetected. Based on the cumulative experience gained in cryptanalyzing the six digital signature schemes mentioned above, Brickell and DeLaurentis propose a new scheme in their paper that appears to avoid the weaknesses exploited in the earlier cryptanalyses.

It is an easy matter to adapt the Brickell-DeLaurentis digital signature scheme to accommodate a subliminal channel, however the resulting channel has a protocol weakness, common to all of the subliminal channels thus far devised, that we wish to avoid. In this paper we first point out the nature of this weakness and then propose a modified form of the Brickell-DeLaurentis digital signature scheme in which a subliminal channel can be embedded -- free of the protocol weakness.

The Protocol Weakness (Problem)

The problem is that in all subliminal channels devised thus far, the subliminal receiver -- by virtue of the side information that must be given to him by the transmitter to enable him to recover the subliminal communications -- is in a priviledged position to impersonate the transmitter. In other words, the transmitter and subliminal receiver have to be mutually trusting and trustworthy parties. There are, of course, some applications in which this is the case, but in general the transmitter prefers that the ability to receive subliminal communications not be synonymous with an ability to forge indetectable signatures in his stead. Since the same protocol weakness runs through all of subliminal schemes, we illustrate it using the channel which we proposed at Eurocrypt 84 based on the Ong, Schnorr and Shamir quadratic representation digital signature scheme [2,4]. In the interest of both completeness and brevity we summarize the essential points in their scheme for the three steps: key generation, signature generation and signature verification.

Key Generation

1. Tx chooses a composite n which is computationally infeasible to factor. The factorization of n is kept secret (if known).
2. Tx chooses a random u, $(u,n) = 1$, and calculates $k = -u^{-2} \pmod{n}$. u is kept secret.
3. Tx publishes n and k as his authentication key.

Signature Generation

Given a message m, (m,n) = 1, to be "signed":

1. Tx chooses a random r, (r,n) = 1. r is kept secret.
2. Tx calculates

$$s_1 = \frac{1}{2}\left(\frac{m}{r} + r\right) \pmod{n}$$

$$s_2 = \frac{u}{2}\left(\frac{m}{r} - r\right) \pmod{n}$$

3. The triple $(m; s_1, s_2)$ is transmitted as the "signed" message.

Authentication of Signature

1. Rx receives $(m; s_1, s_2)$
2. Rx calculates

$$a \equiv s_1^2 + k \cdot s_2^2 \pmod{n}$$

3. The message m is accepted as authentic if and only if

$$a = m \quad .$$

To set up the subliminal channel, in addition to the steps taken by the transmitter in the key generation procedure for the digital signature scheme, the transmitter secretly communicates u to the designated receiver, $Rx^{\dagger}$, for the subliminal channel. Now, when the transmitter wishes to send a signed message m through the overt channel and a covert message m^* through the subliminal channel, where it is still desired that both the $Rx^{\dagger}$ and third parties be able to verify the authenticity of the signature to m, the transmitter generates the signature as follows.

Signature Generation for the Subliminal/Signature Channel

Given a message m, (m,n) = 1, to be "signed" and a message m^*, $(m^*,n) = 1$, to be communicated subliminally:

1. Tx calculates

$$s_1 = \frac{1}{2}\left(\frac{m}{m^*} + m^*\right) \pmod{n}$$

$$s_2 = \frac{u}{2}\left(\frac{m}{m^*} - m^*\right) \pmod{n}$$

2. The triple $(m; s_1, s_2)$ is transmitted as the "signed" message.

Authentication of the signature by either the subliminal receiver, $Rx^{\dagger}$, or by third parties is unaffected by the presence of the subliminal communication. The subliminal receiver, however, knowing u can solve for the subliminal message as follows:

Decoding the Subliminal Message

The subliminal $Rx^{\dagger}$, given $(m; s_1, s_2)$ and knowing u, calculates

$$m^* = \frac{m}{s_1 + s_2 u^{-1}} \pmod{n}$$

to recover the covert message m^* "hidden" by the Tx in the signature of m.

Since the subliminal transmitter and receiver share the same piece of secret information, u, they are clearly interchangeable in terms of their capabilities. This is also true of the subliminal channel based on the Brickell-DeLaurentis digital signature scheme. In the next section, we show how to avoid this serious protocol failure in a subliminal channel embedded in a digital signature scheme similar to the one proposed by Brickell and DeLaurentis.

The Secure Subliminal Channel (?)

We borrow from Brickell and DeLaurentis the notion of basing the cryptosecurity of a digital signature on the difficulty of extracting approximate k^{th} roots in Z_n, n composite. While $n = p^2q$ in their scheme, we require $n = p^2qr$ for reasons that will become apparent later; p,q and r are all appropriately chosen primes $p > q$ and $q > r$. Again, in the interest of brevity, we summarize the essential points involved in signing messages using the modified Brickell-DeLaurentis digital signature scheme.

Key Generation

1. Tx chooses three primes $p > q > r$ sufficiently large that p^2q is computationally infeasible to factor. p, q and r are kept secret.

2. Tx publishes $n = p^2qr$ as his authentication key. The receivers need to know (or calculate) a bound $\delta = O(n^{2/3})$. The Tx may choose to treat δ as a redundant part of the key.

3. Both the Tx and Rx(s) know a one-way hashing function on messages, $h(m)$: $m \in Z_n$, $h(m) \in Z_n$ and an exponent $k \geq 4$.

Signature Generation

Given a message m, $m \in Z_n$, to be "signed":

1. Tx chooses a random $x \in Z^*_{pqr}$ (Z^*_{pqr} is the set of integers less than pqr and relatively prime to q, p and r).
2. Tx first calculates the one-way hashing function h(m), and then calculates the signature s of m as follows:

   a. $w = \left[\frac{h(m) - x^k \pmod n}{pqr}\right]$

   b. $y = \frac{w}{kx^{k-1}} \pmod p$

   c. $s = x + ypqr$.

3. The pair (m; s) is transmitted as the "signed" message.

Authentication of Signature

1. Rx receives (m; s).
2. Rx calculates the hashing function h(m).
3. The message is accepted as authentic if and only if

   (1) $\qquad h(m) \leq s^k \pmod n < h(m) + \delta$

In the Appendix we show that an s (signature) generated according to this protocol satisfies (1).

This modification of the Brickell-DeLaurentis scheme is at least as crypto-secure as their scheme. If these schemes turn out to be cryptosecure, this modification leads to the simplest subliminal channel yet devised. The transmitter secretly gives to the intended subliminal receiver(s) the prime r. Once this has been done, subliminal communication takes place as follows.

Signature Generation for the Subliminal/Signature Channel

Given a message $m \in Z_n$ to be "signed" and another message $m^* \in Z_r$ to be communicated subliminally:

1. Tx calculates s using m^*. He chooses a random $u \in Z^*_{pq}$ and calculates

   $$x^* = m^* + ur$$

   which is used instead of a random $x \in Z^*_{pqr}$ to calculate s as before.

Any receiver, including the subliminal receiver(s), $\overset{\dagger}{Rx}$, can authenticate a message exactly as before, but in addition $\overset{\dagger}{Rx}$ can recover m^*.

Decoding the Subliminal Message

1. $\overset{\dagger}{Rx}$, given (m; s) and knowing r calculates

$$s = x^* + ypqr = m^* + ur + ypqr \equiv m^* \pmod{r}$$

On the other hand, since one needs to know pqr in order to sign messages, a subliminal receiver -- knowing only r and $n = p^2qr$ -- needs to factor p^2q in order to recover pqr. It thus appears that this subliminal channel is just as cryptosecure to a subliminal receiver attempting to impersonate the transmitter as the Brickell-DeLaurentis scheme is secure to an outsider attack.

Incidentally, if the same message were signed repeatedly, using either this scheme or in the Brickell-DeLaurentis scheme, a random appearing set of signatures would result.

Appendix

As in the discussion of a secure subliminal channel, let the modulus n be of the form

$$n = p^2qr \qquad p > q > r \qquad \text{all primes}$$

and $M \in Z_n$, $s \in Z_n^*$.

Theorem:

(1) $$M \leq s^K \pmod{n} < M + pqr$$

if and only if

(2) $$s = x + ypqr$$

(3) $$y = \frac{w}{kx^{k-1}} \pmod p$$

(4) $$w = \frac{(M - x^k \pmod n)}{pqr}$$

where $x \in Z^*_{pqr}$, $y \in Z_p$ and $w \in Z_p$.

Proof:

First, assume that (1) holds. We show that (2), (3) and (4) follow.

Given $s \in Z^*_n$, s has a unique representation of the form

$$s = x + ypqr$$

where

$$x \in Z^*_{pqr} \qquad \text{and} \qquad y \in Z_p \ .$$

x and y are given by

$$s \equiv x \pmod{pqr}$$

and

$$y = \left[\frac{s}{pqr}\right]$$

respectively. Now form

$$s^k = x^k + kx^{k-1}ypqr + p^2q^2r^2 \times (\text{higher order terms})$$

$$s^k \equiv x^k + kx^{k-1}ypqr \pmod n \ .$$

Now since (1) was satisfied by hypothesis

$$M \leq s^k \pmod n = x^k + kx^{k+1}ypqr < M + pqr$$

we have

$$\frac{M - x^k \pmod n}{pqr} \leq kx^{k-1}y < \frac{M + pqr - x^k \pmod n}{pqr}$$

or

$$kx^{k-1}y = \left[\frac{M - x^k \pmod n}{pqr}\right] = w$$

and

$$y = \frac{w}{kx^{k-1}} \quad .$$

Next, assume that (2), (3) and (4) hold, then

$$s^k = x^k + kx^{k-1}ypqr + p^2q^2r^2 \text{ (HOT)}$$

$$s^k \equiv x^k + kx^{k-1}ypqr \pmod n \quad .$$

Replacing y by $y = \frac{w}{kx^{k-1}}$ we obtain,

$$s^k \equiv x^k + wpqr \pmod n$$

and finally,

$$s^k \equiv x^k + \frac{M - x^k \pmod n}{pqr} pqr \pmod n$$

from which (1) is an easy consequence.

References

1. G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel," Proceedings of Crypto'83, Santa Barbara, CA, Aug. 21-24, 1983, in Advances in Cryptology, Ed. by D. Chaum, Plenum Press, New York (1984), pp. 51-67.

2. G. J. Simmons, "The Subliminal Channel and Digital Signatures," Proceedings of Eurocrypt'84, to appear.

3. H. Ong and C. P. Schnorr, "Signatures through Approximate Representations by Quadratic Forms," Proceedings of Crypto'83, Santa Barbara, CA, August 21-24, 1983, to be published by Plenum Press.

4. H. Ong, C. P. Schnorr and A. Shamir, "An Efficient Signature Scheme Based on Quadratic Equations," Proceedings of 16th Symposium on Theory of computing, Washington D.C., April 1984, to appear.

5. C. P. Schnorr, "A Cubic OSS-Signature Scheme," private communication, May 1984.

6. T. El Gamal, "A New Public Key Cryptosystem and Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, to appear.

7. J. M. Pollard, "Solution of $x^2 - KY^2 \equiv m \pmod{n}$," Letter to Schnorr, 29/6/84.

8. J. Shallit, "An Exposition of Pollard's Algorithm for Quadratic Congruences," Technical Report 84-006, Department of Computer Science, University of Chicago, Dec. 1984.

9. H. Ong, C. P. Schnorr, and A. Shamir, "Efficient Signature Schemes Based on Polynomial Equations," to appear in Crypto'84, Lecture Notes in Computer Science, Springer-Verlag, NY (1984).

10. D. Estes, L. Adleman, K. Kompella, K. McCurley, G. Miller, "Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields," to appear.

11. T. Okamoto, A. Shiraishi, "A Fast Signature Scheme Based on Quadratic Inequalities," Proc. of the 1985 Symposium on Security and Privacy, April 1985, Oakland, CA.

12. E. Brickell and J. DeLaurentis, "An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi," these Proceedings.