

Subliminal Channels: Some Recent Developments

Gustavus J. Simmons

Rothschild Professor, University
of Cambridge UK

P. O. Box 365, Sandia Park, NM
87047

Abstract:

protocol designer concerned with denying the use of subliminal channels, while the other is important to the designer, or user, of subliminal channels. The first raises the question of whether the notion of a "subliminal-free" communication channel is an oxymoron, while the second is a partial disproof of a conjecture

Preface

third party (warden, censor, monitor etc.) who controls the overt communications channel and who must approve any message before it will be forwarded to the receiver(s). The function of this third party is to prevent covert communication from taking place, while still allowing the source generated

Introduction

security setting for which subliminal channels had originally been devised, seriously restricted their utility in commercial and private applications. If the channel was to be capable of communicating more than a few, to at most a few tens, of bits it was apparently necessary for the subliminal receiver to know the transmitter's

willing to trust the subliminal receiver (unconditionally) with his private signing key, in the first instance the entire session key itself can be the subliminal message. Even if the transmitter is unwilling to trust the subliminal receiver with his signing key, in the second instance he can still conceal small amounts of information in the

protocol. Incidentally, both parties in a Diffie-Hellman protocol can influence the resulting key -- unless the other party takes active steps to prevent it -- although neither of them can determine, i.e. force, the complete value. It is an easy matter to make the Diffie-Hellman protocol be completely

doesn't suit his subliminal purpose. This is a variant of the second type of subliminal channel described above in which the select and reject strategy was used. In that case the transmitter could continue choosing session keys which would produce "random" signatures until one was found that served his subliminal communication needs.

Yung assume a compliant warden who will continue to process signed messages when they are given to him, even though the transmitter is balking half of the time. They compute the capacity of the channel to be slightly more than a half bit for such an obliging warden. This strategy succeeds only because the

The Facts of the Matter

already been adequately described in the literature [7,8,9,10]. What we will do, though, in order to make this presentation be self contained, is discuss the essential points needed to appreciate the new results being presented. For the conve

τρανσπλαντατιον (το ανοτηερ
μεσσαγε) ις \approx 2-δ. Ιν οτηερ
ωορδς, ονλψ ηαλφ οφ τηε 2δ
εξτρα βιτσ — οωερ ανδ
αβοωε τηοσε νεεδεδ το
χομμυνιχατε μ — αρε
αχτυαλλψ υσεδ το προωιδε
φορ τηε σεχυριτψ οφ τηε
σιγνατυρε. Τηε οτηερ δ βιτσ
αρε ποτεντιαλλψ απαιλαβλε

σεχυριτψ οφ τηε διγιταλ
σιγνατυρε αγαινστ φοργερψ
ετχ. ισ 2-β, τηε τρανσμιττερ,
βψ αχχεπτινγ α λεσσερ δεγρεε
οφ σεχυριτψ — φρομ τηε
συβλιμιναλ ρεχειντερ βεινγ
αβλε το φοργε ηισ σιγνατυρε
φορ εξαμπλε — μιγητ βε αβλε
το χομμυνιχατε μορε τηαν α –
β βιτσ συβλιμιναλλψ. Ωε

transmitter unconditionally trusts the subliminal receiver. Referring to the Appendix, consider signatures generated using the DSA. These are of the form $(m; r, s)$ where

$$r \equiv (\gamma \kappa \bmod \pi) \bmod \theta.$$

$$\sigma \equiv \kappa - \lambda(\eta + \xi\rho) \pmod{\theta}$$

digest of the overt message, x is the signers private signing key, k the session key and r and s are of course the appended signature to m . The session key, k , had to be chosen such that

$$k.k^{-1} \equiv 1 \pmod{\theta},$$

Simmons [9], but which need not concern us here. If the transmitter trusted the subliminal receiver, S_x , with his private signing key, x , S_x has only to solve the modular congruence

$$k = s(h + xr) - 1 \bmod q$$

detect that k was not "randomly" chosen from an examination of the signed message. Even if the channel is to be used repeatedly, it is possible to conceal both the fact of its use as well as the content of the communications.

could have been used to generate the observed signature to the known subliminal text, could be exploited to weaken the security of the signers private key, then it could be used by outsiders in the absence of any encoding rules. In other words, the select and reject channels that are possible when the transmitter doesn't trust the subliminal receiver give the

realized was the base two logarithm of the number of digital signature-equivalent computations that one of the transmitter or receiver could, or was willing, to carry out. It is this conjecture that Anderson, Vaudenay, Preneel and Nyberg [1] have addressed in their ingenious construction ; The
Newton Channel

The Subliminal-free Paradox

his trusted agent the key generation authority) verifies that the key which was jointly generated in interaction with the signer is actually the key the signer has used to sign a message are immaterial to the present discussion. The interested reader is referred to [11] for those details. Quoting from [11]:

determine -- or even to know -- k either, since they could then in all probability, and with only minimal computational effort, generate perfect forgeries of the signers signature. In fact, their uncertainty about the signers secret key (not the session key) is reduced by precisely the same amount as they learn about the session key" underlining added

before he is in possession of information enabling him to judge the consequences of what he has committed himself to. In this case, the commitment is to the choice of a key whose value he does not yet know, and consequently, whose utility for any of the subliminal channels he cannot judge.

input prior to making his choice of an input, he could do the same thing. Since A goes first in all of the key generation protocols, the solution is to have A commit himself in a way that he can't subsequently change to a value which is inscrutable to B and hence can't be used by B to influence his choice of an input.

$\alpha \xi \bmod \pi \wedge \delta \sigma \equiv \beta \rho \bmod \pi$
 $\wedge \delta \sigma \wedge \delta \sigma$ της χομμιτμεντ
 (β, σ) το B. Της υνκνοων
 $\epsilon \xi \rho \nu \epsilon \nu \tau \sigma$, $\xi \wedge \delta \rho A$, $\alpha \rho \epsilon \alpha \sigma$
 $\sigma \epsilon \chi \upsilon \rho \epsilon \phi \rho \omicron \mu B$ — $\wedge \delta \phi \rho \omicron \mu$
 $\omicron \upsilon \tau \sigma \iota \delta \epsilon \rho \sigma \phi \omicron \rho$ τηατ ματτερ —
 $\alpha \sigma$ της δισχυρετε λογαριθτημ
 $\rho \rho \omicron \beta \lambda \epsilon \mu$ ισ ηαρδ.

number, r_B , also supposedly
chosen randomly, to be
relatively prime with respect to
 $p - 1$ etc. B then sends r_B to A.

β το περιψ τηατ τηε χορρεχτ
 σεσσιον κεψ ηασ βεεν
 υσεδ το γενερατε τηε
 σιγνατυρε. Β χαλχυλατες ξ−1
 υσινγ τηε Ευχλιδεαν
 Αλγοριτημ, ανδ ινχιδενταλλψ
 προωεσ ιν τηε προχεσσ τηατ
 $(\xi, \pi-1) = 1$.

τηατ ηε κνεω, βυτ ωηιχη ηε
χανετ χηανγε αφτερ β ανδ σ
ηαωε βεεν αννουνηεδ.
Σολωινγ φορ ειτηερ οφ τηε
εξπονεντσ ισ αν ινστανχε οφ
τηε δισχρετε λογαριτημ
προβλεμ ιν $\Gamma\Phi(\pi)$, ωηιχη βψ
ασσυμπτιον ισ ινφεασιβλε το
δο.

χονχεαλεδ φρομ Β. Αφτερ
 Πασσ 3, Β χαν χαλχυλατε $\xi-1$
 μοδ $\pi-1$ — ωηιχη ις ποσσιβλε
 ιφ ανδ ονλψ ιφ ξ ις
 ρελατιωελψ πριμε ωιτη
 ρεσπεχτ το $\pi-1$. Υσινγ $\xi-1$, Β
 χαν τηεν υνσεαλ Αεσ
 χομμιτμεντ ανδ χαλχυλατε
 τηε ωαλυε οφ τηε φιρστ
 χομπονεντ οφ τηε σιγνατυρε
 φορ ανηι μεσσοινε μαδε υσινγ

δελιβερατε υσε οφ αλλ οφ τηε
Σιμμονσə συβλιμιναλ
χηαννελσ. Τηε πριχε τηε
σιγνερ μυστ παψ το γετ τηε
ωαρδεν το αλλοω α μεσσαγε
το βε φορωαρδεδ ις το συβμιτ
το ονε οφ τηεσε φαιρ
προτοχολσ, ι.ε. το αχχεπτ
πρεχομμιτμεντ το α χηοιχε οφ
αν ινπυτ βεφορε ηε κνωωσ
ωρετρεσ προπ υμολογ ωιλλ

φορ ηισ συβλιμινάλ
χομμυνιχατιον πυρποσεσ. Ιφ
ιτ ισ, ηε ωιλλ υσε ιτ. Ιφ ιτ ισ
νοτ, ηε ωιλλ βαλκ ανδ ρεφυσε
το χοντινυε, ι.ε. ηε ωονετ σινγ
τηε μεσσαγε. Ιτ ισ ιμποσσιβλε
το πρεϋεντ ηιμ φρομ δοινγ
τηισ, σινχε τηερε ισ νο ωαψ
το χομπελ α παρτιχιπαντ ιν α
προτοχολ το χοντινυε. Τηε
απορρο παρτιχιπιαντ ανδ ρεφυσε το

συβλιμινάλ ινφορματιον — ιν
ωηιχη χασε τηε ωαρδεν
ωουλδ χερταινλψ φορωαρδ
τηε δεσιρεδ συβλιμινάλ
μεσσαγε, ιρρεσπεχτιϋε οφ τηε
νυμβερ οφ σιγνατυρεσ ηε
χηοοσεσ το σενδ. Ιφ τηε
σιγνερ υσεσ τηισ στρατεγψ,
τηε προβαβιλιτυ τηατ ηε ωιλλ
νοτ βάλκ, ι.ε. τηατ α μεσσαγε
ωιλλ βε φορϋωαρδεσ το τηε

ωηιχη τιμε ηε ις το αωακε
ανδ χαρρψ ουτ ωηατεωερ ηις
ασσιγνμεντ μαψ βε. Ιν τηις
χασε τηε χενσορ οφ τηε
χουντρψ ιν ωηιχη τηε σλεεπερ
ις πλαχεδ ις τηε ωαρδεν ιν
ουρ σεττινγ φορ τηε
συβλιμιναλ χηαννελ.
Χλεαρλψ, ιφ τηε χενσορ
ωαντσ το βε χερταιν τηατ α
σλεεπερ ις ιντερεστωινγκ

πρεχομιτμεντ προτοχολ
αλλοωσ χομμυνιχατιον το
τακε πλαχε ωιτη ονλψ αν
επσιλον προβαβιλιτψ οφ
ρελιαβλε συβλιμιναλ
χομμυνιχατιον οχχυρρινγ. Α
ρεασοναβλε δεφινιτιον,
τηερεφορε, ωουλδ σεεμ βε
τηατ α χηαννελ ισ
συβλιμιναλ φρεε ιφ τηε
ουριπρε ισ ουαβλε το τολλ

A Conjecture Disproved (?)

[1] at first appears to disprove this. Their paper begins; "Simmons asked whether there exists a signature scheme with a broadband covert channel that does not require the sender to compromise the security of her signing key. We answer this question in the affirmative; the ElGamal signature scheme has

logs in $GF^*(p)$ is hard and g a generator of $GF^*(p)$. Let $x \in (1, \dots, p-1)$ be a user's secret signing key and $y = gx$ his public signature verification key. As usual $k \in (1, \dots, p-1)$, (with $(k, p-1)=1$), is the session key and $h = H(m)$ is the hashed version of the message to be signed. Then the ElGamal signature on m is (m, r, s) where

$$r = g^k \pmod{p}$$

$$s = (h-xr)/k \bmod (p-1).$$

discrete logarithms is hard in the subgroup of $GF^*(p)$ of order q that is generated by g . If the subliminal information the transmitter wishes to encode is c , the session key is constructed to be of the form

$$k = c \bmod t$$

some randomly chosen k' . Now, when the receiver receives the signed message $(m; r, s)$, he forms rq and solves for z in the equation

$$(gq)^z = rq \bmod p$$

generated by gq is smooth. Using the Pohlig-Hellman decomposition [5] in combination with Pollard's rho method [6], this is only $O(B^{\epsilon})$

computationally difficult; where B is the smoothness bound (the largest prime factor of t). We will

then have

$$c = z \bmod t$$

be recovered. The discrete log calculation needs to be done only once. Given z , the value of the signer's private key mod t is easily recovered from

$$s = (h-xr)/k \bmod (p-1).$$

so further messages can be
decoded trivially using this same
equation.

is also possible to create what they refer to as narrowcast channels -- intermediate in channel capacity to Simmons broadband channels in which all of the bits in the key k can be used and his logarithmically limited narrowband channels -- that are truly subliminal to outsiders and in which the covert

$$p-1 = tq_1q_2+1$$

then communicate the message c as $k \bmod q_2$ to the intended subliminal receiver, with the assurance that his private signing key will still be just as secure from outsiders as in the general case, but in addition, it will be as secure from the subliminal receiver as the discrete logarithm problem over $GF(q_1)$ is hard.

Newton channel, that does not require the sender to compromise the security of her signing key. However, Simmons' conjecture that such schemes did not exist was not entirely mistaken, since the bandwidth of the Newton channel in bits per signature is exactly equal to the number of bits that the signer is prepared to

signing key."

By sharing $\log_2(q^2)$ bits of information about the signers private key, it is possible to communicate -- in a broadband channel -- $\log_2(q^2)$ bits of subliminal information to receivers with whom the information was shared. The inventors of the Newton channel recognize this, and even have a

subliminal receiver is just the difference between the information content of the signers private key, and the uncertainty about the signers key to that subliminal receiver.

Conjecture 2. Any subliminal channel that exceeds this bound is necessarily narrowband.

the signers private key to the receivers on these different channels. As the Newton channel demonstrates, it may require considerable ingenuity to achieve, or to approximate, the capacity in conjecture 1. It and the Simmons' broadband channels, however, show that it can be asymptotically achieved in some cases.

Conclusions

information content is indistinguishable from the output of a random source to the subliminal receiver, subliminal free is asymptotically achievable. The other, based on the discovery of the Newton channel, redefines the capacity of broadband and narrowband subliminal channels in terms of how much information a subliminal receiver

Acknowledgement:

Sciences, 20 Clarkson Road,
Cambridge, for the honor of
being named Rothschild
Professor and for hospitality
there while this research was
being done.

Bibliography

in Proceedings of the Workshop
on Information Hiding, Isaac
Newton Institute,
University of Cambridge UK, 30
May - 1 June, 1996. To be
published Springer-Verlag
1996

Channels" Proceedings, 9th
IEEE Computer Security
Foundations Workshop,
Kenmare, Ireland June 10-20,
1996 pp. 170-75

Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Info._Theory, Vol. IT-31, No. 4, July 1985, pp. 469-72.

4. NIST, "Digital Signature Standard", Federal Information Processing Standard

(FIPS) Publication 186},
National Institute of Standards
and Technology, US

Department of Commerce,
Washington D.C., May 1994

for Computing Logarithms
over GF(p) and its Cryptographic
Significance", IEEE
Transactions on
Information Theory, v 24, no 1
(Jan 78) pp 106--110}

6. Pollard, J. M., "Monte Carlo Methods for Index Computation (mod p)",

Mathematics of Computation, v 32 no 143 (Jul 78) pp 918--924}

—

- 7. Simmons, G. J., "The Subliminal Channel and Digital Signatures," Eurocrypt '84, Paris, France, April 9-11, 1984, Advances in Cryptology, Ed. by T. Beth et al., Springer Verlag, Berlin, 1985, pp. 364-378.

—

- 8. Simmons, G. J., "Subliminal Communication is Easy Using the DSA", Advances in

Cryptology - EUROCRYPT 93,
Springer-Verlag LNCS v 765 pp
218--232

Channels: Past and Present", in
European Transactions on
Telecommunications vol. 5 no 4
(July-August 1994) pp 459--473

Workshop on Information
Hiding, Isaac Newton Institute,
University of Cambridge
UK, 30 May - 1 June, 1996. To
be published Springer-Verlag
1996

Proceedings of the IMA
Conference on Cryptography
and Coding, Dec. 13-16, 1993,
Cirencester, England, Oxford
University Press, Oxford,
1995 pp.

The ElGamal Digital Signature Scheme

Initial Setup (Performed by a
trusted issuing authority)

◦ α λαργε πριμε, π, ισ ρανδομλψ σελεχτεδ

◦ α primitive root $\alpha \in \Gamma\Phi(\pi)$
ισχουσεν.

Note: π and α are public and
have been used by a community
of users.

Generation of Secret and Public
Keys by Users (Performed by
each user who wishes to be able
to sign messages)

◦ υσερ χηοοσεσ α ρανδομ ξ , $0 < \xi < \pi$, ωηιχη ισ ηις σεχρετ (σιγνινγ) κεψ.

° υσερ πυβλισηες ψ ≡ αξ μοδ
 π ασ ηισ πυβλιχ
 (περιφιχατιον) κεψ.

Note: y is associated with the user in a certified public directory.

Signature Generation (Performed
by a user -- whose public key
must be in the directory --
wishing to sign a message)

digest $h = H(m)$ using a publicly known hashing function $H(-)$ whose range is contained in $GF(p)$; i.e., for all messages m , $H(m) \in \Gamma\Phi(\pi)$.

◦ υσερ χηοοσεσ α ρανδομ κ, $0 < κ < π$, συχη τηατ $(κ, π-λ)=1$

(k is essentially a session key).

◦ υσερ χαλχυλατεσ $\rho = \alpha\kappa \mu\omicron\delta$
 $\pi.$

$\xi\rho) \bmod (\pi-\lambda)$ οηερε $\kappa.\kappa-1 \equiv 1$
 $\bmod (\pi-\lambda)$. Τηε τριπλε $(\mu; \rho, \sigma)$
 $\iota\sigma \quad \sigma\epsilon\nu\tau \quad \alpha\sigma \quad \tau\eta\epsilon \quad \sigma\iota\gamma\nu\epsilon\delta$
 $\mu\epsilon\sigma\sigma\alpha\gamma\epsilon$.

Signature Verification
Performed by a receiver (verifier)

knowing the hashing function $H(-)$, calculates the message digest $h = H(m)$. He also knows p and α and retrieves ψ from the certificate $υσερ\ διρεχτορψ$.

◦ περιφιερ χαλχυλατες $v \equiv \alpha\eta$
 $\text{mod } \pi$.

◦ περιφερ χαλχυλατες $\varpi \equiv$
 $\psi\rho\rho\sigma \bmod \pi$.

The signed message $(m; r, s)$ is accepted as authentic if and only if $u = v$.

The U.S. Digital Signature Algorithm (DSA)

Initial Setup
(Performed by a trusted issuing
authority)

preliminary (public) steps:

64–βιτ ινχρεμεντσ) πριμε, π,
ις ρανδομλψ σελεχτεδ,
συβφεχτ το της χονδιτιον
τηατ π–λ ις διωισιβλε βψ α
160–βιτ πριμε, θ.

° χαλχυλάτε $\gamma = \eta(\pi - \lambda)/\theta \bmod \pi$,
 ωηερε η ις ανψ ιντεγερ, $0 < \eta < \pi$,
 φορ ωηιχη $\gamma > 1$.

Note: p , q and g are public and can be used by a community of users.

Generation of Secret and Public
Keys by Users (Performed by
each user who wishes to be able
to sign message

◦ υστερ χρησιμοποιεσ α ρανδομ ξ , $0 < \xi < \theta$, ωηιχη ισ
ηισ σεχρετ (σιγνινγ) κεψ.

◦ υσερ πυβλισηεσ $\psi \equiv \gamma\xi \bmod \pi$
ασ ηισ πυβλιχ (περιφιχατιον)
κεψ.

Note: y is associated with the user in a certified directory.

Signature Generation (Performed
by a user -- whose public key
must be in the directory --
wishing to sign a message)

message digest $h = H(m)$ using a publicly known hashing function $H(-)$ whose range is contained in $GF(q)$; i.e., for all messages m , $H(m) \in GF(q)$.

◦ user chooses a random k , $0 < k < q$ (k is essentially a session key).

◦ υσερ χαλχυλατες $\rho \equiv (\gamma\kappa \bmod \pi) \bmod \theta$.

° υσερ χαλχυλατεσ σ ≡ κ-
 λ(η+ξρ) μoδ θ ωηερε κ.κ-λ ≡ 1
 μoδ θ.

The triple $(m; r, s)$ is sent as the signed message

Signature Verification Performed
by a receiver (verifier)

knowing the hashing function $H(-)$, calculates the message digest $h = H(m)$. He also knows p , q and g and retrieves y from the certified user directory.

◦ περιφιερ χαλχυλατες $\omega \equiv \sigma - \lambda \pmod{\theta}$.

◦ περιφιερ χαλχυλατες υλ \equiv
ηω mod θ.

◦ περιφερ χαλχυλατες υ2 ≡
ρω μοδ θ.

$$\circ \quad \omega \text{ περιφερ χαλχυλατες } \omega \equiv \\ (\gamma \lambda \psi \gamma 2 \bmod \pi) \bmod \theta$$

The signed message $(m; r, s)$ is
accepted as authentic if and only

if $r = v$.

