两类信息隐匿技术安全性的信息论分析方法

张 彤[1,2], 杨 波[1], 王育民[1], 李真富[2]
(1. 西安电子科技大学 ISN 国家重点实验室 106#, 陕西西安 710071; 2. 西北核技术研究所, 陕西西安 710024)

摘 要: 信息隐匿技术是信息安全研究的一个新的领域, 它与信息加密有着显著的区别. 数字签名中阈下信道是一种传送隐匿信息的安全信道, 但每次传送的信息量很少. 阈上信道是新近提出的一种在通信双方未共享任何密钥情况下的安全信道, 利用阈上信道可以防止中间人攻击. 阈上信息可做为公钥, 用于保护后续的隐匿信息的传送. 本文利用信息理论对这两类信息隐匿技术的安全性作了分析, 得出了确保隐匿信息安全的条件.

关键词: 信息隐匿; 阈下信道; 阈上信道; 信息论
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2001) 10-1346-03

Two Sorts of Information Hiding Technique and the Information Theoretic Security Analyses

ZHANG Tong[1,2], YANG Bo[1], WANG Yu-min[1], LI Zhen-fu[2]
(1. *National Key Laboratory on ISN, Xidian University, Xi'an, Shanxi 710071, China*; 2. *Northwest Institute of Nuclear Technology, Xi'an, Shanxi 710024, China*)

Abstract: Information hiding is a new area in the research of information security. It is significantly distinguished from encryption. Subliminal channel existing in some digital signature schemes is a kind of secure channel used for transmitting hidden information. But the information transmitted through this subliminal channel is very limited. Supraliminal channel is a newly presented secure channel used in the case that the receiver and the transmitter share no key ahead of their communication. Supraliminal channel can avoid man-in-the-middle attack. Supraliminal information may be treated as public key for the protection of the subsequent hidden information. Information theoretic analyses are made for the security of the two sorts of information hiding technique. Some security conditions are given.

Key words: information hiding; subliminal channel; supraliminal channel; information theory

1 引言

信息隐匿技术, 就是把秘密信息嵌入公开传送的文字、图形、图像等信息之中, 而这些公开传送的信息可以是加密的, 也可以是明文, 接收隐匿信息者是掌握某种特殊密钥的人.

从概念上看, 信息隐匿与信息加密都是为了保护秘密信息的存储和传输, 使之免遭敌手的破坏和攻击, 但二者之间存在着显著的区别. 信息加密是利用单钥或双钥密码算法把明文变换成密文通过公开信道送到接收者手中, 由于密文是一堆乱码, 攻击者监视着信道的通信, 一旦截获到乱码, 就可以利用已有的对各种密码体制的攻击方法进行破译了. 由此可见, 信息加密所隐藏的是信息的内容. 信息隐匿则不同, 秘密信息被嵌入表面上看起来无害的宿主信息中, 攻击者无法直观地判断他所监视的信息中是否含有秘密信息; 换句话说, 含有隐匿信息的宿主信息不会引起别人的注意和怀疑. 即信息隐匿的目的是使敌手不知道哪里有秘密, 它隐藏的是信息的存在形式. 近年来, 人们提出了阈下信道、隐匿通信、数字水印、隐匿标记等多种信息隐匿的实用技术[1,2], 但大多数文献只涉及对于隐匿信息的信道容量问题的讨论, 并未运用信息理论对隐匿信息的安全性进行深入研究. 而信息隐匿技术在实际使用中必须考虑如何使敌手破译隐匿信息所须付出的代价最大化. 本文从阈下信道的安全性分析入手, 进而研究了为提高隐匿信息传输效率和防止"中间人攻击"而引入的阈上信道的安全性, 得出了这两类信息隐匿技术在信息论意义上的安全条件.

2 数字签名中阈下信道的安全性分析

阈下信道是指在公开信道中所建立的一种实现隐蔽通信的信道[3], 是实现信息隐匿的一种典型方法. Simmons 最初研究阈下信道时, 是基于非确定性双钥体制数字签名的有关问题[4]. 数字签名中阈下信道的存在机理在于会话密钥的可选择性. 但即使是宽带阈下信道, 每次签名所传送的数据量也是很有限的. 对于任意长的一个消息, 例如一幅数字图像, 对它的签名(r, s)如果共有αbit, 而其中βbit 用于保证签名的安全性, 即防止伪造、篡改或移植等, 那么阈下信道的最大容量为$(\alpha-\beta)$bit. 被签消息虽然很长, 但对于阈下接收者来说只起

收稿日期: 2000-06-19; 修回日期: 2000-11-25
基金项目: 国防科技重点实验室基金(No. 99JS06.3.2.DZ0112)

到验证签名正确性的作用, 阈下信息仅存在于数字签名中, 因此, 数字签名中阈下信道的传输效率是很低的.

以ElGamal数字签名为例, 阈下信息的嵌入过程是在签名过程中完成的. 本文中的符号记法定义如下:

m_0 为任何待签名的原始消息; m 为 m_0 经 HASH 函数运算后得到的消息摘要; M 为所有可能的消息摘要 m 的集合, $m\in M$; emb 为实际的阈下信息; E 为所有可能的阈下信息的集合, $emb\in E$; x 为实际用的签名秘密密钥; X 为所有可能的签名用秘密密钥的集合, $x\in X$; k 为实际用的签名会话密钥; K 为所有可能的 k 的集合, $k\in K$; r 为实际的签名参数; R 为对任何消息摘要 M 签名参数 r 的集合, $r\in R$; s 为实际的签名参数; S 为对任何消息摘要 M 签名参数 s 的集合, $s\in S$; t 为窄带阈下信道中阈下收方和发方共享的随机素数; T 为所有可能的 t 的集合, $t\in T$.

对于两个随机变量 X 和 Y, 它们均取有限值, X 的熵 $H(X)$ 表示 X 的不确定性的度量. 条件熵 $H(X|Y)$ 是已知 Y 时 X 的不确定度. 联合熵 $H(X,Y)=H(X)+H(Y|X)$ 是两个熵的联合. 互信息 $I(X,Y)=H(X)-H(X|Y)$ 是已知 Y 时所能得到的 X 的信息量. 如果要求数字签名中阈下信道是信息理论上安全的, 那么消息的公开收方 Rx 从消息 m_0 和签名三元组 $(m;r,s)$ 无法得到阈下信息 emb, 即:

$$I(E;(M,R,S))=H(E)-H(E|(M,R,S))=0$$
$$\therefore H(E|(M,R,S))=H(E)$$

此式表明, 在已知签名三元组 $(m;r,s)$ 的前提下, E 的熵 $H(E)$ 不减小, 即 E 与 $(M;R,S)$ 相互独立. 下面分宽带和窄带两种情况分别进行讨论.

2.1 宽带阈下信道

按照 Simmons 在 ElGamal 数字签名方案中所构造的阈下信道, 会话密钥 k 作为阈下信息, 签名者 Tx (也就是阈下信道的发方), 与阈下收方 Sx 共享秘密签名密钥 x, 使得 Sx 能恢复出阈下信息 $k\equiv s^{-1}(m-xr) \bmod (p-1)$, 式中 s^{-1} 是 s 关于 $p-1$ 的乘法逆元, 此处假定 $s^{-1} \bmod (p-1)$ 存在, 使用 Euclidean 算法需 $O(\log_2(p-1))$ 步, 这在计算上是容易实现的. 当 $r^{-1} \bmod (p-1)$ 存在时, 若已知 k, 由式 $x\equiv r^{-1}(h-ks) \bmod (p-1)$ 易求出 x. 因而可以认为集合 X 和集合 E 是等同的, 又有 $E=K$, 所以 $H(E)=H(K)=H(X)$.

$$\begin{aligned}I((X,E);(M,R,S))&=H(X,E)-H((X,E)|(M,R,S))\\&=H(X,E)-H(X|(M,R,S))\\&=I((X;(M,R,S))+H(E|X))\end{aligned}$$

又有:

$$\begin{aligned}I((X,E);(M,R,S))&=H(X,E)-H((X,E)|(M,R,S))\\&=H(X,E)-H(E|(M,R,S))\\&=I(E;(M,R,S))+H(X|E)\end{aligned}$$

$$\because H(X,E)=H(X)+H(E|X)=H(E)+H(X|E)$$
$$H(X)=H(E)$$
$$\therefore H(E|X)=H(X|E)$$
$$\therefore I(E;(M,R,S))=I(X;(M,R,S))$$

签名的收方 Rx 由签名三元组所能得到的关于 E 的信息量分析如下:

$$\begin{aligned}I(E;(M,R,S))&=I(X;(M,R,S))\\&=H(X)-H(X|(M,R,S))\end{aligned}$$

$$\because H(E)=H(K)=H(X)$$
$$\therefore I(E;(M,R,S))=H(E)-H(X|(M,R,S))$$

签名算法的安全性是基于有限域上求解离散对数的困难性假设, 在这个假设下有: $H(X)=H(X|(M,R,S))$, 即:

$$I(X;(M,R,S))=0.$$
$$H(E)=H(E|(M,R,S))=H(X|(M,R,S)).$$

此时, 签名的公开收方 Rx 对阈下信息的不确定程度并不会因为知道签名三元组而减小. 由签名三元组来寻找阈下信息的难度相当于攻击秘密密钥 x 的难度.

2.2 窄带阈下信道

首先以 Simmons 设计的 1bit 阈下信道[5] 为例, Tx 和 Sx 共享一个随机素数 t 作为阈下信道的秘密密钥, Tx 可以通过选取随机数 k 作为会话密钥来控制 r 的特性, Tx 和 Sx 通过判断 r 是否模 t 的二次剩余来确定阈下比特是"1"还是"0". 此时签名参数 r 成为阈下信息的宿主.

$$I(E;(R,K))=H(E)-H(E|(R,K))$$

如果 E 的熵 $H(E)$ 不随攻击者所能得到的 R 和 K 的知识而减少, 即 $H(E|(R,K))=H(E)$, 则 $I(E;(R,K))=0$, 那么阈下信息是安全的.

$$\begin{aligned}\text{又}\because I((R,K);E)&=H(R,K)-H((R,K)|E)\\&=H(K)+H(R|K)-[H(K|E)\\&\quad+H(R|(K,E))]\\&=H(K)-H(K|E)=I(K;E)\end{aligned}$$

$\therefore$ 当 $H(K)=H(K|E)$ 时, E 与 (R,K) 的互信息为零, 即 E 与 (R,K) 相互独立, 阈下信息是理论上安全的.

如果假定签名算法是理论上安全的, 可以假定攻击者由 R 攻击 K 的难度不低于直接攻击 E 的难度, 用公式表示为:

$$H(K|R)\geq H(E)$$

而 $H(E)\geq H(E)-H(E|(R,K))=I(E;(R,K))$

$$\therefore H(K|R)\geq I(E;(R,K))$$

上式表明, 即使 $I(E;(R,K))\neq 0$, 只要满足条件 $H(K|R)\geq H(E)$, 则由 R 和 K 所能得到的关于 E 的信息量, 比由 R 得到 K 的计算复杂性小. 也就是说当 $I(E;(R,K))\neq 0$ 时, 阈下信息的安全性依赖于数字签名算法的安全性.

当阈下信道安全时, 攻击者通过数字签名攻击 T 来得到 E 的信息是不会成功的:

$$\begin{aligned}I((T,E);(R,K))&=H(T,E)-H((T,E)|(R,K))\\&=H(T,E)-H(T|(R,K))\\&\quad-H(E|(T,R,K))=0\end{aligned}$$

$$\because H(E|(T,R,K))=0$$
$$\therefore H(T|(R,K))=H(T,E)=H(E)+H(T|E)\geq H(E)$$

上式表明, 攻击者通过数字签名来攻击 T 的难度不低于直接攻击 E 的难度.

3 阈上信道及其安全性分析

阈上信道的概念是 Scott Craver 提出的[6]: 隐匿信息被藏于公开传送的宿主信息中非常明显之处, 如果宿主信息不做

大的改变, 隐匿信息就不可能被修改.

例如对于一幅画有牛的数字图像, Alice 是发方, Bob 是收方, 如果主动攻击者 Wendy 只能改变 1% 的像素, 那么她就不可能把牛变成猪, 对于一个声像片段, 可以把某人说的一段清晰的话语作为宿主, Wendy 要想改变这些话, 须改变声音以及相应的人嘴的动作, 这是很难办到的. 我们把 U 称为宿主稳健成分的集合, $u\in U$, 函数 $f: u \rightarrow \{0,1\}^N$, 要在一个阈上信道中嵌入一个比特串 $x\in\{0,1\}^N$, Alice 选择一个宿主稳健成分 $u\in f^{-1}(x)$ 连同整个宿主信息通过阈上信道发送给 Bob, Wendy 可以怀疑隐蔽信道被使用, 她可以对宿主信息做小的改动以试图破坏噪声成分中可能嵌入的隐匿信息, 但却不能改变宿主稳健成分 u. Bob 收到 u 后, 应用函数 f, 可以恢复出 x, Wendy 要想把 u 修改成 u' 从而使 $f(u')\neq f(u)$ 是难于做到的, 即阈上信息具有稳健性. 函数 f 是公开的, 大家都容易得到, f 和 f^{-1} 是易于计算的. 使用阈上信道进行隐蔽通信, Alice 不能把一个具有明显意义的比特串直接传给 Bob, 因为 Wendy 可以用 f 很容易算出这一比特串(尽管她修改不了), 这样 Alice 和 Bob 之间的通信就会受到更加严密的控制和监视. 如果 Wendy 算出的是一个近似随机的数, 就不会产生怀疑.

阈上信道可用于完成一个隐蔽通信密钥交换的协议. Alice 生成一对公钥 y 和私钥 x, 选 $u\in f^{-1}(y)$, 送给 Bob, 根据阈上信道稳健性的特点, Bob 确信 Wendy 未改变 y, 这就克服了 Anderson 方案[7] 中可能出现的"中间人攻击". 假定 k 是 Alice 和 Bob 即将使用的隐蔽密钥, k 由 Bob 产生. Bob 收到 y 后, 选择 $u'\in f^{-1}(E_y(k))$ 发送给 Alice, Alice 恢复出 $E_y(k)$ 并用私钥 x 解密得到 k, 从而可以进行以数字图像或其它多媒体数据为载体的隐蔽通信. 一般来说, 数字图像中 5~10% 的成分为噪声数据. 可以把隐匿信息嵌入图像的噪声成分中, 以使人眼无法察觉到嵌入信息的存在. 嵌入了隐匿信息的宿主图像的数据量不变, 只是噪声成分的数据有了改变. 在一幅 1024* 1024 点阵像素的 8bit 灰度级图像中, 如果把 5% 的噪声数据用于嵌入隐匿信息, 则可传送 1024* 1024* 0.05= 51.2K 字节的隐匿信息, 远远大于对该图像数字签名中阈下信道的信息量.

下面用到的符号定义如下, 其余符号与前面定义的相同.

C 为所有可用的不含有隐匿信息的宿主信息的集合; U 为宿主信息中稳健成分的集合; k 为将隐匿信息嵌入宿主信息的密钥; K 为所有可能的 k 的集合; L 为把 K 加密后的密文的集合; Y 为公钥密码算法中公开密钥 y 的集合; X 为公钥密码算法中秘密密钥 x 的集合. 根据上述阈上信道的特点, 可以认为: $H(U|Y)=H(Y|U)=0$.

$$\because I((X,K);(L,U,Y))=H(L,U,Y)-H((L,U,Y)|(X,K))$$
$$=H(L,U)-H((L,U)|(X,K))$$
$$=I((X,K);(L,U))$$

又 $\because I((X,K);(L,U,Y))=H(L,U,Y)-H((L,U,Y)|(X,K))$
$$=H(L,Y)-H((L,Y)|(X,K))$$
$$=I((X,K);(L,Y))$$

$\therefore I((X,K);(L,U))=I((X,K);(L,Y))$

如果所用公钥密码算法是安全的, 即由 L 和 Y(或 U)得不到 X 和 K 的信息, 则

$$I((X,K);(L,Y))=H(X,K)-H((X,K)|(L,Y))$$
$$=H(X,K)-H(X|(L,Y))$$
$$-H(K|(L,Y,X))=0$$

$\because H(K|(L,Y,X))=0$

$\therefore H(X|(L,Y))=H(X,K)=H(K)+H(X|K)\geq H(K)$

由此可见, 攻击者由 L 和 Y(或 U)破译 X 的代价不低于直接攻击 K 的代价, 而 K 的安全性依赖于公钥算法本身的安全性, 所以攻击者通过破译 X 来得到 K 不会成功. 如果把隐匿信息 E 嵌入宿主的算法安全, 则 K 未知时便无法得到 E, 因而隐匿信息是安全的.

4 小结

利用数字签名中阈下信道传送隐匿信息时, 如果数字签名算法本身是安全的, 则隐匿信息是信息论上安全的, 但缺点是传输效率很低. 如果利用数字图像或其它多媒体宿主信息的噪声成分, 在其中建立隐蔽信道来传送隐匿信息, 则传输效率大大提高. 为了防止"中间人攻击", 引入阈上信道传递公开密钥, 如果所用的公钥密码算法是安全的, 则实际传送的隐匿信息是信息论上安全的.

参考文献:

[1] Anderson R J editor. Information hiding: first international workshop [A]. LNCS vol. 1174, Isaac Newton Institute, Cambridge [C], UK, May 1996. Springer-Verlag, Berlin, Germany.

[2] Aucsmith D editor. Information hiding: second international workshop [A]. LNCS vol. 1525, Portland Oregon [C], USA, April, 1998. Springer-Verlag, Berlin, Germany.

[3] 王育民, 刘建伟. 通信网的安全——理论与技术 [M]. 西安: 西安电子科技大学出版社, 1999, 4.

[4] Simmons G J. The subliminal channel and digital signatures [A]. Advances in cryptology - EUROCRYPT' 84 Proceedings [C], Berlin: Springer-Verlag, 1985, 364- 378.

[5] Simmons G J. Subliminal communication is easy using the DSA [A]. Advances in Cryptology - EUROCRYPT' 93 Proceedings [C], Berlin: Springer-Verlag, 1994, 218- 232.

[6] Craver S. On Public-key steganography in the presence of an active warden [A]. Information Hiding: second international workshop [C], LNCS vol. 1525, Berlin: Spinger-Verlag, April 1998, 355- 368.

[7] Anderson R J. Stretching the limits of steganography [A]. Information Hiding first international workshop [C], LNCS vol. 1174, Berlin: Springer-Verlag, May 1996, 39- 48.

作者简介:

张 彤 男. 1967 年 6 月生于陕西. 1988 年和 1991 年分别在西安交通大学信控系和西北核技术研究所获学士和硕士学位, 现为西北核技术研究所副研究员、西安电子科技大学通信工程学院博士生. 主要从事网络安全和信息隐藏技术方面的研究工作.