基于 Web 的密码体制完善保密性的实现*)

王云光
(上海理工大学医疗器械学院　上海200093)

摘　要　本文利用熵、互信息、概率统计等工具，从不同的侧面，研究了完善保密密码体制的实现。其结果将有助于推广保密系统的通信理论及基于 Web 的密码体制的设计和应用。
关键词　完善保密性，熵，互信息，概率

Base on Web Implementation of Perfect Secrecy of Cryptosystem

Wang Yun-Guang
(Med. Instrum. College, Shanghai Univ. of Sci. & Technol, Shanghai 200093)

Abstract　By means of the theory of information and probability statistics, the author from different angles of view, researches and testifies the implementation of perfect secrecy of cryptosystem. The results may be of some help to the extension of the communication theory in secrecy system as well as base on Web the design and application of cryptosystem.
Keywords　Perfect secrecy, Entropy, Common information, Probability

1　引言

长期以来，人们主要的精力集中在计算安全性的密码体制的研究上，所谓计算安全性的密码体制就是破译所需的计算复杂度太大而难以实现的密码体制。而完善保密性的安全强度要强于计算安全性，但由于完善保密性难于实现，故对它的研究比较缓慢。本文利用熵、互信息、概率统计等工具，从不同的侧面，研究了完善保密密码体制的实现。为进一步研究完善保密性奠定了基础。

2　密码体制及其完善保密性的定义

定义1　一个密码体制是满足以下条件的五元组$(\rho,e,\kappa,\epsilon,D)$：

1. ρ 表示所有可能的明文组成的有限集。

2. e 表示所有可能的密文组成的有限集。

3. κ 代表密钥空间，是由所有可能的密钥组成的有限集。

4. 对任意的 $k\in\kappa$，都存在一个加密法则 $e_k\in\epsilon$ 和相应的解密算法则 $d_k\in D$。并且对每一 $e_k:\rho\to e$ 和 $d_k:e\to\rho$，对任意的明文$\in\rho$，均有 $d_k(e_k(x))=x$

定义2　如果对于任意的 $x\in\rho$ 和 $y\in e$，有 $P(x|y)=P(x)$，则称密码体制具有完善保密性。

3　完善保密性与条件熵结束语

引理1　对于任意的实数 $x>0$，有 $1-\frac{1}{x}\leqslant Lnx\leqslant x-1$ 其中等号成立当且仅当 $x=1$；

结论1　设五元组$(\rho,e,\kappa,\epsilon,D)$是一个密码体制，$H(X)$、$H(Y)$分别表示由明文和密文组成的随机变量$(X,Y)$的熵，证明当且仅当 $H(X|Y)=H(X)$ 时，密码体制是完善保密的。

证明：设 $P(x,y)$为随机变量(X,Y)的联合概率分布，$P(x)$，$P(y)$分别为随机变量 X，Y 的概率分布，故有 $\sum_y\sum_x P(x,y)=1$，$\sum_x P(x)=1$，$\sum_y P(y)=1$

$$P(x)=\sum_y P(x,y)$$

由熵的定义：

$$H(X)-H(X|Y)=H(x)-H(x|y)$$
$$=\sum_x P(x)\mathrm{Log}_2\frac{1}{P(x)}+\sum_x\sum_y P(y)P(x|y)\mathrm{Log}_2 P(x|y)$$
$$=\sum_x\sum_y P(x,y)\mathrm{Log}_2\frac{1}{P(x)}+\sum_y\sum_x P(x,y)\mathrm{Log}_2\frac{P(x,y)}{p(y)}$$
$$=\sum_y\sum_x P(x,y)\mathrm{Log}_2\frac{P(x,y)}{p(x)p(y)}$$
$$=\sum_y\sum_x P(x,y)\mathrm{Log}_2 e\ \ln\frac{P(x,y)}{p(x)p(y)}$$

由引理1得：

$$\geqslant\mathrm{Log}_2 e\sum_y\sum_x P(x,y)\left(1-\frac{P(x)p(y)}{p(x,y)}\right)$$
$$=\mathrm{Log}_2 e\sum_y\sum_x((P(x,y)-P(x)P(y))$$

*)该课题得到上海理工大学医疗器械学院课程建设与教改基金的资助。王云光　硕士，讲师，主要从事 Web 信息系统安全、医院信息系统等方面的研究。

$=\mathrm{Log_2 e}(\sum_y\sum_x \mathrm{P}(x,y)-\sum_x \mathrm{P}(x)\sum_y \mathrm{P}(y))=0$

当且仅当 $\mathrm{H}(X|Y)=\mathrm{H}(X)$，有 $\frac{p(x)p(y)}{p(x,y)}=1$

即 $\mathrm{P}(x,y)=\mathrm{P}(x)\mathrm{P}(y)$ 而

$\mathrm{P}(x,y)=\mathrm{P}(x)\mathrm{P}(x|y)$

$=\mathrm{P}(y)\mathrm{P}(y|x)$

因此有：$\mathrm{P}(x|y)=\mathrm{P}(x)$，即该密码体制是完善保密的。

4 完善保密性和条件熵、互信息（公共信息）

结论2 设五元组$(\rho,e,\kappa,\epsilon,D)$是一个密码体制，$\mathrm{H}(X)$、$\mathrm{H}(Y)$分别表示由明文和密文组成的随机变量$(X,Y)$的熵，$\mathrm{I}(X,Y)$表示$(X,Y)$的互信息（公共信息）。若密码体制是完善保密的，则有如下结论：

1）互信息 $\mathrm{I}(X,Y)=0$

2）$\mathrm{H}(X,Y)=\mathrm{H}(X)+\mathrm{H}(Y)$

证明：设 $\mathrm{P}(x,y)$为随机变量(X,Y)的联合概率分布，$\mathrm{P}(x)$，$\mathrm{P}(y)$分别为随机变量 X，Y 的概率分布。

1）由互信息的定义有：

$$\mathrm{I}(X,Y)=\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\frac{P(x,y)}{p(x)p(y)}$$

而 $\mathrm{H}(X)-\mathrm{H}(X|Y)=\sum_x \mathrm{P}(x)\mathrm{Log_2}\frac{1}{P(x)}+\sum_x\sum_y \mathrm{P}(y)\mathrm{P}(x|y)\mathrm{Log_2}\mathrm{P}(x|y)$

$=\sum_x\sum_y \mathrm{P}(x,y)\mathrm{Log_2}\frac{1}{P(x)}+\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\frac{P(x,y)}{p(y)}=\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\frac{P(x,y)}{p(x)p(y)}$

$=\mathrm{I}(X,Y)$

由结论1得 $\mathrm{I}(X,Y)=0$，即结论成立。

2）$\mathrm{H}(X,Y)=-\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\,\mathrm{P}(x,y)$

$=-\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\,\mathrm{P}(x)\mathrm{P}(y)-\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\frac{P(x,y)}{p(x)p(y)}=\sum_x \mathrm{P}(x)\mathrm{Log_2}\frac{1}{P(x)}+\sum_y \mathrm{P}(y)\mathrm{Log_2}\frac{1}{P(y)}-\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\frac{P(x,y)}{p(x)p(y)}$

$=\mathrm{H}(X)+\mathrm{H}(Y)-\mathrm{I}(X,Y)$

由1）知若密码体制是完善保密的，有 $\mathrm{I}(X,Y)=0$

故有：$\mathrm{H}(X,Y)=\mathrm{H}(X)+\mathrm{H}(Y)$成立

结论3 设五元组$(\rho,e,\kappa,\epsilon,D)$是一个密码体制，$\mathrm{H}(X)$、$\mathrm{H}(Y)$、$\mathrm{H}(Z)$分别表示由明文、密文、密钥组成的随机变量$(X,Y,Z)$的熵，若密码体制是完善保密的，则有如下结论：

1）$\mathrm{H}(Y|X)=\mathrm{H}(Y)$

2）$\mathrm{H}(X|YZ)=0$，$\mathrm{H}(Y|XZ)=0$

3）$\mathrm{H}(Z)\geqslant\mathrm{H}(X)$

证明：设 $\mathrm{P}(x,y)$，$\mathrm{P}(x|y)$分别表示随机变量(X,Y)的联合概率分布和条件概率分布，$\mathrm{P}(x)$，$\mathrm{P}(y)$，$\mathrm{P}(z)$分别为随机变量 X，Y，Z 的概率分布。

1）$\mathrm{H}(Y)-\mathrm{H}(Y|X)=\sum_y \mathrm{P}(y)\mathrm{Log_2}\frac{1}{P(y)}-\sum_y\sum_x \mathrm{P}(x)\mathrm{P}(y|x)\mathrm{Log_2}\,\mathrm{P}(y|x)$

$=\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\frac{1}{P(y)}+\sum_x\sum_y \mathrm{P}(x,y)\mathrm{Log_2}\frac{P(x,y)}{p(x)}$

$=\sum_y\sum_x \mathrm{P}(x,y)\mathrm{Log_2}\frac{P(x,y)}{p(x)p(y)}$

$=\mathrm{I}(X,Y)$

由结论2中1）得：$\mathrm{I}(X,Y)=0$，故有 $\mathrm{H}(Y)=\mathrm{H}(Y|X)$，结论成立。

2）假设明文 X，密文 Y，密钥 Z 都是随机变量。通信双方 Alice 和 Bob 通过一个安全信道进行相互协商，确定了共享的密钥 Z；Alice 欲通过一个不安全的信道向 Bob 发送明文消息 X，Alice 使用钥控加密算法将明文 X 变为密文 Y，即 $X\to Y$，因此(X,Z)惟一确定了 Y；Alice 通过不安全的信道将密文 Y 发送给 Bob；Bob 使用钥控解密算法将密文 Y 变换为明文 X，即 $Y\to X$，而(Y,Z)也惟一确定了 X。即有 $\mathrm{H}(X|YZ)=0$，$\mathrm{H}(Y|XZ)=0$。

3）由结论1得：$\mathrm{H}(X|Y)=\mathrm{H}(X)$

$\leqslant\mathrm{H}(XZ|Y)$

$=\mathrm{H}(Z|X)+\mathrm{H}(X|YZ)$（由2）$\mathrm{H}(X|YZ)=0$）

$=\mathrm{H}(Z|X)$

$\leqslant\mathrm{H}(Z)$

5 完善保密存在性

结论4 假设一个密码体制对一个特定的明文的概率分布是完善保密的，证明对任意的明文概率分布，这个密码体制仍然是完善保密的。

证明：对于任意的 $x\in\rho$ 和 $y\in e$，在给定明文的条件下，密文的概率为：

$$\mathrm{P}(y|x)=\sum_{|K:x=d(y)|}\mathrm{P}(K=k)=\mathrm{P}(k)$$

因为对任意的 x，y 满足加密函数条件的应有惟一的 k，故有 $\mathrm{P}(y|x)=\mathrm{P}(k)$，其中 $\mathrm{P}(k)$只与概率分布和密钥 k 有关。由题设密码体制对特定的明文（设为 x1）的概率分布是完善保密的，故有 $\mathrm{P}(x1|y)=\mathrm{P}(x1)$。由概率公式得：

$\mathrm{P}(x1,y)=\mathrm{P}(x1|y)\mathrm{P}(y)$

$=\mathrm{P}(y|x1)\mathrm{P}(x1)$

因此有

$\mathrm{P}(y|x1)=\mathrm{P}(y)$

由以上推导有

$\mathrm{P}(y|x1)=\mathrm{P}(k)$

（下转第229页）

计算所得(除传输过程中会引起改变的字段外,这些字段在传送过程中被设成0)。

SIP 主叫端的 IP 数据包鉴权计算需在分段前执行,被叫端的鉴权计算则在分段重新合成后进行。只要 SIP 终端和代理服务器共享密钥,鉴权过程就是安全的。通过对数据的验证能够保证报文在传输的过程中没有被更改。

封装安全有效载荷:

ESP 根据 SIP 会话的特殊需求,支持 IP 分组的私密和数据完整性。它既可用于传送层(如 TCP、UDP、ICMP)的加密,称传送层模式 ESP;同时又可用于整个分组的加密,称隧道模式 ESP。ESP 标记以32位的 SPI 开始,余下字段根据不同的解密逻辑算法而有所不同。标记的开始部份,包括 SPI 和其他一些参数,不以加密的方式传送,其余部份则加密传送。如图4所示。

通过 ESP 报头,保证了数据的机密性。它使得 SIP 会话的双方能够将数据报的内容修改成一种中间设备不可理解的格式。从而保证了 SIP 会话的机密。

总之,IPv6的 IP 安全性(IPSec)机制和服务一致。除了必须提供网络层安全这一强制性机制外,IPSec 还提供认证报头(AH)用于保证数据的一致性,而封装有效载荷报头(ESP)两种服务用于保证数据报级别的数据保密性和数据一致性,加强了 IP 数据报的安全。从而使得基于 SIP 的 VoIP 在网络层的安全得到了保证,进而提高了整个应用的安全性。

5 SIP 对 IPv6的支持

SIP 协议支持 IPv6,并且提供了应用的接口。SIP 消息体采用 SDP 定义,而 SDP 的传送和媒体的协商则由 RTSP,HTTP 等来完成。通过在 SDP (Session Description Potocol)对 IPv6地址的引用描述直接支持 IPv6在 SIP 协议中的应用。如图5是一个 SDP 的描述信息:

```
v=0 //协议版本信息
o-nasal 971731711378798081 0 IN IP6 2201:056D::112E:
    144A:1E24
//用户名 会话 ID 版本信息  网络类型  IP 地址类型  IP
    地址
    其它描述信息……略……
```

图5 SDP 对 IP 地址类型的描述

结束语 IPv6作为网络层的协议,它不仅提供了比 IPv4更多的网络空间地址,而且它对安全有着更多的考虑,增加了报头验证和安全报头封装的扩展报头。报头验证确保了报文在传输的过程中没有被更改。安全报头封装使得双方的数据的机密性得到保证,从而提高了基于 SIP 的 VOIP 的安全性能。

参 考 文 献

1 RFC2543,SIP 协议[S]

2 万敏,万晓榆. 基于 SIP 的 VoIP 在下一代网络中的应用[J]. 重庆邮电学院学报. 2003

3 NGN 呼唤安全[EB/OL]. http://www.ctiforum.com/forum/forum.htm/NGN 呼唤安全.htm. 2003-12-12

4 Shanmugam Ramadas, Padmini R, Nivedita S. Special Edition Using TCP/IP, Second Edition[M]. 北京:电子工业出版社, 2003.8

5 IPv6的安全性[EB/OL]. http://www.erp110.com/netschool/ip/ip1.htm

6 RFC3266,Support for IPv6 in Session Description Protocol[S]

7 RFC2327,Session Description Protocol[S]

(上接第212页)

$P(y)=P(k)$

对于任意的明文 $x\in\rho$ 和密文 $y\in e$ 有:

$P(y|x)=P(y)$

而

$P(x,y)=P(y|x)P(x)$

$=P(x|y)P(y)$

故有:

$P(x|y)=P(x)$

即对任意的明文概率分布,这个密码体制仍然是完善保密的。

结束语 近年来密码学的研究有所改变,一方面人类计算能力愈来愈强,另一方面,大量有扰信道的开通,使得信伙伴之间能够共享源源不断的互信息;使用信息处理技术,将这些互信息中敌手已知的部分去掉,保留并协调敌手未知的部分,通信伙伴之间就获得了源源不断的密钥流,因此不需要精心地设计密码函数,只需用群运算来加密和解密即可,使得完善保密性得以实现。但完善保密性的应用还有待进一步的开发。

参 考 文 献

1 [加]Stinson D R,冯登国译. 密码学原理与实践. 北京:电子工业出版社,2002.1~60

2 孟庆生. 信息论. 西安:西安交通大学出版社,1982.446~536

3 胡予濮,等. 对称密码学. 北京:机械工业出版社,2002. 1~14

4 王云光. 关于密码体制的完善保密性. 大连理工大学学报,2003,43(增刊):69~71

5 王云光. SPN 线性密码分析中的线性逼近函数. 电子信息学报,2003,25(增刊)