第 35 卷 第 7 期 计 算 机 工 程 2009 年 4 月
Vol.35 No.7 Computer Engineering April 2009
·安全技术· 文章编号：1000—3428(2009)07—0144—03 文献标识码：A 中图分类号：TP393.08

基于同态的安全协议攻击及其形式化验证

韩继红，周志勇，郭渊博，王亚弟
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：介绍 2 种利用加密算法同态特性的安全协议攻击，定义安全协议项代数表示和基于角色行为序列的协议模型，提出一种基于角色行为实例交互的安全协议约束序列生成方法，应用等式理论将 Dolev D 等人提出的 Dolev-Yao 模型(IEEE Transactions on Information Theory, 1983, 第 12 期)进行扩展，设计攻击者一阶逻辑演绎系统，采用约束求解方法对 NSL 协议进行建模和形式化验证，发现基于“完美密码系统假设”无法验证的同态攻击。

关键词：安全协议；攻击；同态；等式理论

Attack on Security Protocol Based on Homomorphism and Its Formal Verification

HAN Ji-hong, ZHOU Zhi-yong, GUO Yuan-bo, WANG Ya-di
(Institute of Electronic Technique, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 This paper introduces two attacks on security protocols which have cipher homomorphism, defines term representation and security protocol model based on role's action sequences, proposes a method of transforming role instances interleaving to sequence of constraints, extends the Dolev-Yao intruder model with equational theory, putforwards a intruder deduction system in first-order logic, models and verifies NSL protocol using constraint solving method, discovers the attack based on cipher homomorphism which can not be found under perpect cryptography assumptions.

【Key words】 security protocol; attack; homomorphism; equational theory

1 概述

在安全协议的符号分析方法中，Dolev-Yao[1]模型认为攻击者能完全控制协议运行的通信网络，监听和截获协议主体之间传递的任何消息，并能对其进行变换运算、发送篡改消息或重放原有消息。在攻击者对截获的消息进行处理时，遵循“完美密码系统假设”，即认为密码原语(算法)是完美的，可将其作为一个“黑盒子”处理，只有知道正确密钥的情况下，才可对加密信息进行解密。该假设忽略了密码原语的代数特性，因此，基于 Dolev-Yao 模型的协议验证方法无法发现基于密码原语代数特性的攻击[2]。这些代数特性包括同态(h)、阿贝尔群(AG)和异或的 ACNU 特性等。其中同态特性在密码算法中普遍存在，如 RSA、ElGamal 等加密算法都具有二进制操作符上的同态特性，在电子选举协议中同态特性也极其重要。另外，同态特性还可与其他特性结合作用，如 ACUNh, AGh 等。这些特性都使协议的安全性验证更加复杂。

2 基于同态的安全协议攻击

同态特性具有 $f(g(x,y)) = g(f(x), f(y))$ 的形式，利用该特性，攻击者可获得某些被加密的秘密信息。

2.1 采用ECB模式的NSL协议

NSL 协议是由 G. Lowe 改进的 Needham-Schroeder 公钥协议，该协议的意图是利用可信密钥服务器和公钥实现 2 个主体之间的相互认证。具体形式为：

(1) A- > S: A, B
(2) S- > A:{$PK(B)$, B}$SK(S)$
(3) A- > B:{Na, A}$PK(B)$
(4) B - > S: B, A
(5) S - > B:{$PK(A)$, A}$SK(S)$
(6) B - > A:{Na, Nb, B}PK(A)
(7) A - > B:{Nb}$PK(B)$

协议中 B 产生的随机数 Nb 用 $PK(A)$和 $PK(B)$加密后传输，本意是只有 A、B 可以用其私钥解密得到 Nb，即只让 A, B 知道 Nb。但是，当加密算法采用 ECB 模式且随机数和主体名长度是加密块的整数倍时，攻击者可通过 2 个并行会话欺骗 A 为其解密 Nb，具体攻击过程如下：

(1) A - > I:{Na, A}$PK(I)$
(2) $I(A)$ - > B:{Na, A}$PK(B)$
(3) B - > $I(A)$:{Na, Nb, B}$PK(A)$
(4) I - > A:{Na, Nb, I}$PK(A)$
(5) A - > I:{Nb}$PK(I)$
(6) I - > B:{Nb}$PK(B)$

由于 ECB 模式具有 $\{B_1, B_2, B_3\}K = \{B_1\}K, \{B_2\}K, \{B_3\}K$ 的特性，则在(3)攻击者 I 可由得到的密文 $\{Na, Nb, B\}PK(A)$ 提取出密文 $\{Na, Nb\}PK(A)$，并在(4)再利用同态特性合成 $\{Na, Nb, I\}PK(A)$ 发送给 A，A 解密后在(5)用攻击者的公钥

基金项目：国家自然科学基金资助项目(60503012)；国家“863”计划基金资助项目(2007AA01Z405)
作者简介：韩继红(1966－)，女，教授、博士，主研方向：安全协议形式化分析；周志勇，博士研究生；郭渊博，副教授、博士；王亚弟，教授、博士生导师
收稿日期：2008-08-10 **E-mail**：hnhanjh@163.com

加密 Nb，发送给攻击者，使攻击者可轻易地用其私钥解密得到 Nb。

2.2 TMN密钥分发协议

TMN 是一个对称密钥分发协议，其目的除在 2 个主体之间共享一个对称密钥外，还在于基于对称密钥、可信服务器和公钥实现主体间的认证。具体形式如下：

(1) A -> S:B, $\{Ka\}PK(S)$

(2) S -> B:A

(3) B -> S:A, $\{Kb\}PK(S)$

(4) S -> A:B, $\{Kb\}Ka$

当加密算法具有同态关系时，2 个攻击者合谋可以获得为 A, B 分发的密钥 Kb。例如当采用 RSA 算法时，有

$$\{x\}PK(S)*\{y\}PK(S)=\{x*y\}PK(S)$$

其中，$*$ 为阿贝尔群运算符号。

假定攻击者分别为 C 和 D，则其具体攻击步骤为监听 A, B 之间的协议运行，由(3)得到 $\{Kb\}PK(S)$，并启动一轮新协议：

(1) C -> S:D, $\{Kc\}PK(S)$

(2) S -> D:C

(3) D -> S:C, $\{Kd\}PK(S)*\{Kb\}PK(S)=\{Kd*Kb\}PK(S)$

(4) S -> C:D, $\{Kd*Kb\}Kc$

攻击者 D 在(3)利用加密计算的同态特性产生密文 $\{Kd*Kb\}PK(S)$ 并发送给 S，S 将其解密后用 Kc 加密发送给 C。C 在(4)得到 $\{Kd*Kb\}Kc$ 后，用自己的密钥 Kc 解密，再使用 D 的密钥 Kd 即可导出 A、B 的共享密钥 Kb。

3 基于约束求解的安全协议验证

基于约束求解的安全协议验证是一种将协议验证的可达性问题转换为约束求解问题进行处理的符号方法，该方法可以保证在协议会话数目有限时安全协议的验证是可判定问题[3]，通过求解一个协议约束序列的具体实例可确定针对该协议的实际攻击。

3.1 项

安全协议中交互的协议消息可用项表示。

定义 1(项) 令 F 为一个项操作符集合，每个项操作符 $f\in F$ 至少操作一个项，即其元数 $ar(f)$至少为 1。FC 为与密码操作有关的项操作符集合，FO 为一般操作符集合，$F=FC\cup FO$，且 $FC\cap FO=\varnothing$。令 C 为一个常量(首字母用大写表示，如主体名 A, B, I，随机数 Na, Nb 等)集合，V 为一个变量(用小写字母表示)集合，则 $T(F, C, V)$表示构建于 F, C, V 的项集合，它是满足以下条件的最小集合：

(1)$C\subseteq T(F, C, V)$。

(2)$V\subseteq T(F, C, V)$。

(3)若 $t_1, t_2,\cdots, t_n\in T(F, C, V)$，且 $f\in F$，则 $f(t_1, t_2,\cdots, t_n)\in T(F, C, V)$。$f(t_1, t_2,\cdots, t_n)\in FC$ 的具体语法形式包括：

$[t_1, t_2]$：项的连接。

$senc(t_1, t_2)$：用对称密钥 t_2 加密 t_1 产生的项。

$penc(t_1, t_2)$：用公钥 t_2 加密 t_1 产生的项。

$sign(t_1, t_2)$：用私钥 t_2 签名 t_1 产生的项。

$h(t_1)$：t_1 的哈希值。

$xor(t_1, t_2)$：项 t_1, t_2 异或的结果。

$key(t_1, t_2)$：为主体 t_1 和 t_2 的共享密钥。

$pk(t_1)$, $sk(t_1)$：主体 t_1 的公、私钥。

其中，$t\in T(F, C, \varnothing)$称为基项；$var(t)$表示项 t 中包含的变量集合。

定义 2(子项) 项 t 的子项 $St(t)$是满足以下条件的最小集合：

$t\in St(t)$。

对于 $1\leqslant i\leqslant n$，若 $f(t_1, t_2,\cdots, t_n)\in St(t)$，则 $t_i\in St(t)$。

定义 3(位置) 令λ为一个空序列，$t\in T(F, C, V)$的位置集合 $O(t)$定义如下：

若 $t\in C$，则 $O(t)=\{\lambda\}$。

若 $t\in V$，则 $O(t)=\{\lambda\}$。

若 $t=f(t_1, t_2,\cdots,t_n)$，则 $O(t)=\{\lambda\}\cup\{i, p|1\leqslant i\leqslant n, p\in O(t_i)$。

t 中在位置 $p\in O(t_i)$处的子项记为 $t|_p$。在 t 中用 u 替代 $t|_p$ 得到的项记为 $t[u]_p$。

3.2 协议模型

一个安全协议包括执行协议的主体集合及其相互之间交互的消息集合 2 大部分。以此为基础，可将安全协议抽象为一个“角色”集合，每个角色可以看成是一个“发送”和“接收”消息的有限事件序列。借鉴基于串空间理论对安全协议进行形式化验证的符号表示方法[4]，角色发送一个消息 m 用“$+m$”表示。角色接收到消息 m 用“$-m$”表示。这样一个协议即可表示成若干个由“$+m$”和“$-m$”组成的动作序列。以 NSL 协议进行举例，在不影响分析结果的情况下，去掉其中与服务器交互的步骤，得到如下简化协议：

(1) A -> B:$\{Na, A\}PK(B)$

(2) B -> A:$\{Na, Nb, B\}PK(A)$

(3) A -> B:$\{Nb\}PK(B)$

这样该协议即包括协议发起者(*Init*)和协议响应者(*Resp*) 2 个角色，各角色在协议中的行为可以表示成如下参数化的事件序列：

$$\begin{aligned}Init(a,b,n_a,n_b)=&+penc([n_a,a],pk(b))\\&-penc([n_a,n_b,b],pk(a))\\&+penc(n_b,pk(b))\\Resp(a,b,n_a,n_b)=&-penc([n_a,a],pk(b))\\&+penc([n_a,n_b,b],pk(a))\\&-penc(n_b,pk(b))\end{aligned}$$

一次协议的成功运行即为不同角色实例进行交互形成的一个消息发送与接收的事件序列。

3.3 约束序列

在实际网络环境中可有多个协议会话同时运行，而且存在可以控制整个网络的攻击者，因此，协议在实际运行中有可能偏离其预定目标。这样检验一个协议是否存在攻击时可考察一个违反安全目标的角色动作序列是否能达成。例如为检验在简化 NSL 协议运行过程中，攻击者是否可以获得应该由主体 A, B 共享的随机数 Nb，可以考察如下角色实例的交叉事件序列：

$$\begin{aligned}&+penc([N_a,A],pk(b))-penc([n_a,a],pk(B))\\&+penc([n_a,N_b,B],pk(A))-penc([N_a,n_b,b],pk(A))\\&+penc(n_b,pk(b))-N_b\end{aligned}\qquad(1)$$

它表示 2 个协议会话下，角色实例 $Init(A,b,N_a,n_b)$ 和 $Resp(a,B,n_a,N_b)$ 的交叉事件序列。其中增加了一个事件“$-N_b$”，它表示任意角色可从攻击者处获得 N_b。倘若该交叉序列能够达成，表示协议运行的过程中攻击者能获得 N_b。

可认为所有“+”消息都会被发送给攻击者，所有“–”消息都是由攻击者发来的。这样，交叉序列中的每个“+”消息都可以被加入到攻击者的知识集合中，而每个“–”消息都应该是攻击者从其现有知识中可以构造出来的消息。也就是说，每个“–”消息都可与一个形如 m:T 的约束相对应，即攻

击者要在拥有知识(用项集合表示)T的情况下，产生消息m。于是，一个协议角色交叉事件序列即与一个约束序列相对应。如从式(1)所示的NSL协议交叉序列，可产生如下约束序列：

$$\begin{aligned} &penc([n_a,a],pk(B)):T_1=T_0\cup penc([N_a,A],pk(b))=\\ &\qquad\qquad\{A,B,I,pk(A),pk(B),pk(I),sk(I)\}\cup\\ &\qquad\qquad penc([N_a,A],pk(b)) \qquad (2)\\ &penc([N_a,n_b,b],pk(A)):T_2=T_1\cup\{penc([n_a,N_b,B],pk(A))\}\\ &N_b:T_3=T_2\cup\{penc(n_b,\ pk(b))\} \end{aligned}$$

其中，T_0为攻击者的初始知识。

若存在一个基置换σ，使对于约束序列$C=\{\eta_i:T_i|1\leqslant i\leqslant n\}$中的每一个约束，攻击者都可以从$T_i\sigma$构造出$m_i\sigma$，则说明与该约束序列对应的角色交叉事件序列实例是可以达成的，即攻击者可以成功地实施相应攻击。这样，协议的安全性验证问题就可以归结为任意有限数目会话下约束序列的求解问题，具体过程可以分为2步：(1)确定约束序列的一个基置换；(2)检验对于所有的i，是否每个$m_i\sigma$都可从$T_i\sigma$导出。文献[5]重点讨论了基置换σ的求解问题，本文只讨论具有加密同态特性验证能力的攻击者演绎问题。

4 攻击者演绎问题

攻击者演绎问题是指给定消息项集合T和项s，攻击者是否能由T导出s。该问题是安全协议自动化验证的首要问题。若攻击者根据其计算能力能由T演绎出s，则记为$T\square s$。本文基于Dolev-Yao模型[1]对攻击者能力进行建模，但为能验证具有加密同态特性的协议，赋予攻击者模等式理论的推理能力。

4.1 等式理论

定义4(方程、同余、E-等式)

(1)一个方程是一个项对$(s, t)\in T(F, C, V)\times T(F, C, V)$，记为$s=t$。方程是对称的，即$s=t$与$t=s$等价。

(2)项上的同余关系~是一种适应项结构和置换的等价关系：若对于所有的$s, t, t'\in T(F, C, V)$和$p\in O(s)$，都有$s[t]_p\sim s[t']_p$，则称$t\sim t'$。若对于所有$s, t\in T(F, C, V)$和置换σ，都有$s\sigma\sim t\sigma$，则称$s\sim t$。

(3)对于$T(F, C, V)$上的一个方程集合E，E-等式$=_E$是涵盖E的最小同余。即对于所有$s=t\in E$和置换σ，都有$s\sigma=_E t\sigma$。

采用方程对同态特性进行建模，如等式理论$senc([x,y],\ z)=[senc(x,z),\ senc(y,\ z)]$表示对称密钥加密的同态特性，$penc([x,y],z)=[penc(x,z),penc(y,z)]$表示公钥加密的同态特性。其他代数特性也可以基于等式理论描述，如$key(x,\ y)=key(y,\ x)$表示共享密钥中的主体名具有交换性，

$$\begin{aligned} &\mathrm{xor}(\mathrm{xor}(x,y),z)=\mathrm{xor}(x,\mathrm{xor}(y,z))\\ &\mathrm{xor}(x,y)=\mathrm{xor}(y,x)\ ,\ \mathrm{xor}(x,0)=x\\ &\mathrm{xor}(x,x)=0 \end{aligned}$$

分别表示异或运算的ACNU特性等。

4.2 基于等式理论的Dolev-Yao扩展模型

攻击者的推理和计算能力是决定约束序列可满足性的主要因素，将攻击者能力形式化为演绎规则，得到如下演绎系统，其中$intruder(m)$表示攻击者知道项m：

(1)合成规则

项组合(C)：

$intruder(u)\wedge intruder(v)\Rightarrow intruder([u,v])$

公钥加密(PE)：

$intruder(u)\wedge intruder(v)\Rightarrow intruder(penc(u,v))$

对称加密(SE)：

$intruder(u)\wedge intruder(v)\Rightarrow intruder(senc(u,v))$

哈希(H)：$intruder(u)\Rightarrow intruder(h(u))$

数字签名(S)：

$intruder(u)\Rightarrow intruder(sing(u,sk(I))$

共享密钥构造(KC)：

$intruder(u)\Rightarrow intruder(key(u,I))$

(2)分解规则

项左拆分(LUC)：$intruder([u,v])\Rightarrow intruder(u)$

项右拆分(RUC)：$intruder([u,v])\Rightarrow intruder(v)$

公钥解密(PD)：

$intruder(penc(u,pk(I)))\Rightarrow intruder(u)$

对称密钥解密(SD)：

$intruder(senc(u,v))\wedge intruder(v)\Rightarrow intruder(u)$

解签名(DS)：

$intruder(sing(u,sk(x))\wedge intruder(pk(x))\Rightarrow intruder(u)$

以上规则刻画了Dolev-Yao攻击者的能力，由这些规则可以看出，攻击者只有在知道密钥的情况下，才能得到密文。攻击者没有获得其他主体私钥的能力，也不能构造其他主体之间的共享密钥。

在此基础上，笔者增加一条等式推理规则来扩充攻击者的计算能力。

(3)等式推理规则(E)

$intruder(u)\wedge u=_E v\Rightarrow intruder(v)$

从项集合T对项m的推导可看作是一棵推导树，其根被标记为$intruder(m)$，叶被标记为$intruder(v)|\ v\in T$，每个中间节点及其儿子节点分别构成某个攻击者推理规则实例的结论和前提。若存在这样的一棵推导树，则有$T\square m$。推导的大小是推导树中的节点数目，如果没有更小的从T到m的推导，则称该推导为最小推导。

4.3 同态特性演绎

仍以简化NSL协议为例，并令等式理论E为$penc([x,y],z)=[penc(x,z),penc(y,z)]$。可以看出，在约束序列(2)中，当$\sigma=\{b\mapsto I, n_b\mapsto N_b, n_a\mapsto N_a\}$时，$m_1\sigma\in T_1\sigma$，所以直接有$T_1\sigma\square m_1\sigma$。应用公钥解密($PD$)规则，一步即可由$T_3\sigma$导出$m_3\sigma$。而由$T_2\sigma$导出$m_2\sigma$则需要应用更多的演绎规则，其最小推导如图1所示。

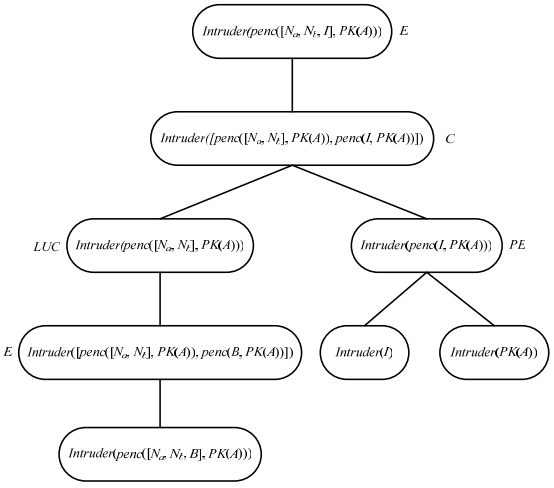

图1 基于同态的攻击者演绎推理

可以看出，在此等式推理规则被应用了2次，这与2.1节所示的实际情况相同。而在不应用E规则的情况下，

(下转第165页)