文章编号:1001 - 9081(2010)04 - 1033 - 05

应用组合方法设计安全协议

邓 帆,邓少锋,李益发
(信息工程大学 信息工程学院,郑州 450002)
(windcctv123456789@163.com)

摘 要:针对目前安全协议的设计方法存在方法抽象、适用范围小及复杂的特点,提出了一种新的安全协议设计方法。先给出协议中基件与组件的定义,分析组件的安全属性并基于组件设计能实现相应安全目标的单步协议;定义组合规则,确保不同的单步协议能够组合成为一个复合协议,同时各个单步协议还能实现各自的安全目标。至此,根据具体的应用背景选择合适的单步协议按照组合规则组合后便可得到满足需求的安全协议。该组合方法可将一个复杂协议分解为若干简单的单步协议,使得协议的设计与分析都易于实现。

关键词:安全协议;单步协议;组件;逻辑分析;组合
中图分类号: TP309 **文献标志码**:A

Security protocol design by composition method

DENG Fan, DENG Shao-feng, LI Yi-fa
(*Institute of Information Engineering, Information Engineering University, Zhengzhou Henan* 450002, *China*)

Abstract: Since the present design methods for security protocol are characterized by being abstract, narrow application range and complexity, this paper presented a new approach to design security protocol. Firstly, it defined the concepts of the base case and the component in the protocol. Secondly, it analyzed the security attributes on the components, and designed the single-step protocols which can implement the special security goals based on the components. Finally, it defined composition rules allowing the combination of several single-step protocols part into a complicated protocol. The rules cannot destroy the security properties established by each independent part. Then it can design security protocol by the choice and composition of the single-step protocols in specific application situation. In other words, the composition framework permits the specification of a complex protocol to be decomposed into the specifications of simpler single-step protocols, and thus making the design and verification of the protocol easier to handle.

Key words: security protocol; single-step protocol; component; logical analysis; composition

0 引言

安全协议是网络安全的一个重要组成部分,可以提供身份标识与认证服务、授权与访问控制服务、非否认服务、机密性服务、完整性服务等。目前安全协议设计通常的模式是:先采用基于经验的、非形式化的方法设计出安全协议,然后采用已有的分析方法对安全协议进行分析。如果发现协议存在缺陷,则对协议进行改进,否则认为协议是安全的。然而事实证明,许多在设计时被认为是正确的安全协议都存在安全缺陷,甚至有些缺陷在协议投入使用多年后才被发现。如果在安全协议设计之初就能够保证协议的安全性,不但可以极大地提高安全协议所在网络应用的安全性,而且能够避免大量的重复性工作。因此,安全协议设计的研究是十分有意义的。

为了解决协议设计过程中可能存在的问题,保证所设计协议的安全性,文献[1]在对协议缺陷进行深刻分析的基础上,提出了安全协议设计的一系列准则,然而设计准则对保证协议的安全性既不是充分也不是必要的。文献[2]提出了基于遗传算法和模拟退火算法的自动化协议设计方法,然而该方法在生成复杂协议时效率较低。文献[3]提出了应用串空间模型和认证测试方法来指导安全协议设计,并且所设计的协议其安全性可以直接由设计过程本身得到保证,然而该方法首先假设协议参与方之间存在共享秘密,因而其适用范围受到限制。文献[4-5]提出了一个计算复杂性理论模型:通用可组合(Universally Composable, UC)安全,简称 UC 安全。在这种模型中设计证明的安全协议,可以和其他任何协议并发组合运行,也可以作为一个子协议嵌入到复杂协议中,仍然能够保持相应的安全性。UC 安全对安全性要求非常高,几乎所有的具有实际意义的安全多方计算函数,要想获得 UC 安全性,必须具备一定的前提假设。文献[6-7]提出了一个用于协议导出的形式化框架,能够从简单的协议成分出发,通过组合、精化和变形等操作导出一系列协议,然而该方法不适用于对称密钥算法。文献[8]指出安全协议之间可以进行组合,在 UC 安全模型下证明了任意两个安全协议组合后仍然是安全的。

本文提出了应用组合方法进行安全协议设计。针对非对称环境下的若干组件,运用安全协议分析本征逻辑(Security Protocol Analysis Latent Logic,SPALL)分析了这些组件所具有的安全属性,同时基于这些组件设计了与其对应的若干单步协议。本文还定义了单步协议的组合规则,通过选择合适的单步协议按照组合规则组合后便可得到所需协议,最后以非对称环境下的安全认证协议和安全密钥协商协议为例说明如何运用该方法设计安全协议。与文献[8-11]中的其他组合设计方法相比,本文提出的方法特点在于:1)本文所定义的组合规则简单、可靠,组合规则不影响单步协议安全目标的实

收稿日期:2009-09-30;**修回日期**:2009-11-27。 **基金项目**:通信技术重点实验室基金资助项目(9140C1103040902)。
作者简介:邓帆(1980-),男,云南曲靖人,硕士研究生,主要研究方向:安全协议设计与分析; 邓少锋(1984-),男,江西高安人,硕士研究生,主要研究方向:安全协议设计与分析; 李益发(1964-),男,安徽芜湖人,副教授,博士,主要研究方向:密码学、信息安全。

现,同时可以保证单步协议能够组合成为复合协议。2)本文指出组件作为协议的基本组成部分,对组件的形式化分析可以从协议底层开始保证协议能够实现安全目标,减少协议可能存在的安全隐患,使安全协议的设计与分析都易于实现。3)该方法适用于不同初始假设的多种环境。该方法的关键在于对具体环境下组件安全属性的正确分析,对初始假设的环境无特别要求。

1 应用组合方法设计安全协议

判断一个协议是否安全,其本质就是考查协议所期望的安全目标是否都能达到。传统的设计方法将所有安全目标作为一个整体,然而,要找到一个协议能同时满足所有安全目标并不是一件容易的事。随着安全目标的增加,找到一个满足条件的安全协议将更加困难。

为解决此问题,本文提出了应用组合方法进行安全协议设计,该方法的步骤如下。

1)定义基件的概念,如用户 A、B, A 生成的随机数 N_A, B 的公钥 K_B 等被称为基件,单个基件是不具有任何安全属性的。将基件进行组合后可得到组件,如 $[A,N_A]K_B$,组件是协议中具有安全属性的基本单位。

2)对不同的组件进行分析,得出一定环境下单个组件所具有的安全属性,如:B 收到 A 产生的组件 $[A,N_A]K_B$ 后回复组件 $[B,N_A]K_A$ 给 A,则 A 认证了 B 的身份,即组件 $[B,N_A]K_A$ 在该环境下具有认证属性。将分析后的组件进行合理组合,可得到能实现相应安全目标的单步协议。如基于组件 $[B,N_A]K_A$ 的单步协议为:$A \rightarrow B:[A,N_A]K_B$; $B \rightarrow A:[B,N_A]K_A$,该单步协议实现了 A 认证 B 身份的安全目标。

3)定义组合规则使单步协议通过组合可得到新的协议,然后根据具体的应用背景和需求选择合适的单步协议,按照规则进行组合后得到满足需求的安全协议。

用这种组合方法设计协议,将协议的安全目标分散为多个子目标由不同的单步协议实现,组件作为协议的基本组成部分,在保证单步协议达到对应安全目标的同时也从底层保证了协议能达到预期的安全目标,这比将所有安全目标作为一个整体来设计协议容易得多。组合规则的使用使协议设计过程有了规范,避免了单纯基于经验或抽象的设计原则设计协议容易造成的安全隐患,确保了协议能够实现所期望的安全目标。

2 基础知识

SPALL[12]逻辑是一种改进的 BAN 类逻辑,它把 BAN 类逻辑置于数理逻辑这一理论基础之上,使 BAN 类逻辑进一步理论化、系统化,同时该逻辑阐释、构建了认证逻辑的理论基础,重新刻划了认证逻辑语义,建立了新的认证逻辑公理系统,把认证逻辑看作该系统的一个特殊解释,省去了理想化过程,克服了其他 BAN 类逻辑在分析协议时需要理想化过程的重大缺陷。因此,SPALL 逻辑的公理可靠,使用简便。

2.1 SPALL 逻辑的基本命题符号

记所有消息的集合为 Σ,ζ 表示所有时戳的集合,N 表示所有随机数的集合。简单命题 A 的否定记作 $\neg A$,A 并且 B 记为 $A \wedge B$,如果 A 那么 B 记为 $A \rightarrow B$,A 当且仅当 B 记为 $A \leftrightarrow B$。如果 Y 是由 X 和其他比特串级联而成或者就是 X,则称 Y 包含了 X,并记作 $Y = \rho(X)$。用 $(X \cong Y)$ 表示从 Y 中可以恢复出 X。由 φ 和 $(\varphi \rightarrow \psi)$ 可直接得到 ψ,该规则称为分离规则,简记为 MP。

$P \ni X$ 表示 P 生成了 X,$P \lhd X$ 表示 P 看见了 X, $X > P$ 表示 X 是给 P 的,$\&(P)$ 表示 P 正在参与执行协议的通信。$P \Rightarrow B$ 表示 P 意定的通信对象是 B,$P \mid\equiv X$ 表示 P 相信 X 是真的,$P \mid\sim X$ 表示 P 说过 X,$\#(X)$ 表示 X 是新鲜的,$K \mapsto P$ 表示 K 是 P 的公开密钥,$P < X > B$ 表示 P 和 B 共享秘密 X,$[X]K$ 表示 K 加密 X 所得密文,$P \mid\equiv \Diamond(X)$ 表示 X 对于 P 来说具有双向可追溯性,所谓双向可追溯性,是指消息 X 由确定的主机给出,由合法的接收者接收。$P \mid\approx X$ 表示 $P \mid\sim X \wedge \#(X)$,称为 P 刚刚说过 X。$\{A,B\} \trianglelefteq K$ 表示 $(\forall R)(R \lhd X \rightarrow R \in \{A, B\})$。

2.2 SPALL 逻辑的公理及定理

本文所用到的公理及定理均来自文献[12],所用编号也与该文献相同。此处列出了本文将用到的一部分公理或定理,其他请参考文献[12]。

1)身份认证公理(Axiom about the Identity of Participator, AIP)。

a) AIP2 $P \mid\equiv (Q \mid\approx X \wedge X \in \Sigma) \rightarrow P \mid\equiv \&(Q)$

其含义是:如果 P 相信 Q 刚刚说过 X,则 P 相信 Q 正在参与通信。

b) AIP6 $(X \in \Sigma \wedge P \mid\sim X > Q) \rightarrow P \Rightarrow Q$

其含义是:如果 P 说过 X,并且 X 是给 Q 的,则 Q 是 P 的通信对象。

2)信宿公理(Axiom about Message Destination, AMD)。

1) AMD1 $K \mapsto P \rightarrow ((\neg (P \ni [X]K) \wedge P \mid\equiv [X]K \in \Sigma) \rightarrow P \mid\equiv X > P)$

其含义是:如果一个主机 P 看见了 $[X]K$,并能确认其消息真实性,则或者 P 自己生成了 $[X]K$,或者拥有 K 的逆,通过解密来确认其真实性。而 P 拥有解密密钥,必然 P 是合法的消息接收者。

3)消息生成公理(Axiom about Message Generation, AMG)。

a) AMG1 $P \ni X \rightarrow (P \mid\equiv X \in \Sigma \wedge P \mid\equiv \Diamond(X))$

其含义是:P 生成了 X,则 P 一定认为 X 是有意义的消息,否则 P 没有必要在执行协议时生成 X。同时,P 也一定清楚 X 的来源和接收对象。

b) AMG2 $X \in \zeta \cup N \rightarrow (P \ni X \rightarrow P \mid\equiv \#(X))$

其含义是:如果 P 所生成的 X 是一个时戳,或者是一个乱数,那么它相信 X 是新鲜的。

4)消息真实性公理(Axiom about Truthful Message, ATM)。

ATM3 $P \lhd [X]K \rightarrow (P \mid\equiv X \cong [X]K \rightarrow (P \mid\equiv X \in \Sigma \leftrightarrow P \mid\equiv [X]K \in \Sigma))$

其含义是:如果 $[X]K$ 是一个密文,则它必须解密该消息并从中还原出可识别的消息 X 后才能相信 $[X]K$ 是一个真实的消息。反过来,如果 P 相信密文 $[X]K$ 是一个消息,同时它又能从中恢复出 X,则它有理由相信解密所得到的 X 是一个消息。

5)关于“Said”谓词的定理(Theorem about said, TAS)

a) TSD2 $\{P \lhd [X]K^{-1}, P \mid\equiv K \mapsto Q, P \mid\equiv X \in \Sigma\} \rightarrow P \mid\equiv Q \mid\sim X$

b) TSD6 $P \mid\equiv X \in \Sigma \rightarrow (P \mid\equiv Q \mid\sim \rho(X) \rightarrow P \mid\equiv Q \mid\sim X)$

6)关于信宿的定理(Theorem About asymmetric Key, TAK)。

TAK11 $K \mapsto P \rightarrow (P \lhd [X]K \rightarrow P \lhd X)$

综合上述介绍可知,如果 $A \mid\equiv \&(B)$,$A \mid\equiv B \Rightarrow A$,则表示 A 认证了 B 的身份。如果 $B \lhd K$,$B \mid\equiv K \in \Sigma$, $B \mid\equiv \#(K)$,$B \mid\equiv \Diamond(K)$, $B \mid\equiv A \lhd K$, $\{A,B\} \trianglelefteq K$,则表示 A 和 B 参与的密钥建立协议的安全目标(A 是密钥生成方但不确认密钥是否被正确接收),其安全目标为:B 验证 A 的身份以及密钥的真实性、新鲜性,同时双方还可保证密钥的机密性(更多详细讨论可参

考原文献)。

3　基件与组件

协议的运行是通过协议消息的交换来完成的,本文定义基本消息与基件的概念如下。

定义 1　下列 4 种消息称为基本消息:1) 协议实体标识 ID。如 A,B 等代表用户, S 代表服务器或管理中心。2) 密钥 K。K 代表各实体的公钥、私钥、会话密钥、共享密钥等。3) 乱数 N。协议实体在协议运行期间产生的临时值,如随机数 N_A,时戳 T_A 等。4) 数据消息 D。实体之间通过协议传送的信息。

定义 2　基本消息和密码函数统称为基件。常见的密码函数有如下一些:1)Hash 函数 $Hash(\cdot)$。2) 签名函数 $SIG_{K^{-1}}(\cdot)$。此处为研究方便,将签名函数表示为 $[\cdot]K^{-1}$,K^{-1} 为用户私钥。3) 加密函数 $E_K(\cdot)$。K 为加密密钥。4)DH 密钥交换体制中用到的 g^x,其中 $x \in Z_q$,g 是群 G_q 的一个生成元 (p、q 为大素数,$q \mid (p-1)$,G_q 为乘法群 Z_p^* 的一个阶为 q 的子群)。

组件通过下列 3 种操作产生。1) 级联操作。两个或多个基件通过级联操作后可得到一个组件。如 A、N_A 是两个基件,级联后形成 $\{A,N_A\}$ 便是一个组件。2) 密码函数操作。如 A、N_A、$Hash(\cdot)$ 是基件, $H(A,N_A)$ 便形成一个组件。3) 混合操作。组件与组件、组件与基件之间通过级联、密码函数的混合操作而形成新的组件。

4　非对称环境下安全协议组件的安全属性分析

4.1　基本假设

在分析协议组件的安全属性时,假定所用的基件都是安全的,如选取的随机数不发生重复,用户间的共享秘密未发生泄漏,用户所使用的密钥、所采用的 Hash 函数和加密函数是安全的,等等。只有在这些基本假设下保证了基件的安全,讨论组件的安全属性才是有意义的。

4.2　组件的安全属性分析

通过对非对称环境下大量协议的归纳总结,得到了如下一些协议中的常用组件,现介绍这些组件及其应用背景(假设 A、B 双方已知对方公钥证书)。

1) $g_{11}:[A,N_A]K_B^{-1}$,A 产生随机数 N_A 后发送组件 $\{A,N_A\}$ 给 B,B 回复组件 g_{11} 给 A。

2) $g_{21}:[H(A,B,N_A)]K_B^{-1}$,$A$ 产生随机数 N_A 后发送组件 $\{A,N_A\}$ 给 B,B 回复组件 g_{21} 给 A。

3) $g_{31}:[B,g^x]K_A^{-1}$,A 生成 g^x 并发送组件 g_{31} 给 B,B 回复组件 $[A,g^y]K_B^{-1}$ 给 A。

4) $g_{41}:E_{pw}(B,N_A,g^x)$,A、B 双方共享口令 pw,A 生成 N_A、g^x 并发送组件 g_{41} 给 B,B 回复组件 $E_{pw}(A,N_A)$ 给 A。

5) $g_{51}:H(A,B,N_A,N_B,g^x,g^y,g^{xy})$,$A$ 生成 N_A、g^x,B 生成 N_B、g^y,A、B 双方已协商达成共享密钥 g^{xy} 并各自计算组件 g_{51}。

6) $g_{61}:[A,N_A,g^x]K_B^{-1}$,$A$ 生成 N_A、g^x 并发送组件 $\{A,N_A,g^x\}$ 给 B,B 收到后回复组件 g_{61} 给 A。

7) $g_{71}:[[A,N_A,g^x]K_B^{-1}]K_A$,$A$ 生成 N_A、g^x 并发送组件 $\{A,N_A,g^x\}$ 给 B,B 回复组件 g_{71} 给 A。

8) $g_{81}:[[B,N_A]K_A^{-1}]K_B$,$A$ 生成 N_A 并发送组件 g_{81} 给 B,B 回复组件 $[B,N_A]K_A$ 给 A。

下面对组件 $[A,N_A]K_B^{-1}$ 运用 SPALL 逻辑进行分析,见表 1(初始假设简记为 BAS)。

通过表 1 分析可知,该组件所具有的安全属性描述为: $A \mid\equiv \&(B)$,$A \mid\equiv B \Rightarrow A$,即该组件所具有的安全属性为 A 认证了 B 的身份,同时由签名函数本身所具有的安全属性可知,该组件还具有签名用户的非否认性。

表 1　组件 $[A,N_A]K_B^{-1}$ 的分析

推理过程	推理依据
(1) $A \mid\equiv K_B \mapsto B$	BAS
(2) $A \lhd [A,N_A]K_B^{-1}$	BAS
(3) $A \ni N_A$	BAS
(4) $N_A \in N$	BAS
(5) $A \ni N_A \rightarrow A \mid\equiv N_A \in \Sigma$	AMG1
(6) $\{(3),(4)\} \rightarrow A \mid\equiv \#(N_A)$	AMG2
(7) $A \lhd [A,N_A]K_B^{-1} \rightarrow A \mid\equiv (A,N_A) \in \Sigma$	ATM3
(8) $\{(1),(2),(7)\} \rightarrow A \mid\equiv B \mid\sim (A,N_A)$	TSD2
(9) $A \mid\equiv B \mid\sim (A,N_A)$	MP
(10) $A \mid\equiv B \mid\sim (A,N_A) \rightarrow A \mid\equiv B \mid\sim N_A$	TSD6
(11) $A \mid\equiv B \mid\sim N_A$	MP
(12) $\{A \models B \mid\sim N_A \wedge A \models \#(N_A)\} \rightarrow A \models B \mid\approx N_A$	$\mid\approx$ 的定义
(13) $A \mid\equiv B \mid\approx N_A$	MP
(14) $A \mid\equiv B \mid\approx N_A \rightarrow A \mid\equiv \&(B)$	AIP2
(15) $A \mid\equiv \&(B)$	MP
(16) $A \models B \mid\sim (A,N_A) \rightarrow A \models B \mid\sim (A,N_A) \succ A$	BAS
(17) $A \mid\equiv B \mid\sim (A,N_A) \succ A$	MP
(18) $\{(7),(17)\} \rightarrow A \mid\equiv B \Rightarrow A$	AIP6
(19) $A \mid\equiv B \Rightarrow A$	MP

下面以组件 $[[A,N_A,g^x]K_B^{-1}]K_A$ 为例运用 SPALL 逻辑进行逻辑化分析,见表 2。

表 2　组件 $[[A,N_A,g^x]K_B^{-1}]K_A$ 的分析

推理过程	推理依据
(1) $A \ni N_A$	BAS
(2) $A \ni g^x$	BAS
(3) $A \mid\equiv \neg (A \ni [[A,N_A,g^x]K_B^{-1}]K_A)$	BAS
(4) $A \ni g^x \rightarrow A \mid\equiv \#(g^x)$	AMG2
(5) $A \ni g^x \rightarrow A \mid\equiv g^x \in \Sigma$	AMG1
(6) $A \ni g^x \rightarrow A \mid\equiv \Diamond(g^x)$	AMG1
(7) $A \lhd [[A,N_A,g^x]K_B^{-1}]K_A$	BAS
(8) $K_A \rightarrow A$	BAS
(9) $\{(7),(8)\} \rightarrow A \lhd [A,N_A,g^x]K_B^{-1}$	TAK11V
(10) $A \lhd [A,N_A,g^x]K_B^{-1}$	MP
(11) $A \lhd [A,N_A,g^x]K_B^{-1} \rightarrow A \mid\equiv [A,N_A,g^x]K_B^{-1} \in \Sigma$	ATM3
(12) $A \lhd CERT(B)$	BAS
(13) $A \lhd CERT(B) \rightarrow A \mid\equiv K_B \mapsto B$	BAS
(14) $A \mid\equiv K_B \mapsto B$	MP
(15) $A \lhd [A,N_A,g^x]K_B^{-1} \rightarrow A \mid\equiv (A,N_A,g^x) \in \Sigma$	ATM3
(16) $\{(10),(14),(15)\} \rightarrow A \mid\equiv B \mid\sim (A,N_A,g^x)$	TSD2
(17) $A \mid\equiv B \mid\sim (A,N_A,g^x)$	MP
(18) $\{(4) \wedge (17)\} \rightarrow A \mid\equiv B \mid\approx (A,N_A,g^x)$	$\mid\approx$ 定义
(19) $A \mid\equiv B \mid\approx (A,N_A,g^x)$	MP
(20) $A \mid\equiv B \mid\approx (A,N_A,g^x) \rightarrow A \mid\equiv \&(B)$	AIP2
(21) $A \mid\equiv \&(B)$	MP
(22) $\{(3),(8),(11)\} \rightarrow A \mid\equiv [A,N_A,g^x]K_B^{-1} \succ A$	AMD1
(23) $A \mid\equiv [A,N_A,g^x]K_B^{-1} \succ A$	MP
(24) $B \lhd \{A,N_A,g^x\}$	BAS
(25) $A \lhd [A,N_A,g^x]K_B^{-1} \rightarrow A \mid\equiv B \mid\sim [A,N_A,g^x]K_B^{-1}$	BAS
(26) $A \mid\equiv B \mid\sim [A,N_A,g^x]K_B^{-1}$	MP
(27) $\{(23) \wedge (26)\} \rightarrow A \mid\equiv B \Rightarrow A$	AIP6
(28) $A \mid\equiv B \Rightarrow A$	MP

通过表 2 分析可知,该组件所具有的安全属性描述为: $A \mid\equiv \&(B)$,$A \mid\equiv B \Rightarrow A$,$B \lhd g^x$,$A \mid\equiv \#(g^x)$,$A \mid\equiv \Diamond(g^x)$,即该组

件所具有的安全属性为A认证了B的身份,A、B间进行会话密钥协商并保证密钥的新鲜性、机密性,对用户B来说还具有非否认性,同时提供了身份保护以防止被动攻击。

其他组件采用类似分析方法可得如下结论。

1)$g_{21}:[H(A,B,N_A)]K_B^{-1}$,该组件的安全属性与组件$g_{11}$相同。

2)$g_{31}:[B,g^x]K_A^{-1}$,该组件的安全属性为A、B进行密钥协商,对用户A来说具有非否认性,但用户之间的身份认证和密钥的新鲜性却无法得到保证。

3)$g_{41}:E_{pw}(B,N_A,g^x)$,该组件所具有的安全属性为A认证B身份的同时与B进行密钥协商,并保证了密钥的新鲜性和机密性。

4)$g_{51}:H(A,B,N_A,N_B,g^x,g^y,g^{xy})$,该组件常作为$A$、$B$间的会话密钥。

5)$g_{61}:[A,N_A,g^x]K_B^{-1}$,该组件所具有的安全属性为$A$认证$B$身份的同时与$B$进行密钥协商,并保证了密钥的新鲜性和$B$的非否认性。

6)$g_{81}:[[B,N_A]K_A^{-1}]K_B$,该组件所具有的安全属性为$A$认证了$B$的身份并保证了传输数据的机密性,对用户$A$来说还具有非否认性,同时提供了身份保护以防止被动攻击。根据组件安全属性分析的结果,可设计与其对应的单步协议,见表3(不难看出,采用与分析组件安全属性的类似方法可证明单步协议的安全目标与组件的安全属性是一致的)。

5 非对称环境下安全协议的设计

5.1 组合规则

5.1.1 单步协议选取原则

利用单步协议设计安全协议时,首先要根据具体的背景和需求选择合适的单步协议,在选取单步协议时需遵循以下原则。

1)选取应用环境相符的单步协议。如安全协议的应用背景为对称环境,则只能选择对称环境下的单步协议,并根据安全协议需要达到的安全目标来选择相应的单步协议。

2)选取安全目标相容的单步协议。选取单步协议P_i和P_j进行组合时必须保证单步协议P_i的安全目标不会影响到单步协议P_j的安全目标。也就是说,基于组件g_i的单步协议P_i实现安全目标的同时,基于组件g_j的单步协议P_j也能实现其安全目标。

3)规范所选单步协议的符号表示。如P_i中用N_A表示A生成的随机数,那么P_j中不能再使用N_A表示B生成的随机数,以免混淆。

5.1.2 组合顺序原则

正确选择完单步协议后,需定义单步协议的组合顺序。假定$P_g=\{P_1,P_2,\cdots,P_n\}$代表基于组件的一系列单步协议的集合,这些单步协议能达到的安全目标是由其基于的组件的安全属性所保障的。P为单步协议组合后得到的安全协议,即$P=P_1\otimes P_2\otimes\cdots\otimes P_n$。各单步协议进行组合时必须遵守某个顺序用$O(P)$表示。记$e$为协议中的运行动作,如果协议消息分别为$P_1:M_1,M_2;P_2:N_1,N_2$。那么每个发送消息的步骤即为一个动作,即动作有$e(M_1),e(M_2),e(N_1),e(N_2)$,$O(P)=e(M_1)<e(M_2)<e(N_1)<e(N_2)$表示协议按发送$M_1,M_2,N_1,N_2$的顺序进行组合。定义协议组合顺序时,需遵守以下原则:1)若协议的安全目标间存在先后关系,则所定义的组合顺序不能与安全目标顺序相矛盾。2)组合顺序需保证协议中任一发起方都有明确的响应方与之共同实现安全目标。3)协议组合原则:如果单步协议P_i并入单步协议P_j中,则将P_i中的消息从P_j中第一个拥有和P_i中相同的消息发送者和接受者的消息开始依次合并,而多余的消息则依次移入P_j。

表3 基于组件的单步协议

组件	单步协议
(1)$g_{11}:[A,N_A]K_B^{-1}$	M_1 $A\rightarrow B:A,N_A$ M_2 $B\rightarrow A:B,[A,N_A]K_B^{-1}$
(2)$g_{12}:[B,N_B]K_A^{-1}$	N_1 $B\rightarrow A:B,N_B$ N_2 $A\rightarrow B:A,[B,N_B]K_A^{-1}$
(3)$g_{21}:[H(A,B,N_A)]K_B^{-1}$	M_1 $A\rightarrow B:A,N_A$ M_2 $B\rightarrow A:B,[H(A,B,N_A)]K_B^{-1}$
(4)$g_{22}:[H(A,B,N_B)]K_A^{-1}$	N_1 $B\rightarrow A:B,N_B$ N_2 $A\rightarrow B:A,[H(A,B,N_B)]K_A^{-1}$
(5)$g_{41}:E_{pw}(B,N_A,g^x)$	M_1 $A\rightarrow B:A,E_{pw}(B,N_A,g^x)$ M_2 $B\rightarrow A:B,E_{pw}(A,N_A)$
(6)$g_{42}:E_{pw}(A,N_B,g^y)$	N_1 $B\rightarrow A:B,E_{pw}(A,N_B,g^y)$ N_2 $A\rightarrow B:A,E_{pw}(B,N_B)$
(7)$g_{61}:[A,N_A,g^x]K_B^{-1}$	M_1 $A\rightarrow B:A,N_A,g^x$ M_2 $B\rightarrow A:B,[A,N_A,g^x]K_B^{-1}$
(8)$g_{62}:[B,N_B,g^y]K_A^{-1}$	N_1 $B\rightarrow A:B,N_B,g^y$ N_2 $A\rightarrow B:A,[B,N_B,g^y]K_A^{-1}$
(9)$g_{71}:[[A,N_A,g^x]K_B^{-1}]K_A$	M_1 $A\rightarrow B:A,N_A,g^x$ M_2 $B\rightarrow A:B,[[A,N_A,g^x]K_B^{-1}]K_A$
(10)$g_{72}:[[B,N_B,g^y]K_A^{-1}]K_B$	N_1 $B\rightarrow A:B,N_B,g^y$ N_2 $A\rightarrow B:A,[[B,N_B,g^y]K_A^{-1}]K_B$
(11)$g_{81}:[[B,N_A]K_A^{-1}]K_B$	M_1 $A\rightarrow B:A,[[B,N_A]K_A^{-1}]K_B$ M_2 $B\rightarrow A:B,[B,N_A]K_A$
(12)$g_{82}:[[A,N_B]K_B^{-1}]K_A$	N_1 $B\rightarrow A:B,[[A,N_B]K_B^{-1}]K_A$ N_2 $A\rightarrow B:A,[A,N_B]K_B$

5.1.3 去除冗余原则

当指定了单步协议的组合顺序后,按顺序组合所得的安全协议可能存在冗余,为解决此问题,本文定义了如下组件合并原则:1)设t是消息i中的一个组件,如果消息i和消息j拥有相同的消息发送者和接受者,且组件t不具有新鲜性,则可以将组件t从消息i移到消息j中。2)如果消息i中拥有多个加密组件,而且这些加密组件采用相同的密码算法和密钥,则可以将这些加密组件合成一个组件。3)如果在协议一步中同样消息出现两次,那么只保留其中的一条。4)如果用于证明新鲜性的数据项(例如随机数)总是和协议中某个具有新鲜性的数据项同时出现,那么用于证明新鲜性的数据项可以删除。

5.1.4 non-Dos 规则

本文定义了 non-Dos 规则。协议具有抗 DoS 攻击的能力,即协议的响应者在对协议发起者的合法身份进行确认之前,不进行任何花销昂贵的操作。本文采用增加 Cookie 的方法[7]使协议具有抗 DoS 攻击的能力。同时,DoS 攻击是盲目

的,即进行 DoS 攻击的攻击者不对协议消息进行任何操作如窃听、消息重放等,这和实际情况是相符的。

假定协议 I 的消息 m_2 可以分成两个部分:m_2^c 及 m_2^e,其中,m_2^c 为消息 m_2 中不执行任何花销昂贵操作的部分;m_2^e 为消息 m_2 中操作花销昂贵的部分。

non-Dos 规则:

$A \rightarrow B:m_1 \Rightarrow A \rightarrow B:m_1$

$B \rightarrow A:m_2 \quad B \rightarrow A:m_2^c, HMAC_{HK_b}(m_1, m_2^c)$

$A \rightarrow B:m_3 \quad A \rightarrow B:m_3, m_1, m_2^c, HMAC_{HK_b}(m_1, m_2^c)$

$B \rightarrow A:m_2^e$

这里 $Cookie = HMAC_{HK_b}(m_1, m_2^c)$,其中 $HMAC$ 是一个单向哈希函数且 HK_b 只对 B 已知。

由上述原则可知,单步协议选取原则保证了所选取的单步协议能够进行组合而不会影响各自安全目标的实现。组合顺序原则规定了整个协议的执行顺序,但对协议中每个单步协议而言,其执行顺序并未改变,因而单步协议所能实现的安全目标也未受到影响。去除冗余原则在不影响组件安全属性的前提下去除了协议中消息重复的部分,因此不会对单步协议所能实现的安全目标有任何影响。non-Dos 规则可保证协议能抵抗 DoS 攻击,同时组件的安全属性以及单步协议的安全目标均未受到影响。综上可知,所有规则在保证单步协议组合的同时未对单步协议所能达到的安全目标造成影响。因此,通过这些规则组合所得到的协议可实现所有单步协议的安全目标,由此说明了组合规则的安全性与正确性。

5.2　双向认证协议的实例设计

协议设计要求:设计非对称环境下的双向认证协议,需要满足的安全属性有:协议参与者彼此之间的身份认证,签名用户的非否认性。根据上述要求,可选择组件 $[A,N_A]K_B^{-1}$ 和组件 $[B,N_B]K_A^{-1}$,它们所对应的单步协议分别为:

P_1:　$M_1: A \rightarrow B:A,N_A$;

$M_2: B \rightarrow A:B,[A,N_A]K_B^{-1}$

P_2:　$N_1: B \rightarrow A:B,N_B$;

$N_2: A \rightarrow B:A,[B,N_B]K_A^{-1}$

定义组合顺序 $O(P) = e(M_1) < e(M_2) < e(N_1) < e(N_2)$,根据协议组合顺序原则可得到如下协议:

1) $A \rightarrow B:A,N_A$;

2) $B \rightarrow A:B,[A,N_A]K_B^{-1},B,N_B$;

3) $A \rightarrow B:A,[B,N_B]K_A^{-1}$。

运用去除冗余原则后可得到如下的协议:

1) $A \rightarrow B:A,N_A$;

2) $B \rightarrow A:B,N_B,[A,N_A]K_B^{-1}$;

3) $A \rightarrow B:A,[B,N_B]K_A^{-1}$。

根据 non-Dos 规则得到最终的协议 P:

1) $A \rightarrow B:A,N_A$;

2) $B \rightarrow A:B,N_B,HMAC_{HK_b}(A,N_A,B,N_B)$;

3) $A \rightarrow B:A,[B,N_B]K_A^{-1},N_A,B,N_B,HMAC_{HK_b}(A,N_A,B,N_B)$;

4) $B \rightarrow A:B,[A,N_A]K_B^{-1}$。

5.3　密钥协商协议的实例设计

协议设计要求:设计非对称环境下的基于 DH 密钥交换体制的密钥协商协议,由 A、B 两方参与。需要满足的安全属性有:会话密钥的新鲜性、机密性,协议参与方彼此之间的身份认证、非否认性和身份保护。根据上述要求,可选择组件 $[[A,N_A,g^x]K_B^{-1}]K_A$,$[[B,N_B,g^y]K_A^{-1}]K_B$,它们所对应的单步协议分别为:

P_1　$M_1: A \rightarrow B:A,N_A,g^x$;

$M_2: B \rightarrow A:B,[[A,N_A,g^x]K_B^{-1}]K_A$。

P_2　$N_1:$　$B \rightarrow A:B,N_B,g^y$;

$N_2:$　$A \rightarrow B:A,[[B,N_B,g^y]K_A^{-1}]K_B$。

定义组合顺序 $O(P) = e(M_1) < e(M_2) < e(N_1) < e(N_2)$ 根据协议组合顺序原则可得到如下协议:

1) $A \rightarrow B:A,N_A,g^x$;

2) $B \rightarrow A:B,[[A,N_A,g^x]K_B^{-1}]K_A,B,N_B,g^y$;

3) $A \rightarrow B:A,[[B,N_B,g^y]K_A^{-1}]K_B$。

运用去除冗余原则后可得如下协议:

1) $A \rightarrow B:A,N_A,g^x$;

2) $B \rightarrow A:B,N_B,g^y,[[A,N_A,g^x]K_B^{-1}]K_A$;

3) $A \rightarrow B:A,[[B,N_B,g^y]K_A^{-1}]K_B$。

根据 non-Dos 规则得到最终的协议 P:

1) $A \rightarrow B:A,N_A,g^x$;

2) $B \rightarrow A:B,N_B,g^y,HMAC_{HK_b}(A,N_A,g^x,B,N_B,g^y)$;

3) $A \rightarrow B:A,N_A,g^x,B,N_B,g^y[[B,N_B,g^y]K_A^{-1}]K_B,HMAC_{HK_b}(A,N_A,g^x,B,N_B,g^y)$;

4) $B \rightarrow A:B,[[A,N_A,g^x]K_B^{-1}]K_A$

5.4　协议安全性说明

采用该组合方法所设计的协议的安全性是建立在底层组件的安全属性基础之上的,通过运用逻辑化方法对组件的安全属性进行分析,保证了基于组件的单步协议能实现对应的安全目标,组合规则在保证单步协议实现安全目标的同时除去了协议中的冗余消息,因此,经单步协议组合后最终得到的安全协议在达到所需安全目标的同时效率也得到了保证。上述两个安全协议根据所需达到的安全目标选择了合适的单步协议进行组合,所得到的安全协议能实现所有预期的安全目标,因此协议是安全的(同时也间接证明了组合规则的正确性与安全性),具体的逻辑化证明可参看协议所对应组件的分析过程。

6　结语

本文提出应用组合方法设计安全协议,该方法将协议的安全目标分散为多个子目标由不同的单步协议实现,同时从底层的组件开始逐层保证协议能够达到预期的安全目标,具有协议设计易于实现、协议安全性易于分析的优点,适用于不同初始假设的多种环境。针对非对称环境下安全协议的若干组件,本文运用 SPALL 逻辑对组件所具有的安全属性进行了分析,设计了与组件相对应的单步协议,定义了单步协议组合时所需遵循的组合规则,并给出了利用该方法设计安全协议的两个实例。下一步的工作重点有两个方面:一是继续分析其他环境下组件的安全属性,为更多安全协议的设计奠定基础;二是完善组合规则,以适应更复杂安全协议的设计需求。

参考文献:

[1] ABADI M, NEEDHAM R M. Prudent engineering practice for cryptographic protocols [J]. IEEE Transactions on Software Engineering, 1996, 22(1):6 - 15.

(下转第 1041 页)

增强了其用于数字图像作品版权保护的实用性,具有一定的应用价值。

表 3　算法对几何攻击及联合的抵抗能力

攻击参数		BER/%	
		本文算法	文献[7]算法
旋转/(°)	5	2.03	6.25
	10	0.98	1.56
	15	2.12	7.81
	20	0	3.12
	25	2.18	4.68
	30	3.09	5.12
	45	4.87	9.76
	60	2.08	6.02
	90	0	0
缩放	0.8	3.86	7.81
	0.9	1.08	1.56
	1.1	1.18	1.75
	1.2	3.90	8.23
	2.0	9.58	15.36
	3.0	18.87	25.68
平移(水平、垂直方向)	10	19.54	48.43
	20	12.62	43.75
	30	10.83	42.18
垂直翻转		0	0
水平翻转		0	0
缩放 1.2 + 旋转 10°		3.86	4.68
缩放 1.2 + 平移 10		11.97	50.00
旋转 10° + 平移 20		11.04	45.31
缩放 1.2 + 旋转 10° + 平移 10		17.58	58.14
缩放 0.8 + 旋转 10° + 平移 20		24.74	65.24

参考文献:

[1] BARNI M, COX I J, KALKER T. Digital watermarking[C]// The 4th International Workshop on Digital Watermarking 2005. Berlin: Springer,2005:15 - 17.

[2] LICKS V, JORDAN R. Geometric attacks on image watermarking system[J]. IEEE Multimedia,2005,12(3):68 - 78.

[3] DONG P, BRANKOV J G, GALATSANOS N P, *et al.* Digital watermarking robust to geometric distortions[J]. IEEE Transactions on Image Processing, 2005,12(14):2140 - 2150.

[4] CHEN QING, YANG XIAOLI, ZHAO JIYING. Robust image watermarking with Zernike moments[EB/OL].[2009 - 06 - 20]. http://citeseerx. ist. psu. edu/viewdoc/download? doi = 10. 1. 1. 112. 9907&rep = rep1&type = pdf.

[5] 李雷达, 郭宝龙, 邵凯. 基于 SIFT 特征与 Zernike 矩的抗几何攻击图像水印[J]. 中国光学快报, 2007,5(6):332 - 335.

[6] 李雷达,郭宝龙,刘雅. 基于伪 Zernike 矩的抗几何攻击图像水印[J]. 光电子·激光,2007,18(2):231 - 235.

[7] XIN YONGQING, LIAO S, PAWLAK M. A multibit geometrically robust image watermark based on Zernike moments[C]// Proceedings of the 17th International Conference on Pattern Recognition. New York: IEEE,2004 :861 - 864.

[8] KANG XIAN-GUI, HUANG JI-WU, LIN YAN, *et al.* A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression[J]. IEEE Transactions on Circuits and Systems for Video Technology,2003,13(8):(2):776 - 786.

[9] JIN S S, CHANG D Y. Image watermarking based on invariant regions of scale-space representation[J]. IEEE Transactions on Signal Processing, 2006,54(4):1537 - 1549.

[10] PAUTE J, JORDAN F. Using fractal compression scheme to embed a digital signature into an image[EB/OL].[2009 - 06 - 20]. http://www. alpvision. com/pdf/jp_spie2915. pdf.

[11] PI MING-HONG, LI CHUN-HUNG, LI HUA. Anovel fractal image watermarking watermarking[J]. IEEE Transactions on Multimedia, 2006, 8(3):488 - 499.

[12] XIE RONG-SHENG, YANG SHU-GUO. A digital image watermarking method based on fractal transform in DWT domain[C]// 1st International Conference on Modelling and Simulation. Nanjing:[s. n.],2008.

[13] HADDADNIA J, AHMADI M, FAEZ K. An efficient feature extraction method with pseudo-Zernike moment in RBF neural network-based human face recognition system[J]. EURASIP Journal on Applied Signal Processing,2003(9): 890 - 901.

(上接第 1037 页)

[2] CLARK J A, JACOB J L. Protocols are programs too: The meta-heuristic search for security protocols [J]. Information and Software Technology, 2001, 43(14): 891 - 904.

[3] GUTTMAN J D. Security protocol design via authenti cation tests [C]// Proceedings of the 2002 IEEE Computer Security Foundation Workshop. Los Alamitos: IEEE Computer Society Press, 2002: 92 - 103.

[4] CANETTI R. Universally composable signature, certification, and authentication [C]// Proceedings of 17th IEEE Computer Security Foundations Workshop. [S. l.]: IEEE computer Society, 2004: 219 - 245.

[5] CANETTI R, KUSHILEVITZ E, LINDELL Y. On the limitations of universally composable two-party computation without set-up assumptions [J]. Journal of Cryptology, 2006, 19(2): 135 - 167.

[6] DATTA A, DEREK A, MITCHELL J C, *et al.* A derivation system and compositional logic for security protocols [J]. Journal of Computer Security, 2005, 13(3):423 - 482.

[7] DATTA A, DEREK A, MITCHELL J C, *et al.* Protocol composition logic (PCL) [J]. Electronic Notes Theoretical Computer Science, 2007, 172: 311 - 358.

[8] CORTIER V, DELAUNE S. Safely composing security protocols [J]. Formal Methods in System Design, 2009, 34(1):1 - 36.

[9] ARAPINIS M, DELAUNE S, KREMER S. From one session to many: Dynamic tags for security protocols [C]// LPAR'08: Proceedings of 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning, LNAI 5330. Berlin: Springer, 2008: 128 - 142.

[10] DELAUNE S, KREMER S, RYAN M D. Composition of password-based protocols [C]// CSF'08: Proceedings of the 21st IEEE Computer Security Foundations Symposium. Washington, DC: IEEE Computer Society, 2008: 239 - 251.

[11] ANDOVA S, CREMERS C, STEEN K G, *et al.* Sufficient conditions for composing security protocols [J]. Information and Computation, 2008,206(2/4):425 - 459.

[12] 李益发. 密码协议安全性分析中的逻辑化的方法——一种新的 BAN 逻辑 [D]. 郑州: 信息工程大学, 2001.