密码协议的 SPIN 建模和验证

邵晨曦,胡香冬,熊 焰,蒋 凡
(中国科学技术大学计算机科学技术系,安徽合肥 230027)

摘 要: 为了将模型检测这种强有力的系统验证技术应用于网络协议的安全分析,形式化建模仍然是目前的关键问题和难点所在.本文提出了一种基于高级过程描述语言的建模方法.根据入侵者角色和攻击目标的不同,从入侵者的角度分析协议的运行模式,为每个主体建立过程模型,用模型检测工具进行分析验证.对 BAN-Yahalom 协议的 SPIN 分析验证了这种方法的可行性.该方法具有一定的通用性,对其它网络协议的分析有很好的参考价值.

关键词: 模型检测; BAN-Yahalom 协议; SPIN
中图分类号: TP311.133.1 **文献标识码:** A **文章编号:** 0372-2112 (2002) 12A-2099-03

Modeling and Verifying Cryptographic Protocols Using SPIN

SHAO Chen-xi, HU Xiang-dong, XIONG Yan, JIANG Fan
(*Department of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, China*)

Abstract: *In order to use the strong system verification technology model checking in the security property analysis of network protocols, formal modeling method is still the critical problem. In this paper, a modeling method based on a high-level process description language is presented According to the categorizing based on intruders' objectives and roles, we analyze the running mode of protocols from the point of view of the intruders, constructing individual process specification for each principal, then verify them using model checking tools. The analysis of the BAN-Yahalom protocol illustrates the feasibility of the approach. This approach has some generality, and provids a good reference for analysis of other network protocols.*

Key words: model checking; BAN-Yahalom protocol; SPIN

1 引言

随着密码协议在计算机网络和分布式系统中的广泛应用,它们的安全性显得越发重要了.

形式化方法已经被证明是一种强有力的系统分析和验证技术.各种模型检测工具在大规模电路设计、硬件分析以及软件模块设计中得到了广泛地应用.近年来,国内外一些学者对模型检测方法在密码协议的安全分析中的应用进行了一些有益的尝试[1~3].研究结果表明模型检测是一种有效的网络协议分析工具.然而网络协议的形式化建模是一项很具技巧性的工作,目前仍是其形式化分析的关键问题和难点所在.

SPIN* 是一个优秀的分布式系统形式化验证软件.它采用 Promela(PROcess MEta LAnguage)作为建模语言,主要通过过程和消息通道来描述分布式系统.它可以进行如死锁和不可达状态等常规检测,也可以作为一个模型检测器进行 model checking 分析.

本文采用 SPIN 系统验证工具对 BAN-Yahalom 密码协议进行了形式化分析研究,提出了一种基于高级过程描述语言建模方法,应用该方法成功地找到了针对该协议的著名攻击,验证了这种方法的可行性.

2 密码协议的建模与分析方法

2.1 针对入侵者的形式化建模

形式化建模是密码协议分析的第一步也是关键的一步,一些不诚实的甚至是恶意的入侵者在网络中的出现增加了建模过程的复杂性.为了得到一个准确的形式化规范,须对入侵者攻击目标、在协议运行中扮演的角色及其能力有很好的理解.

本文假定入侵者的攻击目标为破坏协议的身份认证或破坏密钥分配或两者兼有.

攻击能力和攻击手段的假设是对入侵者建模的重点.通过对大量密码协议及相应攻击实例的分析后,假设入侵者为了对一个密码协议发动攻击可以采取如下方法:

(1)以自己的身份作为发起者或响应者参与协议运行;

(2)假扮其它合法主体参与协议运行;

(3)窃听或拦截系统中传送的消息,并尝试进行解密以获取新的信息;

(4)保存获取到的密钥在以后进行重现;

收稿日期:2002-05-28;修回日期:2002-10-03
基金项目:国家高性能计算基金(No.00215)

(5)保存未能解密的消息在以后重放;

(6)注入自己的密钥;

(7)注入自己生成的消息.

根据 TMN 密码协议的形式分析[3],假设协议的其它主体严格遵守协议规定的参与规则参与协议运行,并且假定协议中使用的加密算法是完备的,即任何一个主体在不知道解密密钥的情况下不可能对消息密文进行破解.

根据入侵者在协议运行中所扮演的角色不同,对协议的运行模式进行分类.进一步分析入侵者的出现对协议中各合法主体造成的影响,并用 Promela 高级过程描述语言对每个主体行为过程进行描述,就可以得到面向安全分析的协议形式化规范.

2.2 模型规范的 model checking 分析

有了形式化规范就可以利用模型检测技术对密码协议的安全属性进行分析.本文采用 SPIN 作为模型检测器.

(1)根据入侵分析对协议的运行模式进行分类,写出 Promela 模型规范;

(2)写出需要验证的系统属性要求,用 LTL(linear temporal logic)方程描述;

(3)利用 SPIN 对系统属性进行验证;

(4)若属性为假,SPIN 会生成一个 trail 文件,利用该文件进行引导仿真,跟踪协议运行过程,找出攻击序列;

(5)否则系统属性为真,验证结束.

3 BAN-Yahalom 协议分析

3.1 BAN-Yahalom 协议

BAN-Yahalom 协议[4]在第三方服务器 S 的帮助下,对发起者 A 和响应者 B 进行身份认证并为它们分配对话密钥.协议运行过程如下所示:

[1] $A \rightarrow B$: A, Na

[2] $B \rightarrow S$: B, Nb, {A, Na} Kbs

[3] $S \rightarrow A$: Nb, {B, Kab, Na} Kas, {A, Kab, Nb} Kbs

[4] $A \rightarrow B$: {A, Kab, Nb} Kbs, {Nb} Kab

其中 Ni 为由 I 生成的随机数 nonce;Kis 为由 I 与 S 共享的密钥;Kab 为 A 和 B 的对话密钥,由第三方服务器 S 生成.

3.2 协议模型

首先定义协议中使用的消息格式以及全局消息通道 network:

```
chan network = [N] of {
    mtype,   消息类型
    mtype,   消息接收者
    mtype,   主体身份符号
    mtype,   nonce
    code ,   加密数据组件 1
    code     加密数据组件 2
};
```

其中 mtype 为 Promela 的符号类型;N 为网络容量,$N = 0$ 时即为同步消息通道,$N > 0$ 则为缓冲消息通道,一般取 N 为 2 ~ 4.加密数据组件类型 code 定义如下:

```
typedef code {
    mtype id,     主体身份符号
    mtype nonce,  nonce
    mtype dt,     由服务器生成的对话密钥数据
    mtype key     数据使用的加密密钥
};
```

本文协议分析的目的在于发现可能的攻击,故下文协议规范仅考虑如下运行模式:

(1)Alice 为发起者,Bob 为响应者;

(2)Intruder 以自己的身份或假扮 Bob 为发起者,Alice 为响应者;

(3)Intruder 以自己的身份或假扮 Alice 为发起者,Bob 为响应者.

基于上述讨论,我们为参与协议运行的每个主体分别建立自己的 proctype,其中 statusA、statusB 分别表示 Alice 和 Bob 的运行状态,partnerA、partnerB 分别为 Alice 和 Bob 认为与其参与协议运行的另一方.下面是对各主体行为的描述.

Alice 的行为:

(1)给 Bob 发送 msg1,设置 partnerA 为 Bob,等待从 Server 发来的 msg3;接收从 Server 发来的 msg3,验证数据,给 Bob 发送 msg4,设置 statusA 为 ok,完成一次协议运行;

(2)以响应者的身份,接收 msg1,给 Server 发送 msg2,等待接收 msg4.

Bob 的行为:接收 msg1,根据其内容设置 partnerB,给 Server 发送 msg2,等待 msg4;接收从 partnerB 发送来的 msg4,验证数据,设置 statusB 为 ok,完成一次协议运行.

Server 的行为:接收从响应者发来的 msg2,为参与运行的双方生成对话密钥 Kab,向发起者发送 msg3,如此循环,持续运行.

Intruder 的行为:定义 knowNA 和 knowNB 分别表示入侵者是否知道 Na 和 Nb;消息 2、3、4 的缓冲区存储相应消息的加密数据组件.以下 Intruder 行为描述忽略它以自己的合法身份参与协议运行的行为:

(1)以自己的身份向 Alice 或 Bob、假扮 Alice 向 Bob 或假扮 Bob 向 Alice 发送 msg1,若 knowNA 或 knowNB 为 true 则使用获取到的 nonce,否则注入自己的 nonce;若获取由 Alice 向 Bob 发送的 msg1 则设置 knowNA 为 true;

(2)若存有 msg2 加密数据组件 1,则假扮 Alice 或 Bob 向 Server 发送 msg2,若 knowNA 或 knowNB 为 true 则使用已知的 nonce,否则注入自己的 nonce;若获取由 Alice 或 Bob 向 Server 发送的 msg2,则相应地设置 knowNA 或 knowNB 为 true 并把加密数据组件 1 保存;

(3)假扮 Server 向 Alice 或 Bob 发送 msg3,若存有 msg3 的加密数据组件则使用该组件否则注入任意 bit-string,若 knowNA 或 knowNB 为 true 则使用已知 nonce 否则注入任意 nonce;若获取由 Server 发送的 msg3 则保存其加密数据组件;

(4)假扮 Alice 向 Bob 发送 msg4,若存有 msg4 的加密数据组件则使用该组件否则注入任意的 bit-string;若获取由 Alice 或 Bob 发送的 msg4 则保存其加密数据组件.

最后给出系统属性的 LTL 方程,这里只考虑 Alice 和 Bob 的行为属性:

[](((statusA = = ok)&&(partnerA = = Bob))

〈-〉((statusB = = ok)&&(partnerB = = Alice)))

其中算符 && 和〈-〉分别表示逻辑与和逻辑等价,时序算符[]表示 always.

4 分析结果

对 Promela 规范进行验证,发现它并不满足所给的系统属性.对 trail 文件进行引导仿真就可以发现针对 BAN-Yahalom 协议的三个著名攻击[5,6],攻击序列如下所示,其中 M 为入侵者,M(B)表示入侵者假扮 *Bob*:

攻击 1:

[1] $A \rightarrow M(B)$: A, Na

[1′] $M(B) \rightarrow A$: B, Na

[2′] $A \rightarrow M(S)$: A, Na, {B, Na}Kas

[2″] $M(A) \rightarrow S$: A, Na, {B, Na}Kas

[3″] $S \rightarrow M(B)$: Na, {A, Kab, Na}Kbs, {B, Kab, Na}Kas

[3] $M(S) \rightarrow A$: Ne, {B, Kab, Na}Kas, {A, Kab, Na}Kbs

[4] $A \rightarrow M(B)$: {A, Kab, Na}Kbs, {Ne}Kab

攻击 2:

[1] $A \rightarrow M(B)$: A, Na

[1′] $M(B) \rightarrow A$: B, Nb

[2′] $A \rightarrow M(S)$: A, Na′, {B, Nb}Kas

[2″] $M(A) \rightarrow S$: A, Na, {B, Nb}Kas

[3″] $S \rightarrow M(B)$: Na, {A, Kab, Nb}Kbs, {B, Kab, Na}Kas

[3] $M(S) \rightarrow A$: Nany, {B, Kab, Na}Kas, bit-string

[4] $A \rightarrow M(B)$: bit-string, {Nany}Kab

攻击 3:

[1] $A \rightarrow M(B)$: A, Na

[1′] $M(A) \rightarrow B$: A, Na

[2′] $B \rightarrow S$: B, Nb, {A, Na}Kbs

[3′] $S \rightarrow M(A)$: Nb, {B, Kab, Na}Kas, {A, Kab, Nb}Kbs

[3] $M(S) \rightarrow A$: Nany, {B, Kab, Na}Kas, bit-string

[4] $A \rightarrow M(B)$: bit-string, {Nany}Kab

在上述攻击中,入侵者 M 成功地破坏了协议的身份认证过程,使得 *Alice* 将其当作 *Bob*.然而由于入侵者不能获取 *Kab*,它不能对由 *Alice* 发送给 *Bob* 的由 *Kab* 加密的消息进行解密.

5 结论

上述分析,成功地验证了利用 SPIN 进行密码协议安全分析的可行性.基于入侵者角色分类的协议运行模式,分析不仅有助于建立准确的形式化模型,还有助于加深对协议本身以及对密码协议攻击手段的理解.相对于硬件系统描述语言来说,此方法易于对数据通信协议形式化建模,能更准确地反映协议运行的动态性质且具有一定的通用性,对其它网络协议的分析具有很好的参考价值.

参考文献:

[1] A W Roscoe. Modeling and verifying key-exchange protocols using CSP and FDR[A]. In CSFW Ⅷ[C]. Kenmare, county Kerry Ireland: IEEE Computer Soc Press, 1995. 98 - 107.

[2] Lowe G. Reaking and fixing the needham-schroeder public-key protocol ssing FDR[A]. Proceedings of TACAS[C]. Passau, Germany, Springer Verlag, 1996. LNCS-1055. 146 - 166.

[3] 张玉清,胡玉濮,肖国镇. TMN 密码协议的形式分析[A]. 卿斯汉,冯登国,信息和通信安全—CCICS' 99[C]. 北京:科学出版社,2000. 147 - 152.

[4] Michael Burrows, Martin Abadi, Rodger Needham. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18 - 36.

[5] Paul Syverson. A taxonomy of replay attacks[A]. In Proceedings of the Computer Security Foundations Workshop Ⅶ[C]. Franconia NH, USA, June 1994. 187 - 191.

[6] Chong Xu, Gershon Kedem. Categorizing attacks on cryptographic protocols based on intruders' objectives and roles[A]. 2000 Workshop on Formal Methods and Computer Security[C]. Chicago, USA, July 2000.

作者简介:

邵晨曦　男,1954 年 7 月生于浙江杭州,副教授,研究方向:定性仿真,智能计算,CIMS,网络安全.(Email: cxshao@ustc.edu.cn).

胡香冬　女,1977 年 5 月生于浙江永康,硕士研究生,研究方向:人工智能,网络安全,软件工程.

熊　焰　男,1960 年生于安徽合肥,博士,副教授,研究方向为分布式处理、移动计算、移动通信,计算机网络及信息安全.

蒋　凡　男,1956 年 2 月生于江苏涟水,教授,研究方向:协议工程,信息安全.