doi:10.3969/j.issn.1672 - 4348.2015.03.007

安全协议验证中 DY 模型的构建框架

唐郑熠[1], 杨芳[2,3], 薛醒思[1]

(1. 福建工程学院 信息科学与工程学院, 福建 福州 350118;
2. 湖南大学 信息科学与工程学院, 湖南 长沙 410082; 3. 湖南医药学院 图书馆, 湖南 怀化 418000)

摘要: 攻击者建模是安全协议验证工作的一个重要部分,直接影响到验证的效率与质量,但目前却还没有一个可遵循的形式化框架,影响了建模工作的准确性与客观性。针对这一问题,通过对在安全协议验证中具有广泛影响的 DY 模型进行形式化,建立了一个 DY 模型的构建框架,刻画了攻击者的构成要素、行为规则以及行为模式,从而保证了攻击者具有合理的行为与能力,并能在攻击过程中获取新的知识,不断增强攻击能力。最后,将该工作运用到 Otway-Rees 协议的验证中,找出了该协议中所存在的漏洞,从而证明了该构建框架的有效性。

关键词: 安全协议; 形式化; DY 模型; 攻击者; Otway-Rees 协议
中图分类号: TP393.08　　**文献标志码**: A　　**文章编号**: 1672 - 4348(2015)03 - 0239 - 05

A framework for constructing DY model in security protocol verification

Tang Zhengyi[1], Yang Fang[2,3], Xue Xingsi[1]

(1. College of Information Science and Engineering, Fujian University of Technology, Fuzhou 350118, China;
2. College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China;
3. Library of Hunan University of Medicine, Huaihua 418000, China)

Abstract: The modelling of intruders is an important part of security protocol verification, which directly affects the efficiency and correctness of verification. There is no available formal framework of introders modelling, which is a disadvantage for modelling work. A framework for formalizing/constructing DY model that has extensive influence on security protocol verification was proposed. The framework can depict the components, behaviours and behaviour model of the intruders, which ensures that the intruder has reasonable behaviours and ability and can acquire new knowledges in the attacking process to enhance contantly the attacking ability. The effectiveness of the framework was confirmed in the verification of Otway-Rees protocol in which a fault in the protocol was found.

Keywords: security protocol; formalization; Dolev and Yao (DY) model; intruder; Otway-Rees protocol

安全协议又称为密码协议,是以密码学为基础的信息交换协议,其目的是在一个开放的网络环境中,提供保密的信息交换和传递服务。它解决了包括主体认证、保障消息完整、防止消息伪造、防止消息抵赖等一系列关键的安全问题,并成为目前最重要的通信安全保障手段。然而设计高质量的安全协议是十分困难且容易出错的,即使是最简单的、只包括若干有限主体和消息的认证协议,迄今也没有一种技术能够保障所设计的协议能够绝对正确、符合需求。

收稿日期: 2015 - 04 - 20
基金项目: 福建省中青年教师教育科研项目(JB14069); 福建工程学院科研启动基金项目(GY - Z13112)
第一作者简介:唐郑熠(1984 -),男,福建福州人,博士,讲师,研究方向:形式化方法。

形式化方法是目前最有效的安全协议分析技术,它将协议主体、攻击者与协议环境进行抽象,建立数学模型,通过模型所支持的计算技术验证模型所具有的性质,从而发现协议中所存在的缺陷。这种分析技术的一个关键问题在于攻击者的建模,不恰当的攻击者模型无法有效找出协议的漏洞。迄今为止的大部分相关工作,都是以 Dolev 与 Yao 所提出的 DY 模型[1]作为攻击者建模的依据。

尽管 DY 模型在实际的安全协议验证中具有重要的作用与意义,并被许多研究工作所引用,但基本都集中于用不同的语言或工具对其进行实现[2-6],而鲜有对其进行形式刻画、为具体实现提供框架。这导致当研究人员在用不同的方法实现 DY 攻击者模型时,缺乏一个可遵循的统一而精确的框架,从而造成不同的实现之间可能存在差异,并可能偏离 DY 模型的真实行为与能力。针对这一问题,本文构建了一个 DY 模型的形式化框架,定义了 DY 模型的构成要素、行为规则以及行为模式,为攻击者的建立提供了可遵循的统一标准,可作为安全协议自动验证技术的基础。

1 DY 模型概述

DY 模型是 Dolev 与 Yao 在 1983 年提出的,它基于安全协议的分层次分析的思想,即先研究安全协议本身的行为逻辑是否存在缺陷,然后再考虑实现方法是否存在问题(如所采用的密码算法)。

因此,对安全协议的验证,都建立在假定完善的底层密码体制及算法的基础之上,攻击者被认为不具有攻破密码算法的能力。具体来说,就是在未掌握对应密钥的情况下,攻击者无法获知加密消息中的信息。在这个前提下,DY 模型规定了攻击者可以具有以下行为与能力:

· 攻击者可以在不被协议主体察觉的情况下,窃听到通讯网络中的所有消息。

· 攻击者可以在不被协议主体察觉的情况下,拦截并存储通讯网络中的所有消息。

· 攻击者可以伪造消息。

· 攻击者可以发送消息。

· 攻击者也可以作为合法的协议主体,参与协议的运行。

DY 模型下的攻击者具有控制整个网络的能力,协议的整个执行过程都可能暴露在攻击者的监视之下,并且攻击者还能够随时干扰或参与协议的执行过程。

尽管 DY 模型对攻击者的行为进行了限定,但却并没有给出必要的规则,例如行为执行的顺序、伪造消息的方法、如何成为合法主体等,这导致在建模过程中 DY 模型难以被精确实现,并且在不同的验证工作中存在差异性。

2 DY 模型的构建框架

依据有关 DY 模型研究的相关文献[7-8],本节将首先给出 DY 模型的形式化定义,即总体的构建框架。

在安全协议中,主体之间是通过网络交换消息来进行交互,因此首先给出消息的形式化定义。本文的工作基于非对称密钥体制,但也可以运用在对称密钥体制上。

定义 1(消息) 安全协议的主体之间交换的消息 M 符合以下形式之一:

· $M = m$:m 是不可再分的原子消息,如主体标识、临时值等.

· $M = \{M_1, M_2 \cdots M_n\}$:由多个消息构成的普通消息.

· $M = K_X\{M_1, M_2 \cdots M_n\}$:使用主体 X 的公钥加密的消息.

· $M = K_X^{-1}\{M_1, M_2 \cdots M_n\}$:使用主体 X 的私钥签名的消息

遵循 DY 模型的攻击者在运行时,需要使用到一些自身掌握或在运行过程中获取的信息,称为知识。

定义 2(知识) DY 模型中的知识指的是伪造消息时所用到信息,包括各种类型的原子消息、密钥以及签名消息等。

攻击者所采取的行为需遵循一定的顺序,称为行为模式。为了描述行为模式,需要用到以下行为模式运算符:

定义 3(行为模式运算符) 在 DY 模型的行为模式中,包含以下行为模式运算符:

·→:顺序运算符,描述两个行为的执行具有先后顺序,形如 $act_1 \rightarrow act_2$.

· $\vee$:随机运算符,描述随机选取两个行为中的一个执行,形如 $act_1 \vee act_2$.

· $R(\varphi)$:重复运算符,描述一个行为重复执

行，形如 $R(\varphi)[\mathrm{act}]$；φ 是重复条件，可用逻辑公式表示，当它的取值为假时，行为 act 中止.

下面给出 DY 模型的形式化构建框架：

定义 4（DY 模型的构建框架）　DY = (KN, ACT, BS, MD, NET)，其中：

· $\mathrm{KN} = \mathrm{kn}_1 \cup \mathrm{kn}_2 \cup \cdots \mathrm{kn}_n$：是攻击者的知识库，$\mathrm{kn}_i$ 表示不同类型的知识库。

· ACT = {Intercept, Resolve, Forge, Choose, Send}：是攻击者的行为集合。

· BS = R(true)[(Intercept → Resolve) ∨ ((Forge ∨ Choose) → Send)]：是攻击者的行为模式，刻画了攻击者的行为执行顺序。

· $\mathrm{MD} = <\mathrm{M}_1, \mathrm{M}_2, \cdots \mathrm{M}_n>$：是攻击者的消息库，用于存放攻击者所需保存的消息。

· $\mathrm{NET} = <\mathrm{M}_1, \mathrm{M}_2, \cdots \mathrm{M}_n>$：是攻击者所监听的网络，同时也是协议的其他主体所使用的网络；攻击者能够从中拦截一条消息，也能够向其中添加一条消息。

DY 模型的构建框架限定了攻击者可以具有的 5 种行为，同时通过行为模式限定了这 5 种行为的执行顺序：

· Intercept：攻击者执行 Intercept 行为时，会从其所监听的网络中拦截并存储一条消息。

· Resolve：攻击者执行 Resolve 行为时，会运用知识库中的知识，将一条消息进行分解，并扩充自己的知识库。

· Forge：攻击者执行 Forge 行为时，会运用知识库中的知识，构造一条消息。

· Choose：攻击者执行 Choose 行为时，会从消息库中随机选取一条以前拦截过的消息。

· Send：攻击者执行 Send 行为时，会将一条消息发送到其所监听的网络中。

攻击者通过 Intercept 行为获取通讯网络中所传输的消息，将其存储并分解，从而扩充消息库与知识库。而随着消息库与知识库的扩充，攻击者的能力将会不断增强，并能够通过发送不同来源的消息干扰或参与协议的运行，并可能最终攻破协议。各行为之间的关系如图 1 所示。

DY 模型的构建框架明确了在实现 DY 模型时所需要描述的攻击者要素，并限定了攻击者所能够采取的行为以及行为的顺序，这为 DY 模型的实现提供了依据与准则。

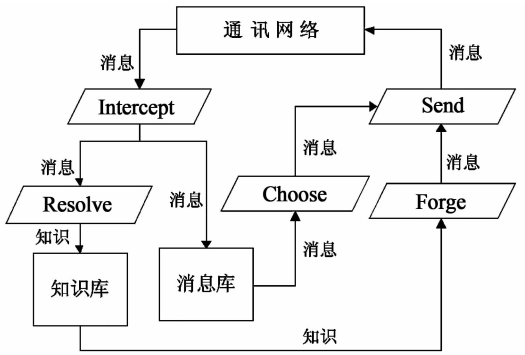

图 1　DY 模型行为之间的关系

Fig. 1　The relationship among the behaviours in DY model

3　消息分解与构造

在 DY 模型的 5 种行为中，Resolve（分解消息）行为与 Forge（构造消息）行为是最为重要的，前者是攻击者的攻击能力不断增强的关键，后者则是攻击者的重要攻击手段。基于“安全协议底层的密码体制与算法假定完善”的基本假设，给出消息分解与构造的算法。

对于一条非加密的消息，攻击者可以直接进行分解；而对于加密消息，则要根据知识库中的知识判定是否能够分解。消息分解的过程如算法 1 所述。

算法 1　RMA（Resolve Message Action）

Input：A Message M.

Output：None.

if $M = m$ then {

　KN：= KN ∪ {M};

}

if $M = \{M_1, M_2, \cdots M_n\}$ then {

　for each $M_i \in M$ {

　　RMA (M_i);

　}

}

if $M = K_X\{M_1, M_2, \cdots M_n\} \wedge K_X^{-1} \in \mathrm{KN}$ then {

　for each $M_i \in M$ {

　　RMA (M_i);

　}

}

if M = KX − 1{ M_1, M_2, … M_n} ∧ K_X ∈ KN then {
  for each $M_i \in M$ {
    RMA(M_i);
  }
}

攻击者可以运用知识库中的知识,构造一条新的消息。但对于具体的安全协议,构造该协议中不存在的消息类型是没有意义的。为了避免这个问题,通过参数来指定构造消息的类型。消息构造的过程如算法 2 所述。

算法 2 FMA(Forge Message Action)

Input: A Message M.

Output: A New Message M.

if $M = m$ then {
  Get a m from KN;
  $M := m$;
}
if $M = \{M_1, M_2, \cdots M_n\}$ then {
  for each $M_i \in M$ {
    $M_i := \mathrm{FMA}(M_i)$;
  }
}
if $M = K_X\{M_1, M_2, \cdots M_n\}$ then {
  for each $M_i \in M$ {
    $M_i := \mathrm{RMA}(M_i)$;
  }
  Get a K_Y from KN;
  KX: $= K_Y$;
}
if $M = K_X^{-1}\{M_1, M_2, \cdots M_n\}$ then {
  for each $M_i \in M$ {
    $M_i := \mathrm{RMA}(M_i)$;
  }
  Get a K_X^{-1} from KN;
  $K_X^{-1} = K_Y^{-1}$;
}
return M;

4 实例验证

SPIN 模型检测是一种实现安全协议自动验证的有效技术,属于形式化方法的一类。使用 SPIN 技术验证安全协议的过程如图 2 所示。

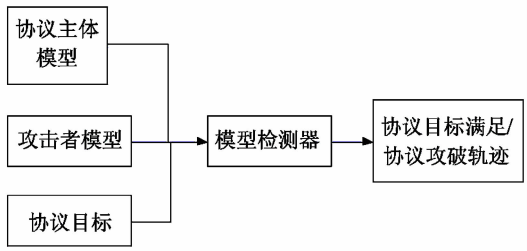

图 2 基于 SPIN 的安全协议自动验证过程

Fig. 2 The automatic verification process based on SPIN safety protocol

建模工作包括三个部分:协议主体的建模、攻击者的建模以及协议目标的形式化。然后,将模型直接输入模型检查器,由其进行自动验证。最终,模型检测器将给出验证结果:协议目标满足,或者攻击者攻破协议的轨迹。

为了验证前文所构建的攻击者建模框架的有效性,本节对一个密钥协商协议——Otway-Rees 协议[9]进行验证。OR 协议的目的,是为会话双方,建立一个相同的会话密钥。OR 协议本身存在缺陷,因此之后又出现了它的改进版本[10],本文以这个改进版本作为验证的实例:

(1) $A \rightarrow B$:A, B, n_a

(2) $B \rightarrow S$:A, B, n_a, n_b

(3) $S \rightarrow B$:$K_{AS}\{n_a, A, B, K\}$, $K_{BS}\{n_b, A, B, K\}$

(4) $B \rightarrow A$:$K_{AS}\{n_a, A, B, K\}$

协议主体使用主体标识(A 与 B)和临时值(n_a 与 n_b)向服务器中心申请会话密钥,服务中心(S)为会话双方各生成一个会话密钥包,其中包含:会话方的临时值(用于确认证书的有效性)、主体标识(用于标识会话密钥的适用对象)、共享会话密钥(K)。会话密钥证书适用会话方与服务中心的共享密钥加密(K_{AS} 与 K_{BS})。

协议主体的建模遵循上述的描述,而攻击者的建模则遵循前文所构建的形式化框架。OR 协议的目标有两个:

(1)保证服务中心 S 分发的会话密钥 K,不会被除 A 和 B 外的第三方获知。

(2) 保证 A 和 B 所获得的会话密钥是一致的。

验证结果表明,本文所构建的攻击者无法破

坏 OR 协议的第一个目标，即无法获得会话密钥 K。但对于第二个目标，在攻击者(P) 的干扰下，则无法达成。攻击者攻破协议的轨迹如图 3 所示。

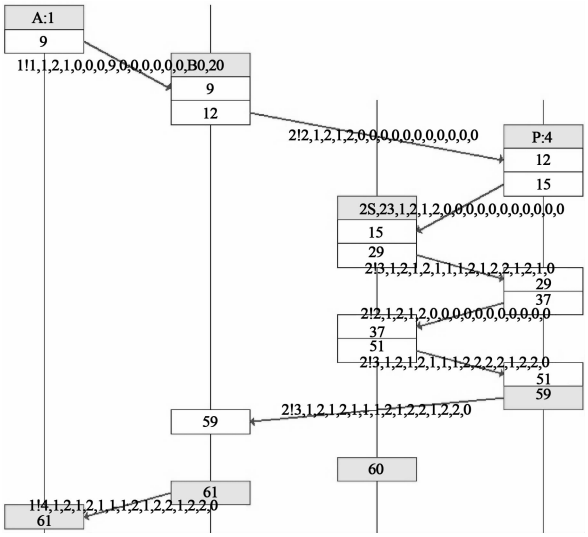

图 3　攻破协议的轨迹

Fig. 3　The trail of breaking through the protocol

通过对攻击轨迹的分析，得出以下攻击过程：

(1) $A \rightarrow B$: A, B, n_a

(2) $B \rightarrow P$: A, B, n_a, n_b

(3) $P \rightarrow S$: A, B, n_a, n_b

(4) $S \rightarrow P$: $K_{AS}\{n_a, A, B, K_1\}$, $K_{BS}\{n_b, A, B, K_1\}$

(5) $P \rightarrow S$: A, B, n_a, n_b

(6) $S \rightarrow P$: $K_{AS}\{n_a, A, B, K_2\}$, $K_{BS}\{n_b, A, B, K_2\}$

(7) $P \rightarrow B$: $K_{AS}\{n_a, A, B, K_1\}$, $K_{BS}\{n_b, A, B, K_2\}$

(8) $B \rightarrow A$: $K_{AS}\{n_a, A, B, K_1\}$

由于会话双方的临时值是不加密的，因此攻击者可以使用临时值申请到多个不同的会话密钥包，并进行组合，从而让会话双方得到不一致的会话密钥。在这个攻击过程中，攻击者所用到的操作包括：拦截消息、发送消息、分解消息、构造消息。这些都是本文所构建的攻击者所具备的能力。

5　结论

本文分析了安全协议验证工作具有重大影响的 DY 模型，给出了构建该模型的形式化框架，定义了遵循 DY 模型的攻击者所应具有的要素、行为以及行为模式，并给出了消息分解与构造的算法。同时，通过对 Otway－Rees 协议的实例验证，证明了该构建框架的有效性。这一工作可以运用在安全协议验证工作中的攻击者建模的部分，使得攻击者的建模工作更为客观，并保证在不同的验证工作中，攻击者能够具有一致的行为与能力。

参考文献：

[1] Dolev D, Yao A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198－208.

[2] 钟军，吴雪阳，江一民，等. 一种安全协议的安全性分析及攻击研究[J]. 计算机工程与科学，2014，36(6)：1077－1082.

[3] 冉俊铁，吴尽昭. 基于 SPIN 的安全协议形式化验证技术[J]. 计算机应用，2014：34(S2)：85－90.

[4] 陈春玲，田国良. 安全协议的 SPIN 建模与分析[J]. 南京航空航天大学学报，2009，41(5)：672－676.

[5] Fu Yulong, Ousmane K. A finite transition model for security protocol verification[C]//Proc of 6th International Conference on Security of Information and Networks. Aksaray, Turkey, 2013.

[6] 龙士工，王巧丽，李祥. 密码协议的 Promela 语言建模及检测[J]. 计算机应用，2005，25(7)：1548－1550.

[7] Kanovich M, Kiriginc T B, Nigamd Vi, et al. Bounded memory Dolev-Yao adversaries in collaborative systems[J]. Information and Computation, 2014, 238: 233－261.

[8] Mazare L. Satisfiability of Dolev-Yao constraints[J]. Electronic Notes in Theoretical Computer Science, 2005, 125(1): 109－124.

[9] Otway D, Rees O. Efficient and timely mutual authentication[J]. ACM Operating Systems Review, 1987, 21(1): 8－10.

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

(责任编辑：肖锡湘)