数字证书语义的形式化描述

Formal Description of Digital Certificate Semantics

王礼强[1] 龚俭 {lqwang,jgong@njnet.edu.cn}
Wang LiQiang Gong Jian
东南大学计算机系
Southeast University Computer Science Dept

摘要：为了对证书的语义有一个准确的理解，本文定义了一个形式化系统。利用形式化的表述方法对证书作了分析。文章还举了两个利用该系统进行推理的例子。

Abstract: In order to understand the precise semantics of digital certificate, this article defines a formal system which is used to analyze the meaning of certificate. Besides, two examples which utilize that tool to deduce results are explained.

关键词：形式化描述，证书，实体

Key words: Formal description, Certificate, End-entity

1 引言

由于电子安全通信，安全交易的需求不断增加，密码学的重要性得到提高。而且，这一趋势将随着信息产业的发展得到加强。从密码学的技术角度而言，它受到了充分的重视。然而，对它的意义和作用还没能准确理解。其中的一个重要的概念是公钥和实体的绑定关系。它是获得认证和无否认的基础。下面主要是对这种绑定关系和数字签名的正规分析。

2 实体和公钥绑定关系的概念

从字面上说，所谓绑定是一句表示公钥代表实体的话。一个经过数字签名的声明声称一个实体与一个公钥具有绑定关系通常被称作“基于实体的证书”。但是绑定的准确意义却不是很明确。我们知道，一个密钥对有两部分，公钥部分是用来验证签名或加密数据。私钥部分用来产生数字签名或解密数据；实体一般是人或合法组织。一个实体如果可以用私钥进行解密或签名，那么他就拥有公钥。

在 X509 中，如果实体拥有公钥的话，那么那个公钥就与该实体有绑定关系。该实体有责任保护私钥的安全。但不明确的是，一个 X509 证书应该被如何解释。它是表示证书发布者声明实体拥有证书中的公钥还是仅仅表示它拥有密钥？而且，密钥持有者对私钥的保密程度是多少？他对用私钥签名的通信内容承担多大的责任？

3 形式化系统的定义

为了能够对以上问题有一个准确理解，这里引进一个形式化系统。利用该系统，我们能够进一步探讨数字证书。下面首先定义一些重要的术语：

3.1 声明（Statement）

对于任何一个正规系统而言，它都需要定义一些基本的单元。在数理逻辑中这些基本单位称为公式，它们根据真值表可以得到真或假的值。这里定义的基本单元称为声明。该声明的值可以是有效的或无效的。这里假设甲作了一个声明 S（甲说了 S），同时声明 S 被一个签名私钥签了名。这种一个实体根据自己的观点判断甲说了 S 的过程是一个认证过程。如果实体根据法律的观点并且由给定证据得出该结论，那么这是一个无

[1] 作者 王礼强 东南大学计算机系硕士 研究方向 网络安全

否认过程。对于无否认，它的最终目标不是得出实体说了什么的结论，而是某些特权、价值等被转移到另一个实体。

3.2 观点（Views）

一个人的结论一般是根据他拥有的证据和声明，应用推导规则得出的。这些推导规则和证据可以认为是一个人的观点（View）。这个观点反映了他的最初信念。根据这个信念可以推导出一些声明。根据某个人的观点，一个声明 S 是有效的并不是意味着该声明是绝对准确，只是根据他的观点是合理的。相反，根据某个人的观点，一个声明 S 是无有效的并不是意味着该声明是绝对错误，只是根据他的观点是不合理的。对于一个声明只有有效或无效而没有正确与否的概念。

3.3 语法定义

让 SSK 和 SPK 分别表示主体公钥和主体私钥集合。K 表示所有密钥集合（K＝SSP∪SPK）。E 表示实体的集合。R 为权力的集合。所有单个变量和实体名都用小写字母表示。为了形式化描述方便，这里采用扩展的 Backus-Naur 范式（EBNF）。

定义 1

短语：term(T)　　=element(T)|variable(T)

声明：statement　=own(term(E),term(K))|
term(E ∪ SSK) says statement |

commit(term(E),term(SSK),statement) |
trust(term(E),statement)

推导规则：　＝statement {“,”statement} “⊢” statement

定义 2

一个实体 a 的观点表示为$View_a$。它表示一系列声明和规则的集合。

定义 3（替代规则）

让 V，W 表示类型为 T 的变量，v 为类型为 T 的一个元素。S[V=v]表示在声明 S 中把所有变量为 V 的替换为 v。S[V=W]表示在声明 S 中变量 V 替换成变量 W（相当于重新命名）。

定义 4

一个声明以观点$View_a$而言是有效的，当且仅当至少存在下列之一情况：

（1）该声明存在于$View_a$中。

（2）可以通过推导规则从$View_a$中得到该声明。

声明的意义

现在可以讨论一下声明的含义。现在小写字母表示元素而不是变量（x∈E, k∈K,ssk∈SSK,e∈E∪SSK,r∈R）。s 表示一个具体的声明。

Trust(x,s)：就声明 s 而言，实体 x 是可以信任的。声明 trust(x)表示对所有的声明，实体 x 都是可以信任的。

ssk says s ：声明 s 用主体私钥 ssk 进行了签名。这里假定所有的签名验证计算都是正确的。每个端实体都有能力进行该项验证。

x says s ：一个实体可以有多种途径发表声明。它可以是读出来的，可以是写在纸上的，可以是输入计算机的语句等等。对声明进行的签名本身并不是声明的一部分，它是作为证明实体 x 说了 s 的一个证据。

own(x,k) ：实体 x 对密钥 k 有绝对的拥有权。也就是说它可以无条件的使用它的私钥。

commit(x,ssk,s) ： 实体 x 对用私钥 ssk 签名的声明 s 承担责任。换句话说，实体 x 通过其数字签名在法律意义上同意其说过声明 s。Commit(x,ssk)表示实体 x 愿意对所有使用私钥 ssk 进行签名的声明承担责任。

推导规则

规则 1（信任关系）

$$\frac{trust(x,s),\ x\ says\ s}{s}$$

信任可以被认为是让一个实体相信一个声明是另一个实体作出的一个基本机制。如果对声明 s 而言相信实体 x,而且实体又表示作

了该声明，那么我们有理由相信声明 s。

规则 2a

$$\frac{x\ says\ own(x,k)}{own(x,k)}$$

无论是解密还是验证数字签名，我们都需要确信发送者拥有签名密钥。虽然拥有权不需要证明，但发送者应该声明一下他拥有该密钥。由于冒充拥有别人的公钥或私钥没有什么实质性的好处，而且通过其它途径也可以得到同样的结果。因此，对于实体的该项声明我们可以信任。

规则 2b

$$\frac{own(x,ssk),ssk\ says\ s}{x\ says\ s}$$

如果只有一个实体拥有签名密钥 ssk，而且声明 s 是经该密钥签名的，那么可以认为实体发表了该声明。

规则 3a

$$\frac{x\ says\ commit(x,ssk,s)}{commit(x,ssk,s)}$$

规则 3b

$$\frac{commit(x,ssk,s),ssk\ says\ s}{x\ says\ s}$$

在法律上以数字签名作为证据需要非常小心。这不仅是因为存在很多技术性问题（例如：密钥泄露，系统缺陷）、加密算法问题和用户使用疏忽等问题，而且是因为所有权声明与上下文环境有着密切的关系。实体拥有密钥 ssk，但这并不意味着实体愿意承担用该密钥进行操作产生的责任。因此，实体应首先声明他愿意承担责任。

4 实例分析

为了验证该系统的有效性，下面通过两个典型的实例来证明。设 IR 表示以上推导规则的集合（IR＝{1,2a,2b,3a,3b}）。

4.1 通过非数字途径验证签名

a 和 b 是通信的双方， a 可以直接（通过见面或打电话）从 b 那里取得密钥。在这种情况下，a 可以验证 b 的声明 $own(b,ssk_b)$ 是有效的。假设 a 后来得到一个经数字签名的消息 s。这时他的观点包含以下两个声明：

$$View_a=\{ssk_b\ sayss,b\ saysown(b,ssk_b)\}\cup \mathrm{IR}$$

a 可以利用规则 2a 和规则 2b 来得到 b 声明了 s。

$$b\ says\ own(b,ssk_b)\Rightarrow own(b,ssk_b) \quad (2a)$$

$$own(b,ssk_b),ssk_b\ says\ s\Rightarrow b\ says\ s \quad (2b)$$

a 还可以通过可信任实体的声明来得到 $b\ says\ own(b,ssk_b)$ 假设 a 的朋友 c 说 $b\ says\ own(b,ssk_b)$，并且 a 信任 c 提供的其它实体与密钥之间的关系。设 x' 和 ssk' 都是变量。

$$View_a=\{ssk_b\ says\ s,c\ says\ b\ says\ own(b,ssk_b),\ trust(c,x'\ says\ own(x',ssk'))\}\cup IR$$

由于 a 信任 c 提供的其它实体与密钥之间的关系，因此在 a 看来 c 所说的 $b\ says\ own(b,ssk_b)$ 是有效的。A 可以利用规则 1 得到 $b\ says\ own(b,ssk_b)$。现在不难看出，a 可以利用至少两种方法得出 $b\ says\ s$。

4.2 通过证书和证书链验证签名

在上一个例子中，a 可以直接获得声明 $c\ says\ b\ says\ own(b,ssk_b)$。但是更为常见的是，他是从证书中得到该声明的。当然还需要声明 $c\ says\ own(c,ssk_c)$。现在可以得到 a 的观点 $View_a$：

$View_a = \{ssk_b\ says\ s,$
$ssk_c\ says\ b\ says\ own(b, ssk_b),$
$c\ says\ own(c, ssk_c),$
$trust(c, x'\ says\ own(x', ssk'))\} \cup IR$

由于 c 是可以信任的，a 通过规则 2a 得出 $own(c, ssk_c)$。因此再根据规则 2b，a 可以推导出 $c\ says\ b\ says\ own(b, ssk_b)$。最后，a 再利用相同的规则得出 $b\ says\ s$。

现设 a 的另一个朋友 d，他知道 $c\ says\ own(c, ssk_c)$。如果 a 相信他并且知道 $d\ says\ own(d, ssk_d)$。那么 a 的观点如下：

$View_a = \{ssk_b\ says\ s,$
$ssk_c\ says\ b\ says\ own(b, ssk_b),$
$d\ says\ own(d, ssk_d),$
$ssk_d\ says\ c\ says\ own(c, ssk_c),$
$trust(c, x'\ says\ own(x', ssk')),$
$trust(d, x'\ says\ own(x', ssk'))\} \cup IR$

在这里 d 向 c 颁发一个证书，c 向 b 颁发一个证书，从而形成一个证书链。以下是推导过程：

$d\ says\ own(d, ssk_d) \Rightarrow own(d, ssk_d)$ (2a)

$own(d, ssk_d),$
$ssk_d\ says\ c\ says\ own(c, ssk_c)$ (2b)
$\Rightarrow d\ says\ c\ says\ own(c, ssk_c)$

$d\ says\ c\ says\ own(c, ssk_c),$
$trust(d, x'\ says\ own(x', ssk'))$ (1)
$\Rightarrow c\ says\ own(c, ssk_c)$

$c\ says\ own(c, ssk_c) \Rightarrow own(c, ssk_c)$ (2a)

$own(c, ssk_c),$
$ssk_c\ says\ b\ says\ own(b, ssk_b)$ （2b)
$\Rightarrow c\ says\ b\ says\ own(b, ssk_b)$

$c\ says\ b\ says\ own(b, ssk_b),$
$trust(c, x'\ says\ own(x', ssk'))$ (1)
$\Rightarrow b\ says\ own(b, ssk_b)$

$b\ says\ own(b, ssk_b) \Rightarrow own(b, ssk_b)$ （2a）

$own(b, ssk_b), ssk_b\ says\ s \Rightarrow b\ says\ s$（2b)

由此可见，利用证书链同样可以验证 b 向 a 发送的数字签名。

5 结束语

通过这里定义的形式系统可以得到一个数字签名验证的形式化过程。虽然它还不能够直接作为正规化工具来分析由证书引起的各种问题，但是希望它能对数字证书的正规化表示和推导起到一个启示的作用。

参考文献：

〖1〗R.Housley, W.Ford, W.Polk 和 D.Solo. <<Internet X.509 Public Key Infrastructure Certificate and CRL Profile>> RFC 2459, 1998. 6

〖2〗IETF PKIX WG," Representation of Key Exchange Algorithm (KEA) Keys in Internet Public Key Infrastructure Certificates", draft-ietf-pkix-ipki-kea-01.txt, 1997.10

〖3〗IETF PKIX WG," Representation of Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and Signatures in Internet X.509 Public Key Infrastructure Certificates",draft-ietf-pkix-ipki-ecdsa-01.txt, 1997.11

〖4〗IETF PEM WG, " Part I: Message Encryption and Authentication Procedures ", RFC1421, 1993.2

〖5〗龚俭，"计算机网络安全概论"，东南大学教材, 1997.8