串空间理论扩展*

沈海峰[1+], 薛 锐[2], 黄河燕[1,3], 陈肇雄[1,3]

[1](中国科学技术大学 计算机科学技术系,安徽 合肥 230026)

[2](信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

[3](中国科学院 计算机语言信息工程研究中心,北京 100083)

Extending the Theory of Strand Spaces

SHEN Hai-Feng[1+], XUE Rui[2], HUANG He-Yan[1,3], CHEN Zhao-Xiong[1,3]

[1](Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China)

[2](State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)

[3](Engineering Research Center of Computer Language Information, The Chinese Academy of Sciences, Beijing 100083, China)

+ Corresponding author: Phn: +86-10-82382581, Fax: +86-10-62312262, E-mail: supershf@hotmail.com, http://www.ustc.edu.cn

Received 2004-03-04; Accepted 2004-11-15

Shen HF, Xue R, Huang HY, Chen ZX. Extending the theory of strand spaces. *Journal of Software*, 2005,16(10):1784−1789. DOI: 10.1360/jos161784

Abstract: Current strand spaces model can not analyze some complex security protocols on account of their poor cryptographic primitives' abstract. So it is very necessary to extend original theory of strand spaces so that it can be applied to analyze real world protocols. The penetrator's strands are extended through adding signature, signature verification and HMAC (keyed-hashing for message authentication code) traces to them. A new notion of ideal is defined and the relevant propositions or theorems are therefore modified and proved. The extended honest ideals model not only inherits its original characters, but also is adaptive to the analysis of protocols with more cryptographic primitives such as JFK or IKE2.

Key words: security protocol; strand spaces; ideal; honest ideal

摘 要: 现有的串空间模型由于没有抽象更多的密码学原语,因此不能分析较复杂的安全协议.希望通过对串空间理论的扩展使其充分地表达较多的密码学原语,以满足分析复杂安全协议的需要.对入侵串轨迹增加了签名、签名验证和 HMAC(keyed-hashing for message authentication code)函数模型,重新定义了理想概念并对衍生出的相关命题和定理进行了证明.扩展的诚实理想分析模型不仅继承了原理论的性质,而且适合分析含丰富密码原语的协议,如 JFK 和 IKE2.

* Supported by the National Natural Science Foundation of China under Grant No.60373048 (国家自然科学基金)

作者简介: 沈海峰(1975−),男,安徽合肥人,博士,主要研究领域为密码学,安全协议;薛锐(1963−),男,博士,研究员,CCF 高级会员,主要研究领域为理论密码学,密码协议分析,形式化方法在密码学中的应用;黄河燕(1963−),女,博士,教授,博士生导师,主要研究领域为自然语言处理,机器翻译,面向对象程序设计;陈肇雄(1961−),男,博士,教授,博士生导师,主要研究领域为智能应用系统,网络信息智能处理.

关键词: 安全协议;串空间;理想;诚实理想
中图法分类号: TP309 文献标识码: A

串空间理论[1−5]是建立在 Dolev-Yao 模型[6]基础上的安全协议分析模型.它的丛(bundle)概念、理想(ideal)概念(借鉴于代数学[7])和认证测试(authentication test)方法组成了它的 3 个核心理论,共同形成了一套验证协议安全性的方法族.在 Internet 环境下,IPsec 和 SSL 为通信双方提供安全的通信信道,由于这两个协议要求通信双方在共享简单的秘密,甚至没有共享秘密的基础上实现双向认证和密钥交换,因此它们的消息结构是非常复杂的.分析这些协议的形式化方法必须能足够地抽象协议中的密码原语.原始串空间理论[1,2,4],包括文献[8],在分析这些协议时都存在着不足,主要表现为不能表达丰富的密码原语,例如签名和散列函数.虽然我们可以用加密模型代替签名,但这样就不能提供丰富的语义信息.其次,在健壮的协议中,签名和加密通常使用不同的密钥对[9],如果我们把主体的加密和签名表示成同样的模型,那么某些协议中就会出现相同但密码原语性质不同的消息成分,这样使得协议的分析变得极其不方便,因为我们需要区分什么是加密,什么是签名.另外,对现在协议中广泛使用的钥控散列函数,我们在现有的串空间理论中还找不到可以代替的模型.我们希望通过对串空间理论的扩展使其充分地表达较多的密码学原语,以满足分析复杂安全协议的需要.

1 串空间简介

一个串(strand)是协议参与者的事件序列,既发送接受消息的序列.一个串空间(strand spaces)是串的集合,其中既包括合法参与者的串,又包括入侵者串.设 $\boldsymbol{A}$ 是协议执行中所有可能消息的集合,$\boldsymbol{A}$ 中元素称为项(term),$t_1 \sqsubset t$ 表示 t_1 是 t 的子项.

定义 **1.1**. $\langle \sigma, a \rangle$ 是有符号项,σ 是+或−号,$a \in \boldsymbol{A}$,一个有符号项记为 $+t$ 或 $-t$,$(\pm \boldsymbol{A})^*$ 是全体有符号项的有限序列集合.$(\pm \boldsymbol{A})^*$ 中一个典型元素是 $\langle\langle \sigma_1, a_1 \rangle, ..., \langle \sigma_n, a_n \rangle\rangle$.

定义 **1.2**. 一个串空间是集合 Σ,并具有一个轨迹(trace)映射 $tr: \Sigma \to (\pm \boldsymbol{A})^*$.

定义 **1.3**. 对一个固定的串空间 Σ,有:

1. 结点是 $\langle s, i \rangle$,$s \in \sum$,i 是整数,$1 \le i \le length(tr(s))$,结点集合为 N.$\langle s, i \rangle$ 属于 s,每一个结点都属于唯一的一个串.

2. 如果 $n = \langle s, i \rangle \in N$,那么 $index(n) = i$ 且 $strand(n) = s$,串 s 轨迹的第 i 个有符号项 $term(n)$ 是 $(tr(s))_i$;无符号项 $un\_term(n)$ 是 $((tr(s))_i)_2$.

3. 如果 $n_1, n_2 \in N$,那么 $n_1 \to n_2$ 意味着 $term(n_1) = +a,\ term(n_2) = -a$,即 n_1 发送消息,n_2 接受消息.

4. 如果 $n_1, n_2 \in N$,那么 $n_1 \Rightarrow n_2$ 意味着 n_1,n_2 发生在同一个串上,n_1 是 n_2 的直接前继,有 $index(n_1) = index(n_2) - 1$.

5. 一个无符号项 t 发生在 $n \in N$,当且仅当 $t \sqsubset term(n)$.

6. 一个无符号项 t 起源在 $n \in N$,当且仅当 $term(n)$ 是正号,$t \sqsubset term(n)$,而且对同一个串上 n 的任何前继 n' 没有 $t \sqsubset term(n')$.

7. 一个无符号项 t 唯一起源在 $n \in N$,当且仅当 t 起源在唯一的结点 $n \in N$.

8. N 加上两种边集合 $n_1 \to n_2$ 和 $n_1 \Rightarrow n_2$ 就组成一个有向图.

9. $n_1 \Rightarrow^+ n_2$ 表示在同一个串上 n_1 经过一个或多个 $\Rightarrow$ 边到达 n_2.

定义 **1.4**. 消息集合 $\boldsymbol{A}$ 中包含两个互斥子集:$\boldsymbol{K}$(密钥集合),$\boldsymbol{T}$(原子文本消息).$\boldsymbol{A}$ 上有 3 种运算:加密 $encr: \boldsymbol{K} \times \boldsymbol{A} \to \boldsymbol{A}$;逆密钥 $inv: \boldsymbol{K} \to \boldsymbol{K}$;合成 $join: \boldsymbol{A} \times \boldsymbol{A} \to \boldsymbol{A}$.$encr$ 的值域是 $\boldsymbol{E}$,$join$ 的值域是 $\boldsymbol{C}$.

设 $\boldsymbol{K}_P$ 是入侵者的密钥集合,其中包括:所有用户的公钥,入侵者与用户 X 共享的对称密钥 K_{PX},丢失或被破解的密钥等.设 $\boldsymbol{B}$ 是 $\boldsymbol{A}$ 的子集,函数 $f: \boldsymbol{B}^n \to \boldsymbol{K} \cup \boldsymbol{M} \cup \boldsymbol{B}$ 满足:每个 $y = f(x_1, ..., x_n)$ 有太多的原像以至于不可能辨别某个 y 的正确原像;或者 f 是一一映射的.但计算 $f^{-1}(y)$ 非常困难.文献[1]扩展了以下两个入侵者行为串:

$\boldsymbol{B}$ 域:$\langle \pm b \rangle$,$b \in \boldsymbol{B}_P \subseteq \boldsymbol{B}$,$\boldsymbol{B}_p$ 是入侵者知识集.

$\boldsymbol{B}_f$函数: $\langle -x_1,...,-x_n,+y=f(x_1,...,x_n)\rangle$.

公理 **1.5**. $\boldsymbol{K}\cap\boldsymbol{T}=\varnothing$, $\boldsymbol{B}\cap\boldsymbol{C}=\varnothing$, $\boldsymbol{B}\cap\boldsymbol{E}=\varnothing$.

公理 **1.6**(自由加密假设). $\{m\}_K=\{m'\}_{K'}\Leftrightarrow m=m'\wedge K=K'$.

定义 **1.7**. 设 C 是一个有向图,C 中有两种边→和⇒,N_C是 C 的结点集合.如果下面条件满足,则说 C 是一个丛(bundle).

1. C 是有限的.
2. 如果 $n_1\in N_C$,且 $term(n_1)$ 是负号,那么有唯一的结点 n_2 满足 $n_1\to n_2\in C$.
3. 如果 $n_1\in N_C$,且 $n_2\Rightarrow n_1$,那么 $n_1\Rightarrow n_2\in C$ 并且 $n_2\in N_C$.
4. C 是无环的.

定义 **1.8**. 如果 S 是一个边集: $S\subset\{\to\}\cup\{\Rightarrow\}$, N_S 是依附 S 的结点,那么 $\prec_S$ 是 S 的传递闭包; $\preceq_S$ 是 S 的自反的传递闭包.两者都是关系 $N_S\times N_S$ 的子集.

2 串空间理想理论扩展

2.1 入侵串类型扩展

我们进一步为入侵者增加签名,验证和钥控散列函数类型串,从而使这些运算模型能够广泛地抽象密码学原语.新增加的这 3 个入侵串如下,记 $(h)_K$ 表示用密钥 K 对 h 签名, $H_K(h)$ 表示密钥 K 控制下对 h 求散列值:

$\boldsymbol{S_i}$签名: $\langle -K,-h,+(h)_K\rangle$, $K\in\boldsymbol{K}$, $h\in\boldsymbol{A}$.

$\boldsymbol{V_e}$验证: $\langle -K^{-1},-(h)_K,+h\rangle$, $K\in\boldsymbol{K}$, $h\in\boldsymbol{A}$.

$\boldsymbol{H_k}$HMAC 散列: $\langle -K,-h,+\mathrm{H}_K(h)\rangle$, $K\in\boldsymbol{K}$, $h\in\boldsymbol{A}$.

这里之所以加入 $\boldsymbol{H_k}$ 模型,是因为在现代安全协议里,钥控散列函数是普遍采用的认证和数据完整性保护密码算法.其次,许多协议的 HMAC 函数含有非原子项参数,因此 f 函数不适合抽象散列函数.

定义 **2.1**. $\boldsymbol{A}$ 中新定义两种运算:签名 $sign:\boldsymbol{K}\times\boldsymbol{A}\to\boldsymbol{A}$;HMAC 函数 $hmac:\boldsymbol{K}\times\boldsymbol{A}\to\boldsymbol{A}$.sign 的值域是 $\boldsymbol{S}$,HMAC 的值域是 $\boldsymbol{H}$.

定义 **2.2**. 一个项是简单项,如果这个项是 $\boldsymbol{K}\cup\boldsymbol{T}\cup\boldsymbol{B}\cup\boldsymbol{E}\cup\boldsymbol{S}\cup\boldsymbol{H}$ 中的元素.

这里新增加下面两个自由假设公理:

公理 **2.3**(自由签名假设). $(m)_K=(m')_{K'}\Leftrightarrow m=m'\wedge K=K'$.

公理 **2.4**(自由散列假设). $\mathrm{H}_K(m)=\mathrm{H}_{K'}(m')\Leftrightarrow m=m'\wedge K=K'$.

公理 **2.5**. 对 $m_0,m_0',m_1,m_1'\in\boldsymbol{A}$, $K,K'\in\boldsymbol{K}$,

1. $m_0m_1=m_0'm_1'\Rightarrow m_0=m_0'\wedge m_1=m_1'$;
2. $m_0m_1=m_0'm_1'\Rightarrow m_0=m_0'\wedge m_1=m_1'$;
3. $m_0m_1\neq\{m_0'\}_K$;
4. $\{m_0\}_K\notin\boldsymbol{K}\cup\boldsymbol{T}\cup\boldsymbol{B}$, $(m_0)_K\notin\boldsymbol{K}\cup\boldsymbol{T}\cup\boldsymbol{B}$, $H_K(m)\notin\boldsymbol{K}\cup\boldsymbol{T}\cup\boldsymbol{B}$.

2.2 理想概念

我们将文献[1]中理想的定义调整如下.

定义 **2.6**. 设 $\boldsymbol{\kappa}\subseteq\boldsymbol{K}$, $\boldsymbol{\kappa}=\boldsymbol{ek}\cup\boldsymbol{sk}\cup\boldsymbol{hk}$, $\boldsymbol{ek}$ 为加密密钥集,$\boldsymbol{sk}$ 为签名密钥集,$\boldsymbol{hk}$ 为 HMAC 函数密钥集.子集 $I\subseteq\boldsymbol{A}$ 称为 $\boldsymbol{A}$ 的$\boldsymbol{\kappa}$理想(k-ideal),如果对所有的 $h\in I$, $g\in\boldsymbol{A}$, I 满足下列条件:(1) $hg,gh\in I$;(2) $\{h\}_K\in I$, $K\in\boldsymbol{ek}$;(3) $(h)_K\in I$, $K\in\boldsymbol{sk}$;(4) $\mathrm{H}_K(h)\in I$, $K\in\boldsymbol{hk}$.包含 h 的最小$\boldsymbol{\kappa}$理想记为 $I_{\boldsymbol{\kappa}}[h]$.

定义 **2.7**. 如果 $g\in I_{\boldsymbol{\kappa}}[h]$,则 h 是 g 的子项,记为 $h\sqsubset g$.

命题 **2.8**. $\sqsubset$是自反的、可传递的二元关系.而且如果 $h,g\in\boldsymbol{A}$, $K\in\boldsymbol{K}$,则(1) $h\sqsubset hg$;(2) $h\sqsubset\{h\}_K$, $h\sqsubset(h)_K$, $h\sqsubset H_K(h)$.

证明:1. 自反性显然;传递性:设 $g\sqsubset g'$, $g'\sqsubset h$,则 $g'\in I_{\boldsymbol{\kappa}}[g]$, $h\in I_{\boldsymbol{\kappa}}[g']$,由于 $h\in I_{\boldsymbol{\kappa}}[g']\subseteq I_{\boldsymbol{\kappa}}[g]$,所以 $g\sqsubset h$.

2. 两个结论可由定义 2.6 和定义 2.7 直接得到. □

公理 **2.9**. 如果 t 是简单项且 $gh \in I_{\varnothing}[t]$,则 $g \in I_{\varnothing}[t]$ 或 $h \in I_{\varnothing}[t]$,$\varnothing$表示$\boldsymbol{\kappa}$为空集.

公理 **2.10**. ***K***,***T***,***E***,***C***,***S***,***H*** 两两互不相交.

定义 **2.11**. 设 $\boldsymbol{\kappa} \subseteq \boldsymbol{K}$,当且仅当 $g \in I_{\boldsymbol{\kappa}}[h]$ 时,$h \in \boldsymbol{A}$ 称为 $g \in \boldsymbol{A}$ 的$\boldsymbol{\kappa}$子项,记为 $h \sqsubset_{\boldsymbol{\kappa}} g$.

命题 **2.12**. $\sqsubset_{\boldsymbol{\kappa}}$是自反的、可传递的二元关系,且 $h \sqsubset_{\boldsymbol{\kappa}} g$ 蕴涵 $h \sqsubset g$.

定义 **2.13**. $I_{\boldsymbol{\kappa}}[S]$是包含 S 的最小$\boldsymbol{\kappa}$理想,其中 $S \subseteq \boldsymbol{A}$.

命题 **2.14**. 如果 $S \subseteq \boldsymbol{A}$,则 $I_{\boldsymbol{\kappa}}[S] = \cup_{x \in S} I_{\boldsymbol{\kappa}}[x]$.

引理 **2.15**. 若 $S_{i+1} = \{\{g\}_{eK}, (g)_{sK}, H_{hK}(g) \mid g \in I_{\varnothing}[S_i], eK \in \boldsymbol{ek}, sK \in \boldsymbol{sk}, hK \in \boldsymbol{hk}\}$,$\boldsymbol{\kappa} = \boldsymbol{ek} \cup \boldsymbol{sk} \cup \boldsymbol{hk}$,$S_0 = S$,则 $I_{\boldsymbol{\kappa}}[S] = \cup_i I_{\varnothing}[S_i]$.

命题 **2.16**. 设 $S \subseteq \boldsymbol{A}$,$S$ 是简单项集合,如果 $gh \in I_{\boldsymbol{\kappa}}[S]$,则 $g \in I_{\boldsymbol{\kappa}}[S]$ 或 $h \in I_{\boldsymbol{\kappa}}[S]$.

证明:根据引理 2.15, $\exists i.gh \in I_{\varnothing}[S_i]$,由命题 2.14 得 $\exists x.x \in S_i \wedge gh \in I_{\varnothing}[x]$.若 $i = 0$,则 $S_i = S_0 = S, x$ 是简单项;若 $i > 0$,则 $x \in S_i$ 有形式 $\{h\}_{eK}$ 或 $(h)_{sK}$ 或 $H_{hK}(h)$,也是简单项.所以按公理 2.9 有 $g \in I_{\varnothing}[x] \subseteq I_{\boldsymbol{\kappa}}[S]$ 或 $h \in I_{\varnothing}[x] \subseteq I_{\boldsymbol{\kappa}}[S]$. □

命题 **2.17**. 设某个 $K \in \boldsymbol{K}$,$\boldsymbol{\kappa} \subseteq \boldsymbol{K}$,$S \subseteq \boldsymbol{A}$,$S$ 是简单项集合且不具有形式 $\{h\}_K$,$(h)_K$ 和 $H_K(h)$.如果 $\{h\}_K \in I_{\boldsymbol{\kappa}}[S]$ 或 $(h)_K \in I_{\boldsymbol{\kappa}}[S]$ 或 $H_K(h) \in I_{\kappa}[S]$,则 $h \in I_{\boldsymbol{\kappa}}[S]$.

证明:假设 $h \notin I_{\boldsymbol{\kappa}}[S]$.

① 设 I' 是差集 $I_{\boldsymbol{\kappa}}[S] \setminus \{\{h\}_K\}$.由于 $S \subseteq I'$,$\{h\}_K$ 非 ab 形式,所以 I' 满足理想条件(1);同时 $\forall h_1 \in I', K_1 \in \boldsymbol{\kappa}.\{h_1\}_{K_1} \neq \{h\}_K$,否则按公理 1.6 有 $h = h_1 \in I'$,与 $h \notin I_{\boldsymbol{\kappa}}[S]$ 矛盾,故 I' 满足理想条件(2)~(4), I' 是包含 S 的理想.但 $I' \subset I_{\boldsymbol{\kappa}}[S]$ 与最小的理想 $I_{\boldsymbol{\kappa}}[S]$ 矛盾,所以 $h \in I_{\boldsymbol{\kappa}}[S]$.

② 设 I' 是差集 $I_{\boldsymbol{\kappa}}[S] \setminus \{(h)_K\}$.由于 $S \subseteq I'$,$(h)_K$ 非 ab 形式,所以 I' 满足理想条件(1);同时 $\forall h_1 \in I', K_1 \in \boldsymbol{\kappa}.(h_1)_{K_1} \neq (h)_K$,否则按公理 2.3 有 $h = h_1 \in I'$,与 $h \notin I_{\boldsymbol{\kappa}}[S]$ 矛盾,故 I' 满足理想条件(2)~(4), I' 是包含 S 的理想.但 $I' \subset I_{\boldsymbol{\kappa}}[S]$ 与最小的理想 $I_{\boldsymbol{\kappa}}[S]$ 矛盾,所以 $h \in I_{\boldsymbol{\kappa}}[S]$.

③ 设 I' 是差集 $I_{\kappa}[S] \setminus \{H_K(h)\}$.由于 $S \subseteq I'$,$H_K(h)$ 非 ab 形式,所以 I' 满足理想条件(1);同时 $\forall h_1 \in I', K_1 \in \boldsymbol{\kappa}.H_{K_1}(h_1) \neq H_K(h)$,否则按公理 2.4 有 $h = h_1 \in I'$,与 $h \notin I_{\boldsymbol{\kappa}}[S]$ 矛盾,故 I' 满足理想条件(2)~(4), I' 是包含 S 的理想.但 $I' \subset I_{\boldsymbol{\kappa}}[S]$ 与最小的理想 $I_{\boldsymbol{\kappa}}[S]$ 矛盾,所以 $h \in I_{\boldsymbol{\kappa}}[S]$. □

推论 **2.18**. 设 $K \neq K'$,则:

(1) $\{h'\}_{K'} \sqsubset \{h\}_K \Rightarrow \{h'\}_{K'} \sqsubset h, \{h'\}_{K'} \sqsubset (h)_K \Rightarrow \{h'\}_{K'} \sqsubset h, \{h'\}_{K'} \sqsubset H_K(h) \Rightarrow \{h'\}_{K'} \sqsubset h$;

(2) $(h')_{K'} \sqsubset \{h\}_K \Rightarrow (h')_{K'} \sqsubset h, (h')_{K'} \sqsubset (h)_K \Rightarrow (h')_{K'} \sqsubset h, (h')_{K'} \sqsubset H_K(h) \Rightarrow (h')_{K'} \sqsubset h$;

(3) $H_{K'}(h') \sqsubset \{h\}_K \Rightarrow H_{K'}(h') \sqsubset h, H_{K'}(h') \sqsubset (h)_K \Rightarrow H_{K'}(h') \sqsubset h, H_{K'}(h') \sqsubset H_K(h) \Rightarrow H_{K'}(h') \sqsubset h$.

证明:(1) 按定义 2.7 有 $\{h\}_K \in I_{\boldsymbol{K}}[\{h'\}_{K'}]$, $(h)_K \in I_{\boldsymbol{K}}[\{h'\}_{K'}]$, $H_K(h) \in I_{\boldsymbol{K}}[\{h'\}_{K'}]$.由于 $K \neq K'$,按命题 2.17 有 $h \in I_{\boldsymbol{K}}[\{h'\}_{K'}]$,所以 $\{h'\}_{K'} \sqsubset h$.同理可证(2),(3). □

命题 **2.19**. 设某个 $K \in \boldsymbol{K}$,$\boldsymbol{\kappa} \subseteq \boldsymbol{K}$,$S \subseteq \boldsymbol{A}$,$S$ 是简单项集合且不具有形式 $\{h\}_K$,$(h)_K$ 和 $H_K(h)$.如果 $\{h\}_K \in I_{\boldsymbol{\kappa}}[S]$ 或 $(h)_K \in I_{\boldsymbol{\kappa}}[S]$ 或 $\mathrm{H}_K(h) \in I_{\boldsymbol{\kappa}}[S]$,则 $K \in \boldsymbol{\kappa}$.

证明:由于 $\{h\}_K \notin S$,$(h)_K \notin S$,$H_K(h) \notin S$,故 $\{h\}_K \in I_{\boldsymbol{\kappa}}[S] \setminus S$,$(h)_K \in I_{\boldsymbol{\kappa}}[S] \setminus S$,$H_K(h) \in I_{\kappa}[S] \setminus S$.按公理 2.10, $\{h\}_K$, $(h)_K$, $H_K(h)$ 只能由加密、签名和散列函数得到.所以, $\exists K_1 \in \kappa, h_1 \in I_{\kappa}[S].\{h_1\}_{K_1} = \{h\}_K$, $\exists K_1 \in \boldsymbol{\kappa}, h_1 \in I_{\boldsymbol{\kappa}}[S].(h_1)_{K_1} = (h)_K$, $\exists K_1 \in \boldsymbol{\kappa}, h_1 \in I_{\boldsymbol{\kappa}}[S].H_{K_1}(h_1) = H_K(h)$.按公理 1.6,2.3,2.4,得到 $K_1 = K \in \boldsymbol{\kappa}$. □

2.3 诚实性理论

对入侵者的 $\boldsymbol{B}_f$ 串轨迹 $\langle -x_1, ..., -x_n, +y = f(x_1, ..., x_n) \rangle$,函数 f 有下面的定义[8].

定义 **2.20**. 如果当函数 f 起源于丛 C 的入侵结点,原像 $(x_1, ..., x_n)$ 都是 ***B*** 类型入侵串,则 f 关于 $(x_1, ..., x_n)$ 是诚实函数.

定义 **2.21**. 结点 n 是数据集 $I \subseteq \boldsymbol{A}$ 的入点,当且仅当 $term(n)$ 是正号, $term(n) \in I$,而且对同一个串上 n 的任何

前继 n' 有 $term(n')\in I'$.

定义 **2.22**. 项集合 $I\subseteq \boldsymbol{A}$ 关于丛 C 是诚实的,当且仅当一个入侵结点 p 是 I 的入点时,p 是 $\boldsymbol{M}$ 结点、$\boldsymbol{K}$ 结点或 $\boldsymbol{B}$ 结点.

诚实概念反映了一个数据集的安全性:如果入侵者知道某个数据,那么他知道的是自己所掌握的知识.根据新扩展的理想概念,我们将证明如下几个重要的定理和推论.

定理 **2.23**. 设 C 是 $\boldsymbol{A}$ 上的丛, $S\subseteq \boldsymbol{T}\cup \boldsymbol{K}\cup \boldsymbol{B}$, $\boldsymbol{\kappa}\subseteq \boldsymbol{K}$, $\boldsymbol{K}\subseteq S\cup \boldsymbol{\kappa}^{-1}$. f 是诚实函数,且当 $y=f(x_1,...,x_n)$ 起源于入侵结点时, $y\in I_{\kappa}[S]\Rightarrow x_1,...,x_n\in I_{\kappa}[S]$,则理想 $I_{\boldsymbol{\kappa}}[S]$ 是诚实的.

证明:只证 $\boldsymbol{S_i},\boldsymbol{V_e}$ 和 HMAC 不是 $I_{\boldsymbol{\kappa}}[S]$ 的入点.$\boldsymbol{F},\boldsymbol{T},\boldsymbol{C},\boldsymbol{S},\boldsymbol{E},\boldsymbol{D},\boldsymbol{B},\boldsymbol{B}_f$ 型入侵串不含 $I_{\boldsymbol{\kappa}}[S]$ 的入点已在文献[1,2]中证明.

$\boldsymbol{S_i}$: $\langle -K,-h,+(h)_K\rangle$, $I_{\boldsymbol{\kappa}}[S]$ 可能的入点是 $+(h)_K$.如果 $(h)_K\in I_{\boldsymbol{\kappa}}[S]$,则根据命题 2.17, $h\in I_{\boldsymbol{\kappa}}[S]$,这与入点定义矛盾.

$\boldsymbol{V_e}$: $\langle -K^{-1},-(h)_K,+h\rangle$,若+$h$ 是 $I_{\boldsymbol{\kappa}}[S]$ 的入点,则必须有 $K^{-1}\notin I_{\boldsymbol{\kappa}}[S]$,从而 $K^{-1}\notin S$.由于 $K^{-1}\in \boldsymbol{K}\subseteq S\cup \boldsymbol{\kappa}^{-1}$,所以 $K^{-1}\in \boldsymbol{\kappa}^{-1}\Rightarrow K\in \boldsymbol{\kappa}$,既 $(h)_K\in I_{\boldsymbol{\kappa}}[S]$,这与入点定义矛盾.

$\boldsymbol{H_k}$: $\langle -K,-h,+H_K(h)\rangle$,若 $+H_K(h)$ 是 $I_{\boldsymbol{\kappa}}[S]$ 的入点,则必须有 $K\notin I_{\boldsymbol{\kappa}}[S]$,根据命题 2.17, $H_K(h)\in I_{\boldsymbol{\kappa}}[S]\Rightarrow h\in I_{\boldsymbol{\kappa}}[S]$,这也与入点定义矛盾.

综上所证,可得 $I_{\boldsymbol{\kappa}}[S]$ 是诚实的. □

与原始串空间理论[1]相比,这里 $I_{\boldsymbol{\kappa}}[S]$ 是诚实的不仅表示该理想的秘密性,还可能表示它的不可伪造性.I 是诚实的说明了入侵者要获得 I 的入点只能通过猜测:猜出正确的新鲜随机数,密钥或其他新鲜文本.他不能通过加密、解密、签名、散列、连接或分解操作来获得 I 中的消息.基于该定理,我们可以得到下面两个新的推论.

推论 **2.24**. 设 C 是 $\boldsymbol{A}$ 上的丛, $\boldsymbol{B}\cap \boldsymbol{K}=\boldsymbol{B}\cap \boldsymbol{T}=\varnothing$, $\boldsymbol{K}=(S\setminus \boldsymbol{B})\cup \boldsymbol{\kappa}^{-1}$, $S\cap \boldsymbol{K}_P=S\cap \boldsymbol{B}_P=\varnothing$.如果对 $m\in C$, $term(m)\in I_{\boldsymbol{\kappa}}[S]$,则 C 上存在一个常规结点 n 是 $I_{\boldsymbol{\kappa}}[S]$ 的入点.

证明:设 m 是 $\{n\in C\mid term(n)\in I_{\boldsymbol{\kappa}}[S]\}$ 的最小成员,则 m 是 $I_{\boldsymbol{\kappa}}[S]$ 的入点.假设 m 不是常规结点,则 m 是 $\boldsymbol{M},\boldsymbol{K}$ 或 $\boldsymbol{B}$ 型入侵结点(根据定理 2.23, $I_{\boldsymbol{\kappa}}[S]$ 是诚实的).由于 $S\subseteq \boldsymbol{K}\cup \boldsymbol{B}$,所以 $I_{\boldsymbol{\kappa}}[S]\cap \boldsymbol{T}=\varnothing$,$m$ 不是 $\boldsymbol{M}$ 型结点;由 $S\cap \boldsymbol{K}_P=S\cap \boldsymbol{B}_P=\varnothing$ 得到 m 不是 $\boldsymbol{K}$ 型或 $\boldsymbol{B}$ 型结点. □

推论 **2.25**. 设 C 是 $\boldsymbol{A}$ 上的丛, $\boldsymbol{B}\cap \boldsymbol{K}=\boldsymbol{B}\cap \boldsymbol{T}=\varnothing$, $\boldsymbol{K}=(S\setminus \boldsymbol{B})\cup \boldsymbol{\kappa}^{-1}$, $S\cap \boldsymbol{K}_P=S\cap \boldsymbol{B}_P=\varnothing$,且没有常规结点 $n\in C$ 是 $I_{\boldsymbol{\kappa}}[S]$ 的入点,则对 $K\in S$ 任何形如 $\{g\}_K$, $(g)_K$ 和 $H_K(g)$ 的项不起源于入侵结点.

证明:由定理 2.23 可得 $I_{\boldsymbol{\kappa}}[S]$ 是诚实的.根据推论 2.24 的逆否结论可知:如果没有常规结点 $n\in C$ 是 $I_{\boldsymbol{\kappa}}[S]$ 的入点,则 $\forall m\in C.term(m)\notin I_{\boldsymbol{\kappa}}[S]$.

(1) 假设 $t_1=\{g\}_K$ 起源于一个入侵结点, t_1 不可能发生在 $\boldsymbol{F},\boldsymbol{T},\boldsymbol{C},\boldsymbol{S},\boldsymbol{B},\boldsymbol{B}_f$ 型入侵串上.考虑可能的 $\boldsymbol{E},\boldsymbol{D},\boldsymbol{S_i},\boldsymbol{V_e}$ 和 $\boldsymbol{H_k}$ 入侵串:

$\boldsymbol{E}$: t_1 发生在 $\langle -K_0,-h,+\{h\}_{K_0}\rangle$ 串上.由于 $K_0\notin I_{\boldsymbol{\kappa}}[S]$, $K_0\neq K$,按推论 2.18, $\{g\}_K\sqsubset\{h\}_{K_0}\Rightarrow\{g\}_K\sqsubset h$,这与起源定义矛盾.

$\boldsymbol{D}$: t_1 发生在 $\langle -K_0^{-1},-\{h\}_{K_0},+h\rangle$ 串上.由于 $\{g\}_K\sqsubset h\Rightarrow\{g\}_K\sqsubset\{h\}_{K_0}$,与起源定义矛盾.

$\boldsymbol{S_i}$: t_1 发生在 $\langle -K_0,-h,+(h)_{K_0}\rangle$ 串上.由于 $K_0\notin I_{\boldsymbol{\kappa}}[S]$, $K_0\neq K$,按推论 2.18, $\{g\}_K\sqsubset(h)_{K_0}\Rightarrow\{g\}_K\sqsubset h$,这与起源定义矛盾.

$\boldsymbol{V_e}$: t_1 发生在 $\langle -K_0^{-1},-(h)_{K_0},+h\rangle$ 串上.由于 $\{g\}_K\sqsubset h\Rightarrow\{g\}_K\sqsubset(h)_{K_0}$,与起源定义矛盾.

$\boldsymbol{H_k}$: t_1 发生在 $\langle -K_0,-h,+H_{K_0}(h)\rangle$ 串上.由于 $K_0\notin I_{\boldsymbol{\kappa}}[S]$, $K_0\neq K$,按推论 2.18, $\{g\}_K\sqsubset H_K(h)\Rightarrow\{g\}_K\sqsubset h$,这与起源定义矛盾.

(2) $(g)_K$ 和 $H_K(g)$ 项不起源于入侵结点同理可证. □

推论 2.25 说明无论 $\boldsymbol{\kappa}$ 是否包含入侵者掌握的密钥,只要 $I_{\boldsymbol{\kappa}}[S]$ 是诚实的,那么合法的加密、签名和散列值就不可能被伪造.串空间分析协议的特点就是能够一般性地证明出关于攻击者能力的普遍性结论,这些结论可以

重复应用于不同协议的分析.

3 结论及后续研究

开放网络环境下的认证、密钥交换协议已经变得非常复杂,像 IKE 和 SSL 这样的协议都包含了各种丰富的密码原语.原始串空间理论不能为所有的原语建立模型,这必然限制了它的应用领域.我们在分析 IKE2[10]和 JFK[11]协议时充分认识到扩展串空间理论的适用性,这两个协议包含复杂的会话密钥抽取、签名和散列运算.

本文针对理想理论和认证测试理论对串空间模型进行了扩展.文献[2]是串空间分析协议的朴素方法,即利用串空间的丛、丛的偏序关系来分析协议.基于本文增加的入侵模型,我们也可以将文献[2]中的分析方法进行扩展.同时,在混合协议环境下[5,12],基于本文的扩展模型,我们是否可以得到新的协议独立定理?这个问题值得进一步研究.

致谢 在此,我们向对本文的工作给予支持和建议的薛锐研究员表示感谢.

References:

[1] Fábrega FJT, Herzog JC, Guttman JD. Honest ideals on strand spaces. In: Werner B, ed. Proc. of the 11th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1998. 66−77.

[2] Fábrega FJT, Herzog JC, Guttman JD. Strand spaces: Why is a security protocol correct. In: Kelly K, ed. Proc. of the 1998 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998. 160−171.

[3] Fábrega FJT, Herzog JC, Guttman JD. Strand spaces: Proving security protocols correct. Journal of Computer Security, 1999, 7(10):191−230.

[4] Fábrega FJT, Herzog JC, Guttman JD. Authentication tests. In: Titsworth FM, ed. Proc. of the 2000 IEEE Symp. on Security and Privacy (S&P 2000). Los Alamitos: IEEE Computer Society Press, 2000. 96−109.

[5] Fábrega FJT, Herzog JC, Guttman JD. Mixed strand spaces. In: Guttman J, ed. Proc. of the 12th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1999. 72−82.

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

[7] Nie LZ, Ding SS. Introduction to Algebra. 2nd ed., Beijing: Higher Education Press, 2000 (in Chinese).

[8] Maneki AP. Honest functions and their application to the analysis of cryptographic protocols. In: Guttman J, ed. Proc. of the 12th IEEE Computer Security Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 1999. 83−89.

[9] Anderson R, Needham R. Robustness principles for public key protocols. In: Coppersmith D, ed. Proc. of the Int'l Conf. on Advances in Cryptology (CRYPTO'95). London: Springer-Verlag, 1995. 236−247.

[10] Harkins D, Kaufman C, Kent S, Kivinen T, Perlman R. Internet key exchange (IKEv2) protocol. 2003. http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-ipsec-ikev2-11.txt

[11] Aiello W, Bellovin SM. Efficient, DOS resistant, secure key exchange for Internet protocols. In: Atluri V, ed. Proc. of the ACM Computer and Communications Security (CCS) Conf. New York: ACM Press, 2002. 48−58.

[12] Fábrega FJT, Herzog JC, Guttman JD. Protocol independence through disjoint encryption. In: Lee S, ed. Proc. of the 13th IEEE Computer Security Foundations Workshop (CSFW-13). Los Alamitos: IEEE Computer Society Press, 2000. 24−34.

附中文参考文献:

[7] 聂灵沼,丁石孙.代数学引论.第 2 版,北京:高等教育出版社,2000.