2014 密码学报 赵建杰

基于PKI的认证密钥协商协议可证明安全理论研究

总结：综述，介绍认证密钥协商(AKA)协议的分类[1]，研究进展[2]，协议的设计原则和安全目标[3]，可证明安全理论[4]及研究进展[5]，重点关注口令认证密钥协商(PAKA)协议的部分。

AKA协议及其分类

密码协议 → 密钥建立协议 ⟨ KD(分配)；KA(协商) —提供身份认证→ AKA协议

分类

1. 根据参与者长期私钥不同性质 ⟨ 基于PKI的AKA协议(应用广泛)；基于身份的AKA
2. 根据参与者个数不同 ⟨ 2AKA 双方；3AKA 三方；GAKA 群 → 指有第三方参与 ⟨ 可信；半可信

3AKA常见以口令作为长期私钥 3PAKA

基于PKI的AKA协议的研究进展

2AKA：Diffie-Hellman(1976) → MTI → MQV → HMQV → KEA+ → OAKE

3PAKA：口令迎合了公钥基础设施的复杂性，但由于口令低熵易被穷尽搜索，设计更困难

a. 双方口令认证协议

EKE(1992)奠定基石出，PAK协议簇(2002)，AuthA(2003)等方案以及在标准模型下可证明安全的双方口令协议被提出

以上更适用于C-S而非C-C，因为网络规模个，口令数量个

b. 三方口令认证协商协议 3PAKA

引入可信/半可信服务器，用户与server共享口令，server认证双方并协助生成会话密钥，95年首次提出，后续学者不断提出新方案，LSH-3PAKE，CHY-3PAKE等，也对其分析攻击等做分析

GAKA：早期基本上是对DH的推广，如GDH，BCP等，密钥协商扩展性也是一个研究问题

AKA协议设计的基本原则

复杂性：抵抗攻击；简单经济适用

1. 明确的安全目标：保证协议达到安全要求，并在此前提下提高效率
2. 尽量减少使用时间戳：同步+时间戳 ⇒ 异步+随机数
3. 尽可能小的计算复杂度和短的消息长度：降低消息泄露带来的风险，提高效率和适应能力
4. 尽可能少的安全假设：减少初始安全假设数目，允许协议被攻破但将影响降至最低 confine the adverse effects of such failures to the possible minimum.

协议可能受到的攻击

被动攻击：窃听攻击(不可检测，密码技术防范)

主动攻击：篡改，重放，类型，交互…

针对口令的字典攻击：离线～ → 避免公开可用于验证的信息

在线不可检测～：→ 实现CK-1S的显式认证

在线可检测～ → 限制口令验证次数

安全目标(不同应用场景不同，2008报告)

1) 隐式认证：参与者确保除了指定实体，其它者不能得到会话密钥Sk

Basic

2) 密钥协商：保证经过隐式认证的实体可唯一确定算到Sk

3) 密钥确认：参与者确认其它合法实体已获得Sk(两轮KA无法实现)

4) 显式认证：隐式认证+密钥确认

5) 已知密钥安全：敌手已知除本次Sk之外的Sk，不影响本次安全(标准需求)

6) 前向安全性：长期私钥的泄露不会泄露之前的Sk ⟨ 完美前向安全性；弱的…

7) 抗密钥泄露伪装攻击：A的私钥泄露不会使敌手向A伪装为其它参与者

8) 抗未知密钥共享攻击：抵抗敌手欺骗双方实体关于对等身份信息的攻击

9) 抗离线字典攻击(攻击者成功的概率依赖与协议参与者交互的次数)

10) 相对服务器的会话密钥私密性：用户之间不可直接安全通信，经过服务器才可进行口令密钥协商，且应降低对服务器的信任和依赖

安全性的证明方法

1) 启发式：根据经验和相关知识验证安全性，可信度不高

2) 公理化：一般使用数学方法构造安全证明过程

a. 基于信息论的手段：敌手计算能力和资源无限，无条件安全

b. 基于计算复杂性的手段：攻击所需成本比秘密价值高，可认为安全

一般将协议S的安全性归约到另一个问题P的难解性上

称为可证明安全理论(不断发展)

c. 基于符号的手段：利用特定的语法规则定义安全模型

可证明安全理论的研究进展(KA)

相比于低效的标准模型，面向实际的可证明安全性应用更广

如ROM方法论(随机预言模型)

可证明安全理论应用于KA起始于BR模型，是许多模型的基础

后续提出CK和eCK等模型，并引入前向安全性等

应用于PAKA起始于BPR(2000)模型，AFP是首个应用于3PAKA的模型，后续有基于上述的WH，CTB，Seck等。

通用可组合(UC)安全框架下的安全定义和刻画的工作保证了协议的组合安全性和口令任何形式的概率分布

→ BCP04是第一个严格的群认证密钥协商协议的安全模型

有待研究的问题

1. 更强的安全模型和更为高效的协议

隐私等安全需求的提高及敌手能力的增强。

2. 适合复杂应用环境的安全协议设计

新场景的应用需求和安全问题。

3. 现实世界中复杂协议的安全性证明

对复杂协议如何做合理的安全性分析和证明。