安全协议设计与分析：第一讲

课程简介+安全协议概述

- 李晖
  - lihuill@bupt.edu.cn
- 网络空间安全学院

课程目标

- 课程直接目标：
  - 什么是安全协议
  - 如何设计安全协议
  - 如何分析安全协议
- 间接目标：
  - 了解各种安全协议
  - 了解提高系统安全性的方法

课程计划

- This lecture:安全协议设计与分析概述 2课时
  - 安全协议简介、安全协议的设计与分析方法
- Lecture 2:安全协议中的密码算法 2课时
  - 密码学概念及主要的密码算法
- Lecture 3:安全协议需求及目标 2课时
  - 安全协议的需求分析及目标描述
- Lecture 4: 安全协议面临的攻击与设计原则 2课时
  - 安全协议面临的攻击
  - 安全协议设计
- Lecture 5:基本安全协议-认证协议 2课时
  - 认证协议的基本概念及典型认证协议
- Lecture 6:实际使用的安全协议 2课时
  - 移动通信系统中的安全协议
- 课程项目中期汇报 2课时

课程计划

- Lecture 7: 安全协议的形式化分析 2课时
  - 安全协议的分析方法
- Lecture 8: 形式化分析工具简介 2课时
  - ProVerif/CryptoVerif/Tamarin/CPSA.
- Lecture 9: 基于逻辑推理的分析方法 2课时
  - 采用BAN logic验证协议.
- Lecture 10: 基于模型检测的分析方法 4课时
  - Dolev-Yao模型
  - 通信进程方法CSP
- Lecture 11: 基于定理证明的分析方法 4课时
  - Paulson归纳法
- 课程项目结项汇报+课程总结 2课时

课程要求和考核方式

- 理论学习+课程项目
- 本课程在第二次课布置课程项目题目，自由组队（5人），完成课程项目
- 课程成绩：
  - 成绩构成：平时60%+期末40%
  - 平时成绩：课程项目中期检查成绩+结项检查成绩
  - 期末成绩：与课程项目相关的小论文

安全协议设计与分析概述

- 安全协议的背景介绍
- 安全协议概念及分类
- 安全协议的安全性质
- 安全协议的缺陷分析
- 安全协议的设计原则
- 安全协议的分析方法

安全协议的背景介绍

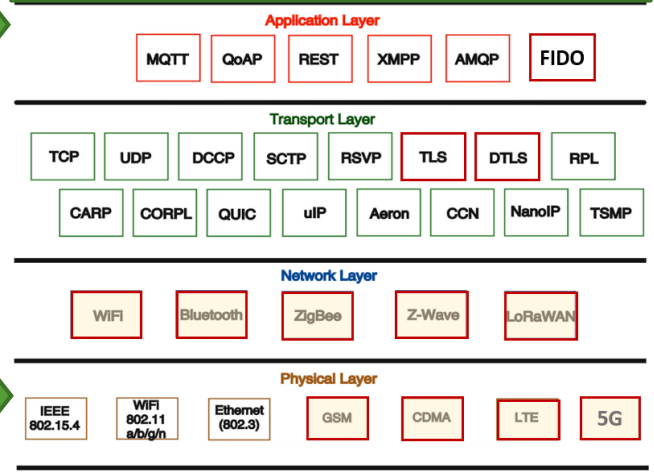
信息技术的发展要求

机密性
完整性
不可否认性

信息传输/处理/存储受到来自环境的攻击

信息截获
信息伪造
信息篡改

安全协议



密码算法

安全协议设计是一项复杂而困难的工作

协议运行环境：复杂
协议安全目标：变化
协议设计要求：简单

设计出来的安全协议并不安全!!!

安全协议的背景介绍

- 分析结果（攻击）

Protocol	Year	Published in	Tool	Main Findings
LoRaWAN	2019	Computer Networks(J)	Scyther	Jamming and replay attacks exists in versions 1.0 (2015), and 1.1 (2017) is secure
ZigBee	2020	HotSoS '20	Tamarin	Leak network key and link key in ZigBee 1.0, and Zigbee 3.0 holds secure properties
BlueTooth	2022	S&P '22	ProVerif	capture 5 known vulnerabilities and discovering 2 new security issues.
WPA2.0	2020	USENIX '20	Tamarin	Capture key-reinstallation attacks and their variants of WPA2
5G-AKA	2018	CCS '18	Tamarin	UE and SN only holds weak agreement; traceability attack, impersonate attack
TLS	2017 2017	INRIA CCS '17	ProVerif Tamarin	TLS 1.3 Candidate, led to discover an unknown key share attack; Uncover applications that assume TLS 1.3 provides strong authentication guarantees may lead to security problems
FIDO	2021	NDSS'21	ProVerif	Capture authenticator rebinding attack, parallel session attack, privacy leakage, DoS attack

安全协议设计与分析概述

- 安全协议的背景介绍
- 安全协议概念及分类
- 安全协议面临的攻击
- 安全协议的安全性质
- 安全协议的设计原则
- 安全协议的分析方法

安全协议的基本概念

- 协议的定义
  - 两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。
- 协议的含义
  - 至少需要两个参与者；
  - 一系列的步骤：参与者之间需要传递消息，参与者需要处理消息
  - 完成某项任务或达成某种共识
- 与算法的区别

安全协议的基本概念（续）

- 安全协议（简单定义）
  - 具有安全性功能的协议称为安全协议，也称作密码协议。
- 安全协议（完整定义）
  - 建立在密码体制基础上的一种高互通协议，为安全需求的各方提供一系列步骤，借助于密码算法来达到密钥分配、身份认证、信息保密以及安全地完成电子交易等目的
- 密码算法和安全协议处于网络安全体系的不同层次
  - 密码算法提供高强度的加解密操作或辅助算法（Hash等）
  - 安全协议为各种网络安全需求提供具体实现方案

安全协议分类（基本安全协议）

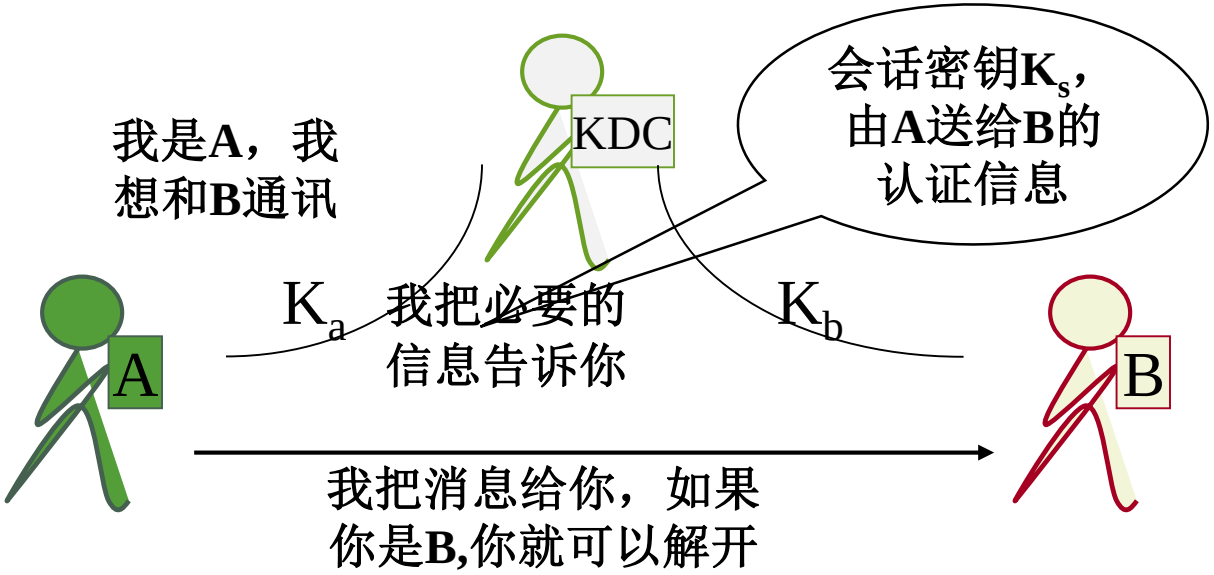
1. 密钥建立协议（Key Establishment Protocol）
   - 建立共享密钥
2. 认证建立协议（Authentication Protocol）
   - 向一个实体提供对他想要进行通信的另一个实体的身份的某种程度的确信
3. 认证的密钥建立协议（Authenticated Key Establishment Protocol）
   - 与另一身份已被或可被证实的实体之间建立共享秘密

1.密钥建立协议

- 依据采用的密码体制可分为
  - 采用单钥体制的密钥建立协议
  - 采用双钥体制的密钥建立协议
- 依据协议的目的可分为
  - 密钥传输协议：由一个实体建立或收到的密钥安全传送给另一个实体
  - 密钥协商协议：由双方（或多方）共同提供信息建立起共享密钥，没有任何一方起决定作用

例1：采用单钥体制的密钥建立协议（NSSK协议）

- 假设A和B要进行通讯，A和B与KDC各有一个共享密钥K_a和K_b，如何利用这两个密钥进行认证，并且商定一个会话密钥K_s



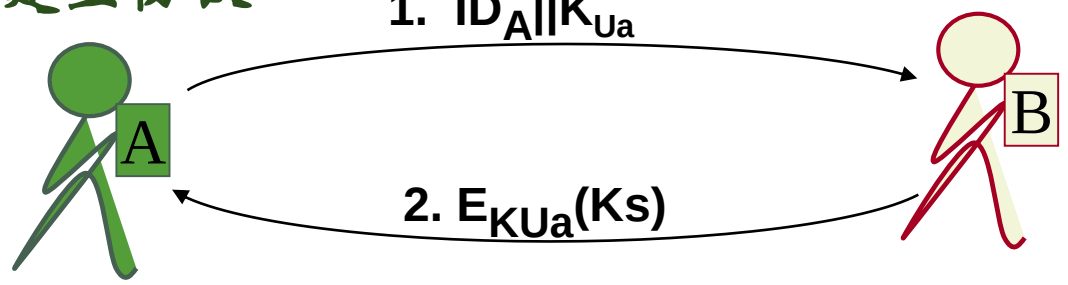
1. A →KDC: (IDA || IDB || **N1**)
2. KDC→ A: E_{Ka}[Ks || IDB || **N1** || E_{Kb}(Ks,IDA)]
3. A → B: E_{Kb}(Ks,IDA) || E_{Ks}(M)

例1：分析

- 是否A可以确认B的身份?
  - 否
- 是否B可以确认A的身份?
  - 否
- KDC的作用？
  - 安全性完全依赖于KDC的安全性；
  - KDC可能成为影响系统性能的瓶颈；

例2： Merkle协议

采用双钥体制的密钥建立协议



- 协议描述
  1. A生成$\{K_{Ua}, K_{Ra}\}$， A → B: (IDA, K_{Ua})
  2. B生成随机密钥Ks, B → A: $E_{KUa}(Ks)$
  3. A解密$E_{KUa}(Ks)$得到Ks: $D_{KRa}(E_{KUa}(Ks))$
  4. A丢弃$\{K_{Ua}, K_{Ra}\}$,B丢弃K_{Ua}
- 分析
  - 通讯前不需存在密钥，通讯后也不存在密钥
  - 问题：能否防止中间人攻击？

例2 – Merkle协议的中间人攻击

1. A生成$\{K_{Ua}, K_{Ra}\}$, A->B: (ID_A, K_{Ua})
2. E截获,生成$\{K_{Ue}, K_{Re}\}$冒充A->B: (ID_A, K_{Ue})
3. B生成随机密钥Ks, B->A: $E_{KUe}(Ks)$
4. E截获,解密后再用E_{KUa}加密Ks->A: $E_{KUa}(Ks)$
5. A丢弃$\{K_{Ua}, K_{Ra}\}$,B丢弃K_{Ua}

- E获得了Ks,故以后只需进行窃听.
- A,B并不知晓它们被攻击了

例3：Diffie-Hellman密钥交换协议

- 允许两个用户可以安全地交换一个秘密信息，用于后续的通讯过程
- 算法的安全性依赖于计算离散对数的难度
- 协议描述：
  - 双方选择素数p以及p的一个原根r
  - A选择$x<p$,计算$X_A=r^x \bmod p$, A→B: X_A
  - B选择$y<p$,计算$Y_B=r^y \bmod p$, B→A: Y_B
  - A计算: $(Y_B)^x \equiv (r^y)^x \equiv r^{xy} \bmod p$
  - B计算: $(X_A)^y \equiv (r^x)^y \equiv r^{xy} \bmod p$
  - 双方获得一个共享密钥$(r^{xy} \bmod p)$
- 素数p以及p的原根r可由一方选择后发给对方

原根的定义

- Euler定理表明,对两个互素的整数a,n,（a<n）

  $a^{\varphi(n)} \equiv 1 \bmod n$

- 定义：

  素数p的原根定义：如果a是素数p的原根，则数

  $a \bmod p,\ a^2 \bmod p,\ \ldots,\ a^{p-1} \bmod p$

  是不同的并且包含1到p-1的整数的某种排列。

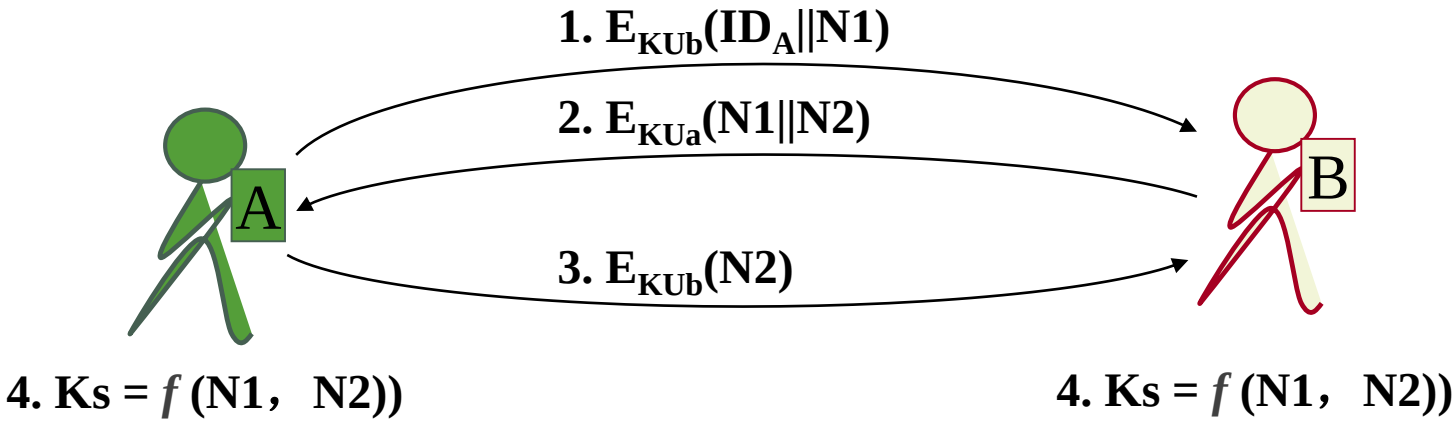
- 对任意的整数b，我们可以找到唯一的幂i满足

  $b=a^i \bmod p \quad 0<=i<=(p-1)$

认证建立协议

- 采用单向函数的认证协议
  - Alice向主机发送她的口令
  - 主机计算该口令的单向函数值；
  - 主机将计算得到的单向函数值与预先存储的值进行比较

认证的密钥建立协议（NSPK协议）



- 假定A和B已经获得了双方的公钥：

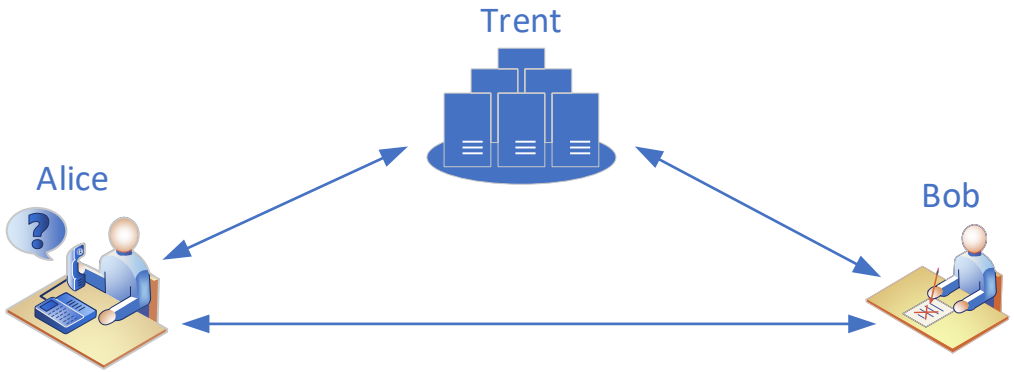
1. A → B: E_{KUb}(IDA,N1)
2. B → A: E_{KUa}(N1 ,N2)
3. A → B: E_{KUb}(N2)
4. A 和 B: Ks= *f* (N1,N2)

安全协议分类（按照参与方数量）

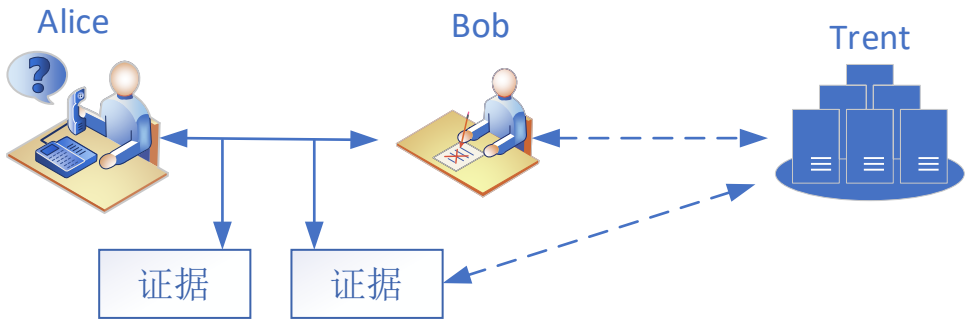
- 双方安全协议
  - 零知识证明协议
  - 掷币协议
- 多方安全协议
  - 基本多方协议，如秘密共享，多方Ping-Pong协议等
  - 电子选举
  - 电子商务

安全协议分类（是否有可信第三方）

- 仲裁协议



- 裁决协议



- 自动执行协议

安全协议设计与分析概述

- 安全协议的背景介绍
- 安全协议概念及分类
- 安全协议面临的攻击
- 安全协议的安全性质
- 安全协议的设计原则
- 安全协议的分析方法

安全协议面临的攻击

- 攻击者能力
  - 1983年Dolev和Yao的工作
  - 假定**密码算法是安全**的基础上研究认证协议的安全性；
  - 给出了**安全协议的攻击模型**，强调对攻击者的知识和能力要有足够的估计，应该认为攻击者可以控制整个通信网络
  - 攻击者能力
    - 可以窃听所有经过网络的消息；
    - 可以阻止和截获所有经过网络的消息；
    - 可以存储所获得或自身创造的消息；
    - 可以根据存储的消息伪造消息，并发送该消息；
    - 可以作为合法的主体参与协议的运行。

安全协议面临的攻击

- 攻击者能力（续）
  - 密码学相关的知识能力：
    - 熟悉加解、解密、散列(hash)等密码运算，拥有自己的加密密钥和解密密钥；
    - 熟悉参与协议的主体标识符及其公钥；
    - 具有密码分析的知识和能力；
    - 具有进行各种攻击能力。

- 目前大部分有关安全协议的研究工作都遵循或借鉴了Dolev 和 Yao 的基本思想。

安全协议面临的攻击

▶ 典型攻击

攻击类型	攻击描述
窃听	攻击者获取所传输的信息。
篡改	攻击者更改发送的信息。
重放	攻击者记录传输的信息，然后在稍后将其发送给相同或不同的接收者。
预重放	攻击者在合法参与者运行之前参与一次协议的运行。
反射	攻击者将协议消息发送给消息的发送者。
拒绝服务	攻击者阻止合法参与方完成协议。
类型攻击	攻击者将协议运行中某一类（可能加密的）消息字段替换成其他类（可能加密）的协议消息字段。
密码分析	攻击者利用在协议运行中获得的消息有用信息来帮助实施密码分析。
证书操纵	攻击者选择或更改证书信息来攻击协议的运行。
协议交互	攻击者选择一个新的协议与已知的协议进行交互。
中间人	攻击者位于通信的中间，在参与方都未发现攻击者身份的情况下实施数据窃听和篡改的攻击类型。
并行会话	攻击者可以利用多个协议的并发运行过程中的一个运行中得到解决另外某个运行中困难问题的答案。

安全协议设计与分析概述

- 安全协议的背景介绍
- 安全协议概念及分类
- 安全协议面临的攻击
- 安全协议的安全性质
- 安全协议的设计原则
- 安全协议的分析方法

安全协议的安全性质

- 密码协议的安全属性集（目标集合）：
  - 保密性（Secrecy）
  - 认证性（Authenticity）
  - 完整性（Integrity）
  - 不可否认性（Non-Repudiation）
  - 公平性（Fairness）
  - 匿名性（Anonymity）
  - 可用性（Usability）
  - 可追究性（Accountability）
  - 原子性（Atomicity）
  - 。。。

- 一个安全协议需要提供的特性和服务只是以上安全属性集的子集，这取决于其具体的应用环境。
- 不存在“绝对安全”、“绝对正确”的安全协议。只是在某些假设环境中，对某几类特定的威胁是安全的。

重要的安全属性

1.保密性

- 含义：
  - 是指入侵者无法发现合法用户的任何活动。换言之，系统中高级用户的活动不会对系统的低级用户或外部观察者产生任何明显的影响。（严格）
  - 保护消息在传输过程中不会泄露给非授权拥有此消息的人（对大多数应用而言）
- 方法：实现安全协议保密性的最直接方法是对机密信息进行加密。

重要的安全属性

2.认证性

- **认证性**是最重要的安全性质之一，所有其他安全性质的实现都依赖于此性质的实现。
- **含义**：认证是一个过程，通过这个过程，一个主体向另一个主体证明某种声称的性质。
- **可细化为**：消息源认证、实体认证、认证的密钥建立。
  - **消息源认证**是指消息的接收者能验证消息所声称的源地址是其真正发出的地址，并进一步确认发出消息的时间值没被篡改过；
  - **实体认证**用于验证主体身份的真实性，即验证某个主体声称的身份是否与其真实身份一致。数据源认证机制是实现实体认证的一种有效方法。
  - **认证的密钥建立**通常与实体认证过程密切相关。主体间进行实体认证的目的在于能够进行安全通信，而密钥是安全信道的基础，所以在主体进行安全通信之前，通常也需要密钥建立过程（也称为密钥交换或密钥协商）。

重要的安全属性

3.完整性

- **含义**：通常是指数据不能被篡改，或者至少针对数据的任何篡改都能被检测出来。
- **目的**：保护消息不被未授权地篡改、删除或替代。可以理解为在储存或传输的数据上再加上一层防止篡改的保护层。
- **常用方法**：封装和签名。

重要的安全属性

4.不可否认性

- **含义**：不可否认性主要是考虑如何保护通信的一方不被对方欺骗，在协议执行过程中能够为用户提供证据，来证明协议中某些步骤确实发生过，而且这些证据是不可伪造的。
- 包含
  - **源发否认**，不能否认发送了信息
  - **接收否认**，不能否认接收了信息
- **不可否认性**是电子商务协议的一个重要性质，是保证交易正常进行的必要条件。
- 保证不可否认性最常用的技术是**数字签名**。

重要的安全属性

5. 公平性

- **目的**：公平的目的在于确保协议参与各方的地位和作用平等，参与各方所拥有的能力也是相同的。
- **含义**：对公平性可以直观地理解为在协议运行的任何时刻每一个参与者都不会得到特别的好处。或者说，没有一方可以得到自己要的证据却可以避免另一方得到相应的证据。
- **应用**：公平性常被用于电子商务、电子选举和电子投票事务当中。

重要的安全属性

6.匿名性

- 含义：匿名性是指保证消息接收者不知道发送者的身份。
- 直观上看，一个在某个事件集E匿名的系统将拥有的特性为：当事件集E中的一个事件发生时，从观察者的角度看，即使他可以推断出发生了事件集E中的一个事件，他也不能确定是哪个事件。

7. 可用性

- 含义：可用性是指在适当的假设下确定协议能够达到某些预定的目标。
- 说明：对于一个必须保证这些特性的系统而言，需要将入侵者的能力限定在某个范围内，不允许攻击者有破坏消息的无限能力。

重要的安全属性

8. 可追究性

- 含义：可追究性是指协议参与的各方必须对自己的行为负责，在协议执行完毕后，参与协议的任何一方主体必须提供充分的证据以解决今后可能出现的纠纷。

9. 原子性

- 目前，原子性主要体现在电子商务协议中。事务的原子性是数据库最基本的概念之一。
- T .D.Tygar于1996年在电子商务中引入了原子性的概念，分为以下3级，并且后者包含前者。
  - 钱原子性
  - 商品原子性
  - 确认发送原子性

安全协议设计与分析概述

- 安全协议的背景介绍
- 安全协议概念及分类
- 安全协议面临的攻击
- 安全协议的安全性质
- 安全协议的设计原则
- 安全协议的分析方法

安全协议的设计原则

Martin Abadi和Roger Needham

提出的设计原则

1. 消息独立完整性原则
2. 消息前提准确原则
3. 主体身份标识原则
4. 加密目的原则
5. 签名原则
6. 随机数的使用原则
7. 可预测值使用原则
8. 密钥新鲜性原则
9. 时戳的使用原则
10. 编码原则

其他设计原则

1. 高效原则
2. 安全假设尽量少原则
3. 算法无关原则
4. 抵抗常见攻击原则
5. 消息简单原则
6. 。 。 。

安全协议设计与分析概述

- 安全协议的背景介绍
- 安全协议概念及分类
- 安全协议面临的攻击
- 安全协议的安全性质
- 安全协议的设计原则
- 安全协议的分析方法

安全协议的分析

- 将安全协议及其所处的环境视为一个系统，那么在这个系统中，一般包括发送和接收信息的诚实主体和一个攻击者（把所有的攻击者都看做一个团伙），以及消息发送和接收的规则，如图所示。

图 安全协议系统模型

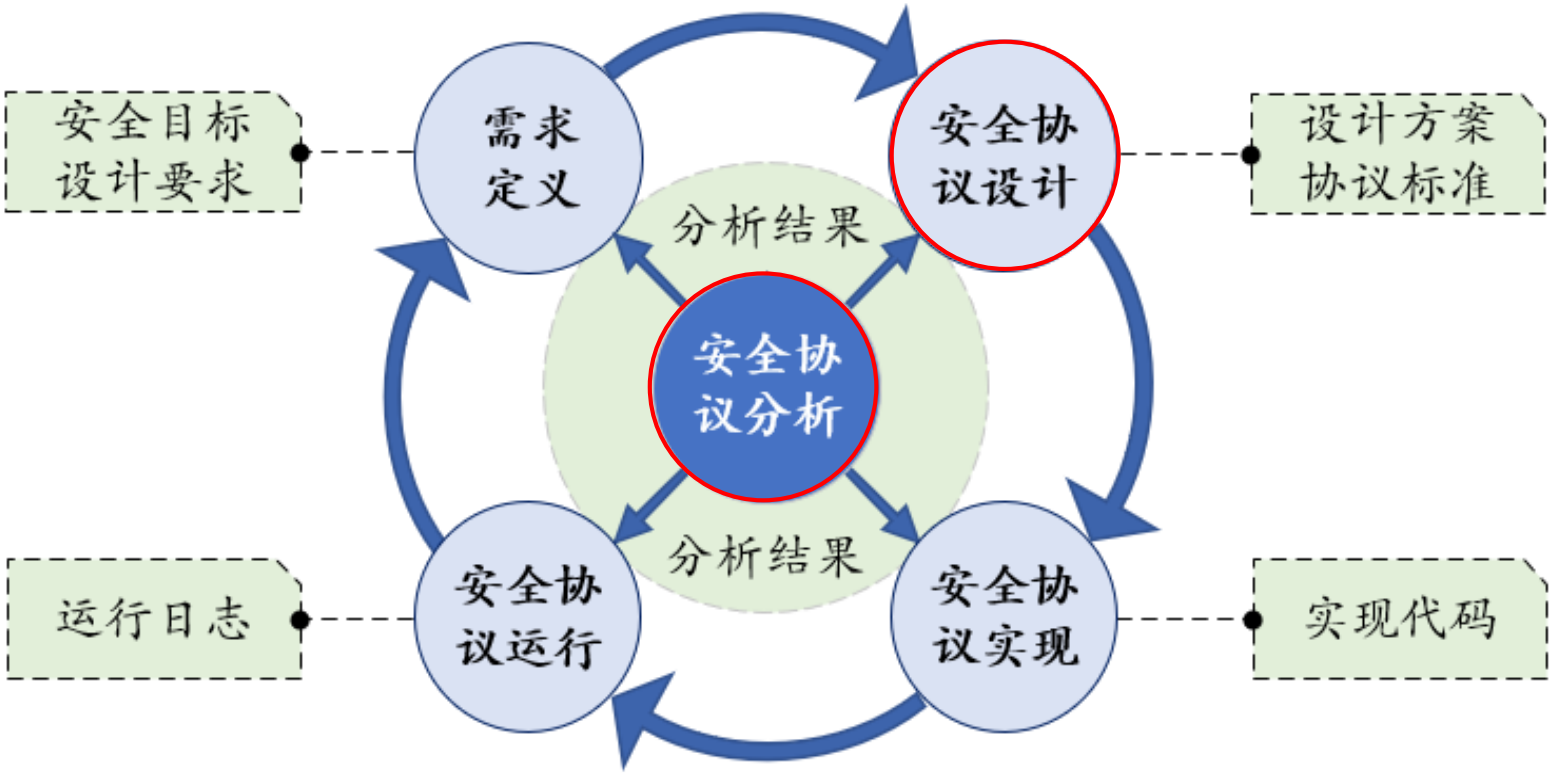
安全协议的分析

- 网络通信环境是安全协议运行的物理基础
  - 刻画安全协议的运行环境和形式化描述攻击者的能力比较困难。
  - 安全协议运行环境的异常复杂性也是导致安全协议的设计和分析比较困难的原因之一。
- **安全协议的分析方法**
  - 安全协议的人工分析
    - 依赖人工经验，分析查找安全协议缺陷
  - 安全协议的形式化分析
    - 最主要的问题在于评价和模拟这个环境，对网络中存在的攻击者的模型具体化。

安全协议分析方法

- 基于**逻辑推理**的分析方法
  - 形式化协议的安全目标、前提和协议过程，定义推理规则，利用推理规则进行推理，得到新的信仰，判断目标是否满足。
- 基于**模型检验**的分析方法
  - 从协议初始状态开始，对所有可能的执行路径进行状态搜索，查找是否存在错误状态。
- 基于**定理证明**的分析方法
  - 对形式化后的协议模型和规约运用证明的技术来证明规约是否在协议模型中满足。
- 密码学可证明安全性分析方法
  - 利用现代密码学中的可证明安全性的理论，在复杂性理论的框架下把协议的安全性规约到某特定的已知难题上，给出特定框架下的安全协议的安全性证明。

安全协议的生命周期


安全目标
设计要求
需求
定义
安全协
议设计
设计方案
协议标准
分析结果
安全协
议分析
分析结果
运行日志
安全协
议运行
安全协
议实现
实现代码

内容总结

- 安全协议的背景介绍
- 安全协议概念及分类
- 安全协议面临的攻击
- 安全协议的安全性质
- 安全协议的设计原则
- 安全协议的分析方法

主要参考书

- 《安全协议设计与分析》李晖、王晨宇编著，预计11月底
- 《安全协议模型与设计》 刘天华、朱宏峰 著
- 《网络安全协议的形式化分析与验证》 李建华主编
- 《无线通信安全》李晖编著
- 《安全协议形式化分析与验证》肖美华编著
- 《安全协议—理论与方法》 范红、冯登国编著
- 《安全协议—实施自动化生成与验证》 孟博、王德军著

谢谢大家！欢迎提问！