安全协议设计与分析：
第九讲

基于逻辑推理的分析方法

- 李晖
- 网络空间安全学院

内容提纲

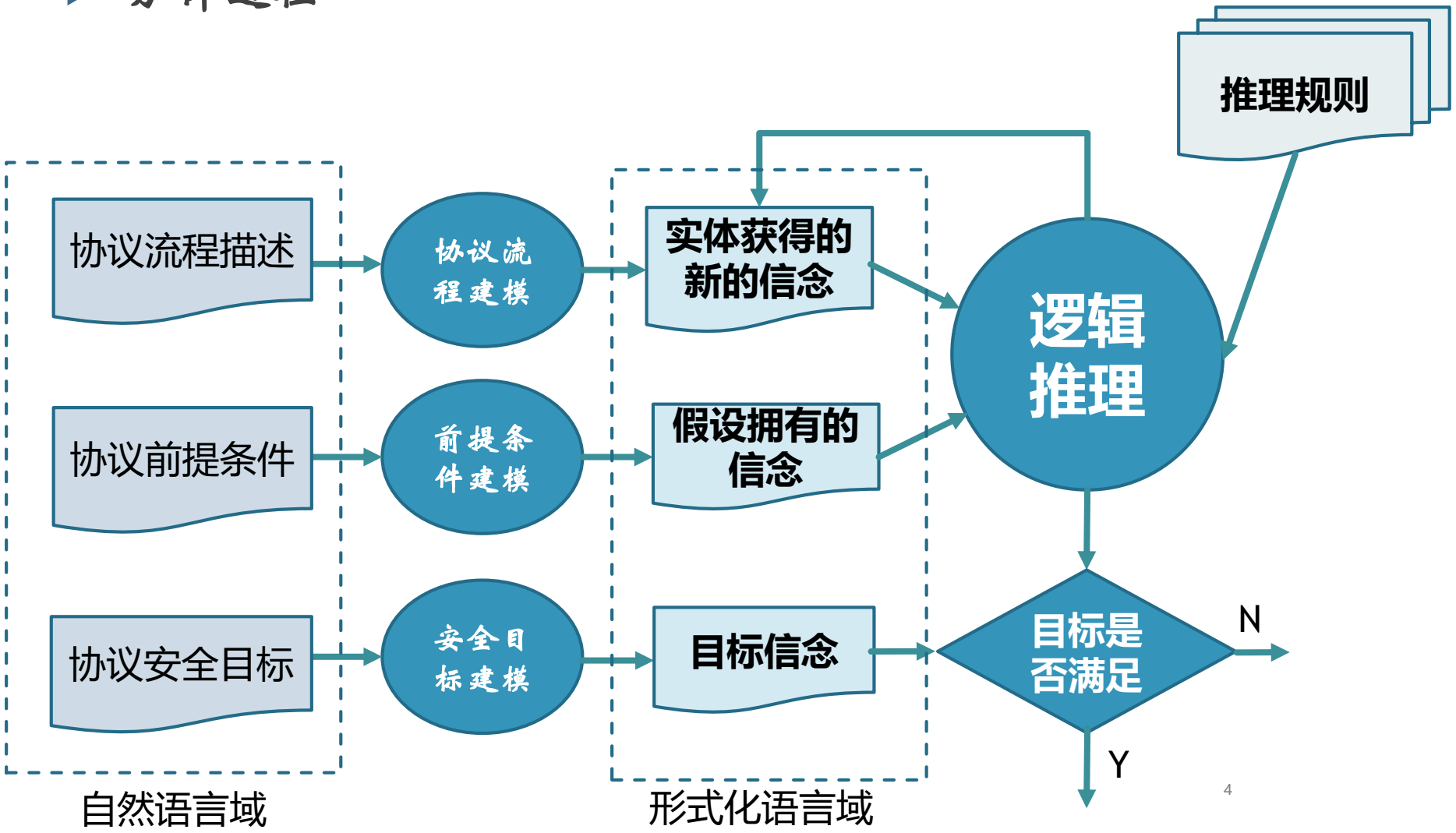
- 基于逻辑推理的分析方法基本原理
- 主要的基于逻辑推理的分析方法
- 典型方法：BAN
  - 基本术语
  - 推理规则
  - 应用实例

基于逻辑推理的分析方法基本原理

- 最早提出的安全协议分析方法，称为**逻辑化方法**，也称为**认证逻辑**
- 基本思想
  - 针对密码协议的背景给出若干基本的**逻辑公理和规则**
  - 针对密码协议的背景给出若干基本的分析前提，称为**假设**
  - 将协议过程和安全目标转化为逻辑公式，称为**协议理想化**
  - 根据逻辑公理使用逻辑规则**进行推理**，看是否能从协议过程推导出安全目标
    - 如果能够推理出表示协议的**目标逻辑公式**，则认为协议是**安全的**
    - 否则认为协议**不安全**，存在**安全漏洞**

基于逻辑推理的分析方法

分析过程



内容提纲

- 基于逻辑推理的分析方法基本原理
- 主要的基于逻辑推理的分析方法
- 典型方法：BAN
  - 基本术语
  - 推理规则
  - 应用实例

主要的基于逻辑推理的分析方法

- BAN逻辑
  - 由Michael Burrows, Mart´ın Abadi和 Roger Needham提出
  - 开辟了密码协议安全性分析的新方向
  - 最初的BAN逻辑存在一些缺陷

Martín Abadi

Roger Needham (1935-2003)

- BAN类逻辑
  - 国外的
    - GNY逻辑、AT逻辑、SVO逻辑、AUTOLOG逻辑、Kailar逻辑、Rubin逻辑等
  - 国内的
    - ZWW逻辑、SPALL逻辑等

内容提纲

- 基于逻辑推理的分析方法基本原理
- 主要的基于逻辑推理的分析方法
- 典型方法：BAN
  - 基本术语
  - 推理规则
  - 应用实例

BAN-基本术语

- BAN逻辑的处理对象包括：
  - 主体（Principals）：如 P、Q、R等
  - 密钥（Keys）：如 K等
  - 公式（Formula），如X、Y等。
- 设A、B表示两个普通主体，S表示认证服务器，则
  - K_{AB}、K_{AS}、K_{BS}表示具体的共享密钥
  - K_A、K_B表示具体的公钥，
  - K_A^{-1}、K_B^{-1}表示相应的私钥，
  - N_A、N_B表示随机值。
  - h(X)表示X的单向散列函数。

BAN-基本术语

- BAN逻辑包含一个**联接词**，用逗号表示；
- 除此之外，它还定义了以下**语法构件**：
  - P|≡X：P相信X，即主体P相信命题X是正确的。
  - P◁X：P看到X，即主体P接收到了包含X的消息，P能读出并重复。
  - P|~X：P曾经说过X，即P曾经发送过一条包含X的消息，并且在发送时，P是相信X的。
  - P|⇒X：P对X有仲裁权，即P对命题X具有权威性，别的主体对此都信服。
  - #(X)：X是新鲜的，即X是本轮协议运行过程中产生的新鲜随机数。

BAN-基本术语

- $P \overset{K}{\longleftrightarrow} Q$：K是P与Q的共享密钥，并且除P、Q及他们所信任的主体之外，其他主体都不知道该密钥。
- $\overset{K}{\longmapsto} P$：P的公钥为K，且除P及他所信任的主体之外，其他主体都不知道对应的私钥K^{-1}。
- $P \overset{X}{\Leftrightarrow} Q$：X为P和Q的共享秘密，且除P和Q以及他们所信任的主体之外，其他主体都不知道X。
- $\{X\}_K$：用密钥K加密X后得到的密文。
- $\langle X \rangle_Y$ 或者 $(X)_Y$：消息X和秘密Y的级联。这里主要是利用Y来证明发出消息<X>Y的主体的身份。

BAN-推理规则

1. 消息意义规则

目的：从加密消息所用的密钥/秘密来判断消息发送者的身份。

R1：
$$\frac{P \mid\equiv Q \overset{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

如果P相信K为P和Q的共享密钥，且P接收到用K加密的X的密文消息$\{X\}_K$，则P相信Q曾发送过消息X。

R2:
$$\frac{P \mid\equiv \overset{K}{\mapsto} Q, P \triangleleft \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$$

R3：
$$\frac{P \mid\equiv Q \overset{Y}{\Leftrightarrow} P, P \triangleleft \{X\}_Y}{P \mid\equiv Q \mid\sim X}$$

BAN-推理规则

2. 随机数验证规则

R4：$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

如果P相信X是新鲜的，且P相信Q曾经发送过X，则P相信Q相信X。

3. 仲裁规则

R5：$$\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

如果P相信Q对X有仲裁权，并且P相信Q相信X，则P也相信X。

BAN-推理规则

4. 信仰规则： 反映了信仰在消息的级联与分割的不同操作中具有一致性及传递性。

R6： $$\frac{P \mid\equiv (X, Y)}{P \mid\equiv X}$$

如果P相信总体，则P也相信局部。

R7： $$\frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)}$$

如果P相信所有局部，则P也相信总体。

R8: $$\frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X}$$

如果P相信Q相信总体，则P相信Q也相信局部。

R9： $$\frac{P \mid\equiv Q \mid\sim (X, Y)}{P \mid\equiv Q \mid\sim X}$$

如果P相信Q说过总体，则P相信Q也说过局部。

BAN-推理规则

5、消息接收规则： 定义了主体在协议运行中对消息的获取能力。

R10：$$\frac{P \triangleleft (X, Y)}{P \triangleleft X}$$

R11：$$\frac{P \triangleleft (X)_Y}{P \triangleleft X}$$

R12：$$\frac{P \overset{K}{\mid\equiv} Q \leftrightarrow P, P \triangleleft \{X\}_K}{P \triangleleft X}$$

R13：$$\frac{P \overset{K}{\mid\equiv} \mapsto P, P \triangleleft \{X\}_K}{P \triangleleft X}$$

R14：$$\frac{P \overset{K}{\mid\equiv} \mapsto Q, P \triangleleft \{X\}_{K^{-1}}}{P \triangleleft X}$$

BAN-推理规则

6、消息新鲜性规则

R15：$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$$

如果P相信X是新鲜的，那么P相信与X级联的整个消息都是新鲜的。

7、密钥与秘密对称规则

R16：$$\frac{P \mid\equiv R \overset{K}{\leftrightarrow} R'}{P \mid\equiv R' \overset{K}{\leftrightarrow} R}$$

R17：$$\frac{P \mid\equiv Q \mid\equiv R \overset{K}{\leftrightarrow} R'}{P \mid\equiv Q \mid\equiv R' \overset{K}{\leftrightarrow} R}$$

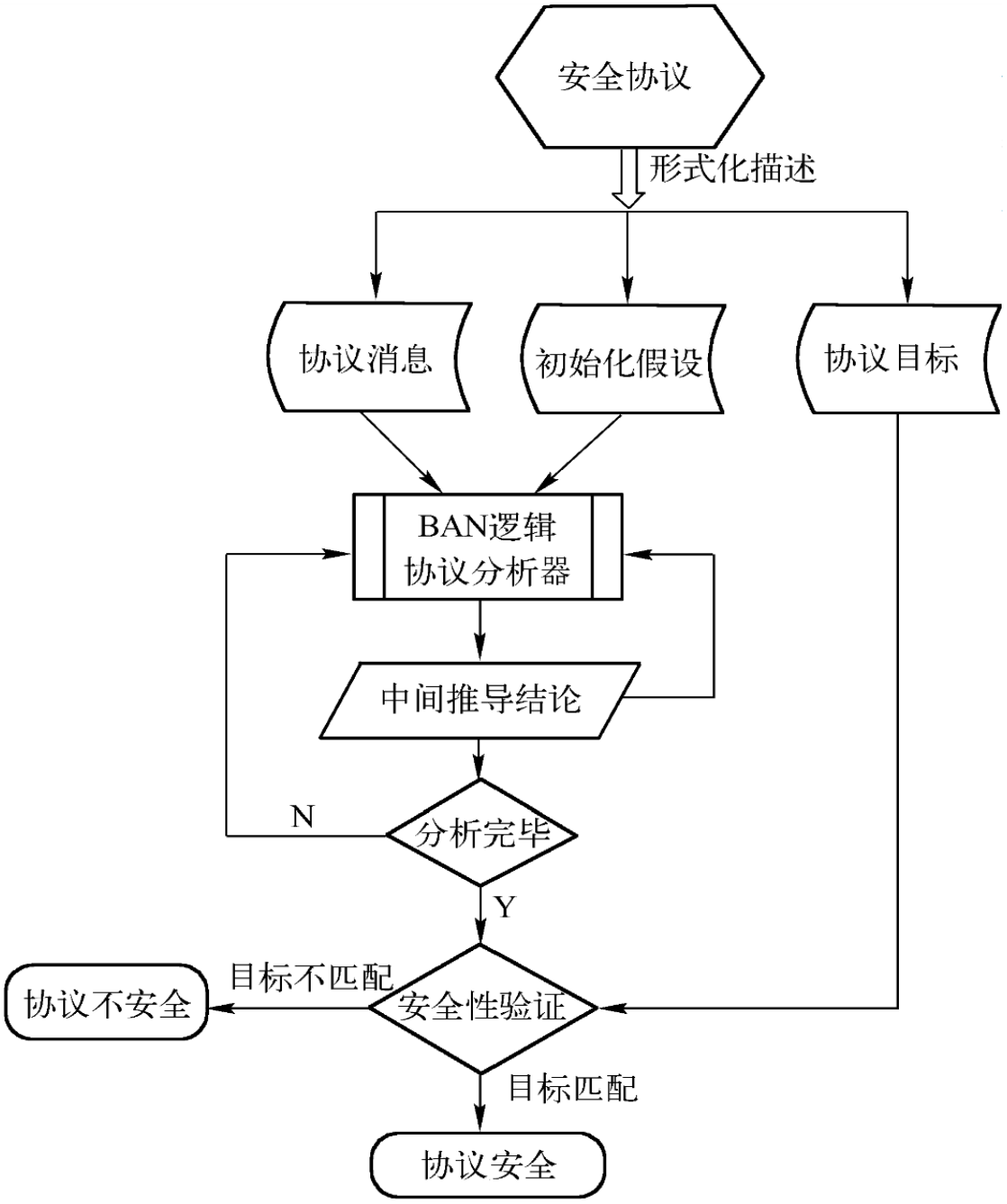
R18：$$\frac{P \mid\equiv R \overset{X}{\Leftrightarrow} R'}{P \mid\equiv R' \overset{X}{\Leftrightarrow} R}$$

R19：$$\frac{P \mid\equiv Q \mid\equiv R \overset{X}{\Leftrightarrow} R'}{P \mid\equiv Q \mid\equiv R' \overset{X}{\Leftrightarrow} R}$$

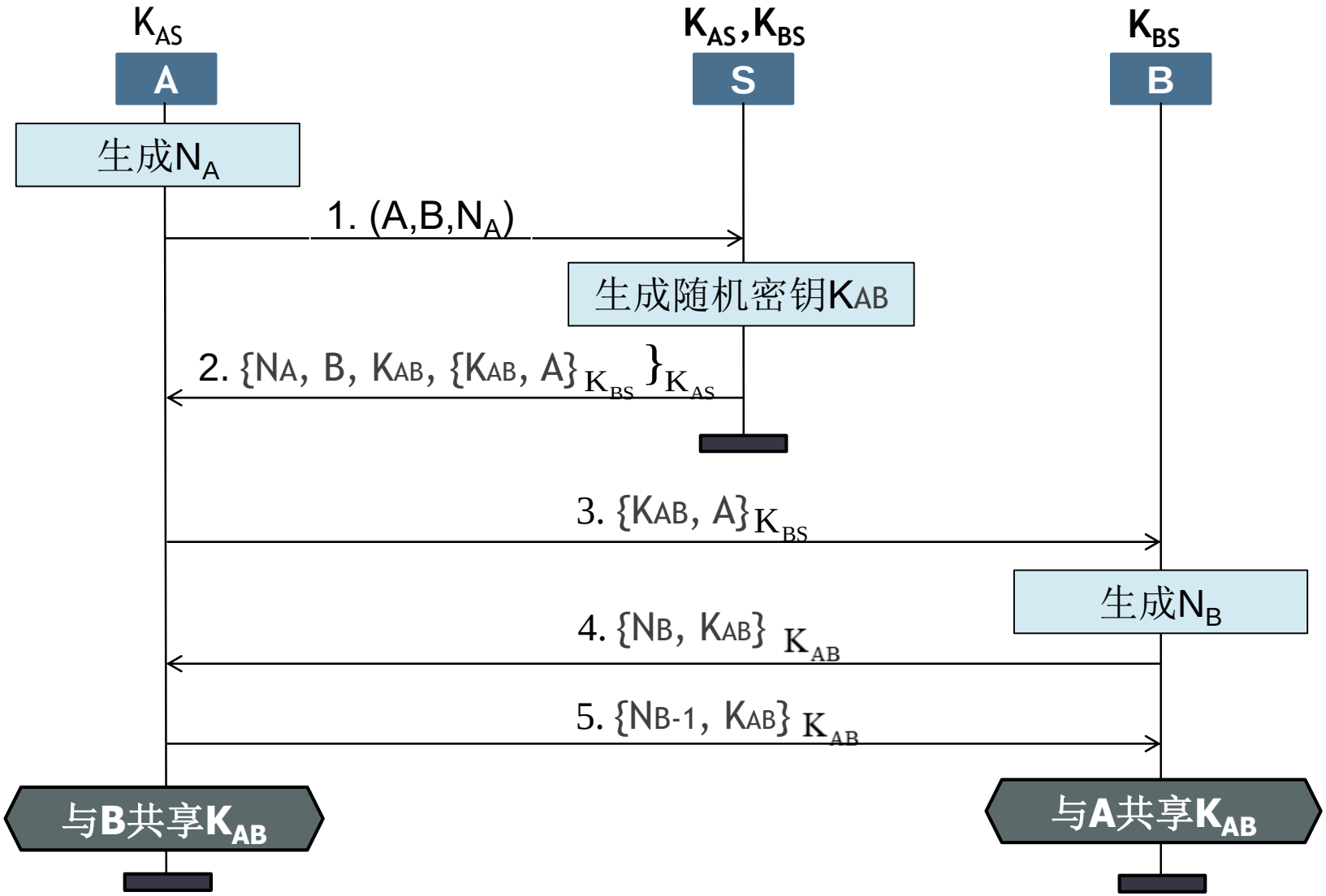
BAN-应用实例

BAN逻辑分析过程：

1. 协议的形式化描述
2. 定义初始化假设
3. 定义协议目标
4. 推理及验证



NSSK协议（参考文献1）



BAN-应用实例

Needham-Schroeder 协议过程如下：

(1) $A \rightarrow S: A, B, N_A$

(2) $S \rightarrow A: \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$

(3) $A \rightarrow B: \{K_{AB}, A\}_{K_{BS}}$

(4) $B \rightarrow A: \{N_B, K_{AB}\}_{K_{AB}}$

(5) $A \rightarrow B: \{N_B\text{-}1, K_{AB}\}_{K_{AB}}$

BAN-应用实例

BAN逻辑分析过程

1、协议的形式化描述(理想化过程)

M2: $S \rightarrow A$: $\{N_A, \overset{K_{AB}}{(A \leftrightarrow B)}, \#\overset{K_{AB}}{(A \leftrightarrow B)}, \overset{K_{AB}}{(A \leftrightarrow B)}_{K_{BS}}\}_{K_{AS}}$

M3: $A \rightarrow B$: $\overset{K_{AB}}{(A \leftrightarrow B)}_{K_{BS}}$

M4: $B \rightarrow A$: $\{N_B, \overset{K_{AB}}{(A \leftrightarrow B)}\}_{K_{AB}}$ from B

M5: $A \rightarrow B$: $\{N_B, \overset{K_{AB}}{(A \leftrightarrow B)}\}_{K_{AB}}$ from A

BAN-应用实例

2、初始化假设

——关于密钥的有效性：

A1: $A \mid\equiv A \overset{K_{AS}}{\leftrightarrow} S$

A2: $B \mid\equiv B \overset{K_{BS}}{\leftrightarrow} S$

A3: $S \mid\equiv A \overset{K_{AS}}{\leftrightarrow} S$

A4: $S \mid\equiv B \overset{K_{BS}}{\leftrightarrow} S$

A5: $S \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$

——关于S的可信性：

A6: $A \mid\equiv (S \mid\Rightarrow A \overset{K_{AB}}{\leftrightarrow} B)$

A7: $B \mid\equiv (S \mid\Rightarrow A \overset{K_{AB}}{\leftrightarrow} B)$

A8: $A \mid\equiv (S \mid\Rightarrow \#(A \overset{K_{AB}}{\leftrightarrow} B))$

——关于随机数的新鲜性：

A9: $A \mid\equiv \#(N_A)$

A10: $B \mid\equiv \#(N_B)$

A11: $S \mid\equiv \#(A \overset{K_{AB}}{\leftrightarrow} B)$

A12: $B \mid\equiv \#(A \overset{K_{AB}}{\leftrightarrow} B)$

BAN-应用实例

3、协议目标的形式化描述

自然语言描述的目标：A和B分别确认K_{AB}是A和B共享的密钥；
同时A和B分别确认对方知道K_{AB}；

BAN逻辑描述的目标：

G1: $A \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$

G2: $B \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$

G3: $A \mid\equiv B \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$

G4: $B \mid\equiv A \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B$

BAN-应用实例

R4: $\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$

4、逻辑推理及验证

由M2可知，$A \triangleleft \{N_A, (A \overset{K_{AB}}{\leftrightarrow} B), \#(A \overset{K_{AB}}{\leftrightarrow} B), (A \overset{K_{AB}}{\leftrightarrow} B)_{K_{BS}}\}_{K_{AS}}$，又由初始化假设A1，应用消息意义规则R1，可得

$$A \mid\equiv S \mid\sim (N_A, A \overset{K_{AB}}{\leftrightarrow} B, \#(A \overset{K_{AB}}{\leftrightarrow} B), (A \overset{K_{AB}}{\leftrightarrow} B)_{K_{BS}}) \qquad (2\text{-}1)$$

再由初始化假设A9，应用随机数验证规则R4，可得

$$A \mid\equiv S \mid\equiv (N_A, A \overset{K_{AB}}{\leftrightarrow} B, \#(A \overset{K_{AB}}{\leftrightarrow} B), (A \overset{K_{AB}}{\leftrightarrow} B)_{K_{BS}}) \qquad (2\text{-}2)$$

应用信仰规则R8，可得

$$A \mid\equiv S \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B, \qquad A \mid\equiv S \mid\equiv \#(A \overset{K_{AB}}{\leftrightarrow} B) \qquad (2\text{-}3)$$

BAN-应用实例

R5：$\dfrac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

由初始化假设A6、A8以及式（2-3），应用仲裁规则R5，得

G1 → $$A|\equiv A\overset{K_{AB}}{\leftrightarrow}B, \quad A|\equiv \#(A\overset{K_{AB}}{\leftrightarrow}B) \tag{2-4}$$

由M3可知，$B \lhd (A\overset{K_{AB}}{\leftrightarrow}B)_{K_{BS}}$，由初始化假设A2，应用消息意义规则R1，可得

$$B|\equiv S|\sim A\overset{K_{AB}}{\leftrightarrow}B \tag{2-5}$$

再由初始化假设A12，应用随机数验证规则R4，可得

$$B|\equiv S|\equiv A\overset{K_{AB}}{\leftrightarrow}B \tag{2-6}$$

再由初始化假设A7，应用仲裁规则R5，可得

G2 → $$B|\equiv A\overset{K_{AB}}{\leftrightarrow}B \tag{2-7}$$

BAN-应用实例

R9：
$$\frac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$$

通过M4、M5，主体A、B均确信对方在线。由M4可知

$$A \triangleleft \{N_B,(A \overset{K_{AB}}{\leftrightarrow} B)\}_{K_{AB}} \text{ from } B$$

由式（2-4）可知A相信K_{AB}，应用消息意义规则R1，可得

$$A \mid\equiv B \mid\sim (N_B, A \overset{K_{AB}}{\leftrightarrow} B) \qquad (2\text{-}8)$$

再由信仰规则R9，可得

$$A \mid\equiv B \mid\sim (A \overset{K_{AB}}{\leftrightarrow} B) \qquad (2\text{-}9)$$

由式（2-4）中K_{AB}新鲜，根据随机数验证规则R4，可得

G3 →
$$A \mid\equiv B \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B \qquad (2\text{-}10)$$

同样，由M5可知，经过类似推理，可得

G4 →
$$B \mid\equiv A \mid\equiv A \overset{K_{AB}}{\leftrightarrow} B \qquad (2\text{-}11)$$

BAN-应用实例

由上述推导过程中的式（2-4）、式（2-7）、式（2-10）及式（2-11）可知，**在12个假设条件均满足的情况下**，协议达到了预期目标。

而为了推证协议满足目标G2，必须借助于初始化假设A12，即B相信会话密钥K_{AB}是新鲜的，而这一假设是不合理的，因为B无从获知K_{AB}是否新鲜。因此该协议可能受到重放攻击。

BAN逻辑的形式化过程也为协议的改进提供了方向。

BAN的影响

- 第一种协议规范语言，开辟了协议安全性分析的新途径
- BAN引入了一种简单而强大的表示法，推理方法简单，推理过程较为简单
- 使用BAN逻辑分析常用密码协议时，确实发现了一些协议是不安全的，具有实用性

BAN的局限性

- BAN语义不够清晰
  - 所以BAN逻辑很难对协议本身所包含的信息和协议的目标作出精确的刻画，而目标的不精确又带来了分析结果的不清晰
- BAN的理想化过程可能会产生问题
  - 使得理想化后的协议与原协议不一致，导致分析结果不准确
- BAN逻辑的公理也存在一些问题
  - 从实际应用来看，**BAN逻辑证明了一些协议是安全的，但后来却被发现存在安全漏洞**，实际上是不安全的；也就是用BAN发现了问题，那么人们确信协议是不安全的，用BAN证明安全的协议，却不能令人信服其安全性。

思考题

- 采用BAN方法分析3G-AKA协议。

参考文献

1. Michael Burrows, Mart´ın Abadi, and Roger Needham. A logic of authentication. Research Report 39, Digital Systems Research Center, February 1989. Revised Feb. 22, 1990.

谢谢大家！欢迎提问！