Formal Methods (Logics)

Jeannette M. Wing

15-827 Security and Cryptography
15 October 1997

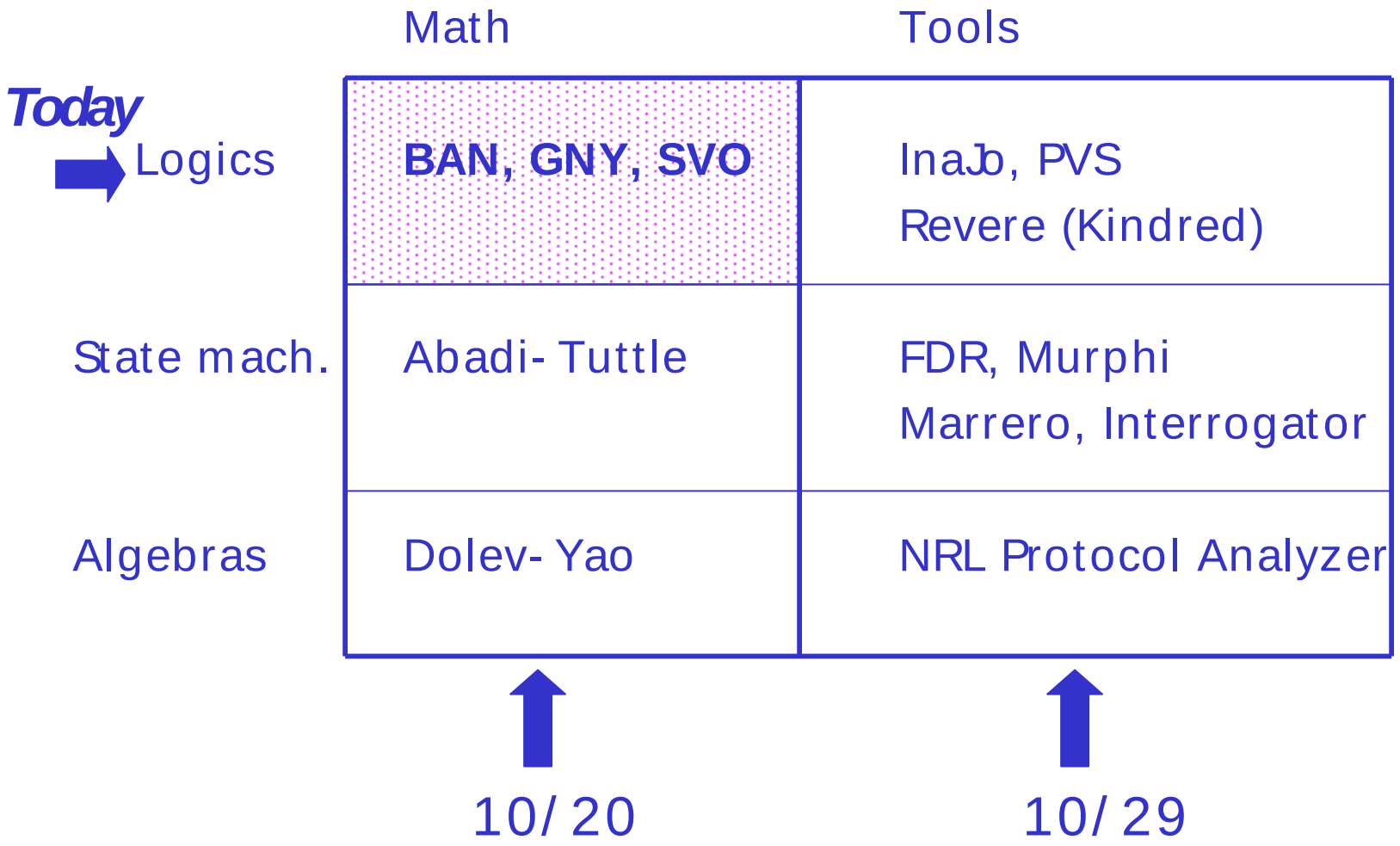
Plan for Today

- Intro
- BAN logic
- BAN in action
  - Otway-Rees
  - Needham-Schroeder
- Summary of BAN analyses
- Interlude
- BAN controversy
- BAN variants
  - GNY
  - SVO

Goals for Today

- What is BAN? How do you use it?
- What are its strengths?
- What are its weaknesses?

Taxonomy of Approaches



Assumptions

- Perfect encryption.
- Trusted parties are trustworthy.
- No failures (in the sense of distributed systems theory).

Intuitively

- If you've sent Joe a number that you have never used for this purpose before and if you subsequently receive from Joe something that depends on knowing that number, then you ought to **believe** that Joe's message *originated recently* - - in fact, after yours.
- If you **believe** that only you and Joe know K, then you ought to **believe** that anything you receive encrypted with K as key comes *originally from Joe*.
- If you **believe** that K is Joe's public key, then you should **believe** that any message that you can decrypt with K comes *originally from Joe.*
- If you **believe** that only you and Joe know X, then you ought to **believe** that any encrypted message you receive containing X comes *originally from Joe*.

Basic Notation

Principals	P, Q, R	A, B, S
Keys	K	K_{ab}, K_a, K_a^{-1}
Formulae/ Statements	X, Y	N_a, $\{X\}_K$, $<X>_Y$

BAN Constructs (I)

P **believes** X — $(P \models X)$. P believes, or would be entitled to believe, X.

P may act as though X is true.

P **sees** X — $(P \triangleleft X)$. Someone has sent P a message containing X.

P can read X and can repeat it in other messages.

P **said** X — $(P \mid\sim X)$. P at some time sent a message containing X.

It is not known whether the message was sent long ago or during the current run of the protocol.

P believed X when he sent it.

BAN Constructs (II)

P **controls** X — (P $\Rightarrow$ X). P has *jurisdiction* over X. P is an authority on X and should be trusted on this matter.

E.g., a server is trusted to generate keys properly.

fresh(X) — #(X). X has not been sent in a message at any time before the current run of the protocol.

P $\overset{K}{\leftrightarrow}$ Q — P and Q may use the *shared* key K to communicate.

$\overset{K}{\mapsto}$ P — P has K as a *public* key.

BAN Constructs (III)

$P \overset{X}{\rightleftharpoons} Q$ — The formula X is a secret known only to P and Q, and possibly to principals trusted by them.

Only — P and Q may use X, e.g., a password, to prove their identities to one another.

$\{X\}_K$ — X encrypted under key K. Formally, $\{X\}_K$ *from P*.

Assume each principal can recognize and ignore his own messages.

$\langle X \rangle_Y$ — X combined with formula Y; Y is intended to be a secret and its presence proves the identity of whoever utters $\langle X \rangle_Y$. In concrete protocols, X is just concatenated with password Y.

BAN Rules (I): Message-Meaning Rules

a. Shared keys:

$$\frac{P \textbf{ believes } Q \overset{K}{\leftrightarrow} P, \quad P \textbf{ sees } \{X\}_K}{P \textbf{ believes } Q \textbf{ said } X}$$

b. Public keys:

$$\frac{P \textbf{ believes } \overset{K}{\mapsto} Q, \quad P \textbf{ sees } \{X\}_{K^{-1}}}{P \textbf{ believes } Q \textbf{ said } X}$$

c. Shared secrets:

$$\frac{P \textbf{ believes } Q \overset{Y}{\rightleftharpoons} P, \quad P \textbf{ sees } \langle X \rangle_Y}{P \textbf{ believes } Q \textbf{ said } X}$$

BAN Rules (II)

Nonce-Verification Rule

$$\frac{P \textbf{ believes fresh}(X),\quad P \textbf{ believes } Q \textbf{ said } X}{P \textbf{ believes } Q \textbf{ believes } X}$$

Jurisdiction Rule

$$\frac{P \textbf{ believes } Q \textbf{ controls } X,\quad P \textbf{ believes } Q \textbf{ believes } X}{P \textbf{ believes } X}$$

BAN Rules (III): Message Rules

$$\frac{P \textbf{ believes } X,\ P \textbf{ believes } Y}{P \textbf{ believes } (X,\ Y)}$$

$$\frac{P \textbf{ believes } (X,\ Y)}{P \textbf{ believes } X}$$

$$\frac{P \textbf{ believes } Q \textbf{ believes } (X,\ Y)}{P \textbf{ believes } Q \textbf{ believes } X}$$

$$\frac{P \textbf{ believes } Q \textbf{ said } (X,\ Y)}{P \textbf{ believes } Q \textbf{ said } X}$$

~~$$\frac{P \textbf{ believes } Q \textbf{ said } X,\ P \textbf{ believes } Q \textbf{ said } Y}{P \textbf{ believes } Q \textbf{ said } (X,\ Y)}$$~~

BAN Rules (IV): Sees Rules

$$\frac{P \textbf{ sees } (X,\ Y)}{P \textbf{ sees } X} \qquad \cancel{\frac{P \textbf{ sees } X,\ P \textbf{ sees } Y}{P \textbf{ sees } (X,\ Y)}} \qquad \frac{P \textbf{ sees } \langle X \rangle_Y}{P \textbf{ sees } X}$$

$$\frac{P \textbf{ believes } Q \overset{K}{\leftrightarrow} P,\ \ P \textbf{ sees } \{X\}_K}{P \textbf{ sees } X}$$

$$\frac{P \textbf{ believes } \overset{K}{\mapsto} P,\ \ P \textbf{ sees } \{X\}_K}{P \textbf{ sees } X}$$

$$\frac{P \textbf{ believes } \overset{K}{\mapsto} Q,\ \ P \textbf{ sees } \{X\}_{K^{-1}}}{P \textbf{ sees } X}$$

BAN Rules (V): Freshness Rule

$$\frac{P \textbf{ believes fresh}(X)}{P \textbf{ believes fresh}(X, Y)}$$

BAN Rules (VI): Other Rules

- Other freshness rules
- The same key is used between a pair of principals in either direction.
- A secret can be used between a pair of principals in either direction.

Idealized Protocols

Transform each concrete protocol step into an idealized form:

$A \rightarrow B: \{A, K_{ab}\}_{K_{bs}}$

$A \rightarrow B: \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$

When this message is sent to B, we may deduce that

B **sees** $\{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$

Using the BAN Logic

1. Derive idealized protocol from original one.
2. State assumptions about initial state.
3. Attach logical formulae to each statement of the protocol, as assertions about the state of the system after each statement.
4. Apply logical rules to assumptions and assertions, in order to discover the beliefs held by parties in the protocol.
5. Conclude what beliefs are held at the end of the protocol.

[*assumptions*] S_1 [*assertion* 1] … [*assertion n*- 1] S_n [*conclusions*]

Authentication Goals

A **believes** A $\overset{K}{\leftrightarrow}$ B

B **believes** A $\overset{K}{\leftrightarrow}$ B

and maybe also

A **believes** B **believes** A $\overset{K}{\leftrightarrow}$ B

B **believes** A **believes** A $\overset{K}{\leftrightarrow}$ B

Otway-Rees [1987]

1. A -> B: $M, A, B, \{N_a, M, A, B\}_{K_{as}}$

2. B -> S: $M, A, B, \{N_a, M, A, B\}_{K_{as}}, \{N_b, M, A, B\}_{K_{bs}}$

3. S -> B: $M, \{N_a, K_{ab}\}_{K_{as}}, \{N_b, K_{ab}\}_{K_{bs}}$

4. B -> A: $M, \{N_a, K_{ab}\}_{K_{as}}$

Otway-Rees Idealized

1. A -> B: $\{N_a, N_c\}_{K_{as}}$

2. B -> S: $\{N_a, N_c\}_{K_{as}}, \{N_b, N_c\}_{K_{bs}}$

3. S -> B: $\{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), (B \text{ said } N_c)\}_{K_{as}}$,
   $\{N_b, (A \overset{K_{ab}}{\leftrightarrow} B), (A \text{ said } N_c)\}_{K_{bs}}$,

4. B -> A: $\{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), (B \text{ said } N_c)\}_{K_{as}}$

Assumptions

A **believes** A $\overset{K_{as}}{\longleftrightarrow}$ S

S **believes** A $\overset{K_{as}}{\longleftrightarrow}$ S

B **believes** B $\overset{K_{bs}}{\longleftrightarrow}$ S

S **believes** B $\overset{K_{bs}}{\longleftrightarrow}$ S

S **believes** A $\overset{K_{ab}}{\longleftrightarrow}$ B

A **believes** (S **controls** A $\overset{K}{\longleftrightarrow}$ B)

B **believes** (S **controls** A $\overset{K}{\longleftrightarrow}$ B)

A **believes** (S **controls** B **said** X)) B **believes** (S **controls** A **said** X))

A **believes fresh**(N_a)

B **believes fresh**(N_b)

A **believes fresh**(N_c)

Otway-Rees Analysis

[Assumptions (from previous slide)]

1. A -> B: $\{N_a, N_c\}_{K_{as}}$

*[B **sees** $\{N_a, N_c\}_{K_{as}}$]*

2. B -> S: $\{N_a, N_c\}_{K_{as}}, \{N_b, N_c\}_{K_{bs}}$

*[S **believes** A **said** (N_a, N_c); S **believes** B **said** (N_b, N_c)]* *% message-meaning*

3. S -> B: $\{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), (B \text{ said } N_c)\}_{K_{as}}$,
   $\{N_b, (A \overset{K_{ab}}{\leftrightarrow} B), (A \text{ said } N_c)\}_{K_{bs}}$,
4. B -> A: $\{N_a, (A \overset{K_{ab}}{\leftrightarrow} B), (B \text{ said } N_c)\}_{K_{as}}$

*[A **believes** A $\overset{K_{ab}}{\leftrightarrow}$ B, B **believes** A $\overset{K_{ab}}{\leftrightarrow}$ B,* *% message-meaning, nonce-*
*A **believes** B **believes** N_c, B **believes** A **said** N_c]* *% verification, jurisdiction*

What BAN Say We Learn From the Analysis

- Protocol doesn't use K_{ab} as an encryption key.
  - Implies A nor B knows whether K_{ab} is known to the other.
    - A was told that B sent a message containing a nonce that A believes to be fresh; so A can infer that B has sent a message recently.
    - B was told that A has used a nonce but has no idea of whether it is a replay of an old message or not.
- Redundancy
  - Two nonces by A; no need for N_a (just use N_c).
  - N_b need not be encrypted in second message.

Needham-Schroeder [1978]

1. A -> S: A, B, N_a
2. S -> A: $\{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. A -> B: $\{K_{ab}, A\}_{K_{bs}}$
4. B -> A: $\{N_b\}_{K_{ab}}$
5. A -> B: $\{N_b - 1\}_{K_{ab}}$

Idealized Needham-Schroeder

[Message 1 irrelevant.]

2. S -> A: $\{N_a, A \overset{K_{ab}}{\leftrightarrow} B, fresh(A \overset{K_{ab}}{\leftrightarrow} B), \{A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$

3. A -> B: $\{A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}$

4. B -> A: $\{N_b, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{ab}}$ *from B*

5. A -> B: $\{N_b, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{ab}}$ *from A*

Assumptions

A **believes** A $\overset{K_{as}}{\longleftrightarrow}$ S

S **believes** A $\overset{K_{as}}{\longleftrightarrow}$ S

S **believes** A $\overset{K_{ab}}{\longleftrightarrow}$ B

B **believes** B $\overset{K_{bs}}{\longleftrightarrow}$ S

S **believes** B $\overset{K_{bs}}{\longleftrightarrow}$ S

A **believes** (S **controls** A $\overset{K}{\longleftrightarrow}$ B)

B **believes** (S **controls** A $\overset{K}{\longleftrightarrow}$ B)

A **believes** (S **controls fresh**(A $\overset{K}{\longleftrightarrow}$ B))

A **believes fresh**(N_a) $\overset{K_{ab}}{\longleftrightarrow}$

S **believes fresh**(A $\overset{K}{\longleftrightarrow}$ B)

B **believes fresh**(N_b) $\overset{K}{\longleftrightarrow}$

B **believes fresh**(A $\overset{K}{\longleftrightarrow}$ B)

Analysis of Idealized Needham-Schroeder

[initial assumptions from previous slide]

[Message 1 irrelevant.]

2. S -> A: $\{N_a, A \overset{K_{ab}}{\leftrightarrow} B, fresh(A \overset{K_{ab}}{\leftrightarrow} B), A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}\}_{K_{as}}$

3. A -> B: $\{A \overset{K_{ab}}{\leftrightarrow} B\}_{K_{bs}}$

*% need assumption B **believes fresh**(A $\overset{K}{\leftrightarrow}$ B) to proceed*

[B believes A $\overset{K_{ab}}{\leftrightarrow}$ B]

4. B -> A: $\{N_b, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{ab}}$ *from B*

5. A -> B: $\{N_b, (A \overset{K_{ab}}{\leftrightarrow} B)\}_{K_{ab}}$ *from A*

*[A **believes** A $\overset{K_{ab}}{\leftrightarrow}$ B, B **believes** A $\overset{K_{ab}}{\leftrightarrow}$ B, A **believes** B **believes** A $\overset{K_{ab}}{\leftrightarrow}$ B, B **believes** A **believes** A $\overset{K_{ab}}{\leftrightarrow}$ B]*

What We Learn From Analysis

- Stronger outcome than in Otway-Rees at the cost of an extra assumption.
- Encryption of certificate in second message under A's key has no effect on properties of protocol.

Summary of BAN Analyses

	Needham-Schroeder shared key	*Otway-Rees*	*Kerberos*	*Wide-Mouthed Frog*	*Yahalom*	*Andrew RPC*	*Needham-Schroeder public key*	*CCITT X.509*	
Proves presence of A and B	A and B	B	A and B	A	A and B	A and B	A and B	A and B	A
Redundancy X	X	X	X		X	X			
Bugs X*	X						X	X	

* Security breaches do not even require key compromise