Cryptographic Protocol Analysis via Strand Spaces

Joshua D. Guttman
Jonathan C. Herzog
F. Javier Thayer
Lenore D. Zuck

May 2001

http://www.ccs.neu.edu/home/guttman/

Supported by the National Security Agency

MITRE

Cryptographic Protocols

- What is a cryptographic protocol?
  - Short, conventional sequence of messages
  - Uses cryptography
  - Goals: authentication, key distribution
- Core trust establishment mechanism
  - E-commerce
  - Remote access
  - Secure networking
- Cryptographic protocols are often wrong
  - Active attacker can subvert goals
  - May fail even if cryptography ideal
  - Hard to predict which protocols achieve what goals

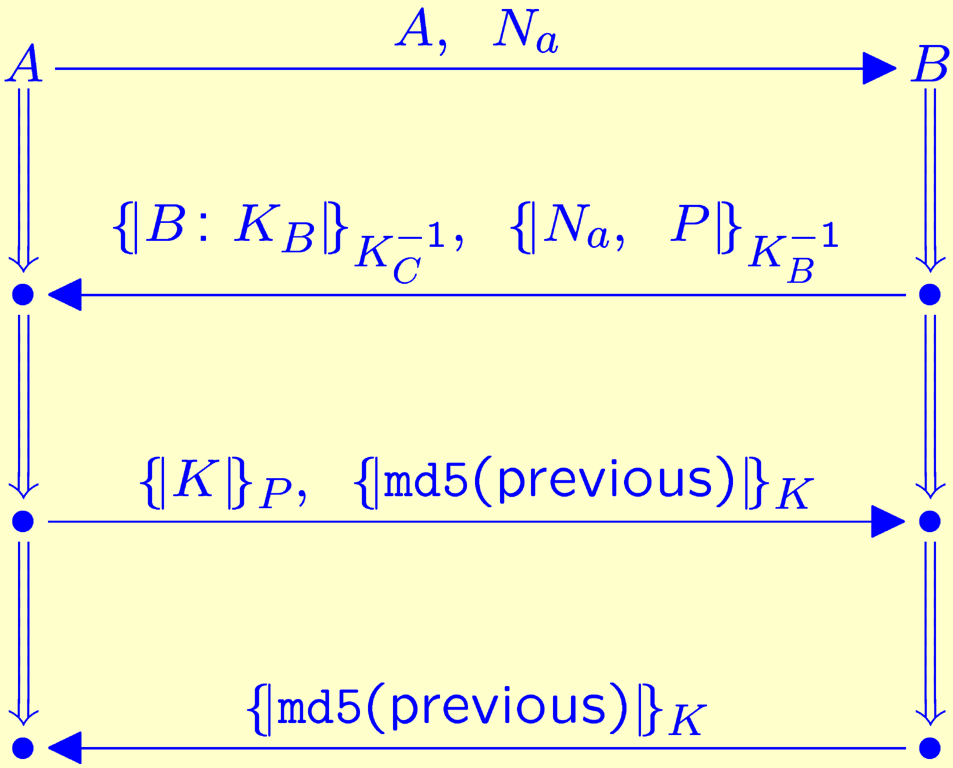
SSL$^-$, A Simplified SSL

- Client A starts exchange, sending
  - Name A
  - Fresh random number N_a (nonce)
- Server B sends
  - Certificate $\{\!|B : K_B|\!\}_{K_C^{-1}}$

    C: certifying authority
  - Signed temporary public key $\{\!|N_a,\ P|\!\}_{K_B^{-1}}$
- Client creates fresh secret K, sends $\{\!|K|\!\}_P$
  - K becomes session key
- Each principal sends the other
  - $\{\!|\text{Hash of previous msgs}|\!\}_K$

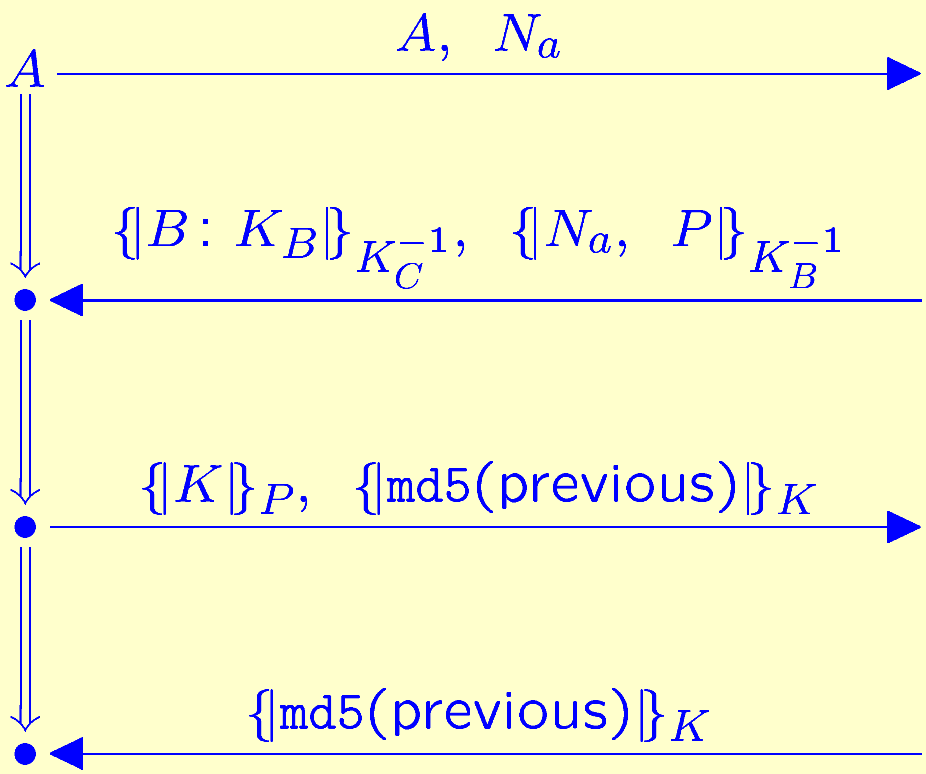
MITRE

SSL^{-}


A
B
$A, \ N_a$
$\{\!|B : K_B|\!\}_{K_C^{-1}}, \ \{\!|N_a, \ P|\!\}_{K_B^{-1}}$
$\{\!|K|\!\}_P, \ \{\!|\mathtt{md5}(\text{previous})|\!\}_K$
$\{\!|\mathtt{md5}(\text{previous})|\!\}_K$

MITRE

SSL^{-} Client View



Security Goals of SSL$^-$

- What does SSL$^-$ guarantee to client?
- Authentication
  - B constructed, sent P
- Freshness
  - P was constructed after N_a
- Secrecy
  - Only possessor of P^{-1} can get K
- Server's guarantees: None
  - Typically gets client's credit card

MITRE

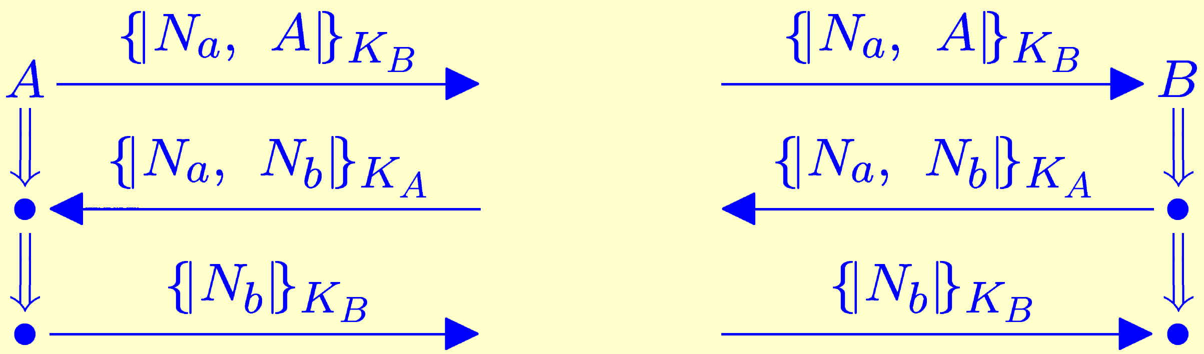
Today's Topics

- Dolev-Yao problem: assume cryptography perfect
  - Find secrecy properties achieved
  - Find authentication properties achieved

  and counterexamples to other properties
- Strand space theory
  - Particular method for answering Dolev-Yao problem
  - Examples
  - Core definitions
  - Reasoning methods
- Cryptographic faithfulness:
  - Does a real (imperfect) crypto primitive falsify security goals?
  - Probabilistic treatment (preliminary)

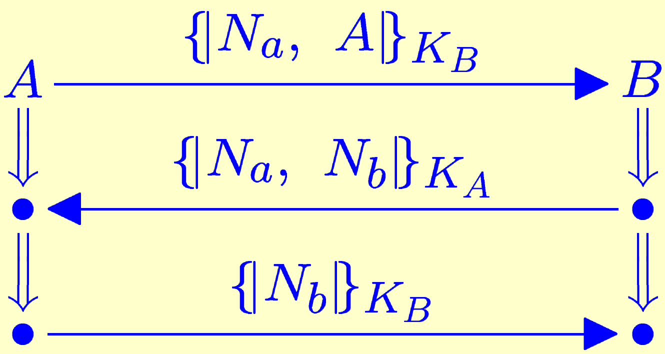
MITRE

Needham-Schroeder, 1978

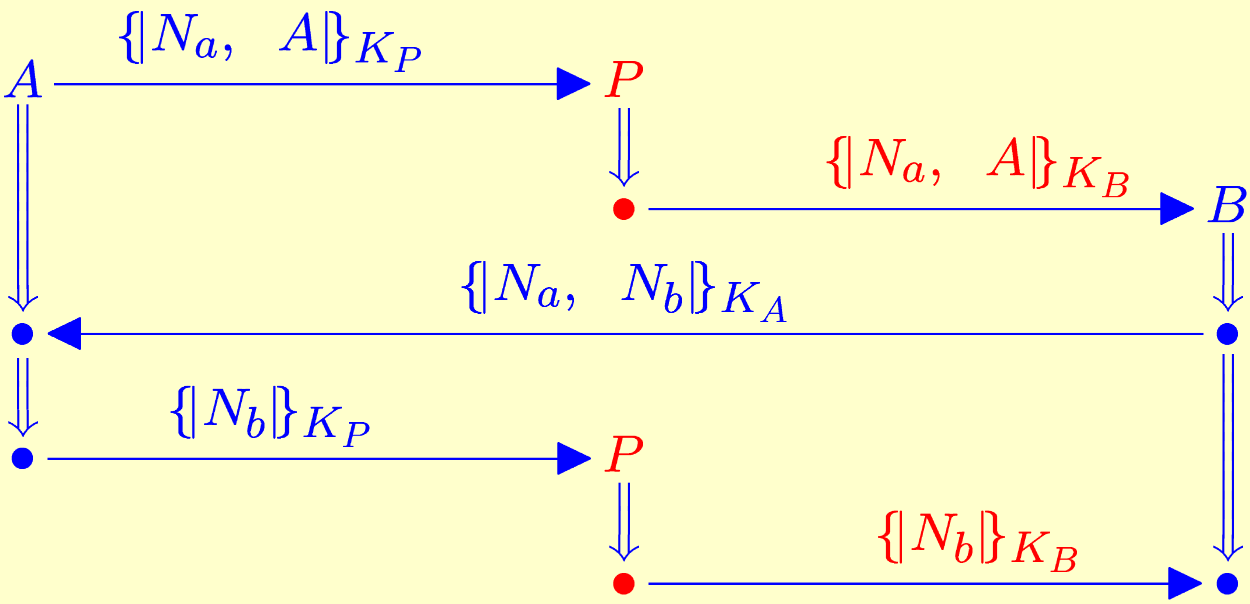


$\mathsf{NSInit}[A, B, N_a, N_b]$ $\mathsf{NSResp}[A, B, N_a, N_b]$

Needham-Schroeder: Intended Run



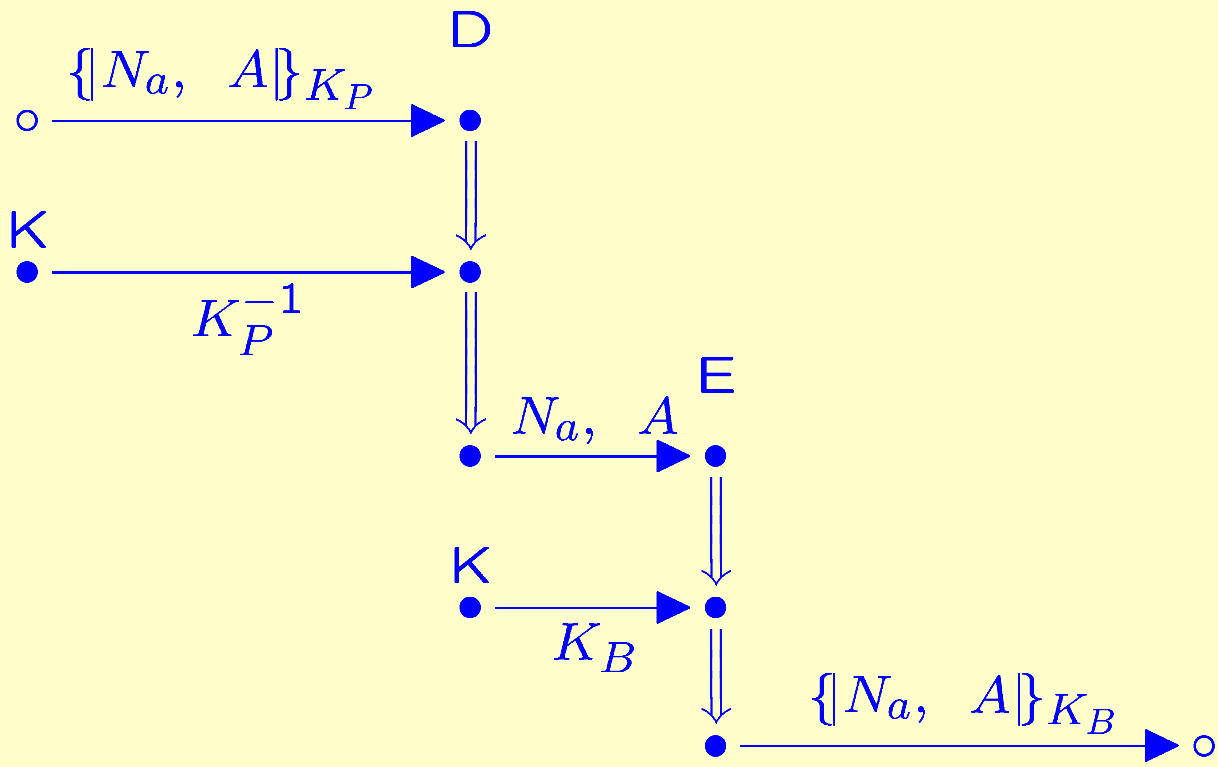
Undesirable Run



NSInit$[A, P, N_a, N_b]$ NSResp$[A, B, N_a, N_b]$

Due to Gavin Lowe (1995)

How the Penetrator Does That

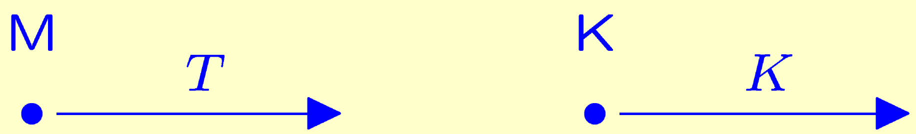


Powers of the Penetrator

- Initiate values
  - Nonces, names, etc.
  - Certain keys $K \in K_{\mathcal{P}}$ (public, compromised, or invented)
- Construct terms
  - Concatenate given terms
  - Encrypt, given key and plaintext
- Destruct terms
  - Separate concatenated terms
  - Decrypt, given ciphertext and matching decryption key
- Represented as strands
  - Sequence of send/receive events by same participant (penetrator in this case)

MITRE

Initial Penetrator Strands

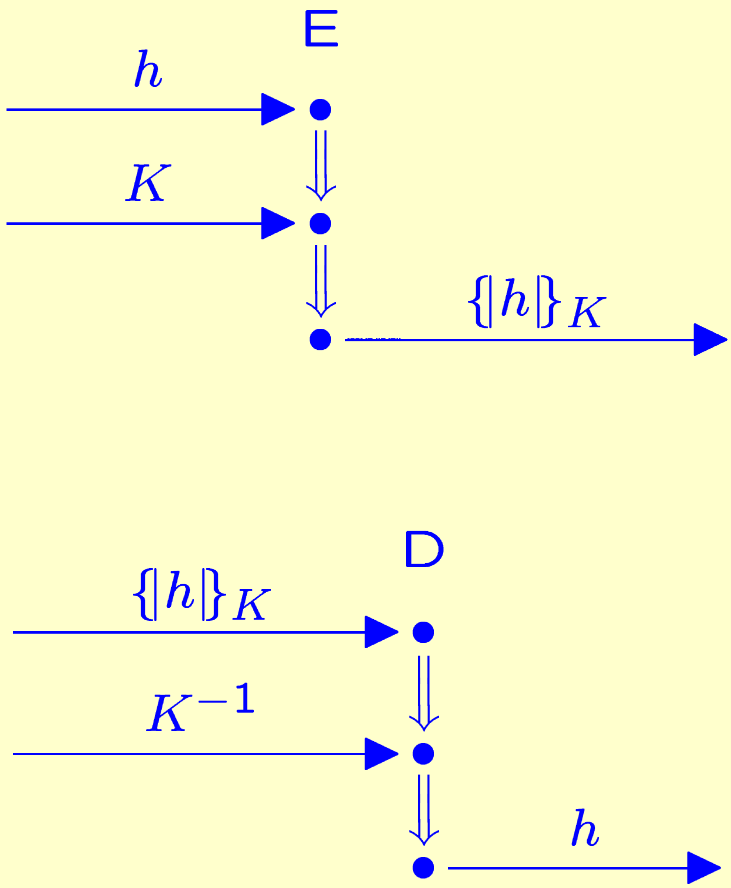


$K \in K_{\mathcal{P}}$

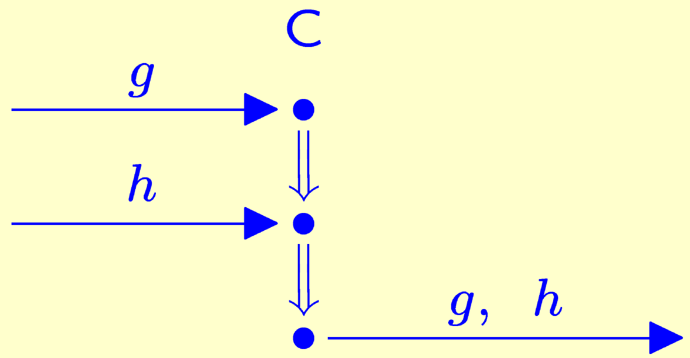
"compromised keys"

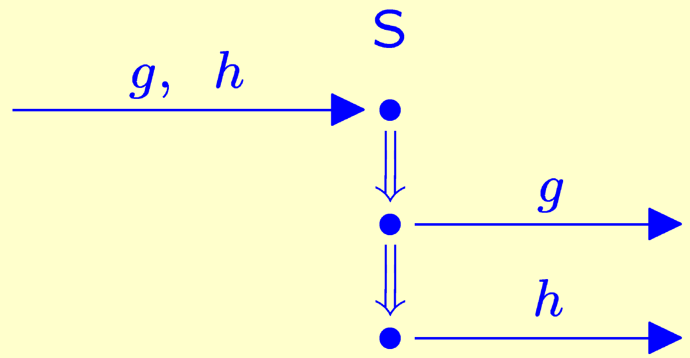
$K_{\mathcal{P}}$ is a parameter of the model

Encryption/Decryption Strands

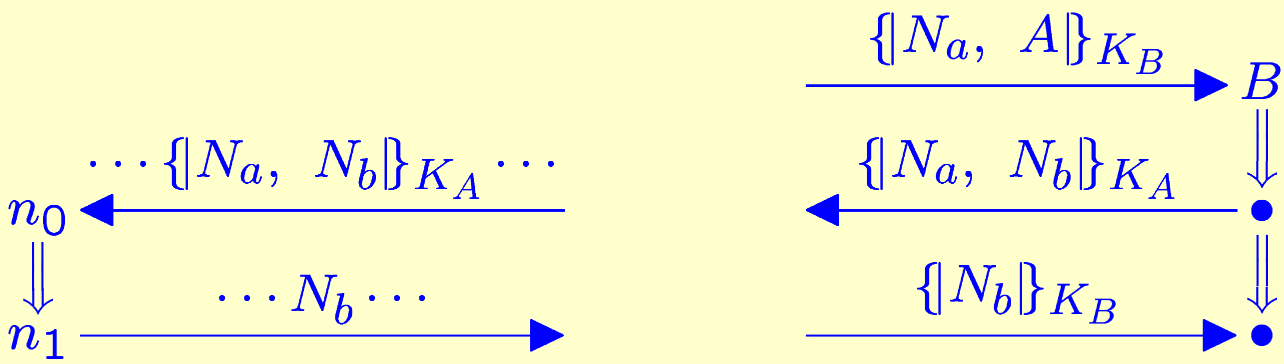


Concatenation/Separation Strands



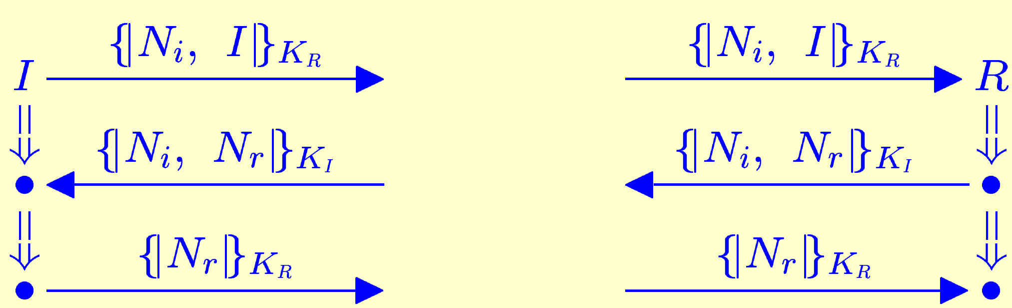


NS: Transforming Edge



N_b occurs only within $\{\!|N_a,\ N_b|\!\}_{K_A}$ at n_0

N_b occurs oustide $\{\!|N_a,\ N_b|\!\}_{K_A}$ at n_1



NS Responder's Guarantee

- If responder B undergoes

$$\mathsf{NSResp}[A, B, N_a, N_b]$$

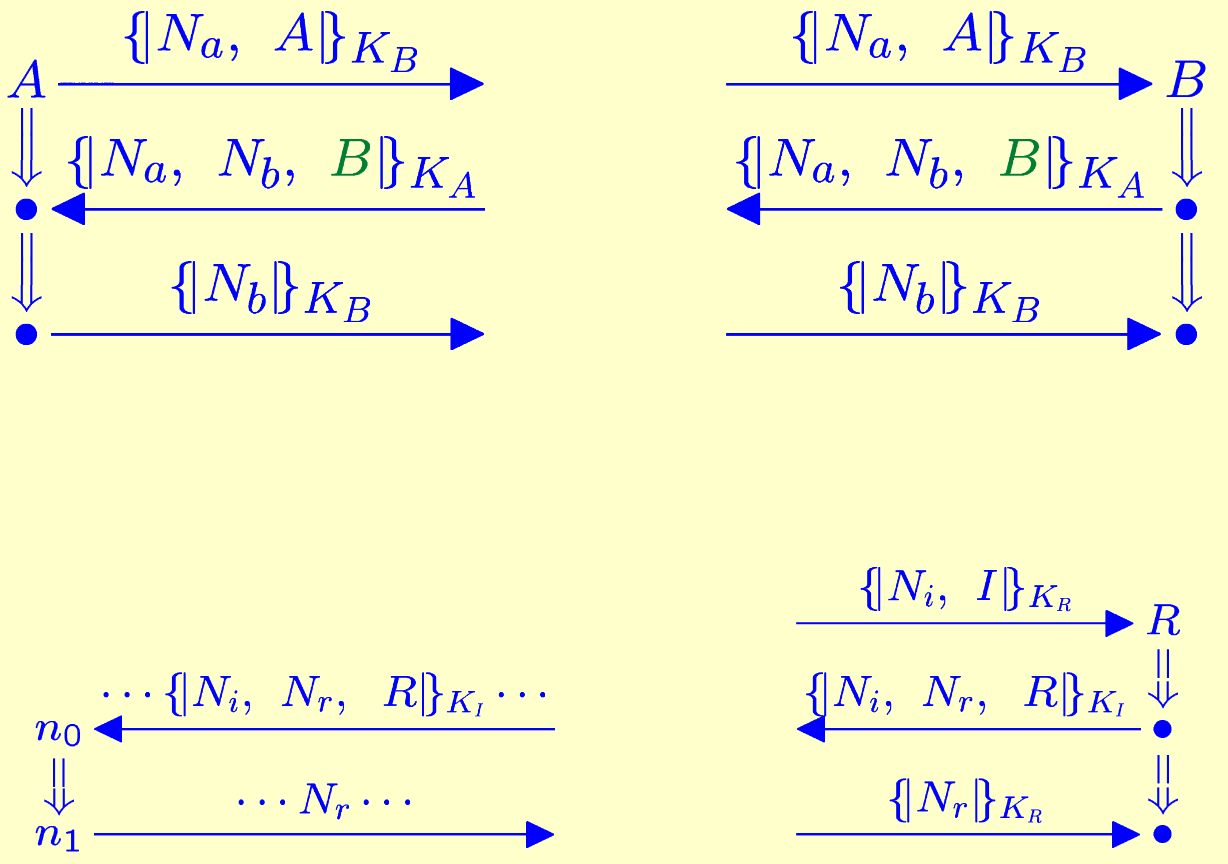
then A engaged in

$$\mathsf{NSInit}[A, X, N_a, N_b]$$

- But: $X \stackrel{?}{=} B$
  - Not necessarily
    see page 10
- If transforming edge contains B's name then $X = B$ follows

MITRE

Needham-Schroeder-Lowe Protocol



MITRE

Formalizing: Strands

- Strand
  - Sequence of transmissions $+t$ and receptions $-t$, connected by $\Rightarrow$
  - Possible behavior:
    penetrator or regular principal
  - "Node" means transmission or reception
- Strand space: set of strands
- Messages: Terms freely generated from
  - Names and nonces (texts)
  - Keys

  by operators

  ◦ Concatenation $t_0, \; t_1$

  ◦ Encryption $\{\!|t_0|\!\}_K$

Different algebras also interesting

Important: concatenation and encryption free

MITRE

Formalizing: Bundles

- Bundle $\mathcal{B}$: Finite graph of nodes and edges representing causally well-founded execution; Edges are arrows $\rightarrow$, $\Rightarrow$
  - For every reception $-t$ in $\mathcal{B}$, there's a unique transmission $+t$ with $+t \rightarrow -t$
  - When nodes $n_i \Rightarrow n_{i+1}$ on strand, n_i in $\mathcal{B}$ if n_{i+1} in $\mathcal{B}$
  - $\mathcal{B}$ is acyclic
- Bundle precedence ordering $\preceq_{\mathcal{B}}$

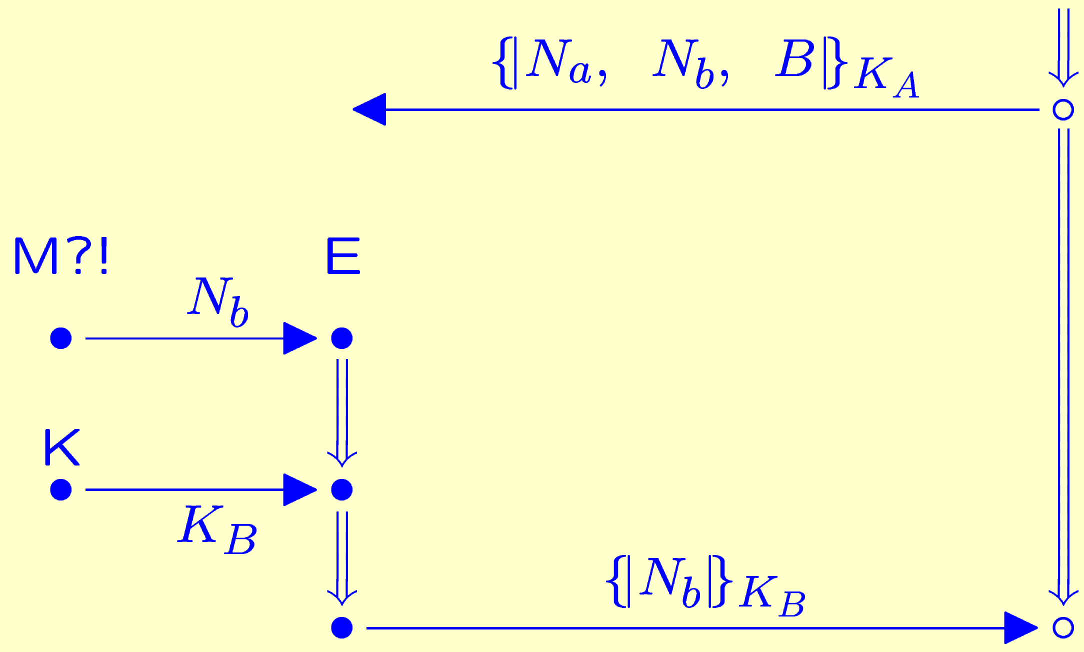
–	$n \preceq_{\mathcal{B}} n'$ means sequence of 0 or more arrows $\rightarrow$, $\Rightarrow$ lead from n to m
$\preceq_{\mathcal{B}}$	is a partial order by acyclicity
$\preceq_{\mathcal{B}}$	is well-founded by finiteness

- Bundle induction: Every non-empty subset of $\mathcal{B}$ has $\preceq_{\mathcal{B}}$-minimal members

MITRE

An Improbable Attack

Guessing a nonce



Guessing a private key (e.g. K_A^{-1})
similarly improbable

MITRE

Subterm, Origination

- Subterm relation $\sqsubset$
  least transitive, reflexive relation with

  $$g \sqsubset g,\ \ h$$
  $$h \sqsubset g,\ \ h$$
  $$h \sqsubset \{\!|h|\!\}_K$$

  N.B. $K \sqsubset \{\!|h|\!\}_K$ implies $K \sqsubset h$
- t **originates** at n_1 means

  n_1 is a transmission $(+)$
  $t \sqsubset \text{term}(n_1)$
  if $n_0 \Rightarrow \cdots \Rightarrow n_1$, then $t \not\sqsubset \text{term}(n_0)$
- t **originates uniquely** in $\mathcal{B}$ if there exists a unique $n \in \mathcal{B}$ s.t. t originates at n
- t is **non-originating** in $\mathcal{B}$ if there is no $n \in \mathcal{B}$ s.t. t originates at n

MITRE

An NSL Authentication Theorem

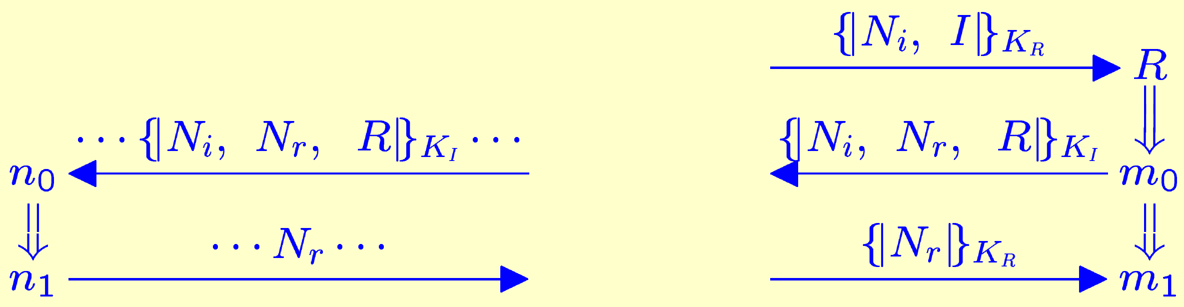
- Suppose:
  - Bundle $\mathcal{B}$ contains a strand Resp$[I, R, N_i, N_r]$
  - K_I^{-1} uncompromised
  - N_r originates uniquely on strand
- Then:
  - $\mathcal{B}$ contains a strand Init$[I, R, N_i, N_r]$

Authentication always takes this form

Correspondence assertion ($\forall\exists$)

MITRE

Proving Authentication: NSL



Consider $S = \{n \in \mathcal{B}:$ term(n) contains N_r
outside $\{|N_i,\ N_r,\ R|\}_{K_I}\ \}$

Assume N_b originates uniquely at m_0 and
K_A^{-1}uncompromised

- $m_1 \in S$
- Let n_1 be minimal in S (by bundle induction)
- $m_0 \prec n_0 \prec n_1$
- n_1 regular (i.e. non-penetrator)

Outgoing Authentication Test

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
n_0 \arrow[d, Rightarrow] & & m_0 \arrow[ll, dashed, "K^{-1} \in \mathit{Safe} \qquad \star a \sqsubset \{\!|h|\!\}_K"'] \arrow[d, Rightarrow] \\
n_1 \arrow[r, dashed, "a \sqsubset t'"] & {} \arrow[r, dashed, "a \sqsubset \mathsf{term}(n_1)"] & m_1
\end{tikzcd}
$$

$\{\!|h|\!\}_K \not\sqsubset t'$ $\qquad$ $\{\!|h|\!\}_K \not\sqsubset \mathsf{term}(n_1)$

$\star a$	means a originates uniquely at m_0
Safe	means keys penetrator can not get
n_0, n_1	these nodes exist in $\mathcal{B}$ and are regular

Some protocol verification becomes case analysis:
What regular strands can n_0, n_1 lie on?

MITRE

Incoming Test

Symmetrically,

$$
\begin{tikzcd}
n_0 \arrow[d, Rightarrow] & & & m_0 \arrow[lll, dashed, "\star a \sqsubset \mathsf{term}(m_0)"'] \arrow[d, Rightarrow] \\
n_1 \arrow[r, dashed, "a \sqsubset \{|h|\}_K"] & {} & {} \arrow[r, dashed, "K \in \mathit{Safe} \quad \{|h|\}_K \sqsubset \mathsf{term}(m_1)"] & m_1
\end{tikzcd}
$$

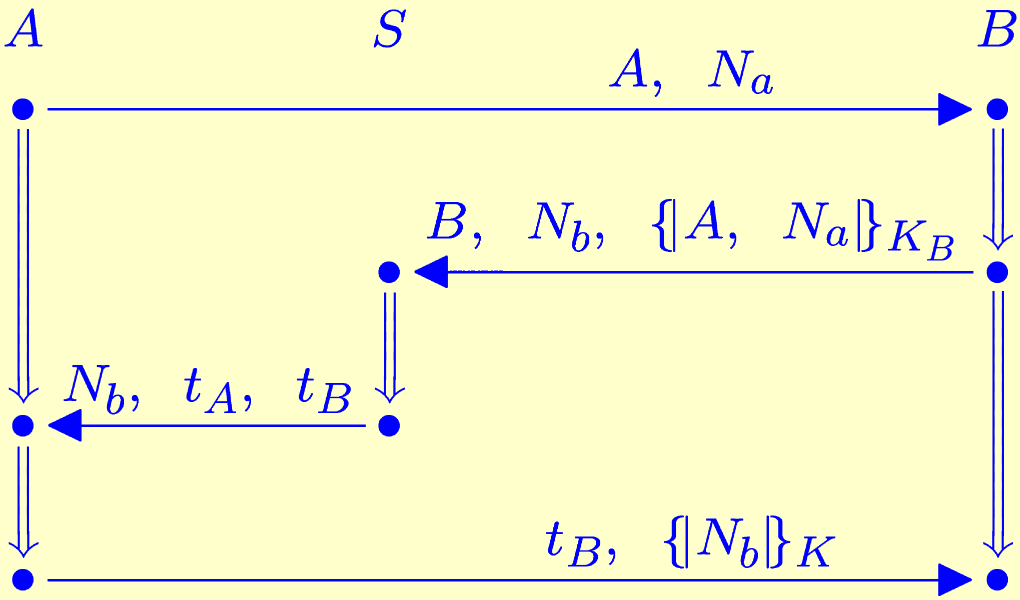
$\{|h|\}_K \not\sqsubset \mathsf{term}(m_0)$

n_0, n_1 must exist in $\mathcal{B}$ and be regular nodes

Note that $m_0 \prec n_0 \prec n_1 \prec m_1$

MITRE

Yahalom-Paulson



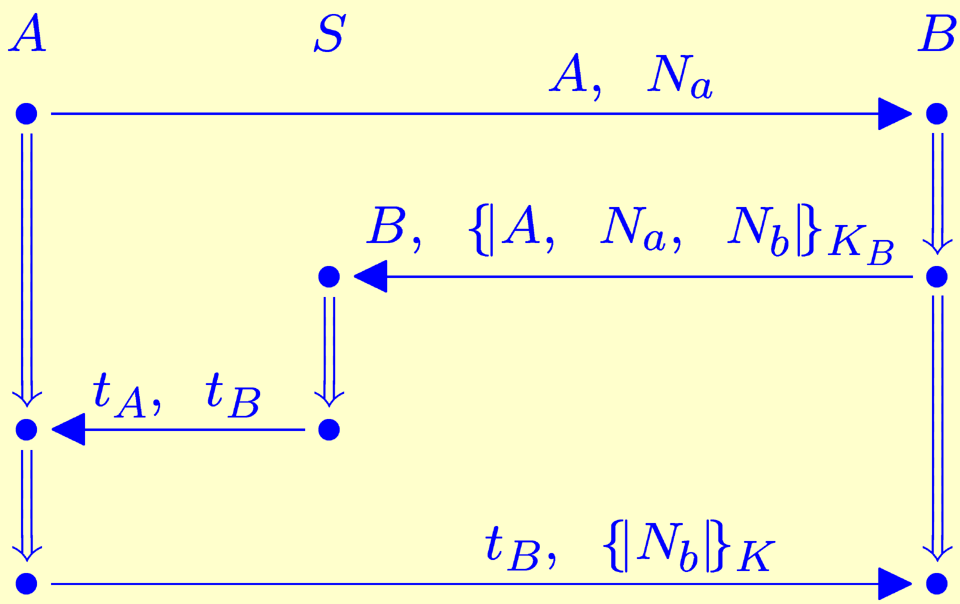
where $t_A = \{\!|B,\ K,\ N_a|\!\}_{K_A}$

and $t_B = \{\!|A,\ B,\ K,\ N_b|\!\}_{K_B}$

Uses 4 incoming tests

MITRE

Yahalom Protocol

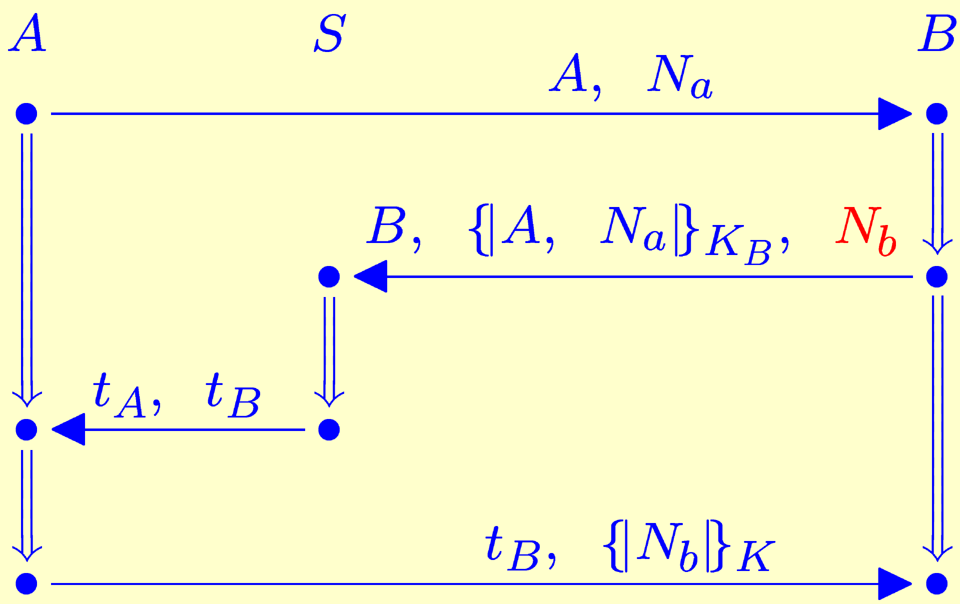


where $t_A = \{\!|B,\ K,\ N_a,\ N_b|\!\}_{K_A}$

and $t_B = \{\!|A,\ K|\!\}_{K_B}$

but why is K recent?

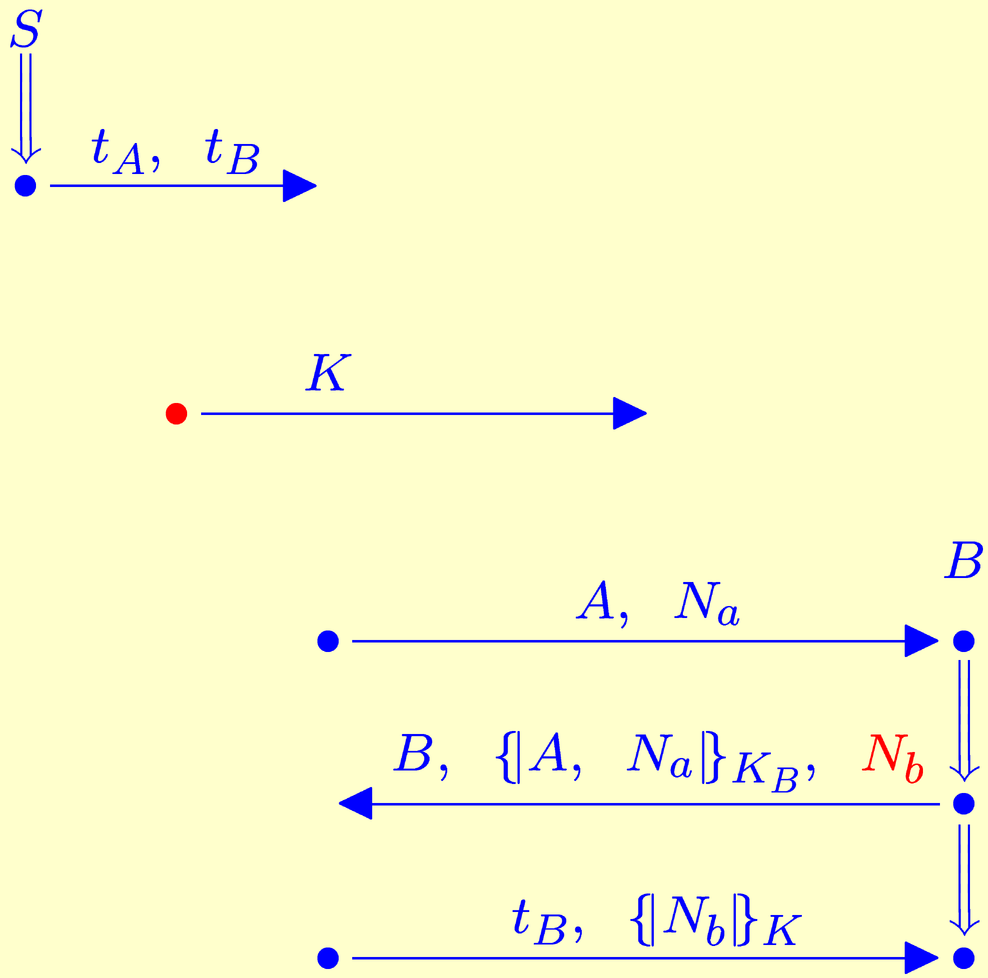
Faulty Yahalom Variant



where $t_A = \{\!|B, \; K, \; N_a, \; N_b|\!\}_{K_A}$

and $t_B = \{\!|A, \; K|\!\}_{K_B}$

Replay Attack on Variant



MITRE

Key Servers and Compromise

- May assume: Recently served key uncompromised until client completes strand
  - Justification: Cryptanalysis lengthy, client strand brief
  - Probabilistic
- Recency: n is recent for m_1 if there exists m_0 such that

  $$m_0 \Rightarrow \cdots \Rightarrow m_1$$
  $$m_0 \preceq n \prec m_1$$

- K **originates uniquely below** m_1 if exists unique n s.t.

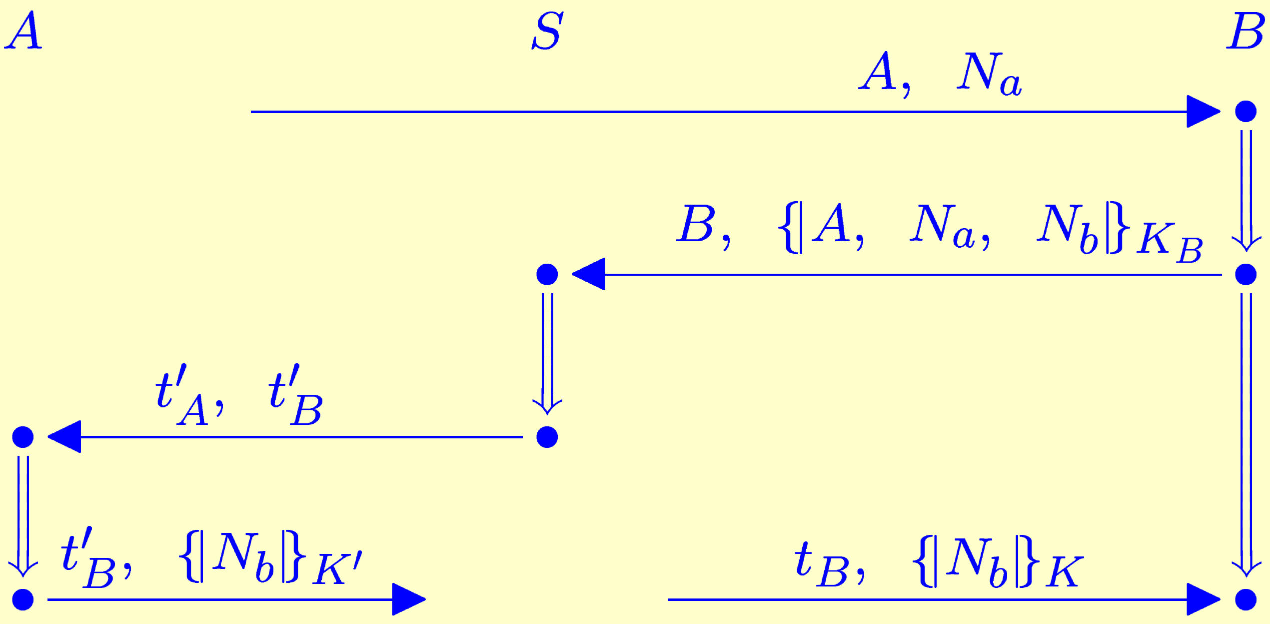
  K originates at n, and $n \preceq m_1$

- Key server assumption

if	$n_0 \Rightarrow n_1 \in \mathsf{Serv}[**, K]$
and	n_1 recent for m
then	K originates uniquely below m

MITRE

Yahalom Responder's Guarantee



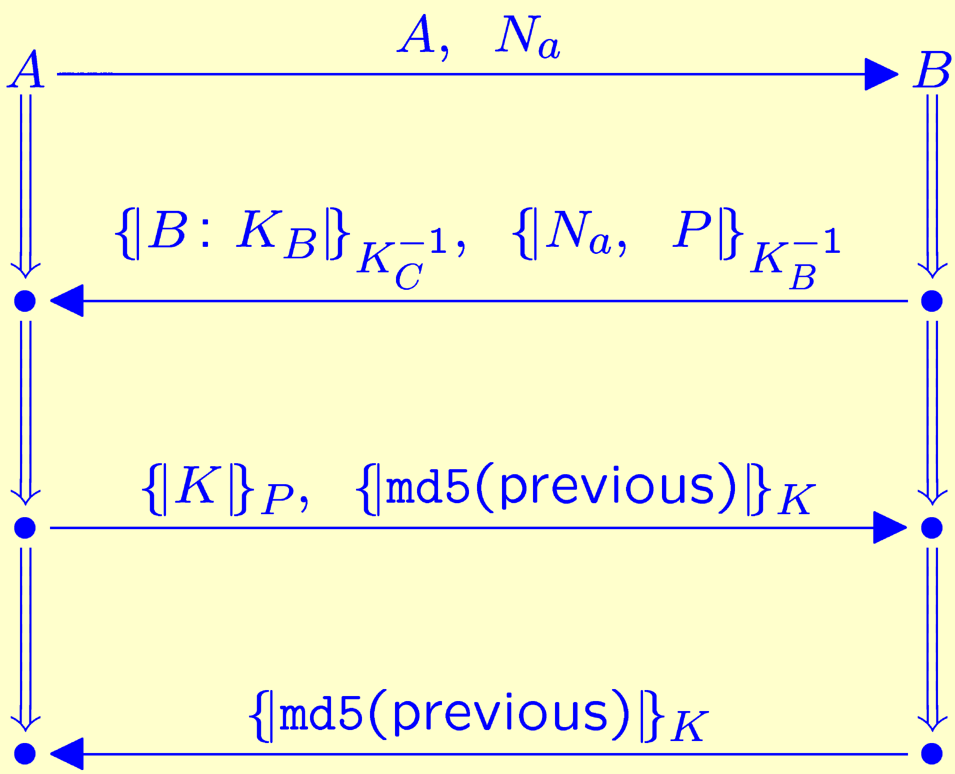
where $t_A = \{\!|B,\ K',\ N_a,\ N_b|\!\}_{K_A}$

and $t_B = \{\!|A,\ K'|\!\}_{K_B}$

Can use *outgoing tests*

MITRE

SSL$^-$



Incoming test on N_a
Outgoing test on K (in key position)

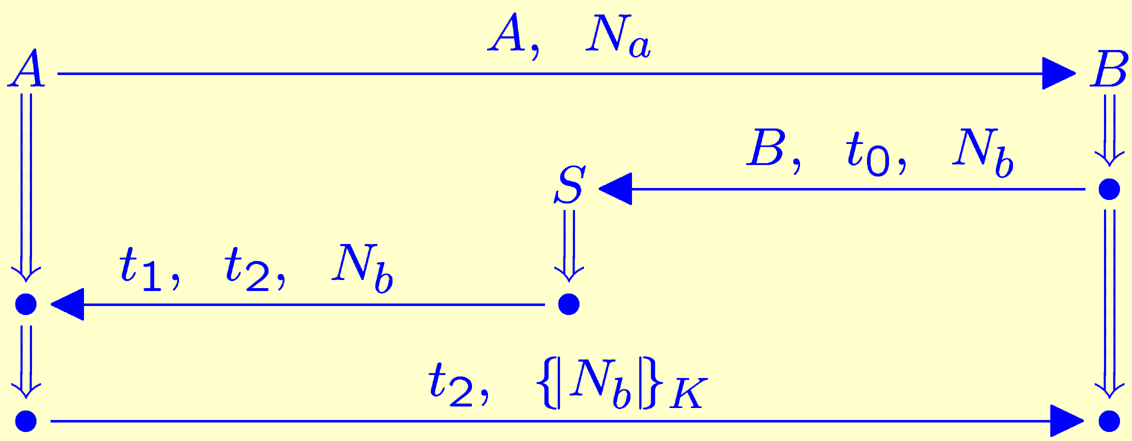
MITRE

Dolev-Yao Protocol Analysis

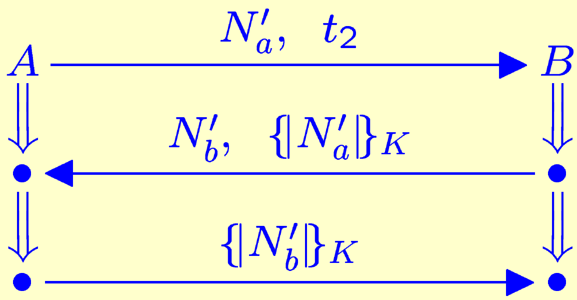
- Strand spaces and the authentication tests
  - Fairly complete method for
    Dolev-Yao authentication problems
  - Assumes perfect encryption
  - Accompanying method resolves secrecy
  - Very geometrical flavor
- Protocol independence
  - Mixing protocols
    with disjoint encryption
    does not undermine guarantees
- But Dolev-Yao is a strong assumption
  - Unique origination
  - Messages form free algebra
  - Penetrator has no other abilities

MITRE

Mixing Protocols



$t_1 = \{\!\vert B, \; N_a, \; K, \; T\vert\!\}_{K_A}$	a "distribution"
$t_2 = \{\!\vert A, \; K, \; T\vert\!\}_{K_B}$	a "ticket"
$\{\!\vert N_b\vert\!\}_K$	a "confirmation"



Bellare/Rogaway Map1

$$
\begin{tikzcd}[column sep=huge]
A \arrow[rrr, "N_a"] \arrow[d, Rightarrow] & & & B \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & & & \bullet \arrow[lll, "\llbracket\, B,\ \ A,\ \ N_a,\ \ N_b \,\rrbracket_f"'] \arrow[d, Rightarrow] \\
\bullet \arrow[rrr, "\llbracket\, A,\ \ N_b \,\rrbracket_f"] & & & \bullet
\end{tikzcd}
$$

- $\llbracket\, t \,\rrbracket_f$ means $\quad t, \ \ f(t)$

  $f : A \to \mathit{Tag}$
- Function $f \in \mathcal{F}$ is a shared secret
- Incoming authentication tests apply

Map1 Interpretations

- Two choices of A
  1. Bitstrings: Fixed-length names, nonces, tags
     Functions on bitstrings: concatenation, f
  2. Abstract terms
- Let $\mathcal{F}$ be Carter-Wegman universal
  - Means ℓ pairs $(t_i, f(t_i))$

    do not constrain $f(t)$

    if $t \not\in \{t_i\}$ and $\ell < n$
  - n called $\mathcal{F}$'s degree of universality
  - Polynomials of degree $n - 1$ work

MITRE

Separating Ideas

- Strand space/bundle method had two ingredients
  1. Summarize causal relations: $\Rightarrow$, $\rightarrow$, $\preceq_{\mathcal{B}}$
  2. Work with free algebra of messages
- Ingredient 1 still useful,
  even if 2 replaced with bitstrings
- Model of penetrator different
  Penetrator may
  - Deliver any bitstring
  - Apply any function to regular messages
  - Select strategy for applying functions

MITRE

Bundles over Bitstrings

- More bundles $\mathcal{B}_c$ over bitstrings exist
  - Penetrator delivers right message by luck
  - Suggests probabilistic treatment
- Want to show:
  - Bundles $\mathcal{B}_c$ without corresponding abstract $\mathcal{B}_a$ are infrequent
  - "Non-abstractable"
- In Map1, non-abstractable bundles have a forgery

  $t, \quad v \qquad$ where $v = f(t)$
- $\mathcal{B}_c$ where unique origination fails also infrequent
- Limit Λ on size of bundles needed, bounding number of regular
  - Nonces used
  - Tagged msgs sent
  - Tagged msgs received

MITRE

Stochastic Model

- Let (Ω, P) be a finite probability space, $B(\omega)$ a bundle-valued random variable
- Auxiliary random variables:

S_i	enumerates regular strands of $B(\omega)$
F	chooses tag function f
R	penetrator's source of randomness
$N_{i,j}$	j^{th} nonce sent on strand S_i
$T_{i,j}$	j^{th} plaintext/tag pair sent on S_i

- Stochastic assumptions

$N_{i,j}(\omega)$	uniformly distributed
$N_{i,j}(\omega)$	independent of $N_{i',j'}$
F	uniformly distributed
F	independent of R, T jointly

MITRE

Probability of Authentication Failure

- If $n \geq 2\Lambda$, then

$$P(\mathit{forge}) \leq \frac{\Lambda}{\mathit{card}(\mathit{Tag})}$$

- $P(\mathit{Clash}) \leq \Lambda^2/2\ \mathit{card}(\mathit{Nonces})$
- An example:
  - Authentication failure tolerance $= 2^{-32}$
  - Nonces have 64 bits
  - Tags have 64 bits
  - $n = 2^{17}$
- Consequence:
  - Annual rekeying allows 175 sessions/day
  - Monthly rekeying allows 2000 sessions/day

MITRE

Strands and Bundles

- Comprehensive method for Dolev-Yao problem
- Preliminary results on cryptographic faithfulness
  - Infer cryptographic requirements from usage in protocols
- Papers available at

`http://www.ccs.neu.edu/home/guttman/`

MITRE