URL: https://www.cs.neu.edu/home/cuttman

and the MIT RE-Sponsored Research Program
Supported by the National Security Agency

July 2003

Lenore D. Zuck
F. Javier Thayer
Jonathan C. Herzog
Shaddin Doghmi
Joshua D. Cuttman

Strand Spaces

Cryptographic Protocol Analysis via
Cryptography protocols are often wrong

- Establish trust
  - Goals: authentication, key distribution
  - Uses cryptography
  - Short, conventional sequences of messages

For instance, the Secure Socket Layer protocol (SSL)

What is a cryptographic protocol?
- Relate Dolev-Yao problem to cryptographic primitives
  - Design protocols without flaws
  - Find if flaws arise when protocols are combined
  - Prove no flaws exist
  - Discover flaws (of this kind)

- Explain how to model cryptographic protocols and their security goals
  (absence of flaws of this kind)
  - A class of security goal
  - A kind of protocol flaw

- For cryptographic protocols, identity
  - Abstract from details of cryptography

- Study Dolev-Yao problem for cryptographic protocols

Purpose of these lectures
New shared secret

Encryption  of  \( t \) with  \( K \)

Nonces, one-time random bitstrings

Public (asymmetric) keys of  \( A \),  \( B \)

\[
N_2 \oplus N_1
\]

\[
K \{ t \}
\]

\[
N_1, N_2
\]

\[
K_A, K_B
\]

Needham-Schroeder
\[ K = K_{-1} \]

- Same key makes ciphertext, extracts plaintext

Symmetric key cryptography: algorithm using

\[ A \text{ public key: } K \]

A's private key: \( K_1 \)

Anyone can verify signature with public key

Signature: Private key makes ciphertext,
- only private key owner can decrypt

Encryption: Public key makes ciphertext,
- two related values, one private, the other public

Public key cryptography: algorithm using

(for today's lecture)

Essence of Cryptography
Whoops

New shared secret
Encryption of $t$ with $Y$

Nonces, one-time random bitstrings

Public (asymmetric) keys of $A$, $B$

Assume $A$'s private key $K_{A \leftarrow 1}$ uncomromised

Needham-Schroeder: How does it work?
(Gavin Lowe)

Needham-Schroeder Failure

\[
\begin{align*}
K_N^2 & \xleftarrow{K_N^1} N^2 &
N^1 & \xleftarrow{K_N^1} N^2,
\end{align*}
\]
New shared secret
Encryption of $t$ with $K$
Nonces, one-time random bitstrings
Public (asymmetric) keys of $A$, $B$

Non-interactive setup

Needham-Schroeder-Lowe
Junk Terms
and
Unintended Services
Finding Flaws
(Gavin Lowe)

\[ p = \exists \exists \]

\[ \text{Needham-Schroeder Failure} \]
But legitimate party creates such a value
- \( N \) in this case
- Attacker needs to compute some value

\( d, pk, k_{N_1}, k_{N_2} \) to \( \{N, N_1, N_2\} \)
- Promised to translate
- Cave
- nonce \( N_1 \)

\( \text{An "unintended service"} \)

\( \text{How? A offered a service:} \)

- A had no run with \( B \)
  - Authentication failed:
    - Secrecy failed: \( p \) knows values

\( B : \text{Thinks he shares } N_1, N_2 \text{ only with } A \)
- Not \( A : \text{Meant to share } N_1, N_2 \text{ with } p \)

- Who was duped?

\textbf{Diagnosis of a Failure}
More authentication
Signatures only

Another Example: ISO Reject
What services are useful?

Only $Y^{-1} \{ B \}_{N}^{1}, N \in N_{2}$ requires work.

$Y^{-1} \{ B \}_{N}^{1}, N \in N_{2}$

Attacker needs to create:

- Other term received is the only challenge.
  - It has no authenticating force.
  - Clearly, $N_{1}$ is "junk".
- Respondent gets only two messages.

Diagnoses of ISO
\[ \text{i.e. use substitution } X/N_{i+1}^{2}, x/B \{y/A \} \]

- Can use \( A \) as respondent, \( B, N_{i}^{2} \) in-bound

\[ \forall N_{i}^{2}, \{B \} \]

\( \forall \} \)

- Wanted to produce
Possible behaviors are all substitution instances.

Behaviors are Parametric.
Counterexample to One Security Goal
What Goal is Refuted?

- In any run with $B$
- But $A$ was not initiator depending what that means
- "Entity authentication" for $A$ may hold
- A executed a signature
Combine unintended services

Criterion: Can they build challenge messages?

Look for unintended services

Penetrator needs to synthesize them

Remain in incoming messages: "Challenge"

They don’t contribute to authentication

Identity and discard "junk" messages

Dolev-Yao Attacks: A Recipe
Example with Symmetric Crypto
Both could produce \{nonce\}_{key}
Woo-Lam Infiltrated, I
Is there an attack?

What are the services?

Which terms have the "authenticating force"?

For A?

What are the junk terms for B?

Exercise (due to Song/Perrig)
Exercise: Available Services
Correction (due to Song/Perrig)
Key-translation service: NS PK
(too obvious?)

Decryption service: None

Encryption service: WOO-Lam

Signature service: ISO reflect protocol

Examples:

\[ K \{ a_N \} \leftrightarrow K \{ a_N \} \quad \text{Translation:} \]

\[ a_N \leftrightarrow a_N \quad \text{Decryption:} \]

\[ K \{ a_N \} \leftrightarrow a_N \quad \text{Encryption:} \]

\[ K \{ a_N \} \leftrightarrow a_N \quad \text{Signature:} \]

What Unintended Services Occur?
Need key to decrypt and recover plaintext
Need key to make encrypted value
No collisions

What does perfect cryptography mean?

Unintended services useful
Find counterexamples to other properties
The protocol achieves

What authentication properties
What secrecy properties

Given a protocol, and assuming all cryptography perfect, find

The Dolev-Yao Problem
The Authentication Tests

Proving Protocols Correct
transmitted only when protected with safe keys
- Recursively, also safe if (written \( K \in S \))

- A key \( K \) with this property is safe since it's never transmitted, only used

- \( K_{AB} \) never can be compromised via protocol

- We assume \( K_{AB} \) initially uncompromised

---

**Perig-Song sample protocol**

**Authentication tests:**
Taking cases on protocol definition, this must be $B$.

Only a regular participant can, since $K_{AB} \in S$.

Challenge is to produce encrypted term encrypted term containing $N_1$ comes back in.

Fresh value $N_1$ goes out.

We call this an incoming test.

How does it work? I. For the initiator.
Among nodes $n_0$, $n_1$, $n_2$, and $n_3$, conclude there exist in $B$ and are regular.

Assume a originates uniquely at $m_0$.

Incoming Tests
For asymmetric crypto, need decryption key $K \leftarrow Y$.

Only a regular participant can, since $K_{AB} \in S$

Challenge is to extract $N^2$ from encrypted term

Encrypted term sent out

We call this an outgoing test.

How does it work? II. For the responder.
Conclude nodes $n_0$, $n_1$ exist in $G$ and are regular

$a$ contained only in $(\text{term}(n_1))$, $a \not\in Y\{\eta\}$

Assume a originates uniquely at $m_0$.

Outgoing Authentication Test
Formalizing the authentication tests

Remainder of today’s lecture:
- Designing new protocols
- FInding flaws
- Proving correctness

Highly effective method for

Establish authentication via
Establish key secretly via safety

The authentication test method
Formalizing these Ideas: Strands and Bundles
Adversary behaviors are strands too

Regular strands generated as all instances, over some set of atoms

Protocol definition: Finite number of parameterized strands

\[ \text{NSResp}[A', B', N_1, N_2] \]

\[ \text{NSInit}[A', B', N_1, N_2] \]

\[ B \xrightarrow{\{N_2\}} \]

\[ A \xleftarrow{\{N_1\}} \]

Regular Strands (NS)
B is acyclic

When nodes \( n_i \) on same strand, \( n_{i+1} \) in \( B \), then \( n_{i+1} \) in \( B \),

\[ t - t \]

For every reception \( t \) in \( B \), there's a unique transmission \( t \) where

\[ \leftarrow \quad \leftarrow \]

Edges are arrows representing causally well-founded execution.

Bundle \( B \): Finite graph of nodes and edges

- Negative for receive
- Positive for send

Send, receive events on strands called "nodes"
A Bundle
originate at only one node
unpredictable values like nonces
May assume

†† t originates at n ††

Origination

\[ b \rightarrow b^{KB}_{N} \]
\[ p \rightarrow p^{KB}_{N} \]
\[ B \rightarrow b^{KB}_{A,N} \]
\[ d \rightarrow d^{KB}_{A,N} \]
\[ A \rightarrow A^{KB}_{N} \]
Note: \( K \{ \eta \} \not\subset Y \)

unless \( K \subset Y \)

\[ u \leftarrow m \text{ if } m \not\in \text{term}(m) \]

If \( t \not\in \text{term transmitted: } t \subset \text{term}(m) \)

\( u \) is a subterm of term transmitted: \( u \not\subset \text{term}(m) \)

\( u \) positive
Guessing a private key is similarly improbable.

A Non-Attack: Guessing a Nonce

\[ K \{ \mathbf{B} \{ \mathbf{B} \{ \mathbf{N} \} \} \} \]

to decrypt,

\[ \mathbf{K}^{-1} \]

such as \( \mathbf{K}^{-1} \).
Only if \( \exists X \subseteq N_q, X^N \subseteq N_q \) must exist in \( B \) for some \( X \)

Attack bundle is a counterexample to this

Authentication: correspondence assertions (of form \( \exists X \))

\[ B \]

\[ \exists \text{ a strand } [A, B, N_q] \text{ in } B \]

- Then:

\[ N_q \text{ originates uniquely in } B \]

\[ \forall \text{ non-originating in } B \]

\[ \exists \text{ a strand } \text{ contains a strand } [A, B, N_q] \]

Suppose:

NS Authentication (Responder's Guarantee)

Security Goals: An Example
Induction on message structure

Bundle induction

Reasoning about protocols combines

has $\subseteq$-minimal members

Bundle induction: Every non-empty subset of $B$

Is well-founded by finiteness $\subseteq B$

Is a partial order by acyclicity $\subseteq B$

Lead from $m$ to $n$

$\Leftarrow$ means sequence of 0 or more arrows, $\Leftarrow$

Bundle precedence ordering $\subseteq B$

Precedence within a Bundle
A does not originate on \( u_1 \), so \( u \) received on \( u_1 \)

Minimal element \( u_1 \in \mathcal{L} \) must be regular

Non-empty because \( m_1 \in \mathcal{L} \)

Let \( \mathcal{L} = \{(u) \in \mathcal{L}^* \mid \{ \cdots a \cdots \} \} \). \( B \ni u \).

Proof:

Consider nodes \( m_0 \), \( u_1 \in \mathcal{L} \).

Conclude nodes \( m_0 \), \( u_1 \) exist in \( \mathcal{L} \) and are regular.

Assume a originates uniquely at \( m_0 \).

Incom ing Tests.
In $\not\iff 0$ on $u$, so $a$ received on $u$

Minimal element $u \in J$ must be regular

Non-empty because $\exists m \in J
\{u \in X \setminus \{Y\} \text{ in } u \} = J$

Let $J
\vdash \neg X \setminus \{Y\}$

Proof

Conclude nodes $n_0, u$, $u$ exist in $B$ and are regular

$X \setminus \{Y\}$ contained only in $(\text{term}(u \downarrow))$

Assume a originates uniquely at $m_0$.

Outgoing Authentication Test
Assume $K_A \notin P$

Initiator Authenticates Server

$\{N_a, B, K\}K_A, \ldots$

$\ldots, \{N_a, B, K\}K_A$

$A, N_a$

$A, N_a$

Initialize $A$
Assume $K, A \not\in B$.

Carlsen: Initiator Authenticates Responder.
New shared secret

Encryption of $t$ with $K$

Nonces, one-time random bitstrings

Public (asymmetric) keys of $A$, $B$

\[ N_1 \oplus N_2 \]
\[ M \{ t \} \]
\[ N_1, N_2 \]
\[ K_A, K_B \]

Needham–Schroeder–Lowe
Yahalom Protocol
URl: http://www.cs.neu.edu/home/guttmann

- Bundle induction
  - Bundles
  - Strands

- Formalize using
  - Determine that matching strands exist in bundle
  - Use incoming, outgoing tests
  - Assume adversary cannot use safe keys
  - Prove correctness

- Offered by the legitimate protocol participants
  - To forge them, combine unintended services
  - Remaining messages have authenticating force
  - Some messages are junk

- Find flaws

Summary, First Day