

Strand spaces: From Key Exchange to Secure Location

Joshua D. Guttman

Jonathan C. Herzog

Vipin Swarup

F. Javier Thayer

The MITRE Corporation
Thanks to the National Security Agency
and to MITRE-Sponsored Research

Workshop on Event-Based Semantics

Key exchange vs. secure location

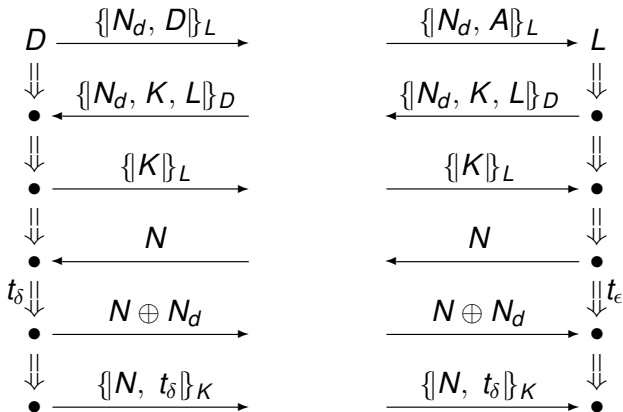
- Key exchange protocols:
 - ▶ Agnostic about communication
 - ★ Space, time, and transmission characteristics
 - ▶ Aimed at logically simple goals
- Strand space theory:
 - ▶ Special-purpose execution semantics
 - ▶ Based on causal partial order
 - ▶ Complete for symbolic analysis of key exchange
- Secure location protocols:
 - ▶ Require assumptions about transmission
 - ▶ Make essential use of geometry
 - ▶ Goals quantitative

Goal: Adapt strands to secure location

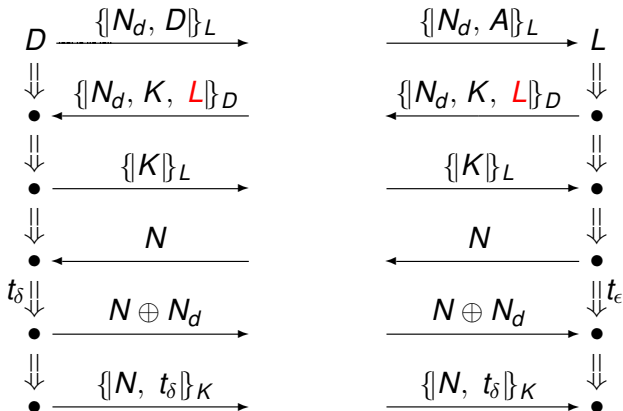
- Explain strand spaces
- Illustrate some secure location techniques
- Embed strand spaces in spacetime, justify reasoning about secure location

Distance approx $\frac{c \cdot (t_\epsilon - t_\delta)}{2}$

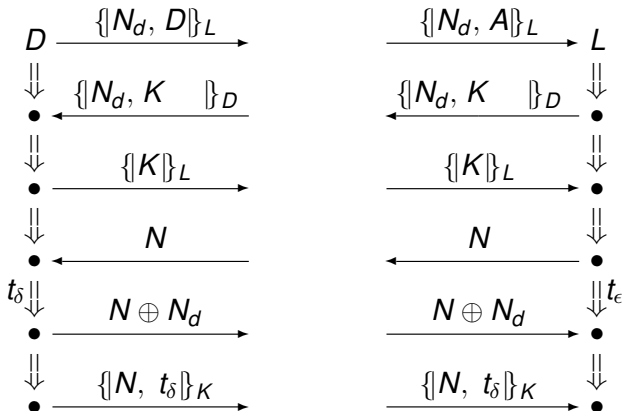
Finding distance



Flawed version

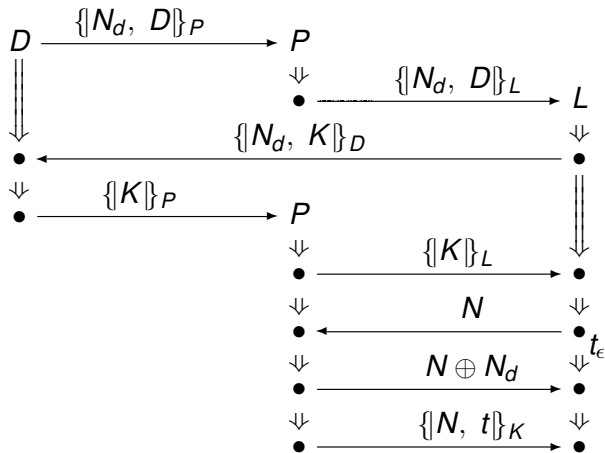


Flawed version



What if L 's name omitted?

A Lowe-style Attack



LORAN: Time difference of arrival

Diagram: V Shmatikov, ASIAN 2007

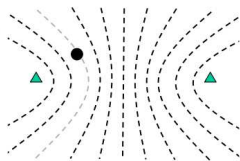


Fig. 5. Family of hyperbolas between two beacons.



Fig. 6. Intersecting hyperbolas.

LORAN: Multiple beacons

Diagram: V Shmatikov, ASIAN 2007

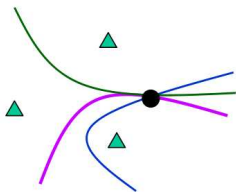


Fig. 6. Intersection of three hyperbolas.

between two

Metric strand spaces

Preliminaries

- Partial pseudometric d :
Partial fn $d: X \times X \rightarrow [0, \infty)$ where
 - 1 $d(x, x) = 0$
 - 2 $d(x, y) = d(y, x)$, if either side defined
 - 3 $d(x, y) \leq d(x, z) + d(z, y)$, if all defined

Metric strand spaces

Preliminaries

- Partial pseudometric d :
Partial fn $d: X \times X \rightarrow [0, \infty)$ where
 - 1 $d(x, x) = 0$
 - 2 $d(x, y) = d(y, x)$, if either side defined
 - 3 $d(x, y) \leq d(x, z) + d(z, y)$, if all defined
- Time elapse function e on (X, \preceq) :
Partial fn $e: X \times X \rightarrow [0, \infty)$ where
 - 1 $x \preceq y$ implies $e(x, y)$ is defined
 - 2 $e(x, x) = 0$
 - 3 $e(x, y) = e(x, z) + e(z, y)$ when $x \preceq z \preceq y$

Metric strand spaces

Execution model

A *geometric bundle* is a tuple $(\mathcal{B}, \text{dist}, \text{elapse}, c)$ where:

- \mathcal{B} is a bundle
- dist is a partial pseudometric on $\text{nodes}(\mathcal{B})$
- elapse is a time elapse fn on $m, n \in \text{nodes}(\mathcal{B})$ where $m \preceq_{\mathcal{B}} n$
- c is a positive real

such that if $m \rightarrow_{\mathcal{B}} n$

$$\text{elapse}(m, n) = \frac{1}{c} \text{dist}(m, n)$$

when both sides defined

Static geometric bundles

Geometric bundle $(\mathcal{B}, \text{dist}, \text{elapse}, c)$ is *static* if:

$$m \Rightarrow^+ n \text{ implies } \text{dist}(m, n) = 0$$

for all $m, n \in \text{nodes}(\mathcal{B})$

i.e. no principal moves during any strand

Protocols with clocks

A protocol Π has *clocks* if

- each principal has a real value t_n associated with every node
- t_n can be sent in messages or used for calculations
- In each $(\mathcal{B}, \text{dist}, \text{elapse}, c)$ for Π ,
if $m \Rightarrow^+ n$, then

$$t_n - t_m = \text{elapse}(m, n)$$

Synchronized clocks

Principals P_1, P_2 have *synchronized clocks* in $(\mathcal{B}, \text{dist}, \text{elapse}, c)$ if, whenever $m \preceq_{\mathcal{B}} n$ for nodes of P_1, P_2 ,

$$t_n - t_m = \text{elapse}(m, n)$$

Secure location goal

A LORAN-like example

Suppose $(\mathcal{B}, \text{dist}, \text{elapse}, c)$ is a static bundle where beacons P_1, \dots, P_k have

- known pairwise distances
- synchronized clocks
- apparently computed location ℓ for P_0 .

If

- long-term keys of P_0, P_1, \dots, P_k are uncompromised
- nonces N_0, N_1 are uniquely originating in \mathcal{B}

then P_0 was located at ℓ .

Key exchange vs. secure location

- Key exchange protocols:
 - ▶ Agnostic about communication
 - ★ Space, time, and transmission characteristics
 - ▶ Aimed at logically simple goals
- Strand space theory:
 - ▶ Special-purpose execution semantics
 - ▶ Based on causal partial order
 - ▶ Complete for symbolic analysis of key exchange
- Secure location protocols:
 - ▶ Require assumptions about transmission
 - ▶ Make essential use of geometry
 - ▶ Goals quantitative