Introduction to Mobile Ambients

Hanne Riis Nielson & Flemming Nielson

Informatics & Mathematical Modelling
Technical University of Denmark

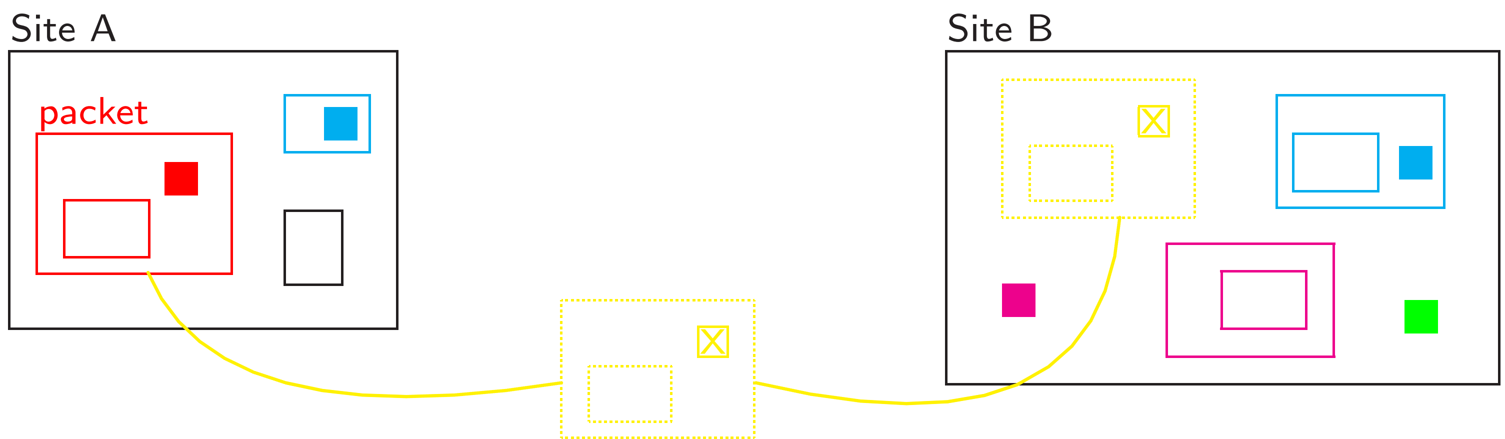
Overview

- The ambient view of the world
- The ambient calculus
  - syntax and semantics
- Secure firewalls

The ambient view of the world

An ambient is a bounded place where computations take place

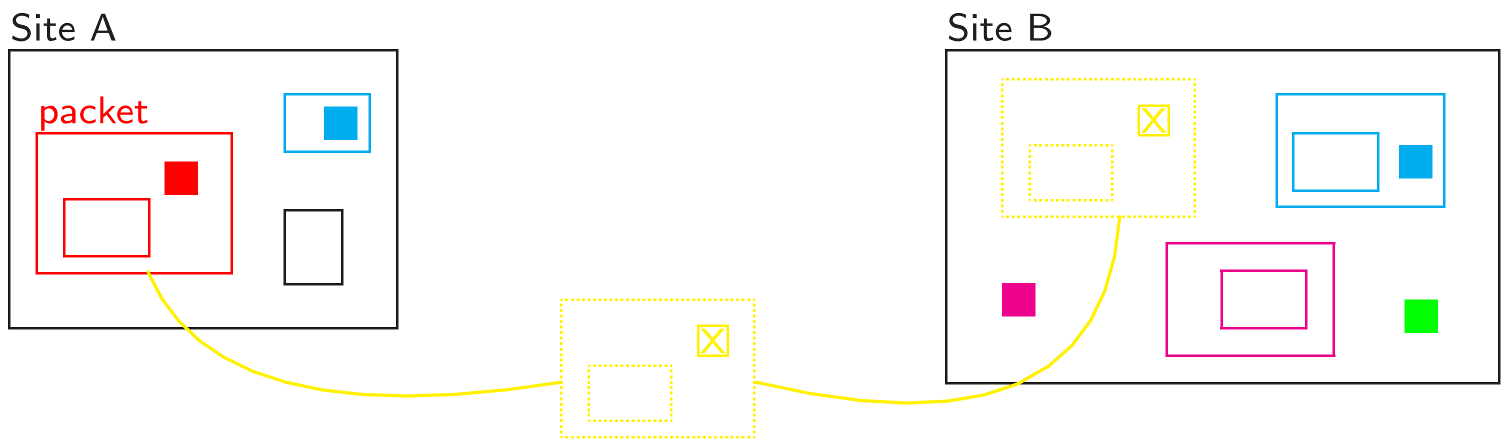
- the boundary determines what is inside and what is outside
  - as such it is a high-level security abstraction
- the ambient moves as a whole
- example ambients: applets, agents, laptops, $\cdots$



The ambient hierarchy

Ambients can be nested inside other ambients forming a tree structure

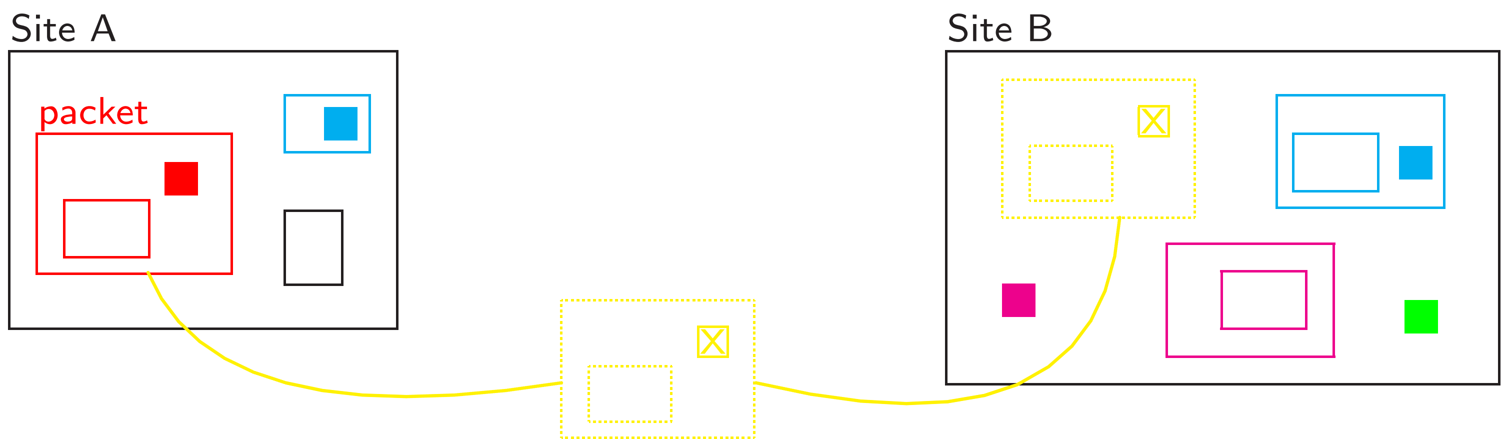
- mobility is represented as navigation within this hierarchy of ambients
- example: to move a packet from one site to another we must first remove it from the enclosing ambient and then insert it in the new enclosing ambient



Controlling the ambients

Each ambient contains a number of multi-threaded running processes

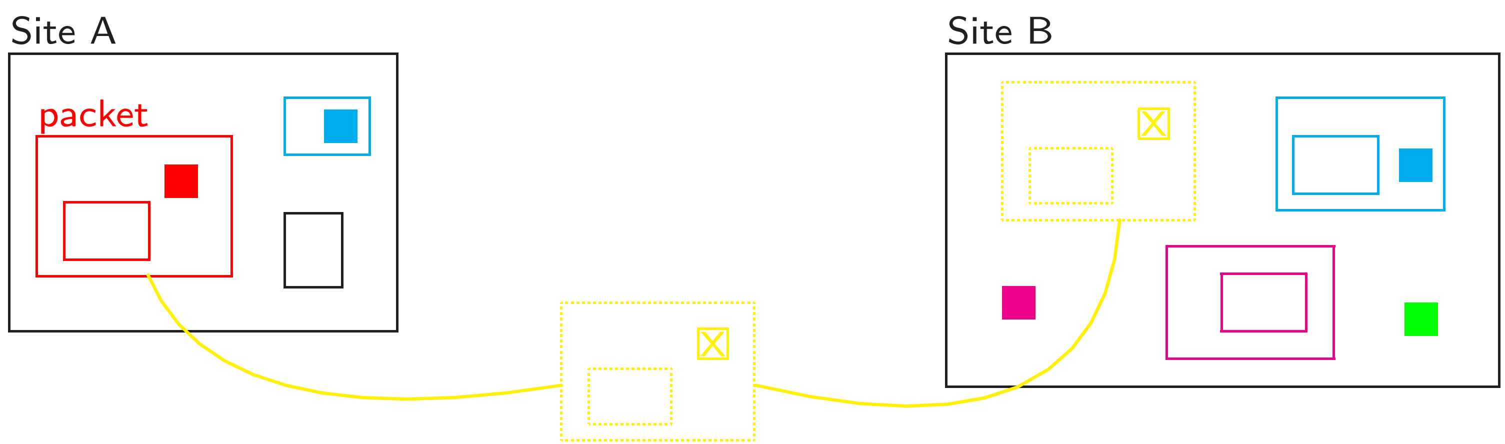
- the top-level processes of an ambient have direct control over it and can instruct it to move and thereby change the future behaviour of its processes and subambients
- the processes of subambients have no control over the parent
- processes continue running while being moved



Naming ambients

Each ambient has a name

- only the name can be used to control the access to the ambient: entry, exit, communication, etc.
- ambient names are unforgeable



Mobility primitives

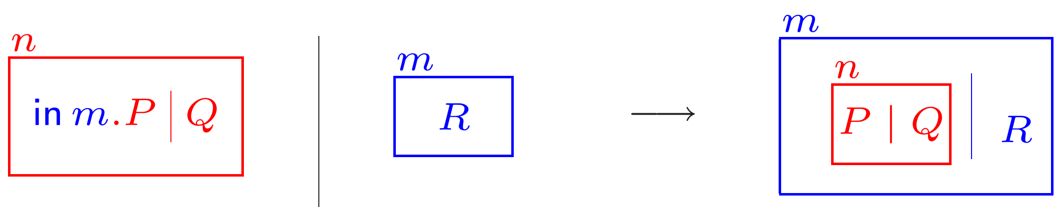
Move into an ambient: $\overset{n}{\boxed{\mathsf{in}\ m.P \mid Q}} \mid \overset{m}{\boxed{R}} \longrightarrow \overset{m}{\boxed{\overset{n}{\boxed{P \mid Q}} \mid R}}$

Move out of an ambient: $\overset{m}{\boxed{\overset{n}{\boxed{\mathsf{out}\ m.P \mid Q}} \mid R}} \longrightarrow \overset{n}{\boxed{P \mid Q}} \mid \overset{m}{\boxed{R}}$

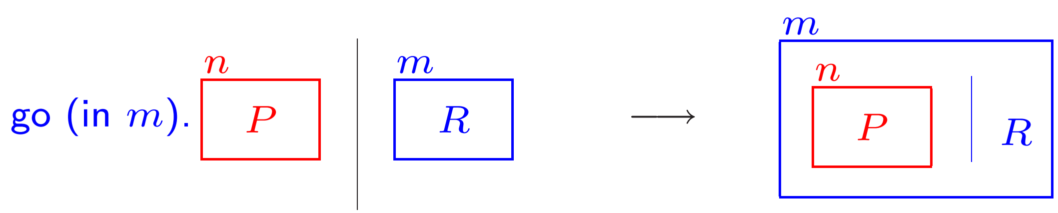
Dissolve an ambient: $\mathsf{open}\ n.P \mid \overset{n}{\boxed{Q}} \longrightarrow P \mid Q$

Design choice:
Subjective versus objective moves

Subjective moves are caused by a process running inside the ambient being moved — “I wish to move there”



Objective moves are caused by a process running outside the ambient being moved — “you should move there”



Which is the better?

Example: kidnapping an ambient

$$(\nu\ \mathsf{k})\big(\overset{\mathsf{k}}{\boxed{}} \mid \mathsf{go}\ (\mathsf{in}\ \mathsf{n}).\ \mathsf{in}\ \mathsf{k}\ \big) \mid \overset{\mathsf{n}}{\boxed{P}}$$

the ambient in k moves into n

$$\longrightarrow (\nu\ \mathsf{k})\ \big(\ \overset{\mathsf{k}}{\boxed{}} \mid \overset{\mathsf{n}}{\boxed{\mathsf{in}\ \mathsf{k} \mid P}}\ \big)$$

the ambient n moves into k

$$\longrightarrow (\nu\ \mathsf{k})\ \big(\ \overset{\mathsf{k}}{\boxed{\overset{\mathsf{n}}{\boxed{P}}}}\ \big)$$

the name k is private so
noone can interact with n

Example: a packet on a network

A[p[out A. in B. · · ·] | · · ·] | B[open p. · · · | · · ·]

the packet p moves out of site A

→ A[· · ·] | p[in B. · · ·] | B[open p. · · · | · · ·]

... and then into site B

→ A[· · ·] | B[p[· · ·] | open p. · · · | · · ·]

... where it is dissolved

→ A[· · ·] | B[· · · | · · · | · · ·]

Example security properties

- packets with sensitive information can only pass through classified sites
- packets with sensitive information may pass through unclassified sites but can only be opened at classified sites

The ambient calculus

- **Syntax:**

  processes and capabilities

- **Semantics:**

  structural congruence and transition relation

Follows the tradition of process calculi as the π-calculus and the spi-calculus.

Example: linearised syntax

$$\mathsf{A}\,[\,\mathsf{p}\,[\,\mathsf{out}\,\mathsf{A}.\ \mathsf{in}\,\mathsf{B}.\ \cdots\,]\mid\ \cdots\,]\ \mid\ \mathsf{B}\,[\,\mathsf{open}\,\mathsf{p}.\ \cdots\mid\cdots\,]$$

$$\longrightarrow\quad \mathsf{A}\,[\,\cdots\,]\ \mid \mathsf{p}\,[\,\mathsf{in}\,\mathsf{B}.\ \cdots\,]\ \mid\ \mathsf{B}\,[\,\mathsf{open}\,\mathsf{p}.\ \cdots\mid\cdots\,]$$

$$\longrightarrow\quad \mathsf{A}\,[\,\cdots\,]\ \mid\ \mathsf{B}\,[\,\mathsf{p}\,[\,\cdots\,]\ \mid\ \mathsf{open}\,\mathsf{p}.\ \cdots\mid\cdots\,]$$

$$\longrightarrow\quad \mathsf{A}\,[\,\cdots\,]\ \mid\ \mathsf{B}\,[\,\cdots\ \mid\cdots\mid\cdots\,]$$

Syntax of mobile ambients

- Processes — based on the π-calculus

P	$::=$	$(\nu\, n\colon \mu)\, P$	introduces a process with private name n in group μ
	$\mid$	$(\nu\, \mu)\, P$	introduces a new group named μ with its scope
	$\mid$	0	the inactive process
	$\mid$	$P_1 \mid P_2$	two concurrent processes
	$\mid$	$!P$	any number of occurrences of P
	$\mid$	$n\,[P]$	an ambient named n $\longrightarrow \overset{n}{\boxed{P}}$
	$\mid$	$M.P$	a capability M followed by P

- Capabilities — of the core calculus

M	$::=$	in n	move the enclosing ambient into a sibling named n
	$\mid$	out n	move the enclosing ambient out of a parent named n
	$\mid$	open n	dissolve a sibling ambient named n

Semantics of mobile ambients

- Structural congruence relation: $\boxed{P \equiv Q}$

Examples: $!P \equiv\, !P \mid P$

$$P \equiv Q \quad \Rightarrow \quad n\,[P] \equiv n\,[Q]$$

- Transition relation: $\boxed{P \rightarrow Q}$

Examples: $n\,[\mathsf{in}\; m.\, P \mid Q] \mid m\,[R] \quad \rightarrow \quad m\,[n\,[P \mid Q] \mid R]$

$$P \equiv P' \quad \wedge \quad P' \rightarrow Q' \quad \wedge \quad Q' \equiv Q \quad \Rightarrow \quad P \rightarrow Q$$

Structural congruence relation

$P \equiv P$

$P \equiv Q \wedge Q \equiv R \Rightarrow P \equiv R$

$P \equiv Q \Rightarrow Q \equiv P$

$P \equiv Q \Rightarrow (\nu\, n\colon \mu)\, P \equiv (\nu\, n\colon \mu)\, Q$

$P \equiv Q \Rightarrow (\nu\, \mu)\, P \equiv (\nu\, \mu)\, Q$

$P \equiv Q \Rightarrow P \mid R \equiv Q \mid R$

$P \equiv Q \Rightarrow\, !P \equiv\, !Q$

$P \equiv Q \Rightarrow n\,[P] \equiv n\,[Q]$

$P \equiv Q \Rightarrow m.\, P \equiv m.\, Q$

$P \mid Q \equiv Q \mid P$

$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$

$P \mid \mathbf{0} \equiv P$

$!P \equiv P \mid\, !P$

$!\mathbf{0} \equiv \mathbf{0}$

$(\nu\, n\colon \mu)\, \mathbf{0} \equiv \mathbf{0}$

$(\nu\, \mu)\, \mathbf{0} \equiv \mathbf{0}$

$(\nu\, n\colon \mu)\, (\nu\, n'\colon \mu')\, P \equiv (\nu\, n'\colon \mu')\, (\nu\, n\colon \mu)\, P$ if $n \neq n'$

$(\nu\, \mu)\, (\nu\, \mu')\, P \equiv (\nu\, \mu')\, (\nu\, \mu)\, P$

$(\nu\, n\colon \mu)\, (\nu\, \mu')\, P \equiv (\nu\, \mu')\, (\nu\, n\colon \mu)\, P$ if $\mu \neq \mu'$

$(\nu\, n\colon \mu)\, (P \mid Q) \equiv P \mid (\nu\, n\colon \mu)\, Q$ if $n \notin \underline{\mathsf{fn}}(P)$

$(\nu\, \mu)\, (P \mid Q) \equiv P \mid (\nu\, \mu)\, Q$ if $\mu \notin \underline{\mathsf{fg}}(P)$

$(\nu\, n'\colon \mu)\, (n\,[P]) \equiv n\,[(\nu\, n'\colon \mu)\, P]$ if $n \neq n'$

$(\nu\, \mu)\, (n\,[P]) \equiv n\,[(\nu\, \mu)\, P]$

$(\nu\, n\colon \mu)\, P \equiv (\nu\, n'\colon \mu)\, (P\{n \leftarrow n'\})$ if $n' \notin \underline{\mathsf{fn}}(P)$

$(\nu\, \mu)\, P \equiv (\nu\, \mu')\, (P\{\mu \leftarrow \mu'\})$ if $\mu' \notin \underline{\mathsf{fg}}(P)$

Transition relation

$$P \to Q \Rightarrow (\nu\, n\colon \mu)\, P \to (\nu\, n\colon \mu)\, Q$$

$$P \to Q \Rightarrow (\nu\, \mu)\, P \to (\nu\, \mu)\, Q$$

$$P \to Q \Rightarrow n\,[P] \to n\,[Q]$$

$$P \to Q \Rightarrow P \mid R \to Q \mid R$$

$$P \equiv P' \wedge P' \to Q' \wedge Q' \equiv Q \Rightarrow P \to Q$$

$$n\,[\mathsf{in}\, m.\, P \mid Q] \mid m\,[R] \;\to\; m\,[n\,[P \mid Q] \mid R]$$

$$m\,[n\,[\mathsf{out}\, m.\, P \mid Q] \mid R] \;\to\; n\,[P \mid Q] \mid m\,[R]$$

$$\mathsf{open}\, n.\, P \mid n\,[Q] \;\to\; P \mid Q$$

Secure firewalls

- A perfect firewall
- A model of a firewall
  - some agents are allowed to enter
  - other agents should be prohibited from entering!

A perfect firewall

$$(\nu\, \mathsf{w} : \omega)\ \overset{\mathsf{w}}{\boxed{P}} \qquad \text{where } \mathsf{w} \notin \underline{\mathsf{fn}}(P)$$

The name w is known neither inside P nor outside $(\nu\, \mathsf{w} : \omega)\, \mathsf{w}\, [P]$ — hence it is neither possible for ambients to enter it nor to exit the firewall:

$$\boxed{(\nu\, \mathsf{w} : \omega)\, \mathsf{w}\, [P] \text{ and } \mathbf{0} \text{ are contextually equivalent}}$$

An abstract model of

- an internet firewall named w enclosing a number of machines P
- a sandbox named w enclosing a number of applets P

Contextual equivalence

Informally: Two processes P and Q are contextually equivalent if and only if they admit the same elementary observations whenever they are inserted in an arbitrary enclosing process.

P exhibits the ambient name m if P has the form

$$(\nu n_1 : \mu_1) \cdots (\nu n_k : \mu_k).(\mathsf{m}[P'] \mid P'')$$

where m is not one of $n_1, \cdots n_k$.

P allows the observation of the ambient name m if either P exhibits the name m or $P \rightarrow R$ and R allows the observation of the name m.

P and Q are contextual equivalent if $C(P)$ and $C(Q)$ allows the observations of the same set of ambient names for all contexts $C(-)$.

A model of a firewall

To be useful the firewall should allow selected agents to enter the firewall while keeping others out.

$$(\nu\ \mathsf{w} : \omega)\ \mathsf{w}\Big[\ \mathsf{k}\big[\ \mathsf{out}\ \mathsf{w}.\mathsf{in}\ \mathsf{k}'.\mathsf{in}\ \mathsf{w}\ \big] \mid \mathsf{open}\ \mathsf{k}'.\mathsf{open}\ \mathsf{k}''.P\ \Big]$$

Secret name of the firewall: w
Passwords: k, k', k''

- Agents knowing the passwords should be allowed to enter the firewall:
  - easy: check that agents of a specific form can enter
- Agents <u>not</u> knowing the passwords should <u>not</u> be allowed enter:
  - hard: we cannot inspect all agents

Agents knowing the passwords

The firewall

$$(\nu\ \mathsf{w} : \omega)\ \overset{\mathsf{w}}{\boxed{\overset{\mathsf{k}}{\boxed{\mathsf{out}\ \mathsf{w}.\mathsf{in}\ \mathsf{k}'.\mathsf{in}\ \mathsf{w}}}\ \mid\ \mathsf{open}\ \mathsf{k}'.\mathsf{open}\ \mathsf{k}''.P}}$$

can be entered by agents of the form

$$\overset{\mathsf{k'}}{\boxed{\mathsf{open}\ \mathsf{k}.\ \overset{\mathsf{k''}}{\boxed{Q}}}}$$

and gives rise to

$$(\nu\ \mathsf{w} : \omega)\ \overset{\mathsf{w}}{\boxed{P\ \mid\ Q}}$$

Contextual equivalence

$\boxed{\mathsf{Firewall} \mid \mathsf{Agent} \text{ and } (\nu\, \mathsf{w} : \omega)\, \mathsf{w}\, [P \mid Q] \text{ are contextually equivalent}}$

This means that for all contexts $C(-)$:

$C(\mathsf{Firewall} \mid \mathsf{Agent})$, and

$C((\nu\, \mathsf{w} : \omega)\, \mathsf{w}\, [P \mid Q])$

allow the same set of ambient names to be observed.

This means that for all m:

$$\begin{array}{ll} \text{If} & C(\mathsf{Firewall} \mid \mathsf{Agent}) \quad \rightarrow^* (\nu n_1 : \mu_1) \cdots (\nu n_k : \mu_k).(\mathsf{m}[\cdots] \mid \cdots) \\ \text{then} & C((\nu\, \mathsf{w} : \omega)\, \mathsf{w}\, [P \mid Q]) \rightarrow^* (\nu n'_1 : \mu'_1) \cdots (\nu n'_{k'} : \mu'_{k'}).(\mathsf{m}[\cdots] \mid \cdots) \end{array}$$

and vice versa.

An agent knowing the passwords

w $\boxed{\text{k } \boxed{\text{out w. in k'. in w}} \mid \text{open k'. open k''. } P}$ $\mid$ k' $\boxed{\text{open k. k'' } \boxed{Q}}$

$\longrightarrow$ w $\boxed{\text{open k'. open k''. } P}$ $\mid$ k $\boxed{\text{in k'. in w}}$ $\mid$ k' $\boxed{\text{open k. k'' } \boxed{Q}}$

$\longrightarrow$ w $\boxed{\text{open k'. open k''. } P}$ $\mid$ k' $\boxed{\text{k } \boxed{\text{in w}} \mid \text{open k. k'' } \boxed{Q}}$

$\longrightarrow$ w $\boxed{\text{open k'. open k''. } P}$ $\mid$ k' $\boxed{\text{in w} \mid \text{k'' } \boxed{Q}}$

$\longrightarrow$ w $\boxed{\text{open k'. open k''. } P \mid \text{k' } \boxed{\text{k'' } \boxed{Q}}}$ $\longrightarrow$ w $\boxed{\text{open k''. } P \mid \text{k'' } \boxed{Q}}$ $\longrightarrow$ w $\boxed{P \mid Q}$

The probe is sent
out of the firewall
to fetch the agent

Agents <u>not</u> knowing the passwords

- an agent that does not initially know the passwords might learn them subsequently
- the firewall might contain a trap door through which agents might enter

How can we ensure that agents not knowing the passwords cannot enter?

An agent learning the passwords

The agent $\overset{\mathsf{e}}{\boxed{\mathsf{in\ t.}\ R}}$

can enter the firewall $(\nu\ \mathsf{w} : \omega)\ \overset{\mathsf{w}}{\boxed{\overset{\mathsf{k}}{\boxed{\mathsf{out\ w.in\ k'.in\ w}}}\ \mid\ \mathsf{open\ k'.open\ k''}.P}}$

when placed in a context with $\overset{\mathsf{t}}{\boxed{\mathsf{open\ e.\ in\ k'}}}\ \mid\ \overset{\mathsf{k'}}{\boxed{\mathsf{open\ t} \mid \mathsf{open\ k.}\ \overset{\mathsf{k''}}{\boxed{Q}}}}$

giving rise to $(\nu\ \mathsf{w} : \omega)\ \overset{\mathsf{w}}{\boxed{P \mid Q \mid R}}$

A firewall with a trap door

The agent $\overset{\mathsf{e}}{\boxed{\mathsf{in}\,\mathsf{t}.\ R}}$

can enter the firewall

$$(\nu \mathsf{w} : \omega)\ \overset{\mathsf{w}}{\boxed{\overset{\mathsf{k}}{\boxed{\mathsf{out}\,\mathsf{w}.\mathsf{in}\,\mathsf{k}'.\mathsf{in}\,\mathsf{w}}} \mid \mathsf{open}\,\mathsf{k}'.\mathsf{open}\,\mathsf{k}''.P \mid \mathsf{open}\,\mathsf{t} \mid \overset{\mathsf{t}}{\boxed{\mathsf{out}\,\mathsf{w}.\ \mathsf{in}\,\mathsf{w}.\ \mathsf{open}\,\mathsf{e}}} \mid \overset{\mathsf{k}'}{\boxed{}} \mid \overset{\mathsf{k}''}{\boxed{}}}}$$

giving rise to

$$(\nu \mathsf{w} : \omega)\ \overset{\mathsf{w}}{\boxed{\overset{\mathsf{k}}{\boxed{\mathsf{out}\,\mathsf{w}.\mathsf{in}\,\mathsf{k}'.\mathsf{in}\,\mathsf{w}}} \mid P \mid R}}$$