Modélisation des protocoles cryptographiques et non-interférence

John MULLINS

École Polytechnique de Montréal

IRCCyN, Nantes, Juin 2008

ÉCOLE POLYTECHNIQUE MONTRÉAL

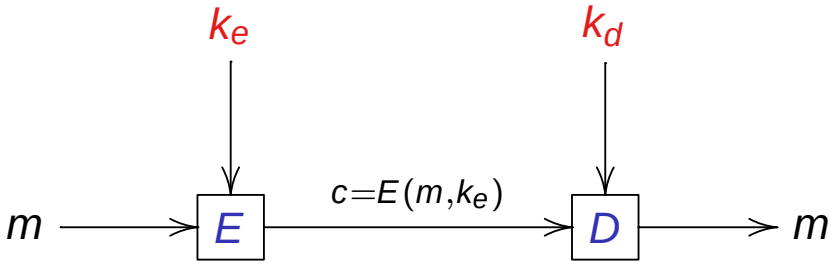
Contenu de la présentation

1. Introduction aux protocoles cryptographiques
   - Primitives cryptographiques
   - Terminologie
   - Taxonomie des attaques
   - Propriétés de sécurité
2. Modélisation des protocoles
   - Modélisation des messages et des primitives cryptographiques
   - Modélisation des participants
   - Modélisation de l'environnement
3. Spécification des propriétés de sécurité
   - Non interférence
   - Interference admissible
4. Vérification
5. Conclusion

ÉCOLE POLYTECHNIQUE MONTRÉAL

Crypto-systèmes

- $\mathcal{M}$: Espace de messages
- $\mathcal{C}$: Espace de cryptogrammes
- $\mathcal{K}$: Espace de clés
- $E : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}$: fonction de chiffrement
- $D : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$: fonction de déchiffrement

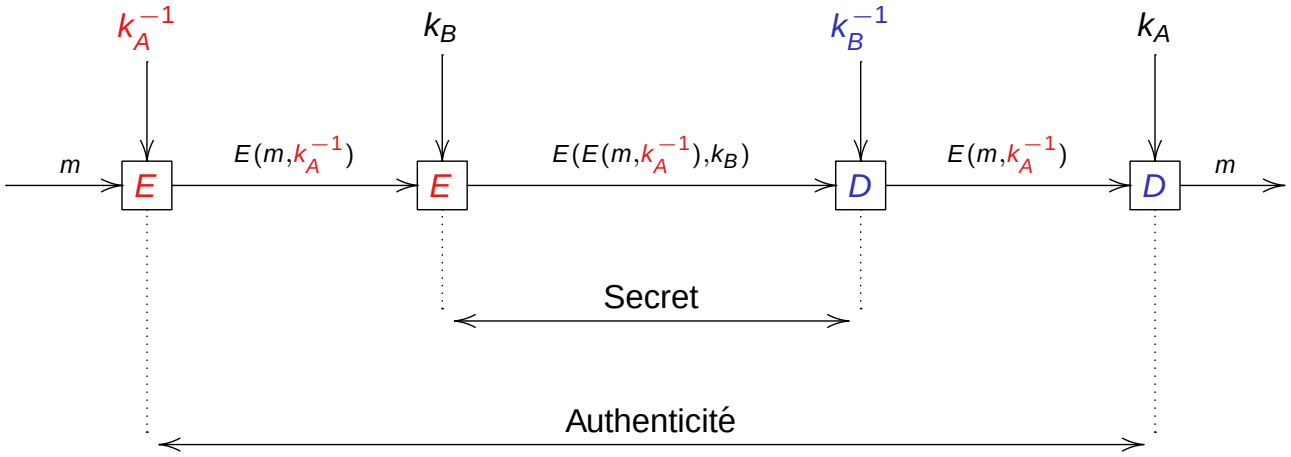


- $k_e = k_d$: chiffrement symétrique
- $k_e \neq k_d$: chiffrement à clé asymétrique

Propriétés générales

- $\forall_{k \in \mathcal{K}} \forall_{m \in \mathcal{M}} \exists_{c \in \mathcal{C}} E(m,k) = c$
- $\forall_{k \in \mathcal{K}} \forall_{m \in \mathcal{M}} \exists_{k^{-1} \in \mathcal{K}} D(E(m,k), k^{-1}) = m$
- Le secret dépend de k (E et D sont publiques)

Propriétés de sécurité des crypto-systèmes



Secret

- Connaissant $E(m,k)$ il est difficile de déduire k^{-1}
- Sans k^{-1} il est difficile d'obtenir m

Authenticité

- Connaissant $E(m,k^{-1})$ il est difficile de déduire k^{-1}
- Sans k^{-1} et connaissant m, il est difficile de construire $E(m,k^{-1})$

Le protocole d'authentification de Needham-Schröder

Definition (Protocole cryptographique)

Un protocole cryptographique est un ensemble de règles d'échange entre les points d'un réseau, basé sur les crypto-systèmes qui permettent de sécuriser les communications dans un environnement hostile.

$$\begin{array}{lccc} \text{Message 1 :} & A & \xrightarrow{\{A,n_A\}_{k_B}} & B \\ \text{Message 2 :} & B & \xrightarrow{\{n_A,n_B\}_{k_A}} & A \\ \text{Message 3 :} & A & \xrightarrow{\{n_B\}_{k_B}} & B. \end{array}$$

Deux agents, un qui joue le rôle A(lice), l'autre celui de B(ob).
Clés : clés publiques k_A, k_B (ou symétriques) utilisées par les cryptosystèmes.
Nonces : nombres aléatoires n_A, n_B générés à chaque session.
Messages : obtenus à partir de constantes par pairage $\langle _, _ \rangle$, chiffrement $\{_\}__$ par une clé, hashing, etc.

Session : un agent peut jouer le rôle A dans une session, B dans une autre, plusieurs sessions en parallèle, pour différentes valeurs de nonces, etc.

ÉCOLE POLYTECHNIQUE MONTRÉAL

L'environnement

Definition (Attaque)

Une attaque est une exécution du protocole qui ne satisfait pas les propriétés de sécurité requises

N-S doit assurer l'authentification :lorsque le protocole se termine correctement, Alice s'est authentifiée à Bob et réciproquement.

Hypothèses sur l'environnement

- Intercepte et analyse tous les messages du réseau (Environnement passif)
- Synthétise et envoie tous les messages qu'il veut (Environnement actif)

Hypothèse sur le crypto-système

- Boîte noire parfaite : Déduire m de $\{m\}_k$ requiert k^{-1}

ÉCOLE POLYTECHNIQUE MONTRÉAL

L'attaque *Man-in-the-middle* de N-S (Lowe)

- 3 agents A, B honnêtes et E, malhonnête
- 2 sessions en parallèle

$$A \xrightarrow{\{A,n_A\}_{k_E}} E$$

$$E \longrightarrow E(A)$$

$$E(A) \xrightarrow{\{A,n_A\}_{k_B}} B$$

$$A \xleftarrow{\{n_A,n_B\}_{k_A}} B$$

$$A \xrightarrow{\{n_B\}_{k_E}} E$$

$$E \longrightarrow E(A)$$

$$E(A) \xrightarrow{\{n_B\}_{k_B}} B$$

B est convaincu de parler à A

ÉCOLE POLYTECHNIQUE MONTRÉAL

La correction de N-S (Lowe)

$$
\begin{array}{lcl}
\text{Message 1 :} & A \xrightarrow{\{A,n_A\}_{k_B}} & B \\
\text{Message 2 :} & B \xrightarrow{\{B,n_A,n_B\}_{k_A}} & A \\
\text{Message 3 :} & A \xrightarrow{\{n_B\}_{k_B}} & B.
\end{array}
$$

- Prouvé formellement en utilisant la logique épistémique BAN
- n_B reste secret même en un nombre arbitraire de session

ÉCOLE POLYTECHNIQUE MONTRÉAL

L'attaque de type de la variante à N-S-L (Millen)

$$\begin{array}{lcl} \text{Message 1 :} & A \xrightarrow{\{A,n_A\}_{k_B}} & B \\ \text{Message 2 :} & B \xrightarrow{\{n_A,n_B,B\}_{k_A}} & A \\ \text{Message 3 :} & A \xrightarrow{\{n_B\}_{k_B}} & B. \end{array}$$

$$\begin{tikzcd} E \arrow[r, "\{A,\underbrace{E}_{n_{E(A)}}\}_{k_B}"] & B \arrow[d] & \\ & B \arrow[r, "\{E,\underbrace{n_B,B}_{n_E}\}_{k_A}"] & A \end{tikzcd}$$

$$E \xleftarrow{\{n_B,B,n_A,A\}_{k_E}} A$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

L'attaque par rejeu de N-S à clé symétrique

Message 1 :	A	$\xrightarrow{\{A,B,n_A\}_{k_{SA}}}$	S
Message 2 :	S	$\xrightarrow{\{n_A,B,k_{AB},\{k_{AB},A\}_{k_{SB}}\}_{k_{SA}}}$	A
Message 3 :	A	$\xrightarrow{\{k_{AB},A\}_{k_{SB}}}$	B
Message 4 :	B	$\xrightarrow{\{n_B\}_{k_{AB}}}$	A
Message 5 :	A	$\xrightarrow{\{n_B-1\}_{k_{AB}}}$	B

$$E(A) \xrightarrow{\{k'_{AB},A\}_{k_{SB}}} B$$

$$E(A) \xleftarrow{\{n_B\}_{k'_{AB}}} B$$

$$E(A) \xrightarrow{\{n_B-1\}_{k'_{AB}}} B$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Definition (Secret)

Une donnée s est secrète s'il n'existe aucune exécution du protocole où l'environnement peut apprendre la valeur de s (Problème d'accessibilité).

Variantes

1. Équivalence observationnelle : La session contenant s est, pour l'environnement, indistinguable de toute session contenant s'
2. Non interférence : s ne peut être correlée à aucune donnée publique.

Definition (Authentification)

Si A émet $\{n_B\}_{k_B}$ alors n_B a été engendré par B (Problème d'accessibilité).

Variantes

1. Secret particulier : A émet $\{n_B\}_{k_B}$ et n_B a été engendré par B ssi n_A est secret (et dualement).
2. Forme duale du secret : Une donnée de l'environnement ($\{A, n_A\}_{k_E}$) ne doit pas être apprise de A ou B (ne peut être correlée à $\{n_B\}_{k_B}$) (Non interférence).

Definition (Anonymat)

Un protocole préserve l'anonymat du participant s jouant le rôle A si le protocole où s joue le rôle A est, pour l'environnement, indistinguable du protocole où s' joue le rôle A (Equivalence observationnelle)

Example

- $A \xrightarrow{\{A\}_{k_B}} B$ ne préserve pas l'anonymat de A

$$\text{E-vote} : A \xrightarrow{\{A,Bush\}_{k_B}} B$$

- $A \xrightarrow{\{A,N\}_{k_B}} B$ préserve l'anonymat de A

Definition (Equité)

Un protocole est équitable pour A si B n'a pas de stratégie gagnante pour obtenir le contrat signé par A à moins que A en ait une pour obtenir le contrat signé par B (Théorie des jeux)

ÉCOLE POLYTECHNIQUE MONTRÉAL

- Algèbre de messages

$$m \quad := \quad m_i \quad | \quad k \quad | \quad (m, m) \quad | \quad \{m\}_k$$

Induit des hypothèses fortes !

1. Il est impossible d'inférer m de $\{m\}_k$ sans la connaissance de k
2. $\{m\}_k = \{m'\}_{k'}$ ssi $m = m'$ et $k = k'$
3. $\{\{m\}_k\}_k \neq m$

- Règles d'inférence de messages

$$\vdash_{pair} \frac{m_1 \quad m_2 \quad \cdots \quad m_n}{(m_1, m_2, \ldots, m_n)} \qquad \vdash_{p_i} \frac{(m_1, \ldots, m_n)}{m_i} \; i \leq n$$

$$\vdash_{enc} \frac{m \quad K}{\{m\}_K} \qquad \vdash_{dec} \frac{\{m\}_K \quad K^{-1}}{m}$$

$$\vdash_{hash} \frac{m}{h(m)}$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Algèbres de processus

Algèbres de processus

Permet une représentation symbolique de l'environnement : l'attaquant peut envoyer des messages en fonction du résultat des comparaisons des messages observés.

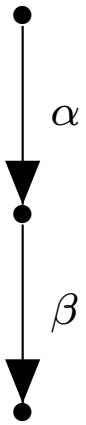
ÉCOLE POLYTECHNIQUE MONTRÉAL

Algèbres de processus

Algèbres de processus

Permet une représentation symbolique de l'environnement : l'attaquant peut envoyer des messages en fonction du résultat des comparaisons des messages observés.

$P = \alpha.\beta.P'$



P'

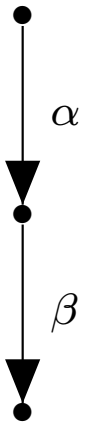
ÉCOLE POLYTECHNIQUE MONTRÉAL

Algèbres de processus

Algèbres de processus

Permet une représentation symbolique de l'environnement : l'attaquant peut envoyer des messages en fonction du résultat des comparaisons des messages observés.

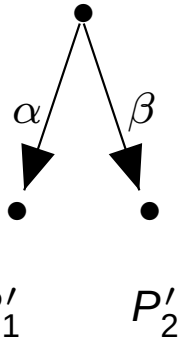
$P = \alpha.\beta.P'$



$P_1 = \alpha.P_1'$

$P_2 = \beta.P_2'$

$P = P_1 + P_2$

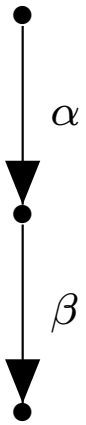


Algèbres de processus

Algèbres de processus

Permet une représentation symbolique de l'environnement : l'attaquant peut envoyer des messages en fonction du résultat des comparaisons des messages observés.

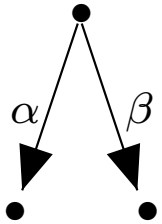
$P = \alpha.\beta.P'$



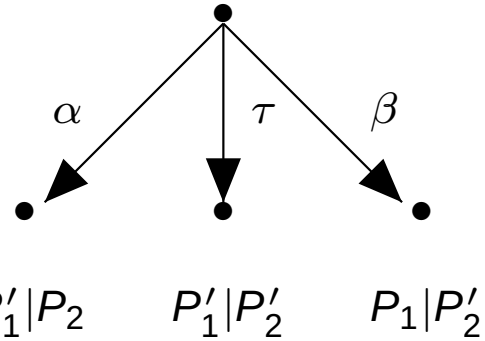
$P_1 = \alpha.P_1'$

$P_2 = \beta.P_2'$

$P = P_1 + P_2$



$P = P_1|P_2 \quad (\beta = \overline{\alpha})$



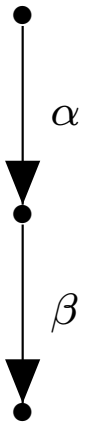
ÉCOLE POLYTECHNIQUE MONTRÉAL

Algèbres de processus

Algèbres de processus

Permet une représentation symbolique de l'environnement : l'attaquant peut envoyer des messages en fonction du résultat des comparaisons des messages observés.

$P = \alpha.\beta.P'$

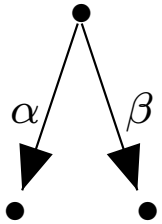


P'

$P_1 = \alpha.P_1'$

$P_2 = \beta.P_2'$

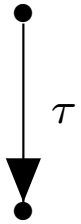
$P = P_1 + P_2$



P_1' P_2'

Communication restreinte

$P = (P_1|P_2) \setminus \{\alpha, \overline{\alpha}\}$



$(P_1'|P_2') \setminus \{\alpha, \overline{\alpha}\}$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Passage de valeurs

Soit $\mathbb{D}$, un domaine dénombrable de valeurs et x, une variable à valeurs dans $\mathbb{D}$

$$c(x).P(x) \stackrel{def}{=} \sum_{d \in \mathbb{D}} c(d).P(d/x)$$

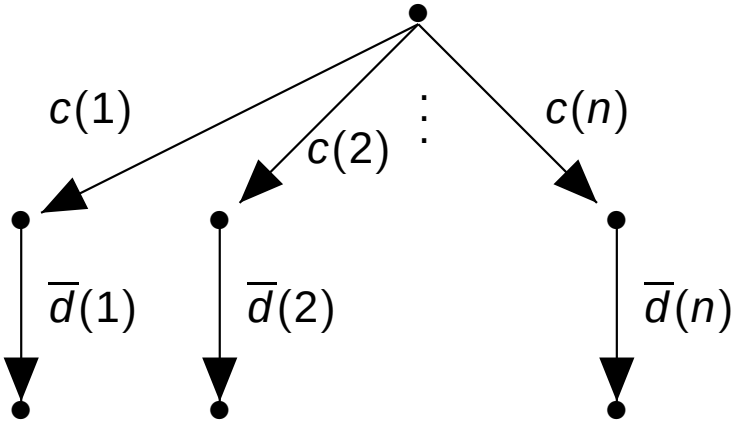
Passage de valeurs

Soit $\mathbb{D}$, un domaine dénombrable de valeurs et x, une variable à valeurs dans $\mathbb{D}$

$$c(x).P(x) \stackrel{def}{=} \sum_{d \in \mathbb{D}} c(d).P(d/x)$$

Example

$$\begin{aligned} P(x) &= c(x).Q(x) \\ Q(x) &= \overline{d}(x).0 \end{aligned}$$



La syntaxe

P	$:=$	$\mathbf{0}$	empty agent
	$\mid$	$c(x).P$	input
	$\mid$	$\tau.P$	internal action
	$\mid$	$\overline{c}(m).P$	output
	$\mid$	$P + P$	non-deterministic choice
	$\mid$	$P \mid P$	parallel composition
	$\mid$	$P \backslash L$	restriction of L-actions
	$\mid$	$A(m_1, m_2, \ldots, m_n)$	principal
	$\mid$	$[\langle m_1, m_2, \ldots, m_n \rangle \vdash_{op} x]P$	message handling
	$\mid$	$[m = m']P$	matching

ÉCOLE POLYTECHNIQUE MONTRÉAL

La sémantique opérationnelle

OUT
$$\frac{-}{\overline{c}(m).P \xrightarrow{\overline{c}(m)} P}$$

IN
$$\frac{-}{c(x).P \xrightarrow{c(m)} P[m/x]}$$

SUM 1
$$\frac{P_1 \xrightarrow{\alpha} P_1'}{P_1 + P_2 \xrightarrow{\alpha} P_1'}$$

SUM 2
$$\frac{P_2 \xrightarrow{\alpha} P_2'}{P_1 + P_2 \xrightarrow{\alpha} P_2'}$$

PAR 1
$$\frac{P_1 \xrightarrow{\alpha} P_1'}{P_1 | P_2 \xrightarrow{\alpha} P_1' | P_2}$$

PAR 2
$$\frac{P_2 \xrightarrow{\alpha} P_2'}{P_1 | P_2 \xrightarrow{\alpha} P_1 | P_2'}$$

SYN
$$\frac{P_1 \xrightarrow{\overline{c}(m)} P_1' \text{ and } P_2 \xrightarrow{c(m)} P_2'}{P_1 | P_2 \xrightarrow{\tau} P_1' | P_2'}$$

RES
$$\frac{P \xrightarrow{\alpha} P' \quad \alpha \notin L \cup \overline{L}}{P \backslash L \xrightarrow{\alpha} P' \backslash L}$$

MATCH
$$\frac{P \xrightarrow{\alpha} P'}{[m{=}m]P \xrightarrow{\alpha} P'}$$

INS
$$\frac{P[m_1/x_1,\ldots,m_n/x_n] \xrightarrow{\alpha} P' \quad A(x_1,\ldots,x_n) \stackrel{def}{=} P \in D}{A(m_1,\ldots,m_n) \xrightarrow{\alpha} P'}$$

INF
$$\frac{\langle m_1,\ldots,m_n\rangle \vdash_{op} m \text{ and } P[m/x] \xrightarrow{\alpha} P'}{[\langle m_1,\ldots,m_n\rangle \vdash_{op} x]P \xrightarrow{\alpha} P'}$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Message 1 : $A \xrightarrow{\{A,n_A\}_{k_B}} B$

Message 2 : $B \xrightarrow{\{n_A,n_B\}_{k_A}} A$

Message 3 : $A \xrightarrow{\{n_B\}_{k_B}} B$.

Example (Needham Schröder)

$$
\begin{aligned}
A(n_A) &\stackrel{def}{=} \overline{c}(msg1).c(x).check_{msg_2}(x)\overline{c}(msg3).\mathbf{0} \\
B(n_B) &\stackrel{def}{=} c(y).check_{msg_1}(y)\overline{c}(msg2).c(z).check_{msg_3}(z).\mathbf{0} \\
P &\stackrel{def}{=} A(n_A)|B(n_B)
\end{aligned}
$$

where

$$
\begin{aligned}
\overline{c}(msg1) &\equiv [\langle A, n_A\rangle \vdash_p i][\langle i, k_B\rangle \vdash_{enc} j]\overline{c}(j) \\
check_{msg_2}(x) &\equiv [\langle x, k_A\rangle \vdash_{dec} q][\langle q\rangle \vdash_{u1} r][r = n_A] \\
\overline{c}(msg3) &\equiv [\langle q\rangle \vdash_{u2} s][\langle s, k_B\rangle \vdash_{enc} t]\overline{c}(t)
\end{aligned}
$$

Environnement hostile

- Processus quelconque Un attaquant ne peut être modélisé par un processus quelconque interagissant avec le protocole à travers ses canaux publics.

Problème : attaquants trop forts !

- $P = c_1(pw)[pw = "MaPoule"]\overline{c_2}("OK").\mathbf{0}$
- $\Pi = \overline{c_1}("MaPoule").\mathbf{0}$: un attaquant admissible ?

Solution

- Contraindre les attaquants par leur base de connaissance.
- L'attaquant ne peut émettre un message que s'il peut l'inférer de sa base de connaissance ϕ selon les règles ci-dessous.

- Règles de synthèse

AX $\frac{m \in \phi}{\phi \vdash m}$ PAIR $\frac{\phi \vdash m_1 \ \cdots \ \phi \vdash m_n}{\phi \vdash \langle m_1, \cdots, m_n \rangle}$ ENC $\frac{\phi \vdash m \ \ \phi \vdash k}{\phi \vdash \{m\}_k}$

- Règles d'analyse

P_i $\frac{\phi \vdash \langle m_1, \cdots, m_i, \cdots, m_n \rangle}{\phi \vdash m_i}$ DEC $\frac{\phi \vdash \{m\}_k \ \ \phi \vdash k^{-1}}{\phi \vdash m}$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Definition

L'ensemble d'attaquants admissibles de connaissance initiale ϕ est dénoté par

$$\mathcal{E}nemy_{\phi} = \{\Pi \in \mathcal{P}roc \mid ID(\Pi) \subseteq \mathcal{D}(\phi)\}$$

- $ID(P)$: ensemble des messages qui apparaissent syntaxiquement dans P.
- $\mathcal{D}(\phi)$: ensemble des messages dérivables de ϕ.

Example

Le processus $\Pi = c(x).[(x,a) \vdash_{dec} y][y = m]\overline{c}(\{m'\}_a).\mathbf{0}$ est un attaquant admissible pour la base de connaissance initiale

$$\phi = \{\langle a, b\rangle, \{m\}_a, \{m'\}_a\}$$

puisque $ID(\Pi) = \{a, m, \{m'\}_a\} \subseteq \mathcal{D}(\phi)$. En effet,

ÉCOLE POLYTECHNIQUE MONTRÉAL

Système de transitions environnementiel

- Représentation implicite des interactions des intrus admissibles avec le protocole
- Les états sont des configurations de la forme :

$$\phi \rhd P$$

- Transitions :

$$\phi \rhd P \xrightarrow{\alpha} \phi' \rhd P'$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Sémantique symbolique environnementielle

Réduction symbolique

Chaque message du protocole reçu de l'environnement est dérivable des connaissances de l'environnement.

OUT
$$\frac{P \xrightarrow{\overline{c}(m)} P'}{\phi \rhd P \xrightarrow{\overline{c}(m)} \phi \cup \{m\} \rhd P'}$$

IN
$$\frac{P \xrightarrow{c(m)} P' \quad \phi \vdash m}{\phi \rhd P \xrightarrow{c(m)} \phi \rhd P'}$$

TAU
$$\frac{P \xrightarrow{\tau} P'}{\phi \rhd P \xrightarrow{\tau} \phi \rhd P'}$$

Example (Attaque de NS)

$$\phi = \{A, B, E, k_A, k_B, k_E, k_E^{-1}\}$$

$$\begin{tikzcd}
\phi \rhd P \arrow[r, "\overline{c}(\{A,n_A\}_{k_E})"] & \phi \cup \{n_A\} \rhd P_1 \arrow[r, "c(\{A,n_A\}_{k_B})"] & \phi \cup \{n_A\} \rhd P_2 \arrow[d, equal] \\
\phi \cup \{n_A\} \rhd P_4 \arrow[d, equal] & \phi \cup \{n_A\} \rhd P_3 \arrow[l, "c(\{n_A,n_B\}_{k_A})"'] & \phi \cup \{n_A\} \rhd P_2 \arrow[l, "\overline{c}(\{n_A,n_B\}_{k_A})"'] \\
\phi \cup \{n_A\} \rhd P_4 \arrow[r, "\overline{c}(\{n_B\}_{k_E})"] & \phi \cup \{n_A, n_B\} \rhd P_5 \arrow[r, "c(\{n_B\}_{k_B})"] & \phi \cup \{n_A, n_B\} \rhd P_6
\end{tikzcd}$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Information flow approach to secrecy

Definition (Non Interference (McLean94))

A process satisfies non interference if there is no information flow from high-level to low-level.

- There is information flow from *Hi* to a *Lo* if high-level behaviour can be infered from the low-level observation.

Definition (SNNI (Focardi-Gorrieri95))

P satisfies Strong Non-deterministic Non Interference (SNNI) if and only if

$$\mathbf{P} \simeq_{\mathcal{O}_{Lo}} \mathbf{P} \setminus Hi$$

MONTRÉAL

Example

P :

$$\cdot \xrightarrow{\alpha} \cdot \xrightarrow{\beta} \cdot$$

Q :

$$\begin{tikzcd} \cdot \arrow[r, "\alpha"] \arrow[d, "\beta"] & \cdot \arrow[d, "\beta"] \\ \cdot & \cdot \end{tikzcd}$$

For $\alpha \in Hi$
and $\beta \in Lo$

1. Causal dependency in **P** : $\alpha \Longrightarrow \beta$

Indeed !

P $\setminus Hi$: $\cdot$

P$/\mathcal{O}_{Lo}$: $\cdot \xrightarrow{\tau} \cdot \xrightarrow{\beta} \cdot$

2. No causal dependency in **Q**.

Example

$$P \stackrel{def}{=} h(x).[x = k]l.\mathbf{0}$$
$$Q \stackrel{def}{=} l.\mathbf{0} + h(x).l.\mathbf{0}$$

1. Causal dependency in **P** : $x = k \Longrightarrow l$

Indeed !

$\mathbf{P} \setminus Hi : \cdot$

$\mathbf{P}/\mathcal{O}_{Lo} : \cdot \xleftarrow{\tau} \cdot \xrightarrow{\tau} \cdot \xrightarrow{l} \cdot$

2. No causal dependency in **Q**.

ÉCOLE POLYTECHNIQUE MONTRÉAL

Admissible Interference

Definition (Interférence Admissible (Mullins 02))

P satisfies Non-deterministic Admissible Interference (NAI) if and only if

$$\forall_{\mathbf{Q}:\mathbf{P}\xrightarrow{*}\mathbf{Q}} (\mathbf{Q} \setminus Dwn) \text{ satisfies SNNI}$$

Example

$$P \stackrel{def}{=} h(x).[x = k]d.l.\mathbf{0}$$
$$Q \stackrel{def}{=} h_1(x).[x = k_1]d.h_2(y).[y = k_2]l.\mathbf{0}$$

1. Admissible causal dependency in **P** : $x = k \Longrightarrow d$
2. Inadmissible causal dependency in **Q**.

Indeed ! $\mathbf{Q}\xrightarrow{*}\mathbf{Q}' \stackrel{def}{=} h_2(y).[y = k_2]l.\mathbf{0}$ and $\mathbf{Q}' \simeq \mathbf{Q}' \setminus \{d\}$ is not SNNI

Environment-sensitive process equivalence

Definition (equivalence under ϕ)

P and **Q** are *equivalent under* ϕ (**P** $\simeq_\phi$ **Q**) iff

$$(\phi \rhd P) \simeq (\phi \rhd Q)$$

Proposition

If **P** $\simeq$ **Q** then **P** $\simeq_\phi$ **Q**

Example (Not the converse !)

$$P \stackrel{def}{=} h(x).[x = k]l.\mathbf{0}$$
$$Q \stackrel{def}{=} h(x).\mathbf{0}$$

P $\not\simeq$ **Q** but for any ϕ s.t. $\phi \not\vdash k$ we have : **P** $\simeq_\phi$ **Q**

Environment-sensitive non interference

Definition (SNNI$^{\phi}$ (Bugliesi-Rossi05))

P satisfies Strong Non-deterministic Non Interference under ϕ (SNNI$^{\phi}$) if and only if

$$\mathbf{P} \simeq^{\phi}_{\mathcal{O}_{Lo}} \mathbf{P} \setminus Hi$$

Example

$$P \stackrel{def}{=} h(x).[x = k]l.\mathbf{0}$$

P $\notin$ SNNI but for any ϕ s.t. $\phi \not\vdash k$ we have : **P** $\in$ SNNI$^{\phi}$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Environment-sensitive admissible interference

Definition (NAI$^\phi$)

P satisfies Admissible interference under ϕ (NAI$^\phi$) if and only if

$$\forall_{\mathbf{Q}:\mathbf{P}\xrightarrow{*}\mathbf{Q}}(\mathbf{Q} \setminus \Sigma_D) \text{ satisfies SNNI}^\phi$$

Proposition

If **P** is NAI then **P** is NAI$^\phi$

Example (Not the converse !)

$$P \stackrel{def}{=} h_1(x).[x = k_1]d.h_2(y).[y = k_2]l.\mathbf{0}$$

P $\notin$ NAI but for any ϕ s.t. $\phi \not\vdash k_2$ we have : **P** $\in$ NAI$^\phi$

POLYTECHNIQUE
MONTRÉAL

Le secret basé sur la NAI$^{\phi}$

Definition (Idéal)

Soit $\mathcal{S}$, ensemble des messages secrets échangés dans le protocole et $\phi \subseteq \mathcal{S}$. L'idéal de $\mathcal{S}$ (noté $I_{\phi}(\mathcal{S})$) relativement à ϕ est le plus petit ensemble t.q.

1. si $m_1 \in I_{\phi}(\mathcal{S})$ ou $m_2 \in I_{\phi}(\mathcal{S})$ alors $\langle m_1, m_2 \rangle \in I_{\phi}(\mathcal{S})$
2. si $m \in I_{\phi}(\mathcal{S})$ et $k^{-1} \notin I_{\phi}(\mathcal{S})$ alors $\{m\}_k \in I(\mathcal{S})$

Intuition

Dans le contexte ϕ des connaissance de l'intrus, il suffit qu'un terme de $\mathcal{I}_{\phi}(S)$ soit compromis pour qu'un terme de S le soit.

ÉCOLE POLYTECHNIQUE MONTRÉAL

Propriété du secret basé sur la NAI$^{\phi}$

Actions de déclassification

Definition (Fonction de décoration)

$\gamma_{\phi}^{\mathcal{S}} : \mathcal{P}roc \longrightarrow \mathcal{P}roc$ relativement à $\mathcal{S}$ et ϕ, est la fonction définie par

$$\forall_{P \in \mathcal{P}roc}\ P \xrightarrow{\alpha} Q \Rightarrow \begin{cases} \gamma_{\phi}^{\mathcal{S}}(P) \xrightarrow{\alpha} \overline{d}(m).\gamma_{\phi \cup \{m\}}^{\mathcal{S}}(Q) \\ \qquad \text{si } \alpha \in H \text{ est de la forme } \overline{c}(m) \text{ et } m \notin I_{\phi \cup \{m\}}(\mathcal{S}) \\ \gamma_{\phi}^{\mathcal{S}}(P) \xrightarrow{\alpha} \gamma_{\phi \cup \{m\}}^{\mathcal{S}}(Q) \\ \qquad \text{si } \alpha \in H \text{ est de la forme } \overline{c}(m) \text{ et } m \in I_{\phi \cup \{m\}}(\mathcal{S}) \\ \gamma_{\phi}^{\mathcal{S}}(P) \xrightarrow{\alpha} \gamma_{\phi}^{\mathcal{S}}(Q) \qquad \text{sinon} \end{cases}$$

Example

1. $K \notin \phi$
2. $P = \overline{c}(\{M\}_K).\mathbf{0} \ \Rightarrow\ \gamma_{\phi}^{\mathcal{S}}(P) = \overline{c}(\{M\}_K).\overline{d}(\{M\}_K).\mathbf{0}.$
3. $P = \overline{c}(M).Q \ \Rightarrow\ \gamma_{\phi}^{\mathcal{S}}(P) = \overline{c}(M).\gamma_{\phi}^{\mathcal{S}}(Q).$

Actions de bas niveau

1. $c_{\mathcal{S}}$: un canal public de domaine $\mathcal{S}$, ne faisant pas partie des canaux public du protocole.
2. $c_{\mathcal{S}}$: un canal de bas niveau de domaine $\mathcal{S}$.
3. $\mathrm{Spec}_{\mathcal{S}}(P) = P|c_{\mathcal{S}}(x).\overline{l_{\mathcal{S}}}(x).\mathbf{0}$.

Theorem (S. Hamadou (2008))

P assure la confidentialité de $\mathcal{S}$ contre tout attaquant de connaissance initiale ϕ si et seulement si

$$\gamma_{\phi}^{\mathcal{S}}(\mathrm{Spec}_{\mathcal{S}}(P)) \in NAI_{\phi}$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Example (Le secret de n_B dans Needham-Schröder)

On a :

$$\phi \rhd P \Longrightarrow^* \phi \cup \{n_A\} \rhd P_4 \qquad\qquad \phi = \{A, B, E, k_A, k_B, k_E, k_E^{-1}\}$$

et

$$(\phi \cup \{n_A\} \rhd P_4)/Hi \cup D \xrightarrow{\tau \cdot c(\{n_B\}_{k_B})} \bullet$$

Mais

$$(\phi \cup \{n_A\} \rhd P_4)\backslash Hi \cup D \overset{\tau^* \cdot c(\{n_B\}_{k_B})\tau^*}{\not\longrightarrow} \bullet$$

$$\begin{tikzcd}
\phi \rhd P \arrow[r, "\overline{c}(\{A,n_A\}_{k_E})"] & \phi \cup \{n_A\} \rhd P_1 \arrow[r, "c(\{A,n_A\}_{k_B})"] & \phi \cup \{n_A\} \rhd P_2 \arrow[d, equal] \\
\phi \cup \{n_A\} \rhd P_4 \arrow[d, equal] & \phi \cup \{n_A\} \rhd P_3 \arrow[l, "c(\{n_A,n_B\}_{k_A})"'] & \phi \cup \{n_A\} \rhd P_2 \arrow[l, "\overline{c}(\{n_A,n_B\}_{k_A})"'] \\
\phi \cup \{n_A\} \rhd P_4 \arrow[r, "\overline{c}(\{n_B\}_{k_E})"] & \phi \cup \{n_A, n_B\} \rhd P_5 \arrow[r, "c(\{n_B\}_{k_B})"] & \phi \cup \{n_A, n_B\} \rhd P_6
\end{tikzcd}$$

ÉCOLE POLYTECHNIQUE MONTRÉAL

Plus grand attaquant

Definition (PGA)

Plus grand attaquant de connaissance de base initiale ϕ

$$Top(\phi) = \sum_{c \in \mathcal{C}} c(y).Top(\phi \cup \{y\}) + \sum_{c \in \mathcal{C}} \sum_{m \in \mathcal{D}(\phi)} \overline{c}(m).Top(\phi)$$

Theorem (S. Hamadou (2008))

$P \in NAI_\phi \Leftrightarrow \forall_{(P',\phi') \in \mathcal{D}_\phi(P)} \; (P' | Top(\phi')) \backslash (D \cup H) \simeq P' \backslash (D \cup H)$.

- $Top(\phi)$ n'existe que pour l'équivalence de trace.

POLYTECHNIQUE MONTRÉAL

Quelques outils

- Casper/FDR : Développé par G. Lowe pour analyser des protocoles spécifiés en CSP par model checking fini, il a servi à détecter la fameuse attaque.
  Information Processing Letters, Vol. 56(3) (1996)
- MURϕ : Aussi par model checking fini.
- Casrul : Protocoles spécifiés par des systèmes de réécriture avec un nombre de sessions et de participants bornné mais avec des clés composées.
- Projet AVISPA : Traduit les protocoles en un langage commun à 3 outils de vérification permettant de retrouver de nombreuses attaques déjà connues
- ASPiC : Protocoles spécifiés en SPASM. Propriétés (anonymat, résistance au déni de service) spécifiés avec la NI intransitive et vérifiées par bisimulation. A détecté une faille dans la spec du protocole de e-commerce SET développé par un consortium (IBM, CTE, RSA, Netscape, ...) pour Visa-Mastercard
  Information Processing Letters, Vol. 97(3) (2006)
- Applied π-calculus : FOO92, un protocoles de e-vote. JFK : résistance au DoS.
- Mocha : Les protocoles sont vus comme des jeux. Permet de vérifier des propriétés comme la non-répudiation ou l'équité.

ÉCOLE POLYTECHNIQUE MONTRÉAL

Quelques problèmes ouverts

- Définition d'un langage de spec (une logique) assez riche pour exprimer toutes les propriétés de sécurité.
- Conception d'un algo de model checking pour ce langage
- Développer un interface de HLPSL, le langage d'entrée d'AVISPA vers SPASM en vue d'intégrer ASPic à AVISPA.
- Analyse de robustesse au DoS : Élaborer un modèle quantitatif (Chaînes de Markov, Réseaux de Petri stochastique, algèbre de processu stochastique) pour modéliser le coût des ressources.
  En cours : Extension de SPASM avec un semi-anneau pour modéliser le coût avec des règles du type :

$$\frac{P \xrightarrow{\alpha} P'}{\langle P, v\rangle \xrightarrow{\alpha} \langle P, v + c(\alpha)\rangle}$$

  où v est une structure de ressources et $c(\alpha)$, le coût de α
- Conception d'un modèle symbolique de l'environnement qui permette une représenttaion finie des systèmes de transitions environnementiels.

ÉCOLE POLYTECHNIQUE MONTRÉAL