Modèle système dynamique pour l'analyse de la menace

Tithnara Nicolas SUN

Philippe Dhaussy (Lab-STICC)
Lionel Van Aertryck (DGA-MI)
Ciprian Teodorov (Lab-STICC)

Sommaire

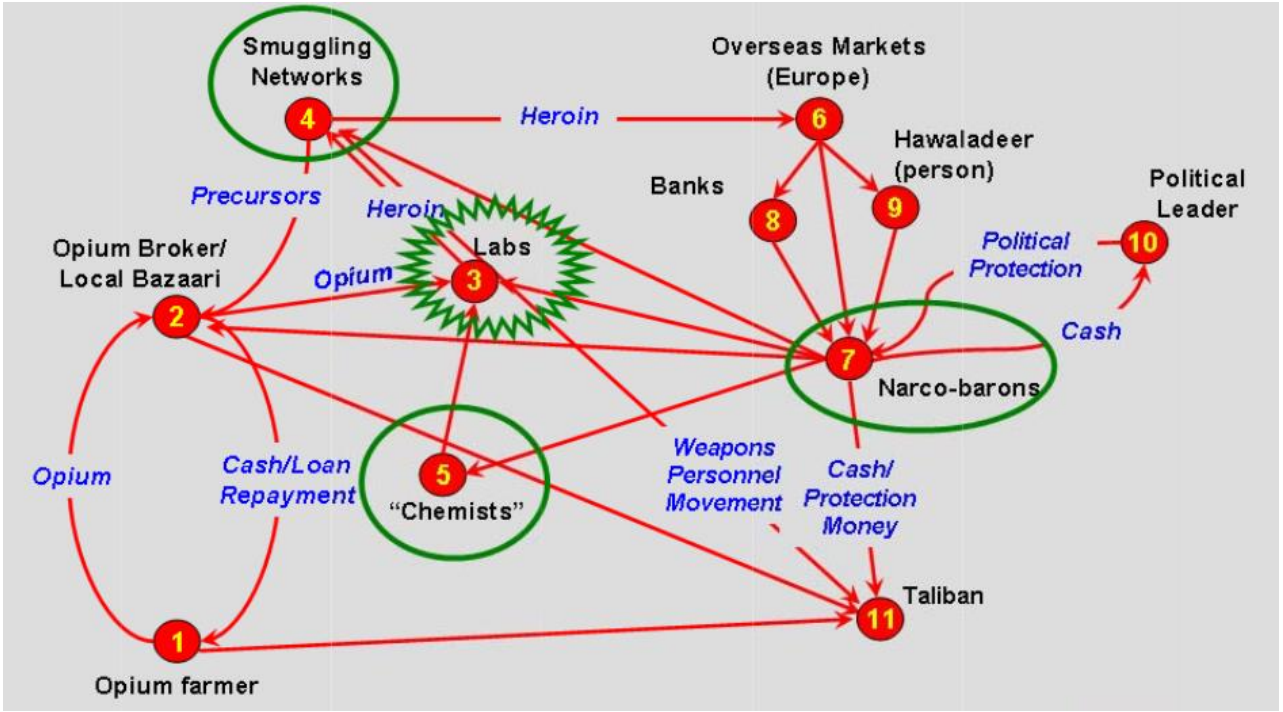
- Contexte
- Problématique
- Avancement
  - Réification de la surface d'attaque
  - Aspect dynamique et exécution
- Conclusion
  - Bilan
  - Perspectives

Sommaire

- **Contexte**
- Problématique
- Avancement
  - Réification de la surface d'attaque
  - Aspect dynamique et exécution
- Conclusion
  - Bilan
  - Perspectives

RAFT

- **R**elations
- **A**cteurs
- **F**onctions
- **T**ensions

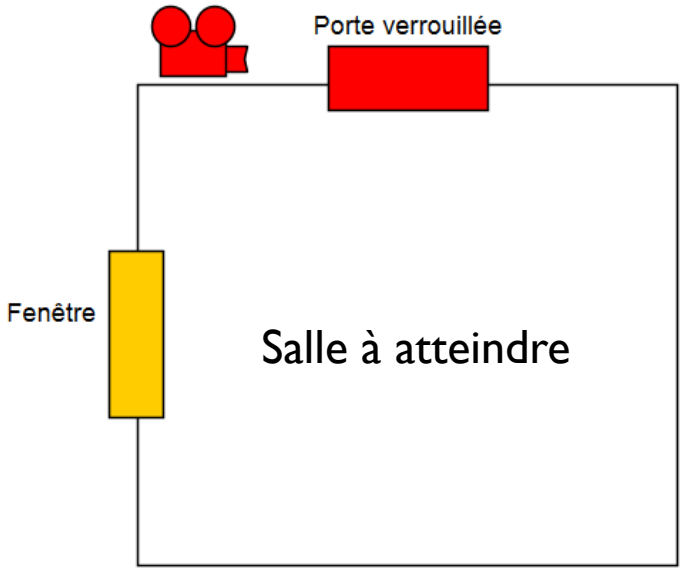


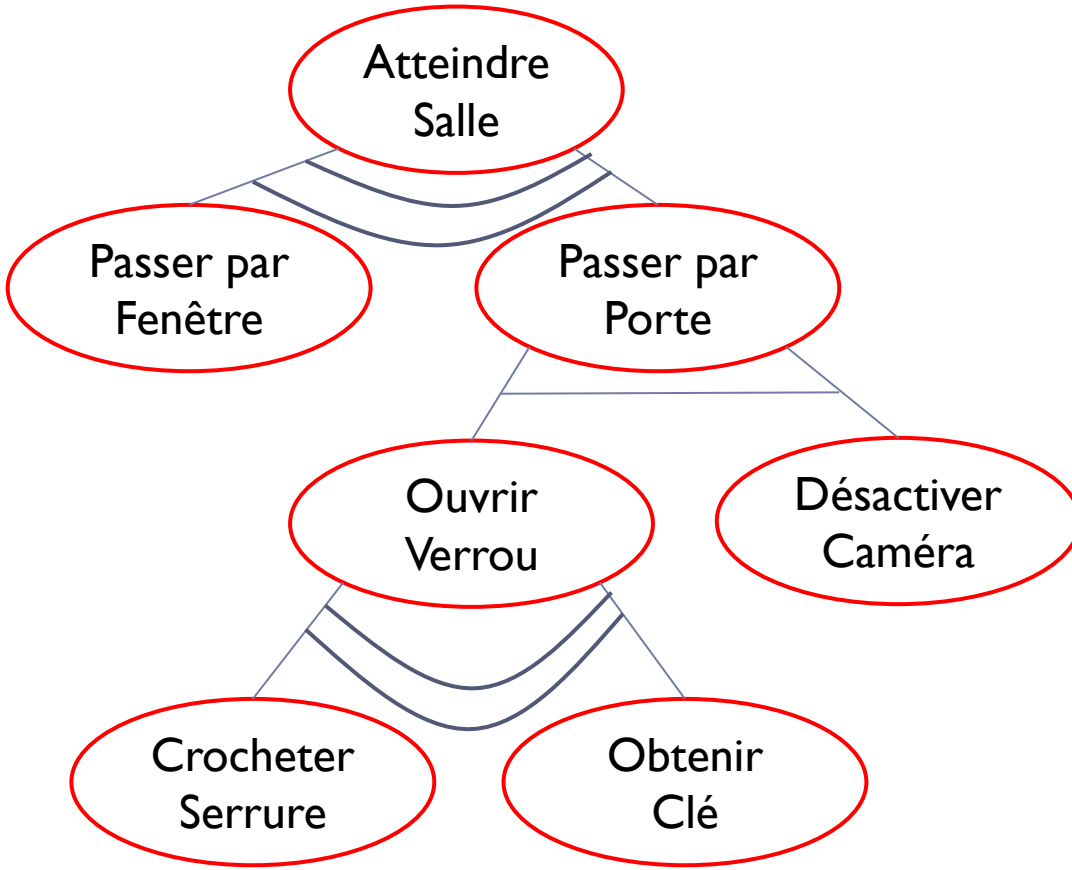
[1]

Pimca

[1] *Redefining the Center of Gravity* in *Joint Force Quarterly (JFQ) issue 59* / Dale C. Eikmeier / Washington D.C. USA / 2010

Arbres d'Attaque :

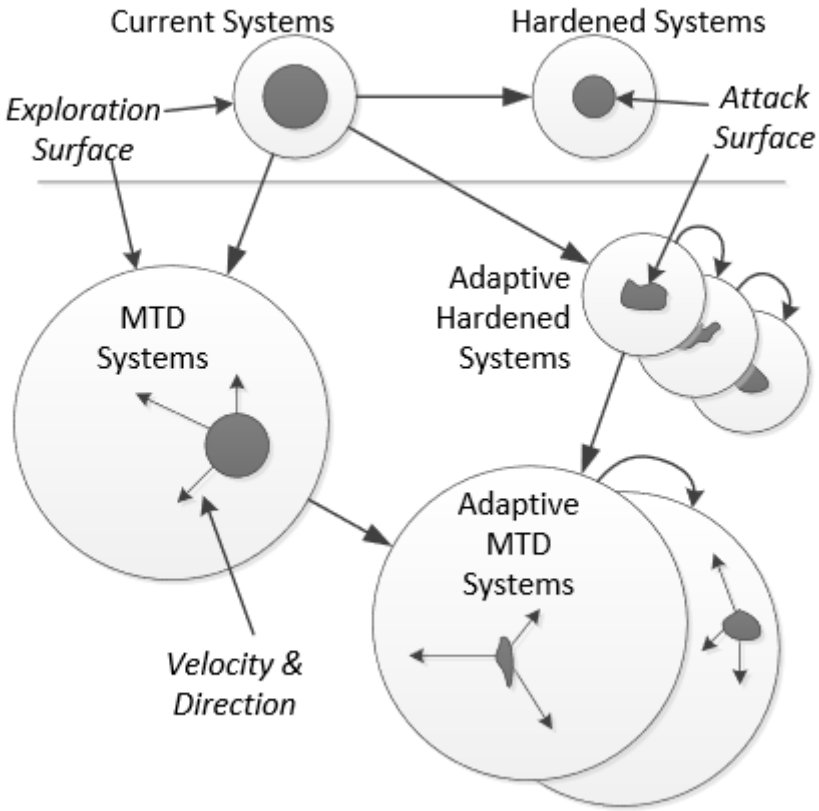




[2][3]

[2] *Attack Modeling for Information Security and Survivability* / Andrew P. Moore, Robert J. Ellison, Richard C. Linger/ Software Engineering Institute, Carnegie Mellon University, USA / Mars 2001
[3] *Is my attack tree correct?* / Maxime Audinot, Sophie Pinchinat, & Barbara Kordy / IRISA Rennes, University Rennes 1, INSA Rennes, France / Août 2017

Moving Target Defense [4]



[4] *Towards a Theory of Moving Target Defense* / Rui Zhuang, Scott A. DeLoach, Xinming Ou /Kansas State University, Manhattan, USA / 2014

Contexte
Quelques limites

- Stratégie attaque-défense
  - Manque de formalisation (Dessin + langage naturel)
  - PimCA mieux, mais pas dynamique
  - Subjectif, besoin de standardiser
- Modélisation d'attaque
  - Statique par rapport à l'évolution du système
  - Point de vue partiel
- Moving Target Defense
  - Modélisation très générique, orientée réseau
  - Besoin d'un parallèle applicatif

Problématique

- Nécessité d'une **vue système** holistique
  - Point de vue **opérationnel**
  - Ressources **hétérogènes**

Modèle système dynamique pour l'analyse de la menace

Modèle système *dynamique pour l'analyse de la menace*

Réification de la surface d'attaque

Axes de recherche

Modèle système ***dynamique*** *pour l'analyse de la menace*

Réification de la surface d'attaque

Aspect dynamique et exécution

Axes de recherche

Modèle système dynamique pour
l'analyse de la menace

Réification de la surface d'attaque

Aspect dynamique et exécution

Diagnostic & métrique

Sommaire

- Contexte
- Problématique
- **Avancement**
  - **Réification de la surface d'attaque**
  - Aspect dynamique et exécution
- Conclusion
  - Bilan
  - Perspectives

Réification de la Surface d'Attaque

A) Terminologie

B) STIX

C) Modèle système

Terminologie

Surface d'attaque :

Ensemble des **points d'entrée** et des **points de communication** qu'un système possède avec l'extérieur.[5]

Zone de contention entre l'attaquant & la défense.

[5] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015

Terminologie

Attaquant, Threat Actor, Adversaire :

Entité ayant pour objectif de **nuire** au système. [6][7]

Vulnérabilité, Faille :

Erreur ou **faiblesse** de conception, d'implémentation ou de fonctionnement. [6][7]

[6] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
[7] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

Terminologie

Menace, Threat :

Adversaire motivé et capable d'**exploiter** une **vulnérabilité**. [6][7]

Définition ambiguë : Expression d'une intention de nuire / Indication d'une telle intention.

Attaque, Incident :

Acte malveillant, moyen [séquence d'actions] d'exploiter une vulnérabilité. [6][7]

[6] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
[7] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

Terminologie

Cyber Threat Intelligence :

Connaissance sur les **adversaires**, leurs **motivations**, leurs **intentions** et leurs **méthodes**, **collectée**, **analysée** et **partagée** entre différents agents à différents niveaux pour protéger les biens critiques. [8]

[8] *Definitive Guide to Cyber Threat Intelligence* / Jon Friedman, Mark Bouchard, CISSP / CyberEdge Group Annapolis, USA / 2015

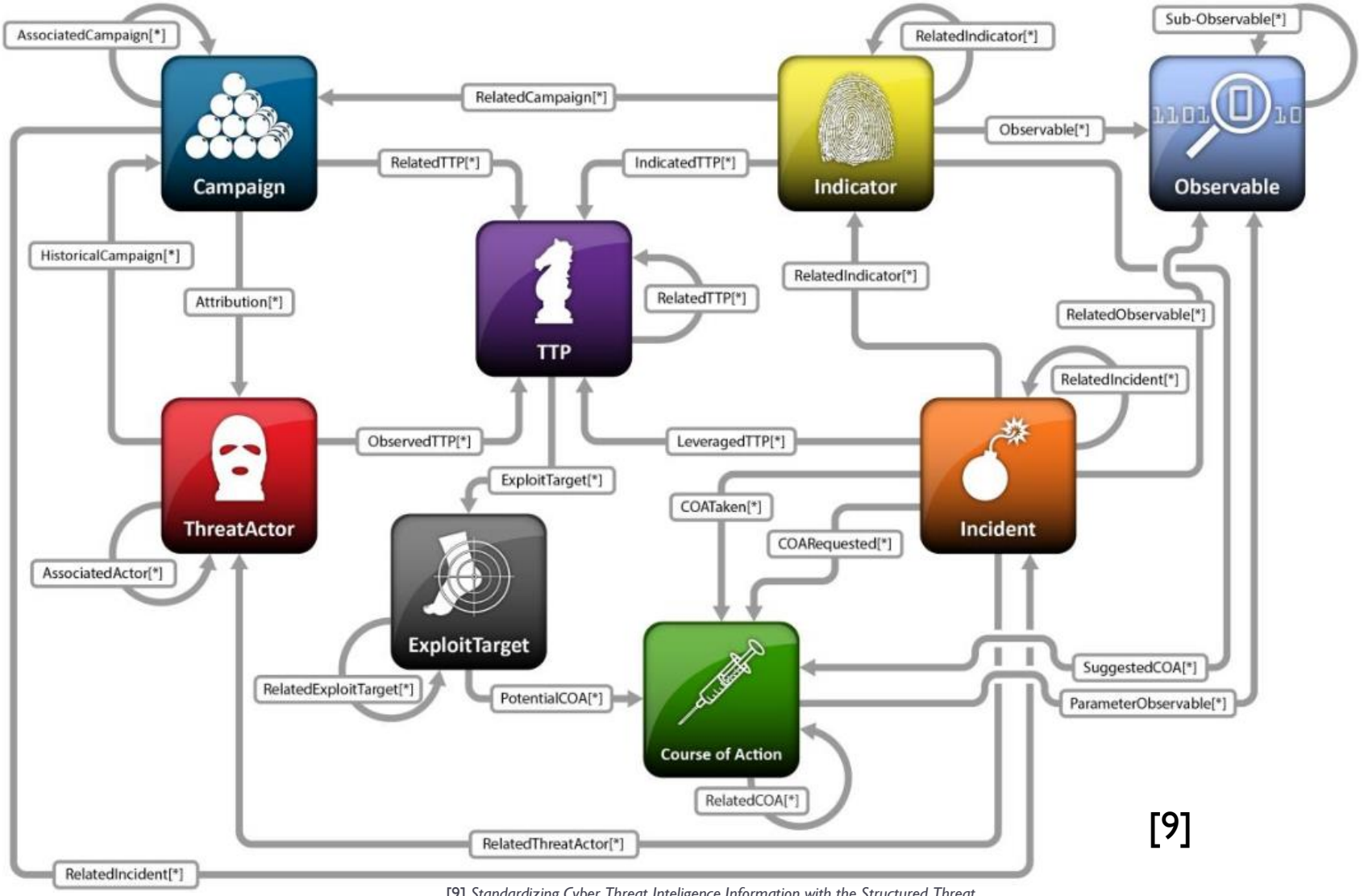
Réification de la Surface d'Attaque

A)Définitions

B)STIX

C)Modèle système

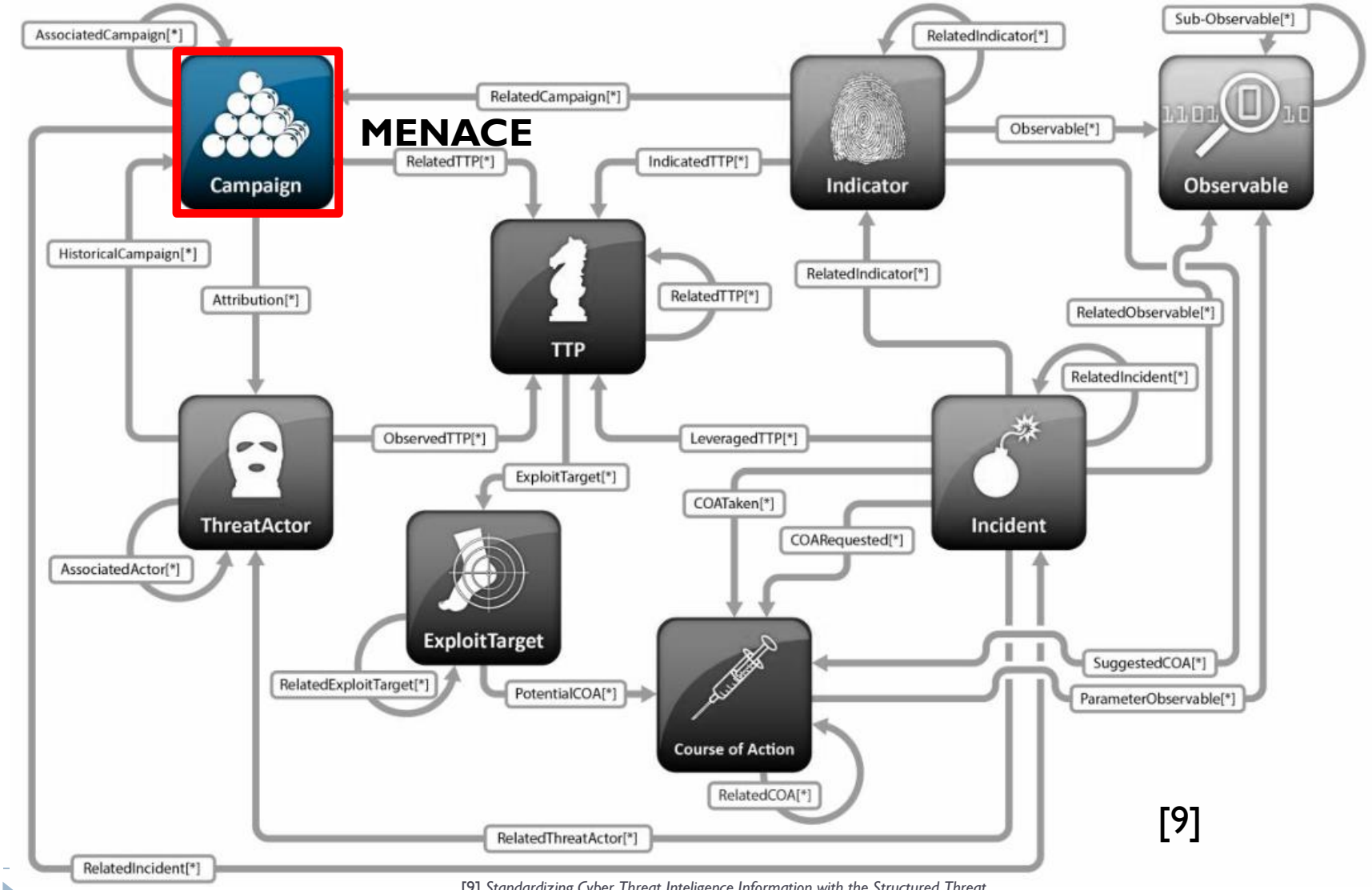
STIX



[9]

[9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

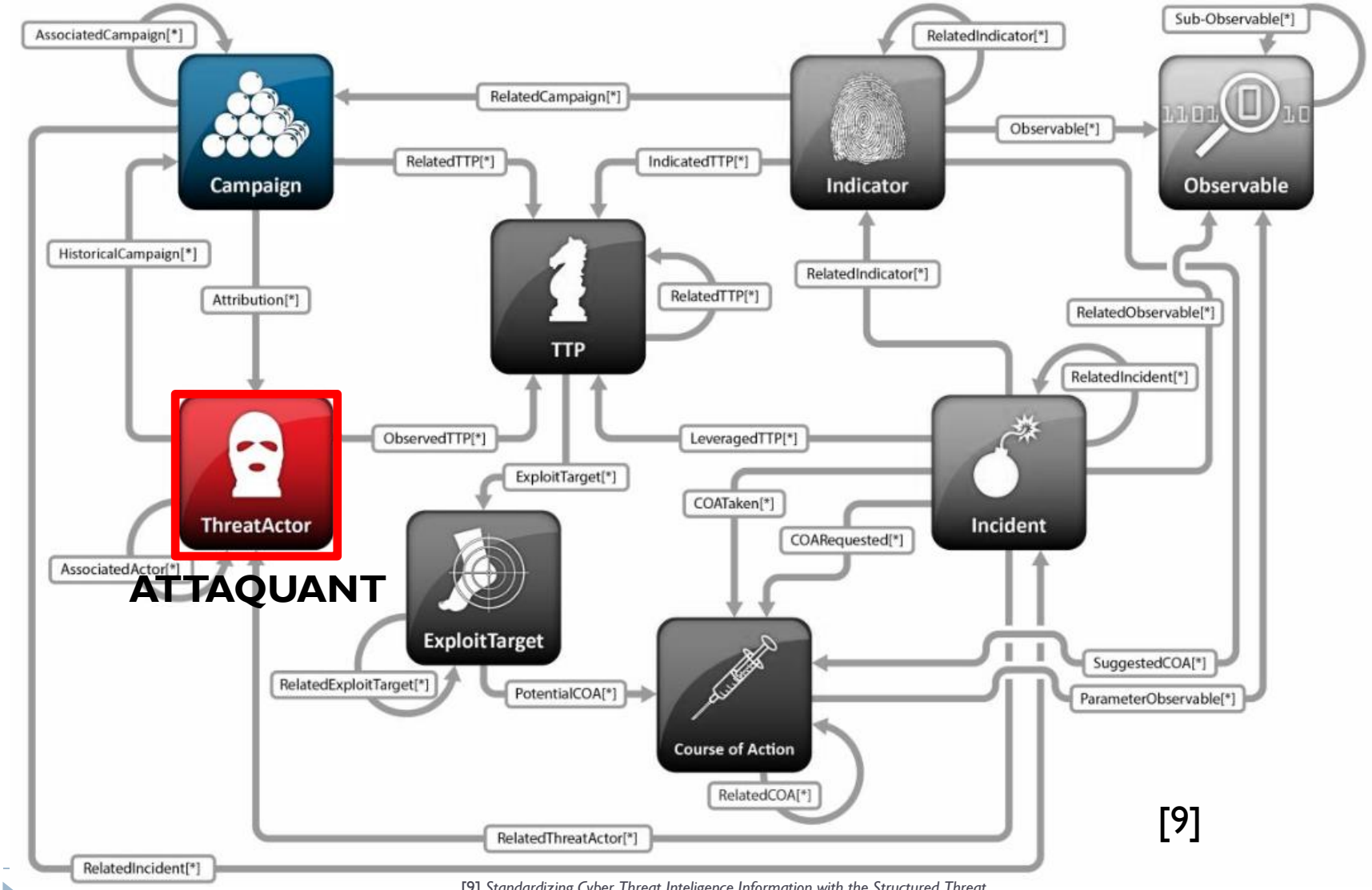
STIX



[9]

[9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

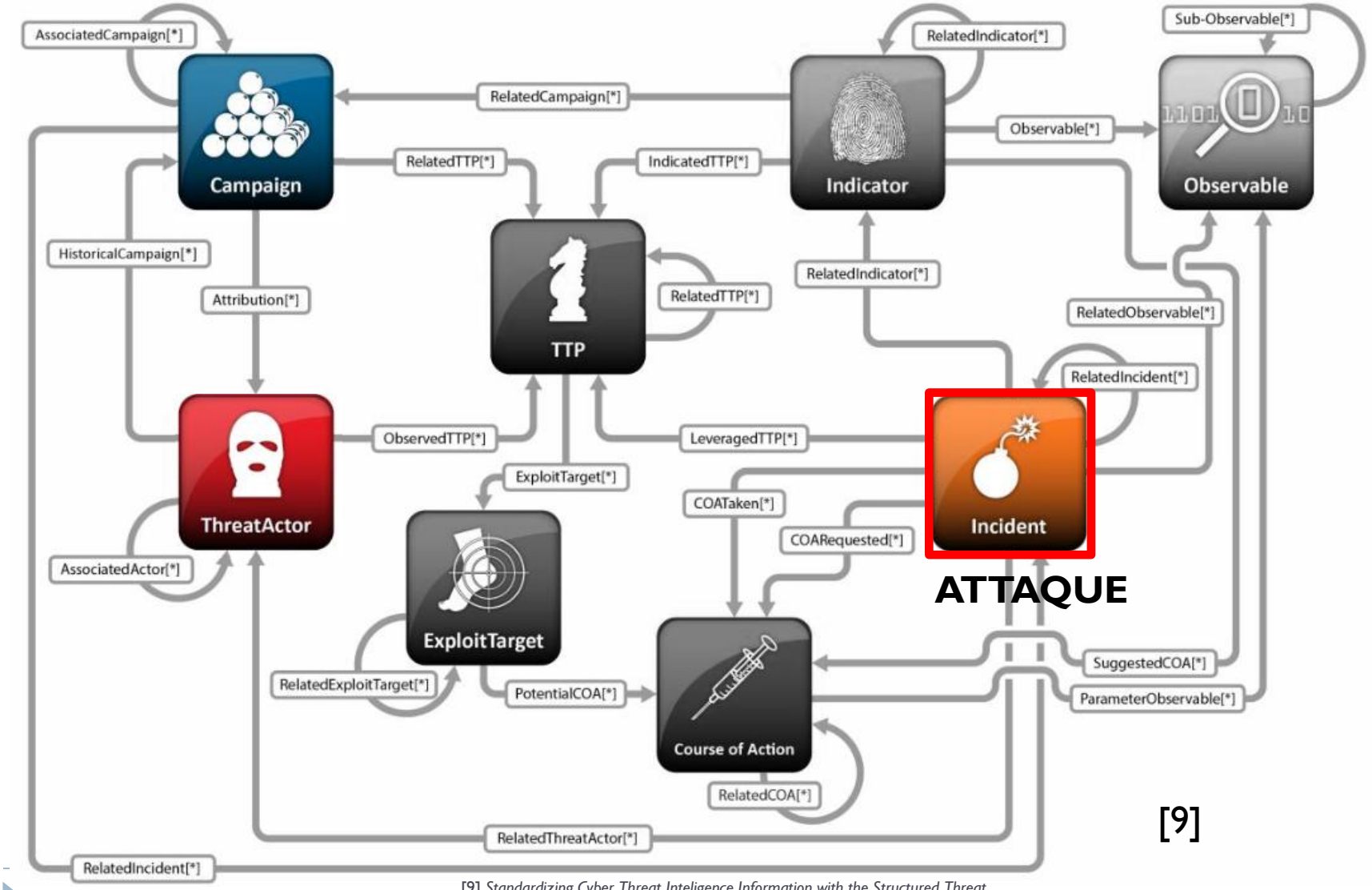
STIX



[9]

[9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

STIX



[9]

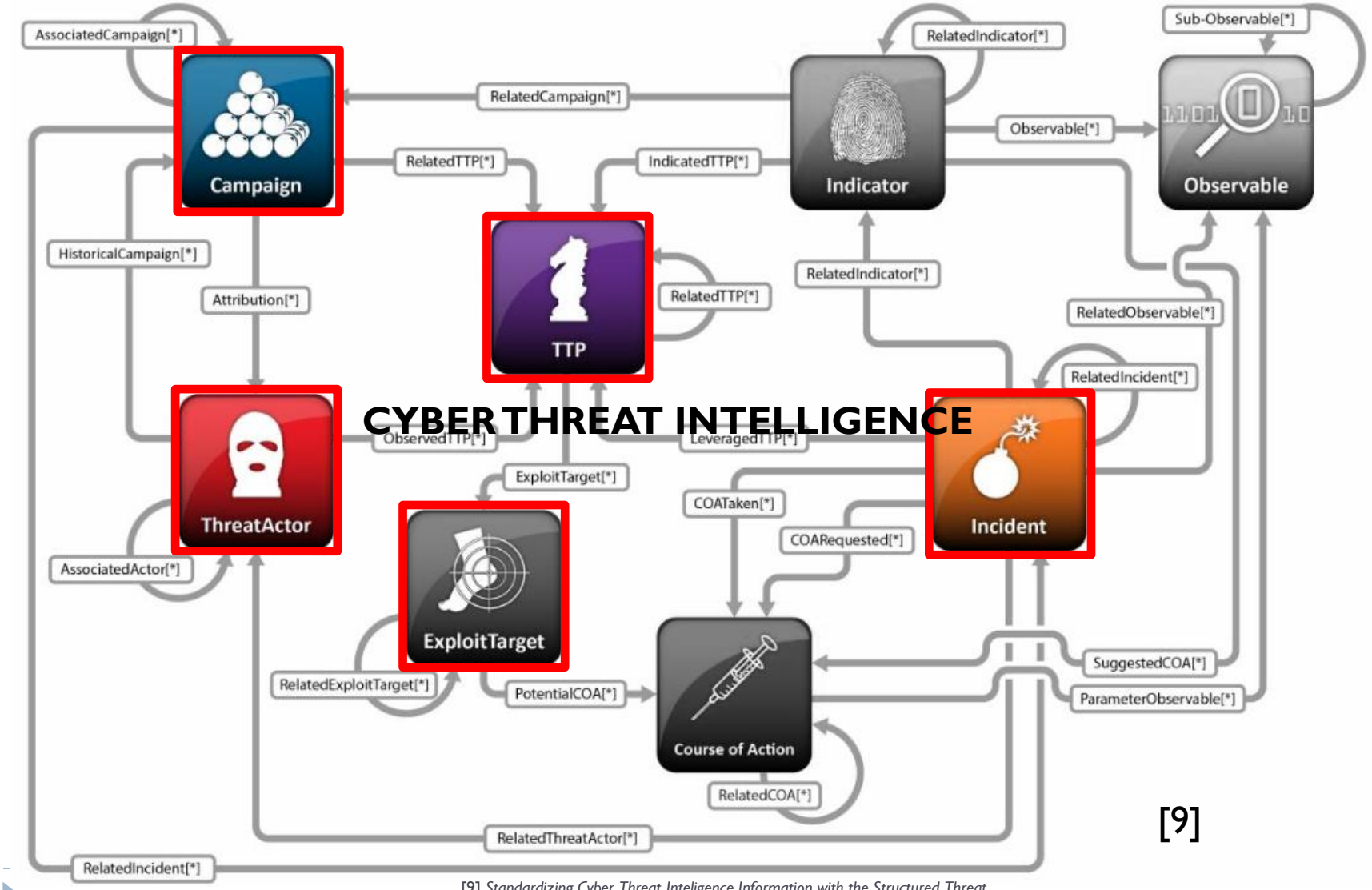
[9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

STIX

[9]

[9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

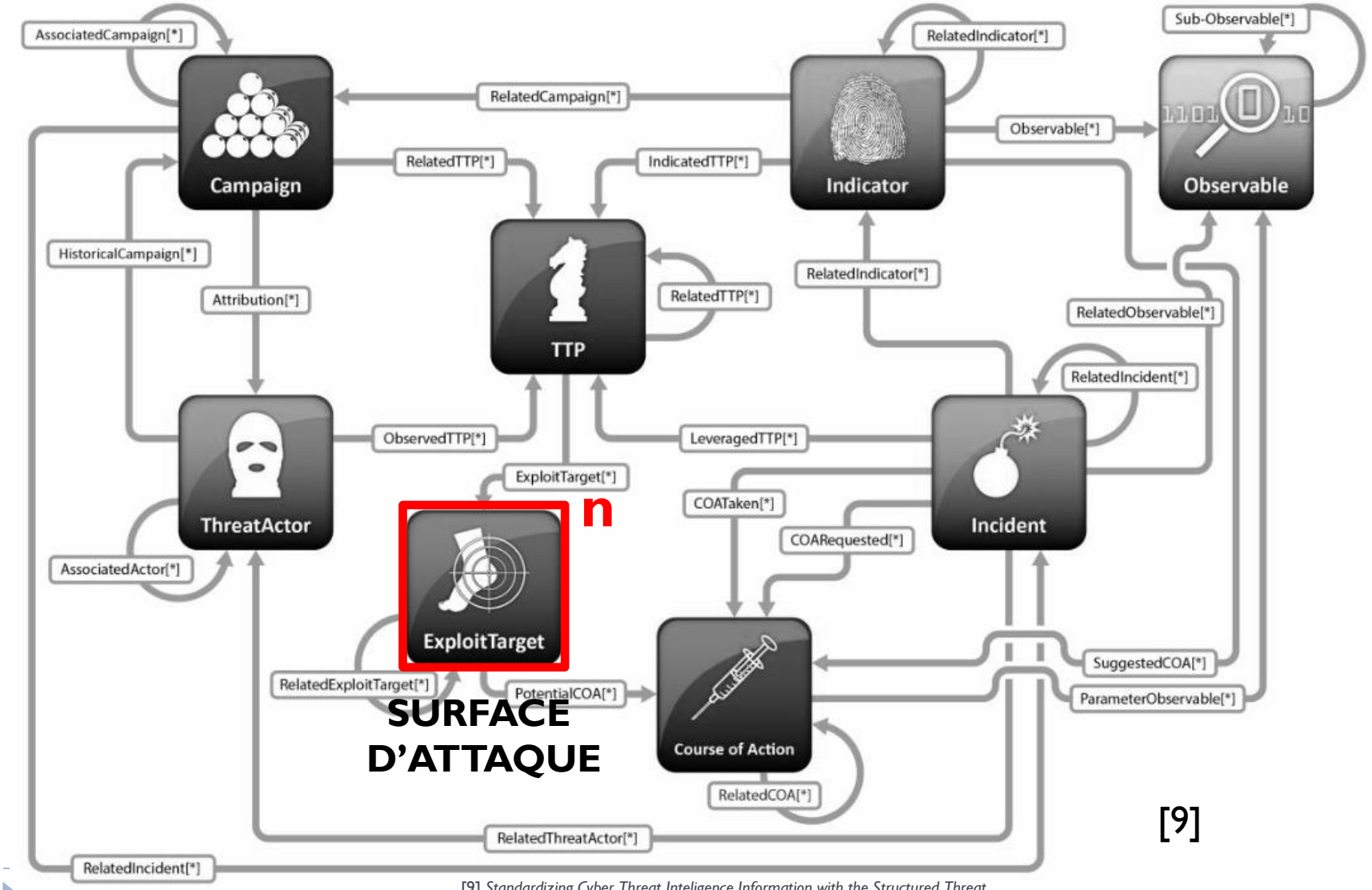
STIX



[9]

[9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

STIX



[9]

[9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

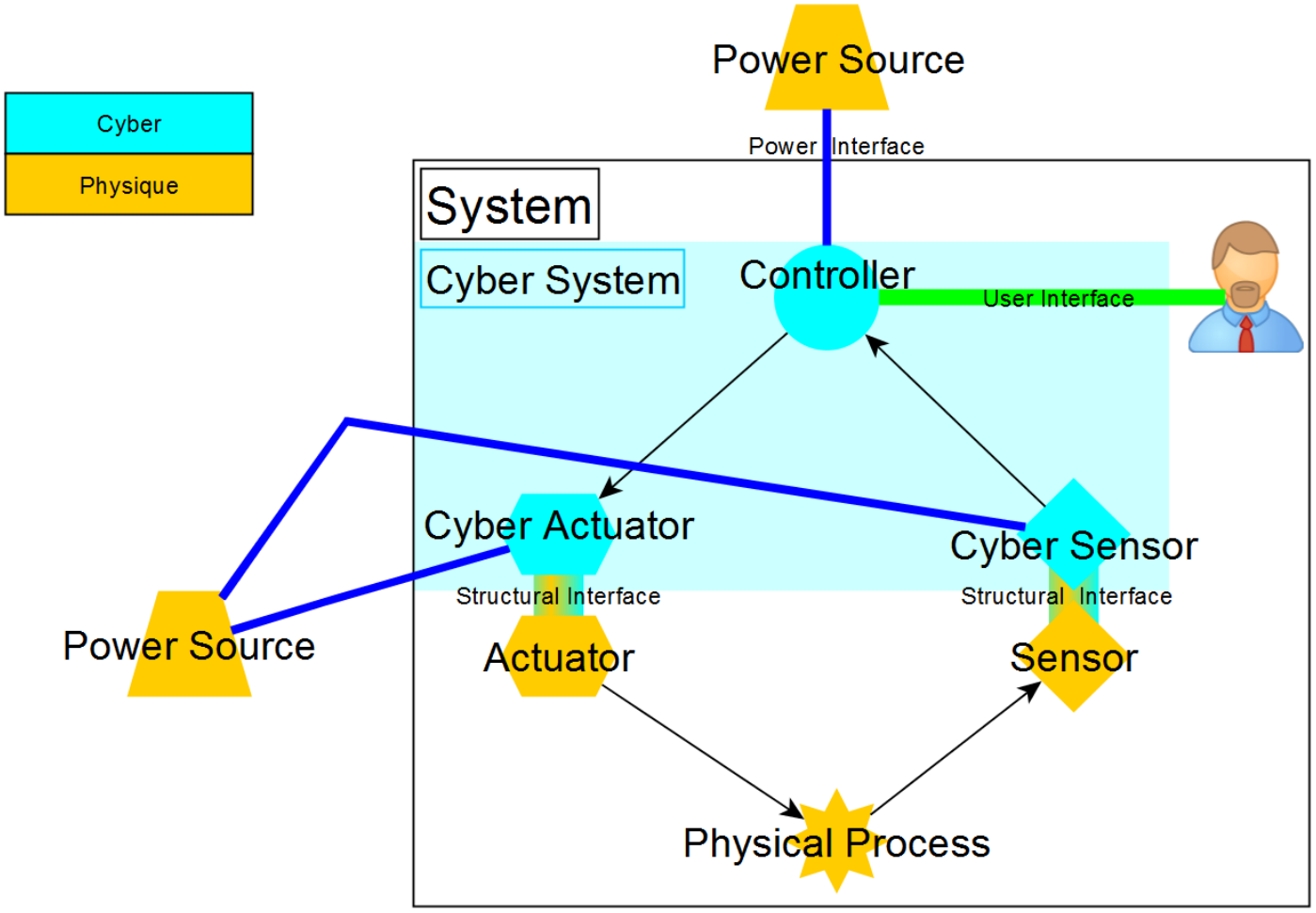
Réification de la Surface d'Attaque

A) Terminologie

B) STIX

C) Modèle système

Modèle Système



[10]

[10] *Introduction to Embedded Systems* A Cyber-Physical Systems Approach / Edward Ashford Lee, Sanjit Arunkumar Seshia / The MIT Press / Cambridge, Massachusetts, USA / 2017

Sommaire

- Contexte
- Problématique
- **Avancement**
  - Réification de la surface d'attaque
  - **Aspect dynamique et exécution**
- Conclusion
  - Bilan
  - Perspectives

Aspect Dynamique & Exécution

A) Théorie des jeux

B) Exécution

C) Implémentation

Théorie des jeux

Théorie des jeux [11] :

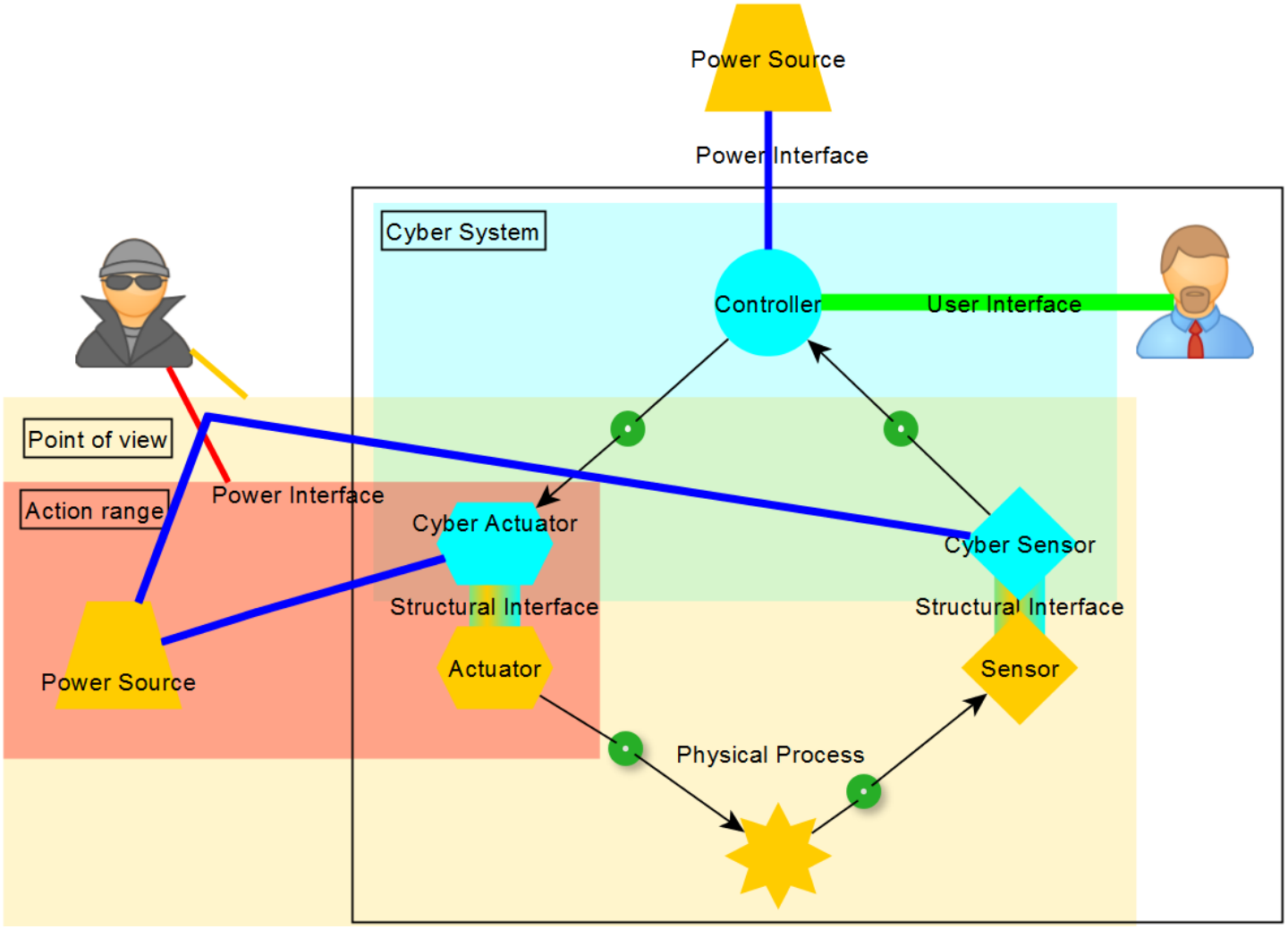
Domaine mathématique s'intéressant aux **problèmes de décisions** entre **différents joueurs** qui sont conscients de leurs **interactions**. Tous les joueurs sont supposés rationnels.

Jeu :

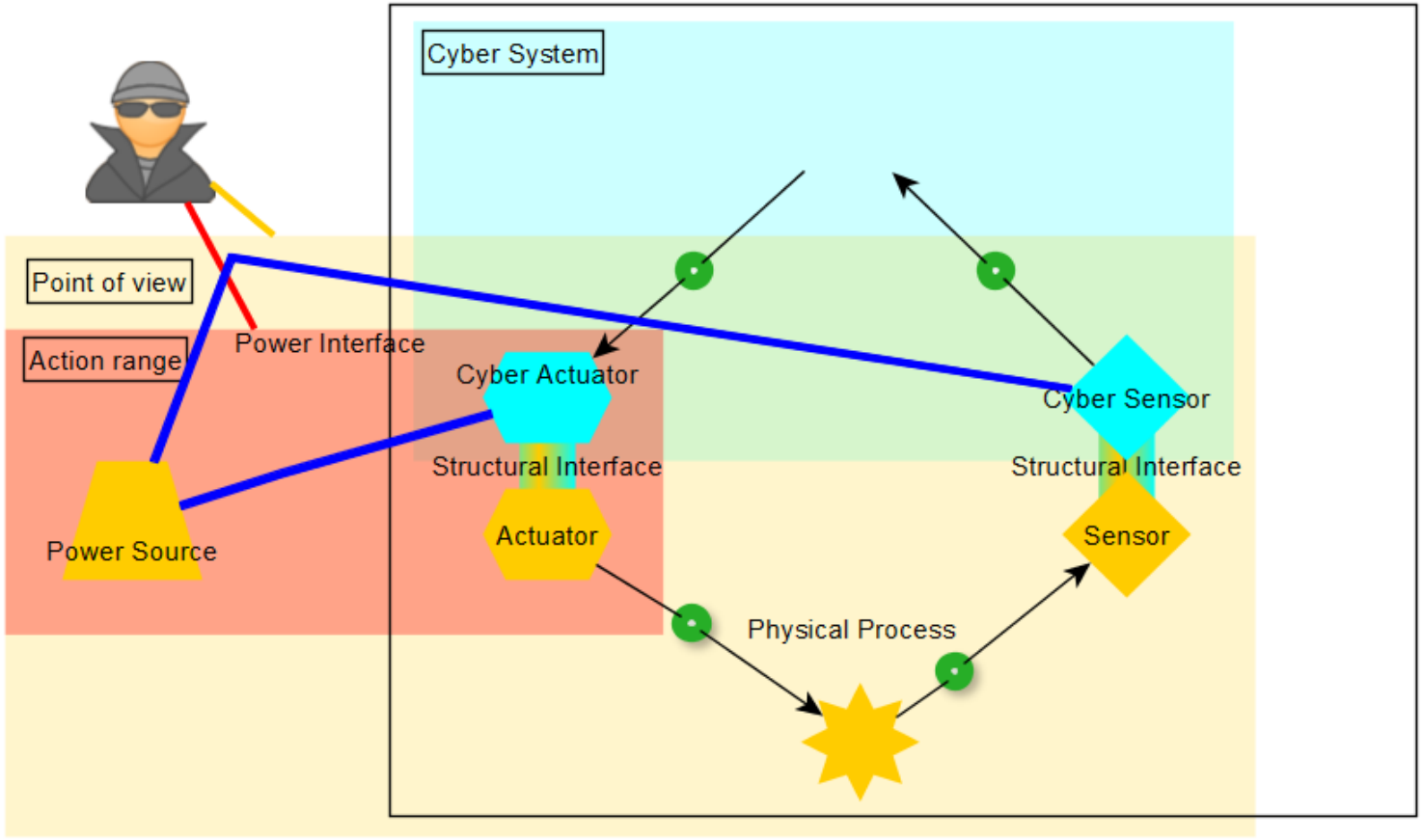
Ensemble de stratégies et de gains de tous les joueurs.

[11] *CyberWar Games: Strategic Jostling Among Traditional Adversaries* / Sanjay Goel, Yuan Hong / University of New York, New York, USA / 2015

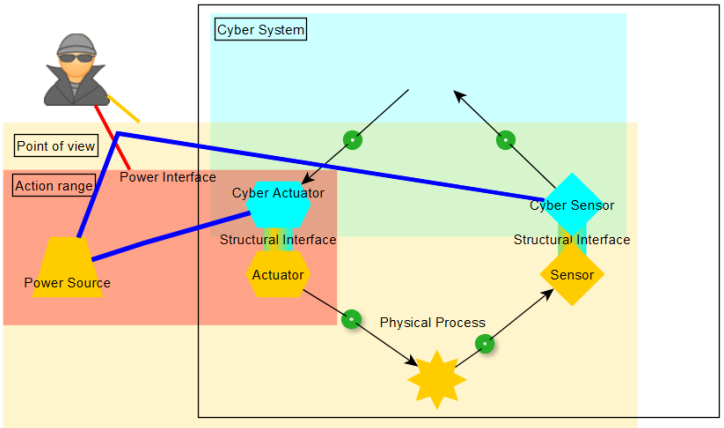
Théorie des jeux

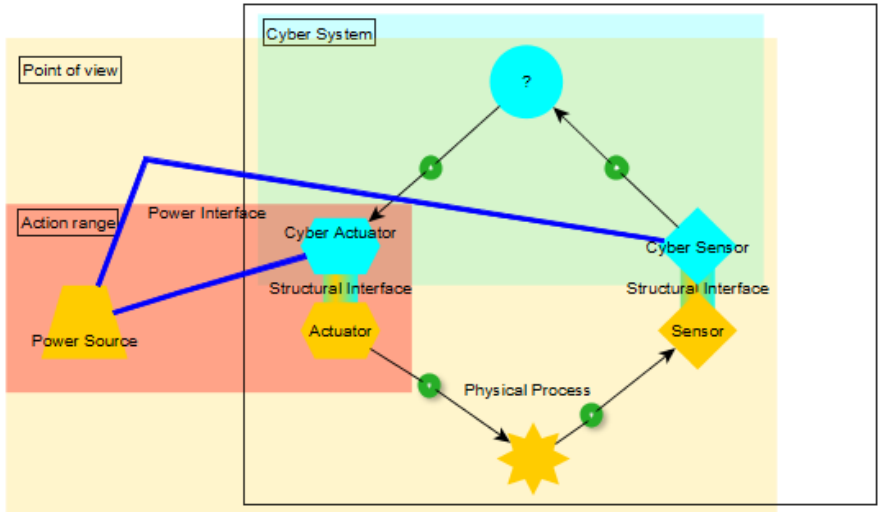


Théorie des jeux

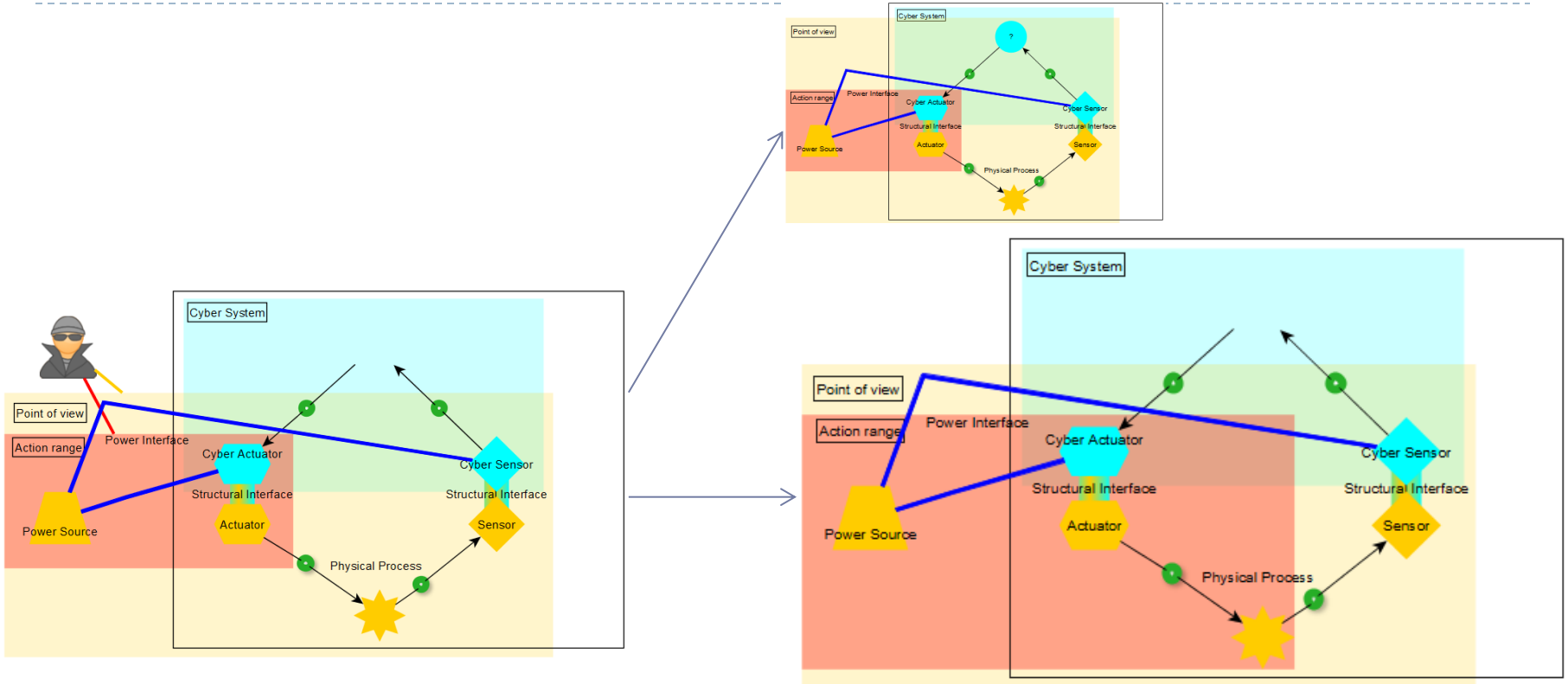


Théorie des jeux

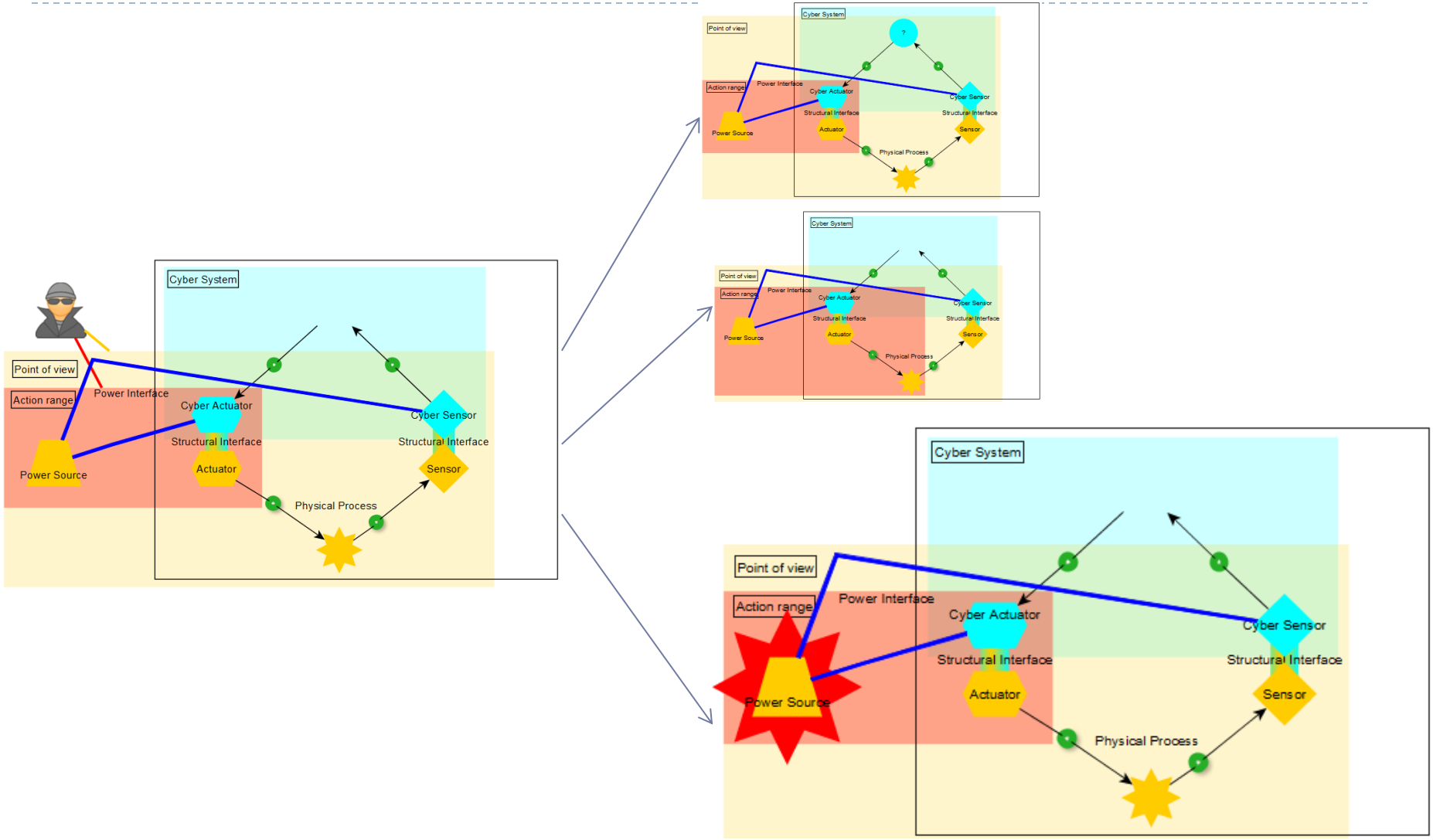




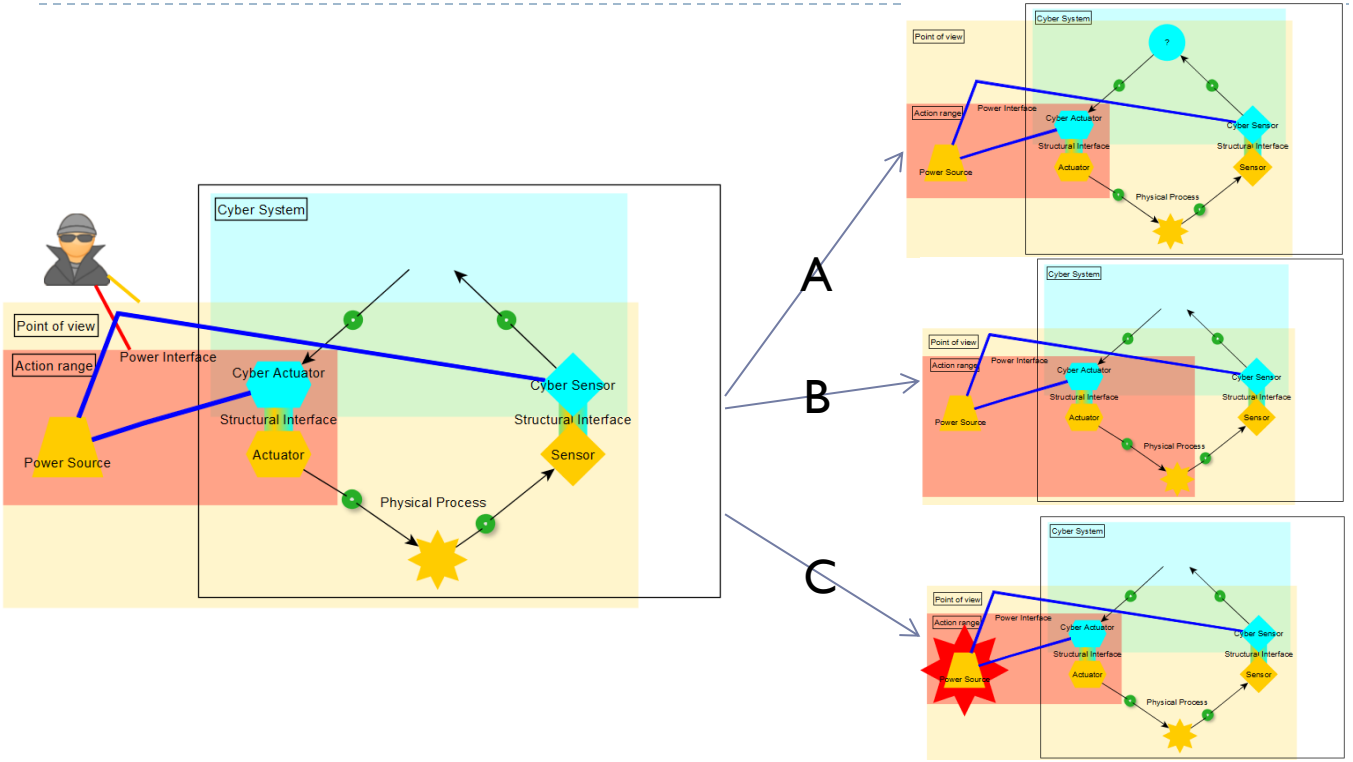
Théorie des jeux



Théorie des jeux



Théorie des jeux



Att\Déf	X	Y	Z
A	+1\-1	-10\+10	+1\-1
B	+6\-6	+6\-6	-4\+4
C	-4\+4	-4\+4	+6\-6

Aspect Dynamique & Exécution

A) Théorie des jeux

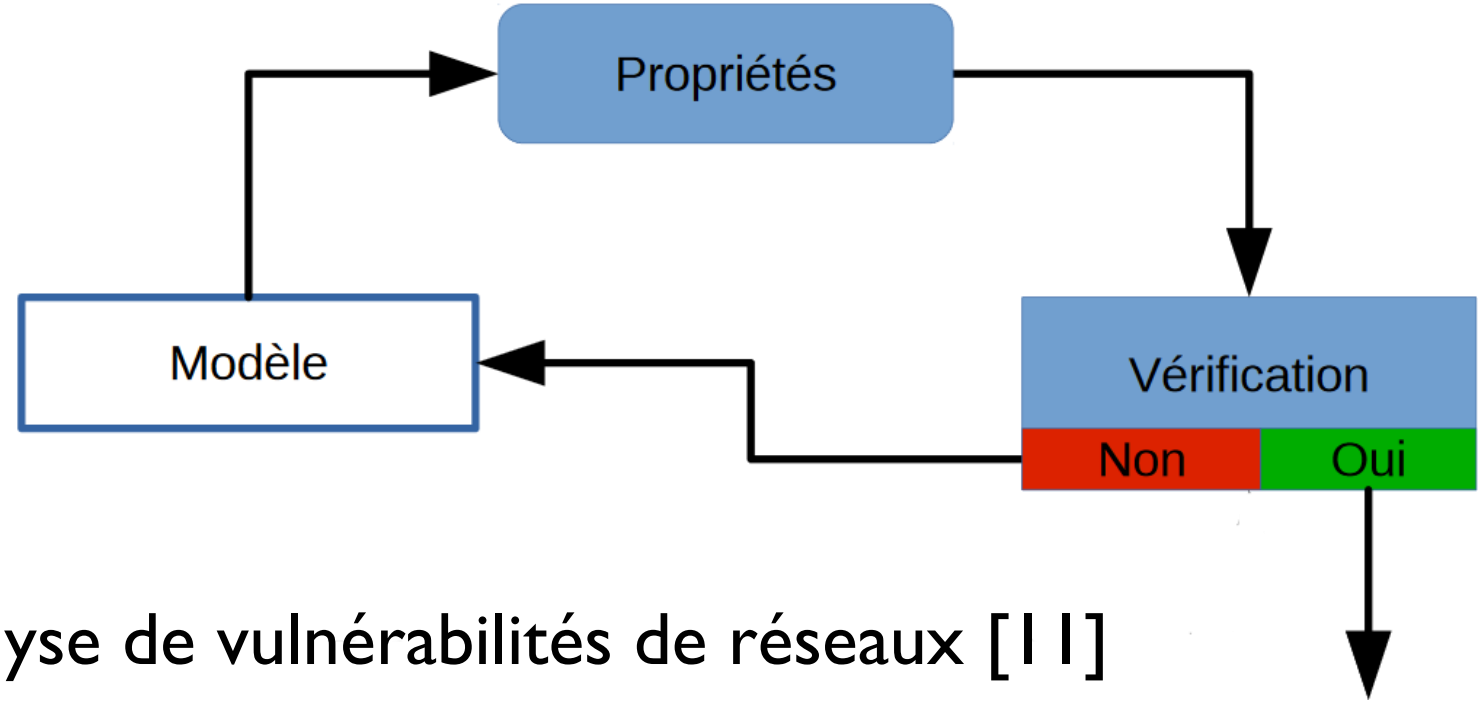
B) Exécution

C) Implémentation

Model checking [10] :

Exécution exhaustive

Propriétés à vérifier

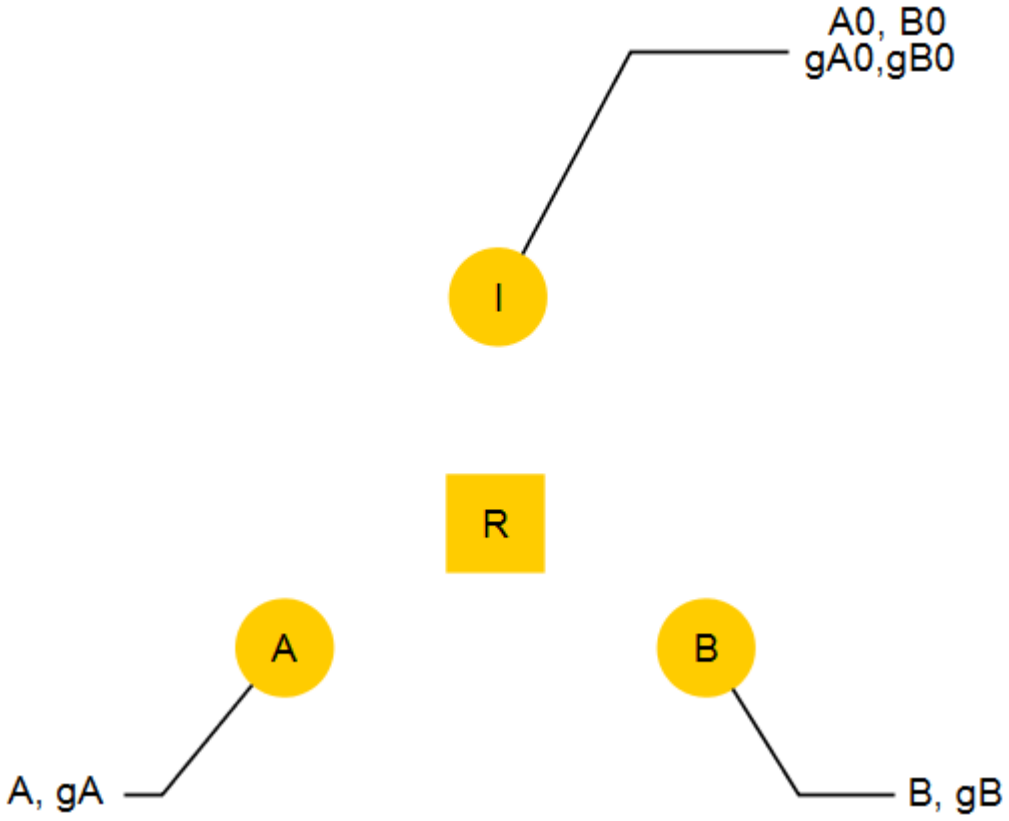


Analyse de vulnérabilités de réseaux [11]

[10] *Contribution à la modélisation et la vérification formelle par model checking - Symétries pour les Réseaux de Petri temporels. Systèmes embarqués* / Pierre-Alain Bourdil / INSA de Toulouse / 2015.

[11] *Using Model Checking to Analyze Network Vulnerabilities* / Ronald W. Ritchey & Paul Ammann / National Security Team Booz Allen & Hamilton & Information and Software Engineering Department George Mason University / Virginia /2000

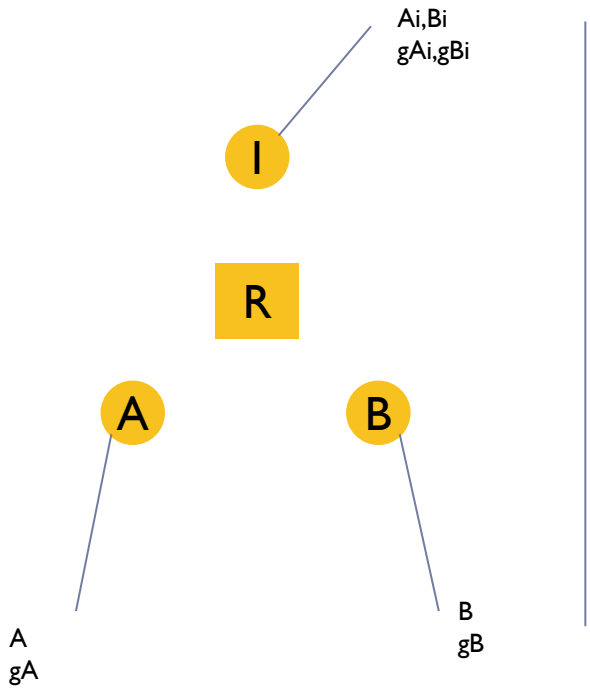
Echange de clés de Diffie-Hellman [14] :



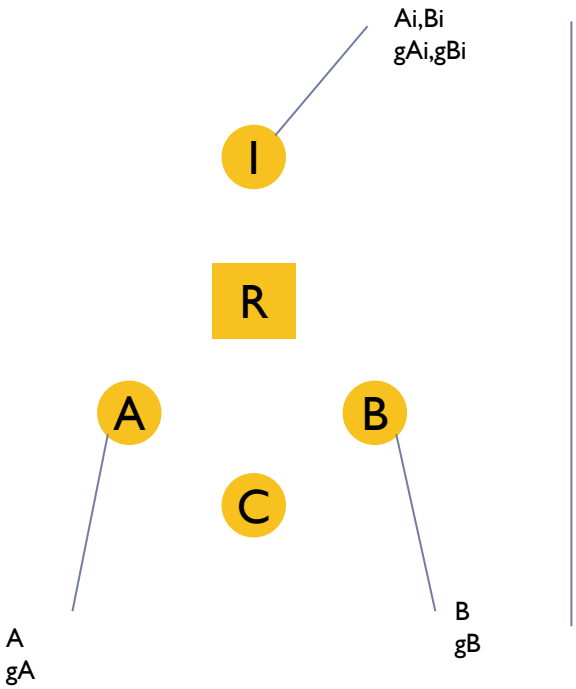
[14] *New Directions in Cryptography* / Whitfield Diffie, Martin E. Hellman / IEEE Transactions on Information Theory / Novembre 1976

Exécution

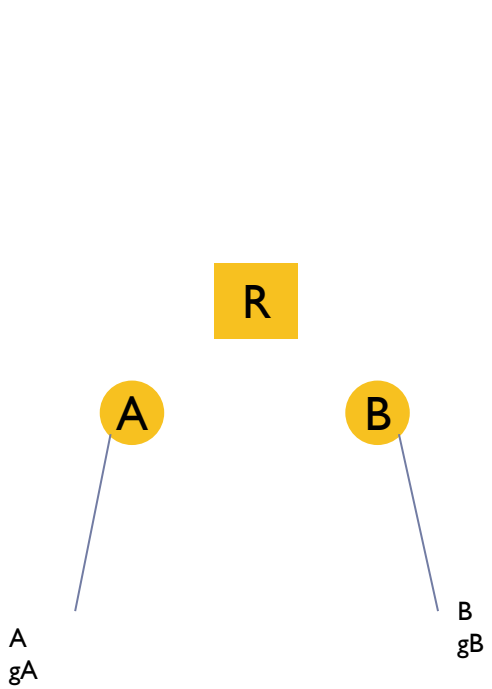
Attaquant



Modèle d'or

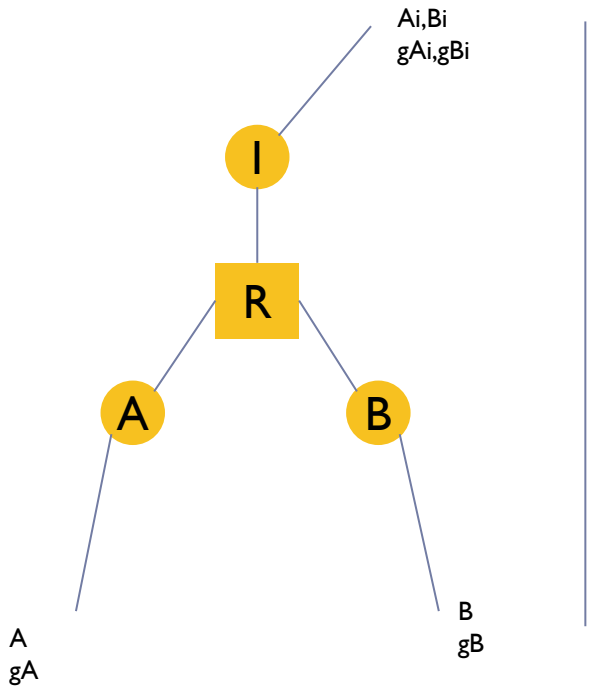


Défenseur

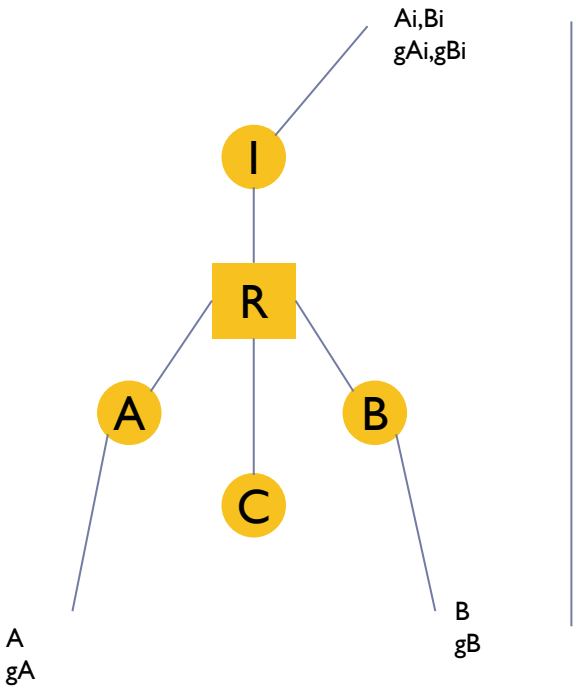


Exécution

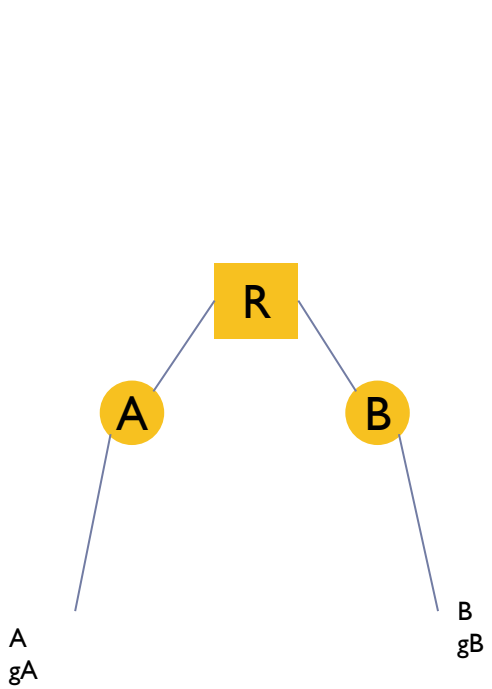
Attaquant



Modèle d'or

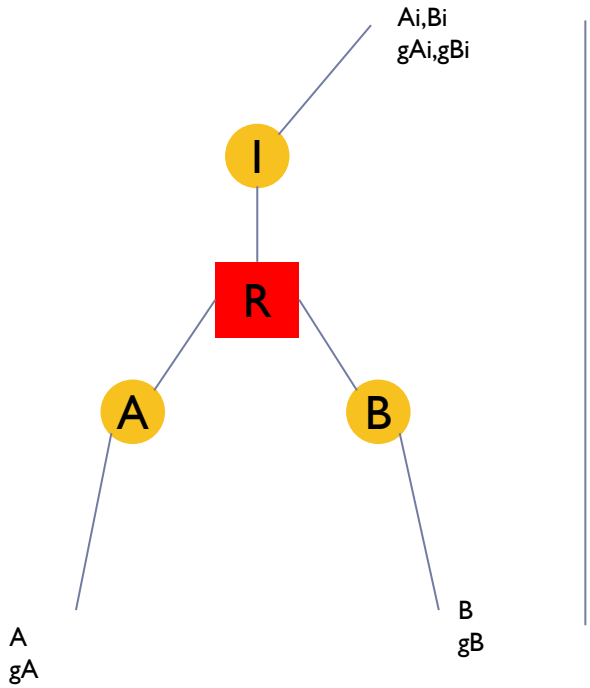


Défenseur

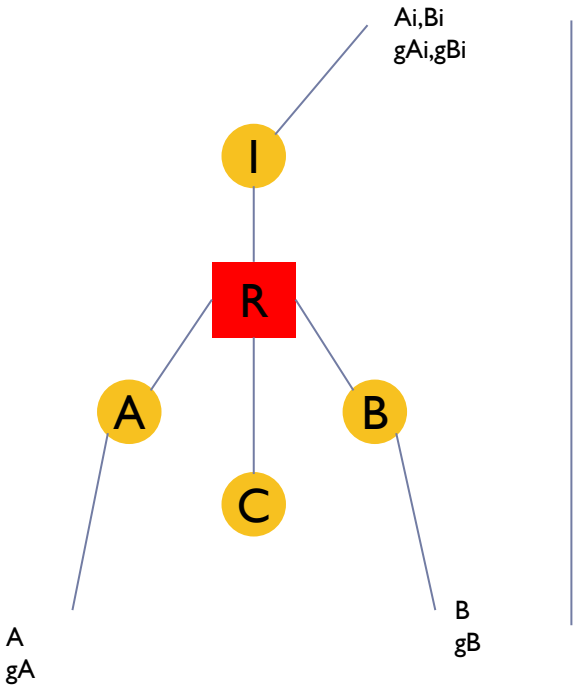


Exécution

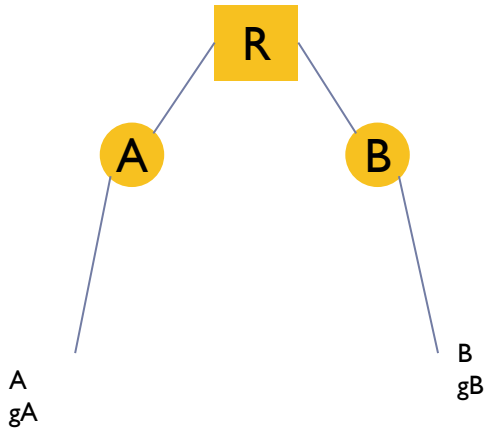
Attaquant



Modèle d'or

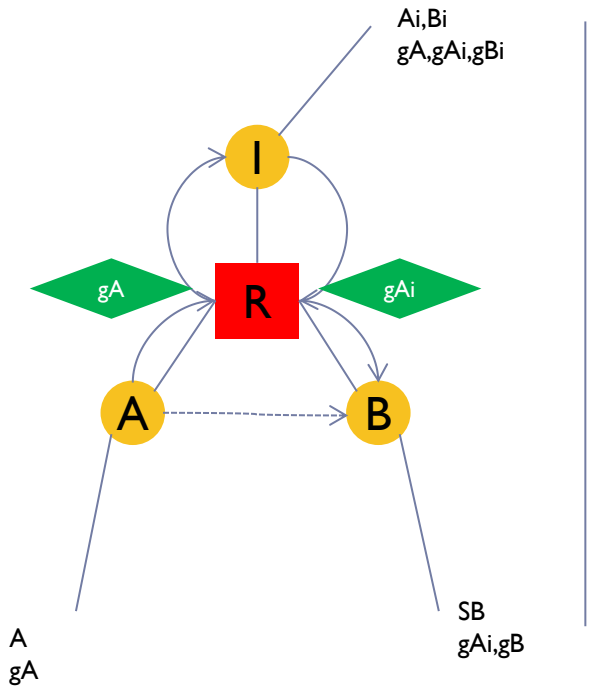


Défenseur

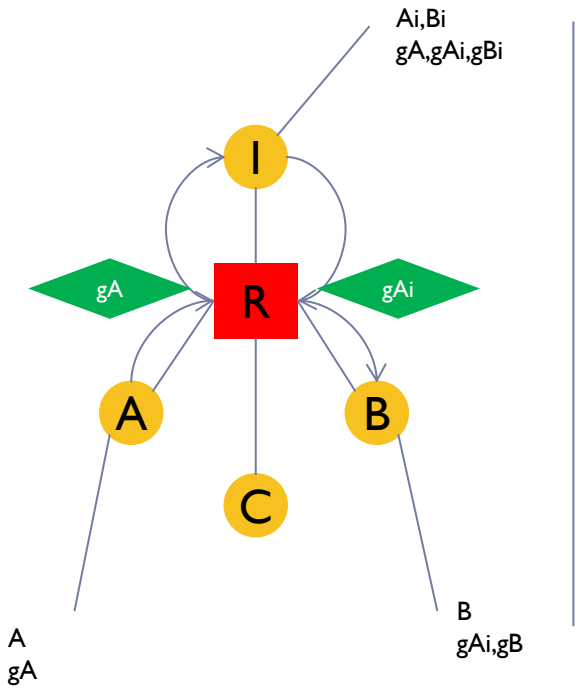


Exécution

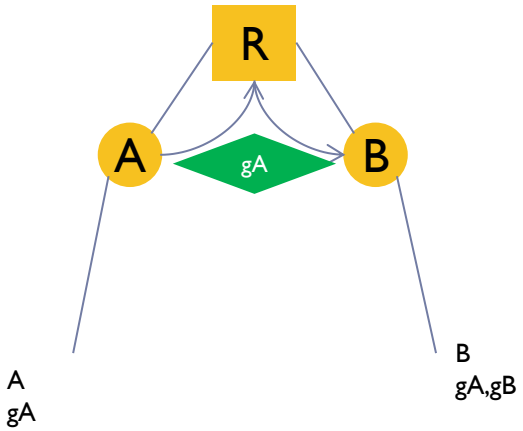
Attaquant



Modèle d'or

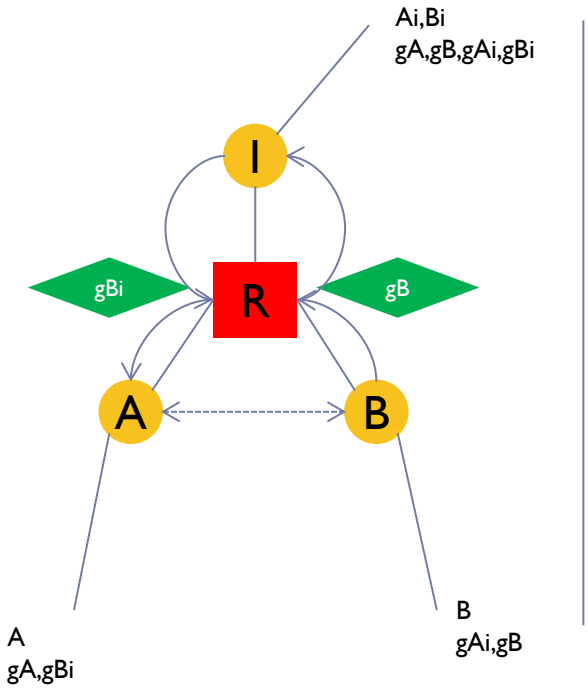


Défenseur

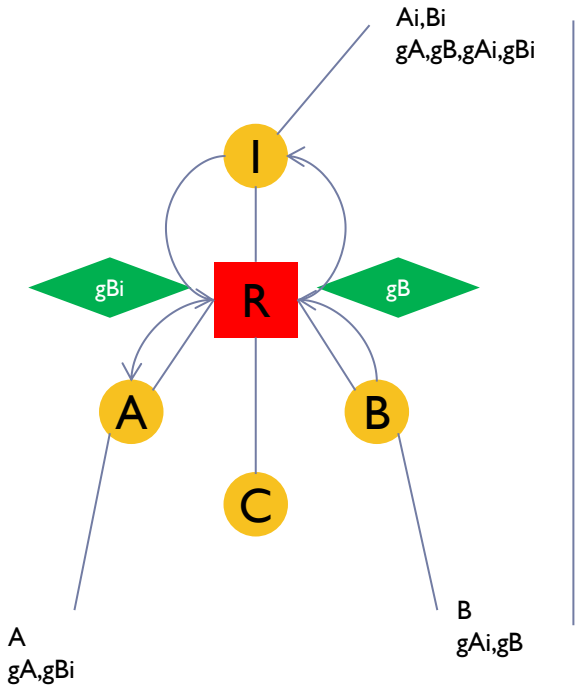


Exécution

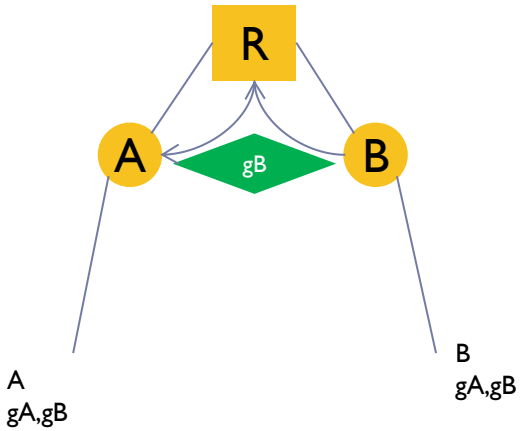
Attaquant



Modèle d'or

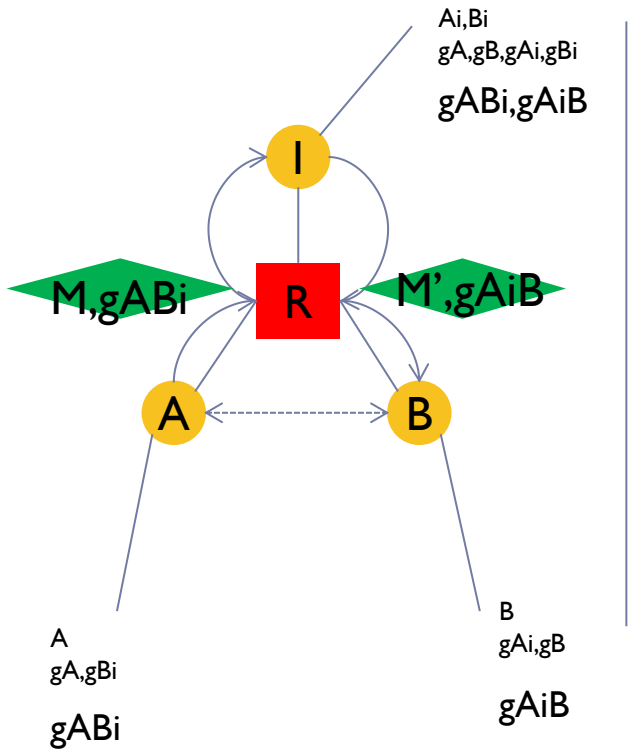


Défenseur

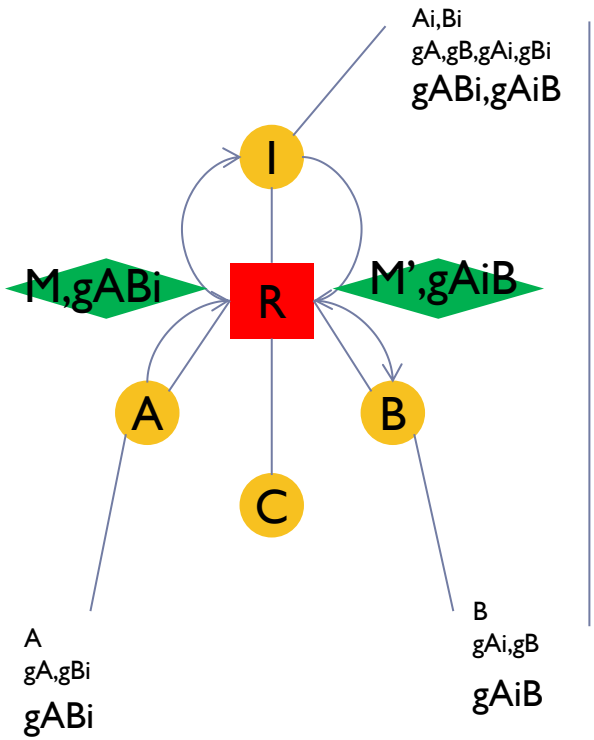


Exécution

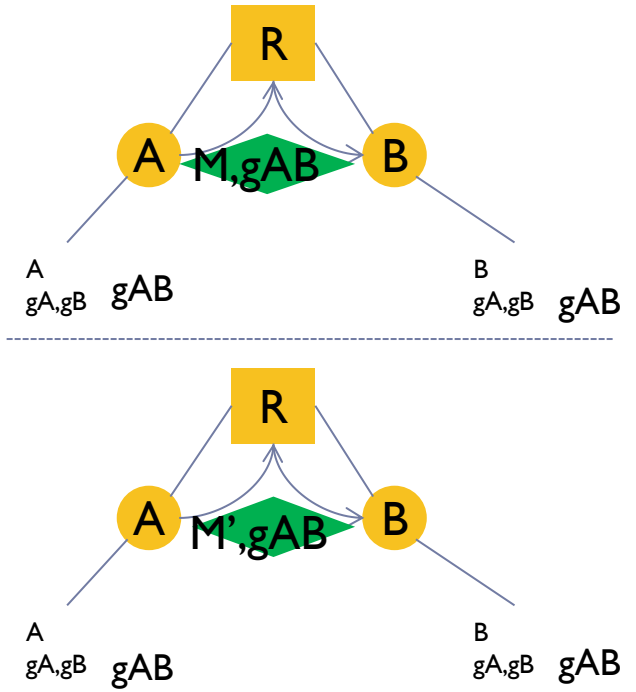
Attaquant



Modèle d'or



Défenseur



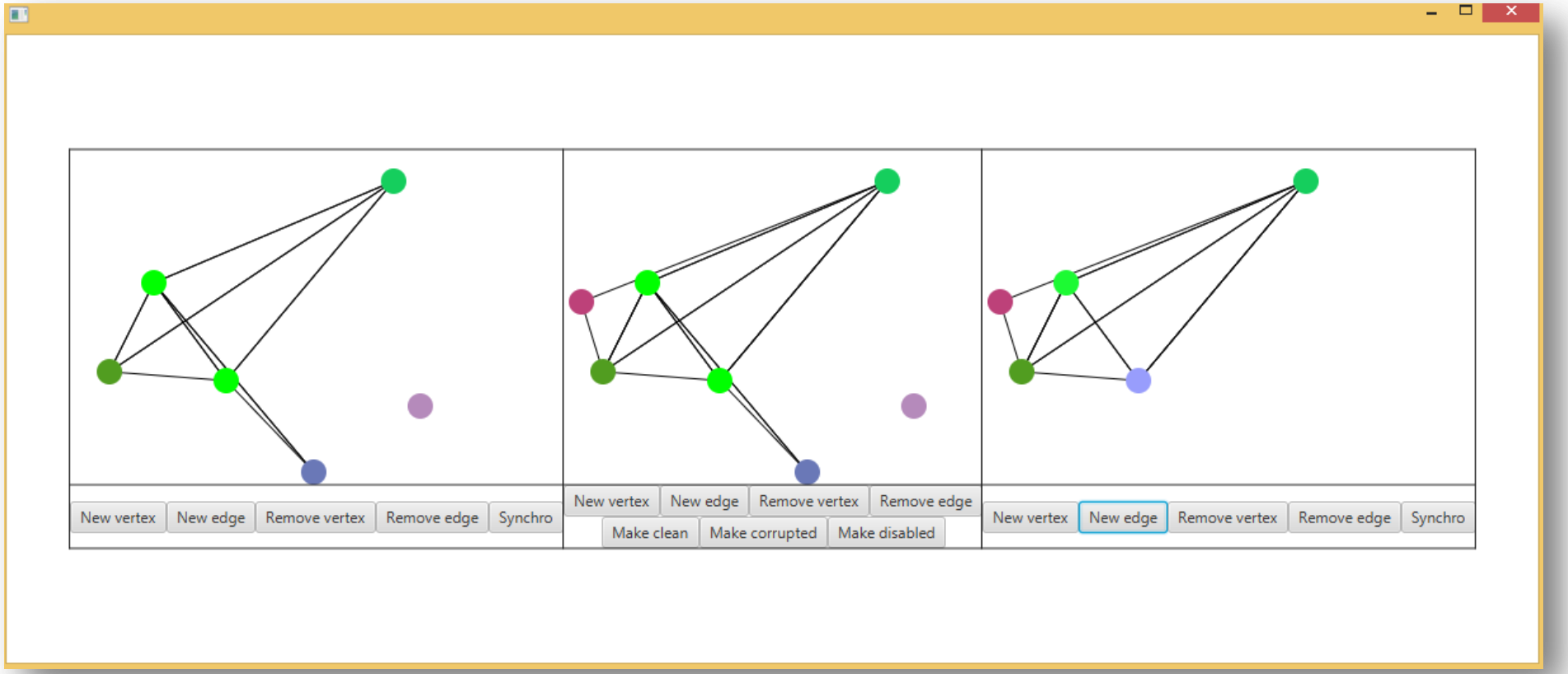
Aspect Dynamique & Exécution

A) Théorie des jeux

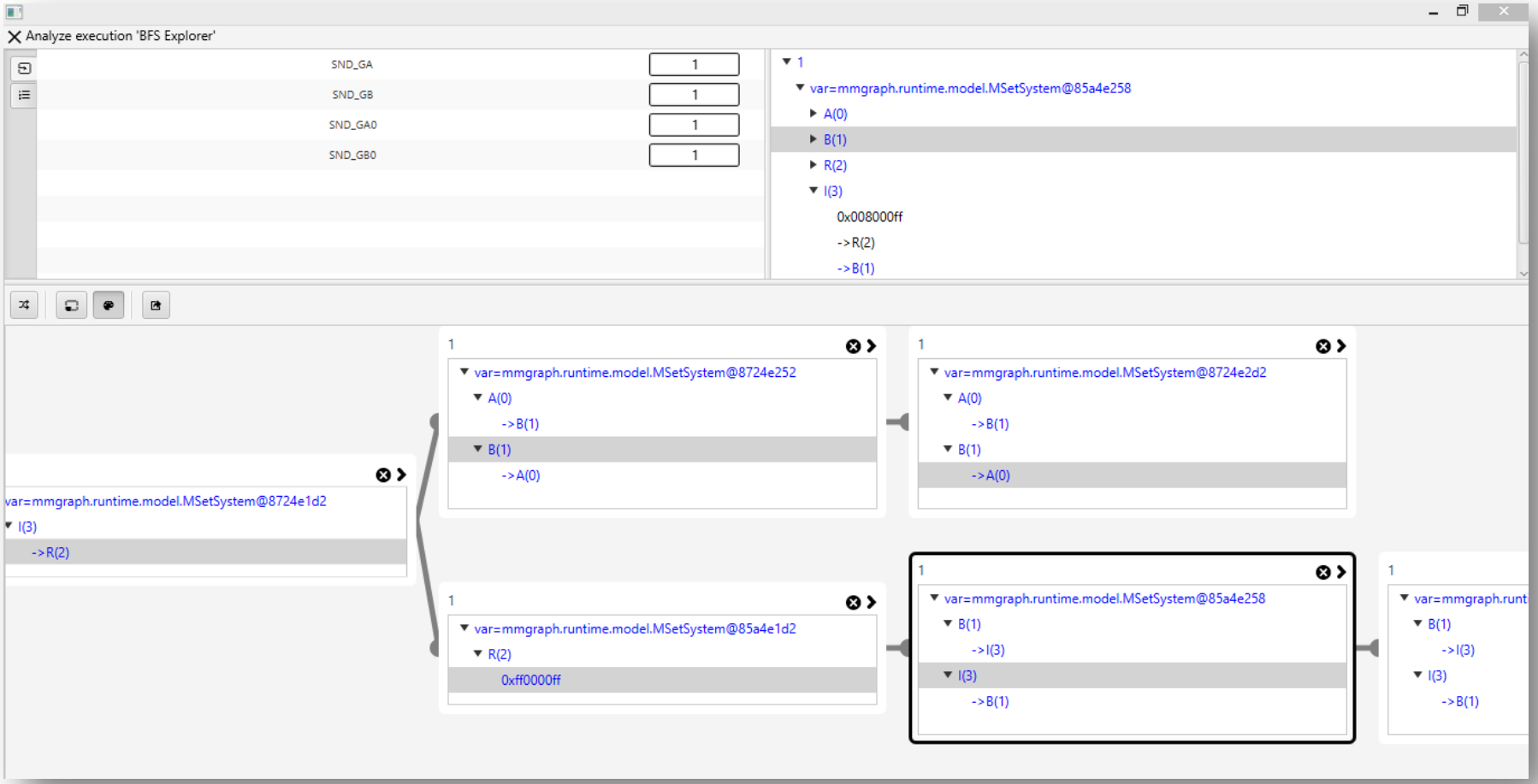
B) Exécution

C) Implémentation

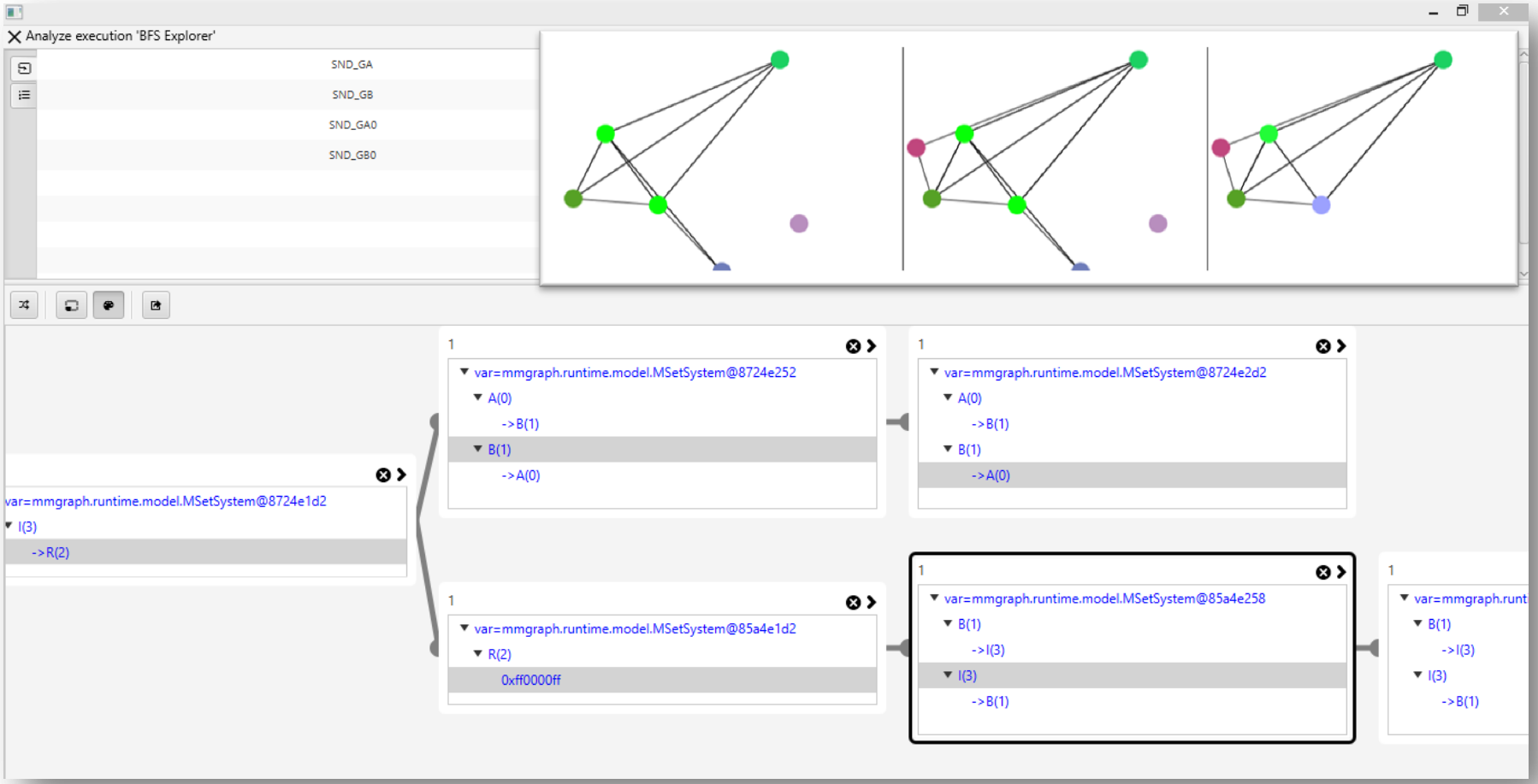
Implémentation



Implémentation



Implémentation (à venir)



Conclusion

Réification de la surface d'attaque

- Terminologie
- STIX

Aspect dynamique

- Théorie des jeux
- Simulation

Mise en œuvre

- Modèle
- Actions
- Intégration dans un cadre logiciel de simulation

Formations:

Rentrée des doctorants MathSTIC
2 Soutenances de thèse (Théotime Bollengier, Fadi Obeid)
Séminaire poster de l'équipe MOCS
Journée des doctorants de 1ère année du Lab-Sticc

Formation LaTeX par la pratique par Vincent LE GARREC
Encadrement de TD Base de données
Encadrement de Projet Informatique Python

Conclusion
Perspectives (court terme)

- Compatibilité avec OBP2
- Enrichissement du modèle
- Traitement d'un autre cas d'étude
- Démarrage d'une dynamique de publication

Conclusion
Perspectives (moyen terme)

- Diagnostic & métrique
- Génération d'arbres d'attaques à partir de scénario
- Estimation de gain pour le calcul de stratégie (Théorie des jeux)

Conclusion
Perspectives (long terme)

- STIX & la surface d'attaque
- Asymétrie inhérente à la cyber-sécurité
  - Initiative de l'attaquant (proactif)
  - Préparation et/ou remédiation du défenseur (passif/réactif)

Merci de votre attention

Bibliographie

- [1] *Redefining the Center of Gravity* in *Joint Force Quarterly (JFQ) issue 59* / Dale C. Eikmeier / Washington D.C. USA / 2010
- [2] *Attack Modeling for Information Security and Survivability* / Andrew P. Moore, Robert J. Ellison, Richard C. Linger/ Software Engineering Institute, Carnegie Mellon University, USA / Mars 2001
- [3] *Is my attack tree correct?* / Maxime Audinot, Sophie Pinchinat, & Barbara Kordy / IRISA Rennes, University Rennes 1, INSA Rennes, France / Août 2017
- [4] *Towards a Theory of Moving Target Defense* / Rui Zhuang, Scott A. DeLoach, Xinming Ou /Kansas State University, Manhattan, USA / 2014
- [5] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015
- [6] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003

Bibliographie

- [7] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999
- [8] *Definitive Guide to Cyber Threat Intelligence* / Jon Friedman, Mark Bouchard, CISSP / CyberEdge Group Annapolis, USA / 2015
- [9] *Standardizing Cyber Threat Inteligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014
- [10] *Introduction to Embedded Systems* A Cyber-Physical Systems Approach / Edward Ashford Lee, Sanjit Arunkumar Seshia / The MIT Press / Cambridge, Massachusetts, USA / 2017
- [11] *CyberWar Games: Strategic Jostling Among Traditional Adversaries* / Sanjay Goel, Yuan Hong / University of New York, New York, USA / 2015
- [12] *Contribution à la modélisation et la vérification formelle par model checking - Symétries pour les Réseaux de Petri temporels. Systèmes embarqués* / Pierre-Alain Bourdil / INSA de Toulouse / 2015.

Bibliographie

- [13] *Using Model Checking to Analyze Network Vulnerabilities* / Ronald W. Ritchey & Paul Ammann / National Security Team Booz Allen & Hamilton & Information and Software Engineering Department George Mason University / Virginia /2000

- [14] *New Directions in Cryptography* / Whitfield Diffie, Martin E. Hellman / IEEE Transactions on Information Theory / Novembre 1976