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)
Joel Champeau (Lab-STICC)

Sommaire

- Sujet de thèse
  - Contexte
  - Problématique
  - Axes de recherches
- Avancement
  - Réification de la surface d'attaque
  - Aspect dynamique et évolution
  - Premier modèle
- Conclusion
  - Bilan
  - Perspectives

Sommaire

- **Sujet de thèse**
  - **Contexte**
  - **Problématique**
  - **Axes de recherches**
- Avancement
  - Réification de la surface d'attaque
  - Aspect dynamique et évolution
  - Premier modèle
- Conclusion
  - Bilan
  - Perspectives

Analyse de la menace

- **Stratégie** attaque-défense
- **Théorie** de la cyber-défense
- **Modélisation** d'attaque

Sujet de thèse
Problématique

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

Modèle système dynamique pour l'analyse de la menace

Réification de la surface d'attaque

Aspect dynamique

Création d'un moteur d'exécution

Sommaire

- Sujet de thèse
  - Contexte
  - Problématique
  - Axes de recherches
- **Avancement**
  - **Réification de la surface d'attaque**
  - **Aspect dynamique et évolution**
  - **Premier modèle**
- Conclusion
  - Bilan
  - Perspectives

Réification de la surface d'attaque

Définitions *[1][2][3]* :

Vulnérabilité

[1] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015
[2] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
[3] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

Définitions [1][2][3] :

Vulnérabilité

[1] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015
[2] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
[3] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

Définitions *[1][2][3]* :

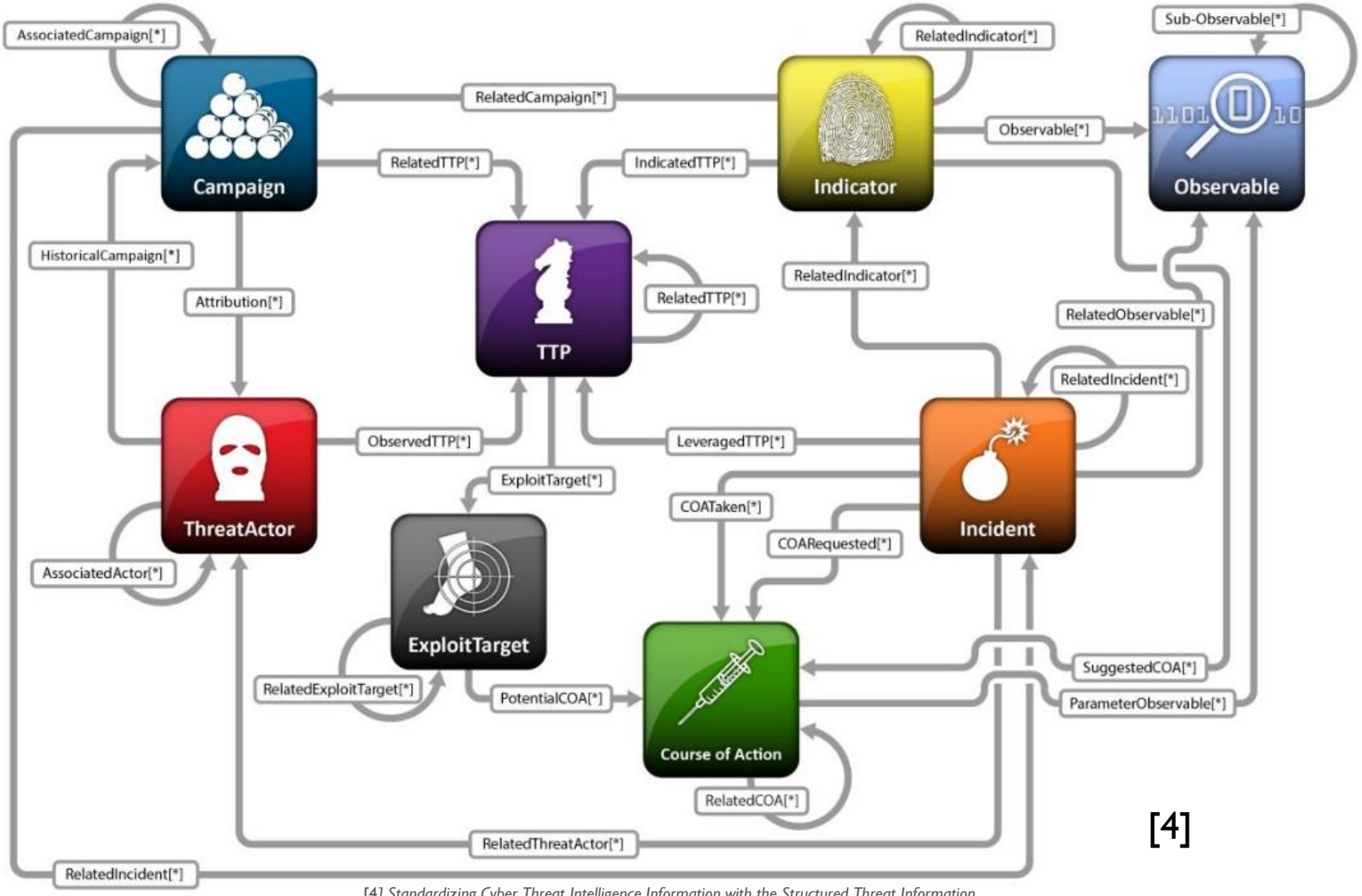
[1] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015
[2] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
[3] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

Réification de la surface d'attaque

Définitions [1][2][3] :

[1] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015
[2] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
[3] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

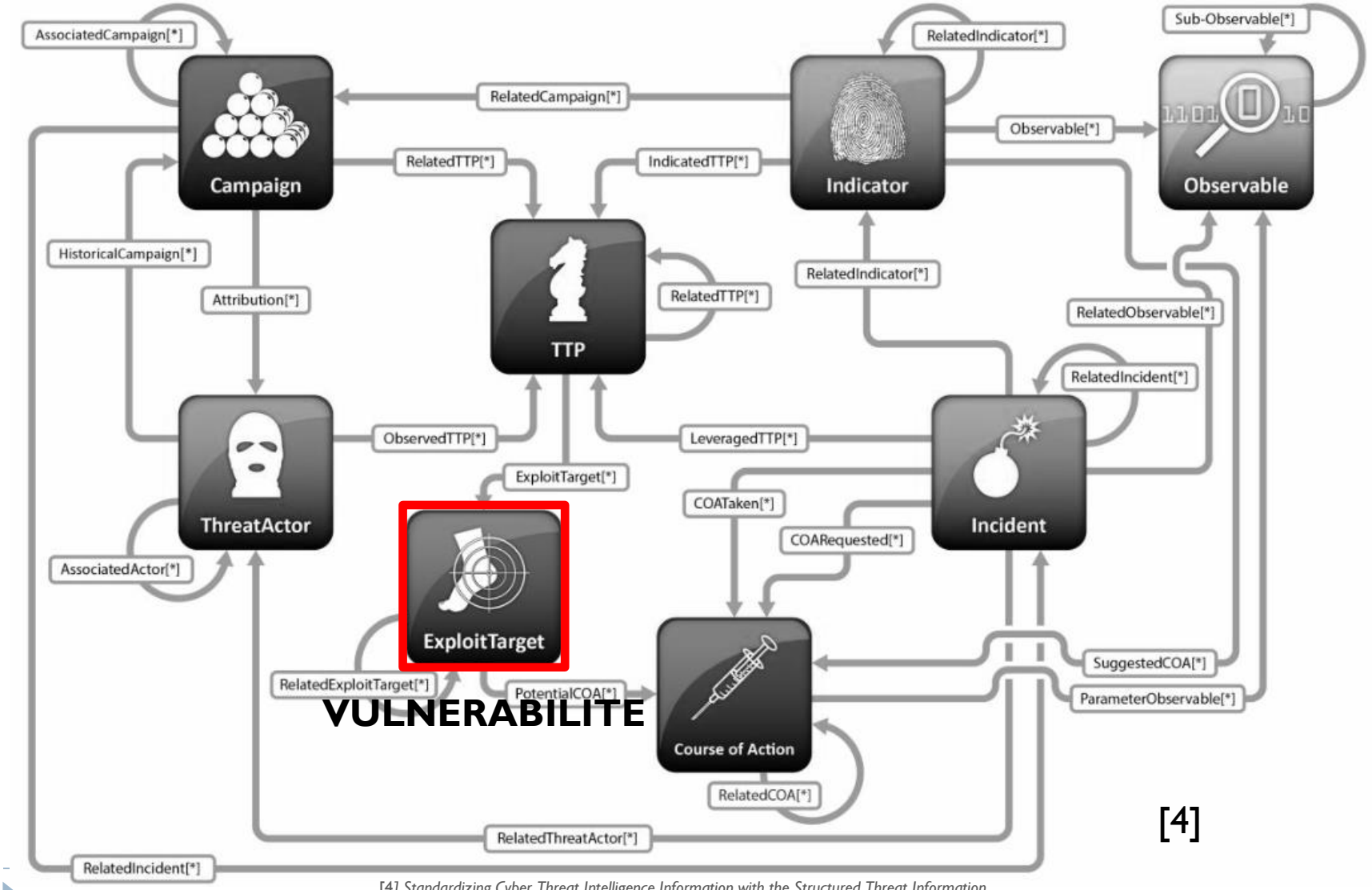
Avancement
Réification de la surface d'attaque



[4]

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

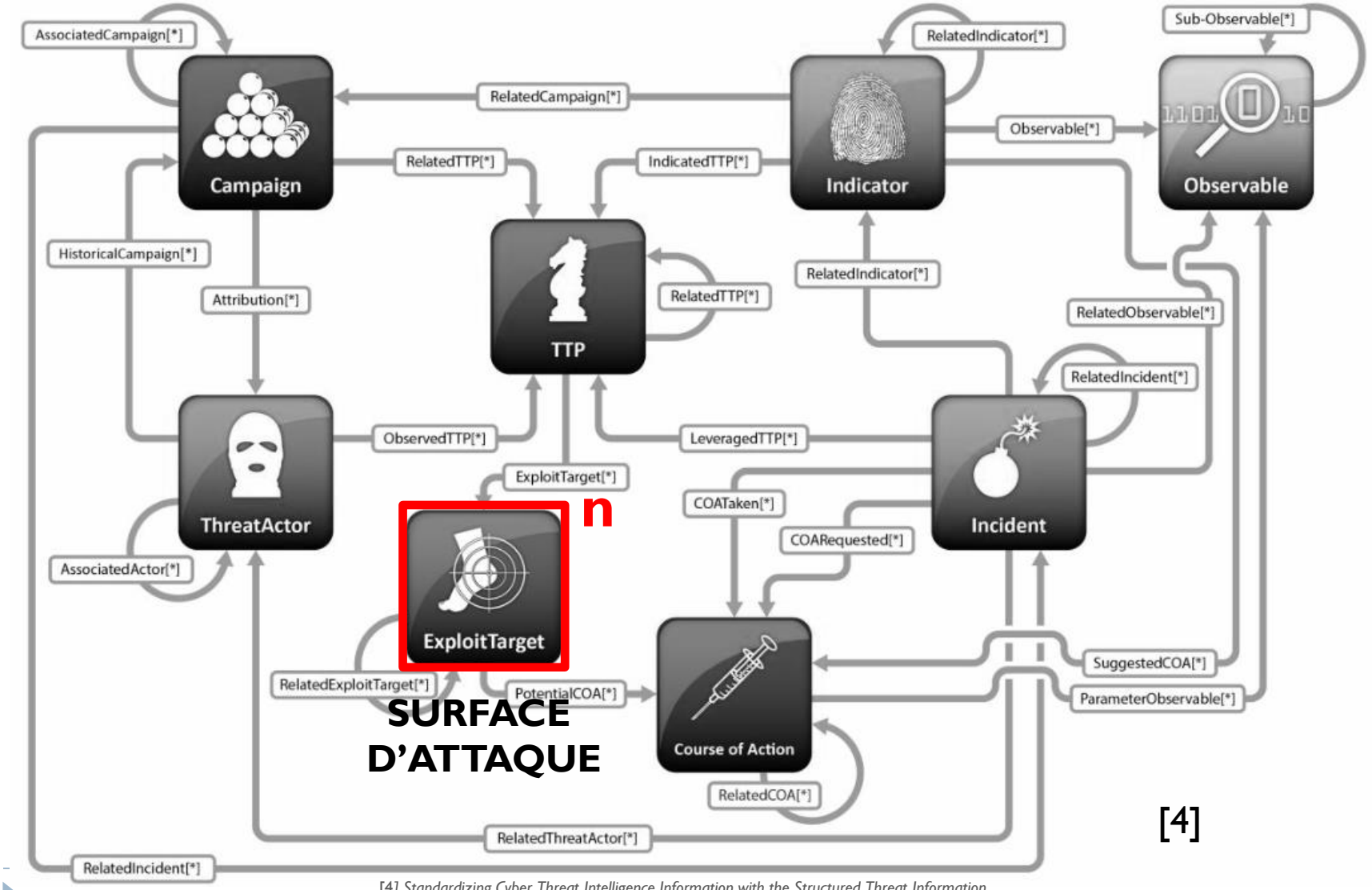
STIX



[4]

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

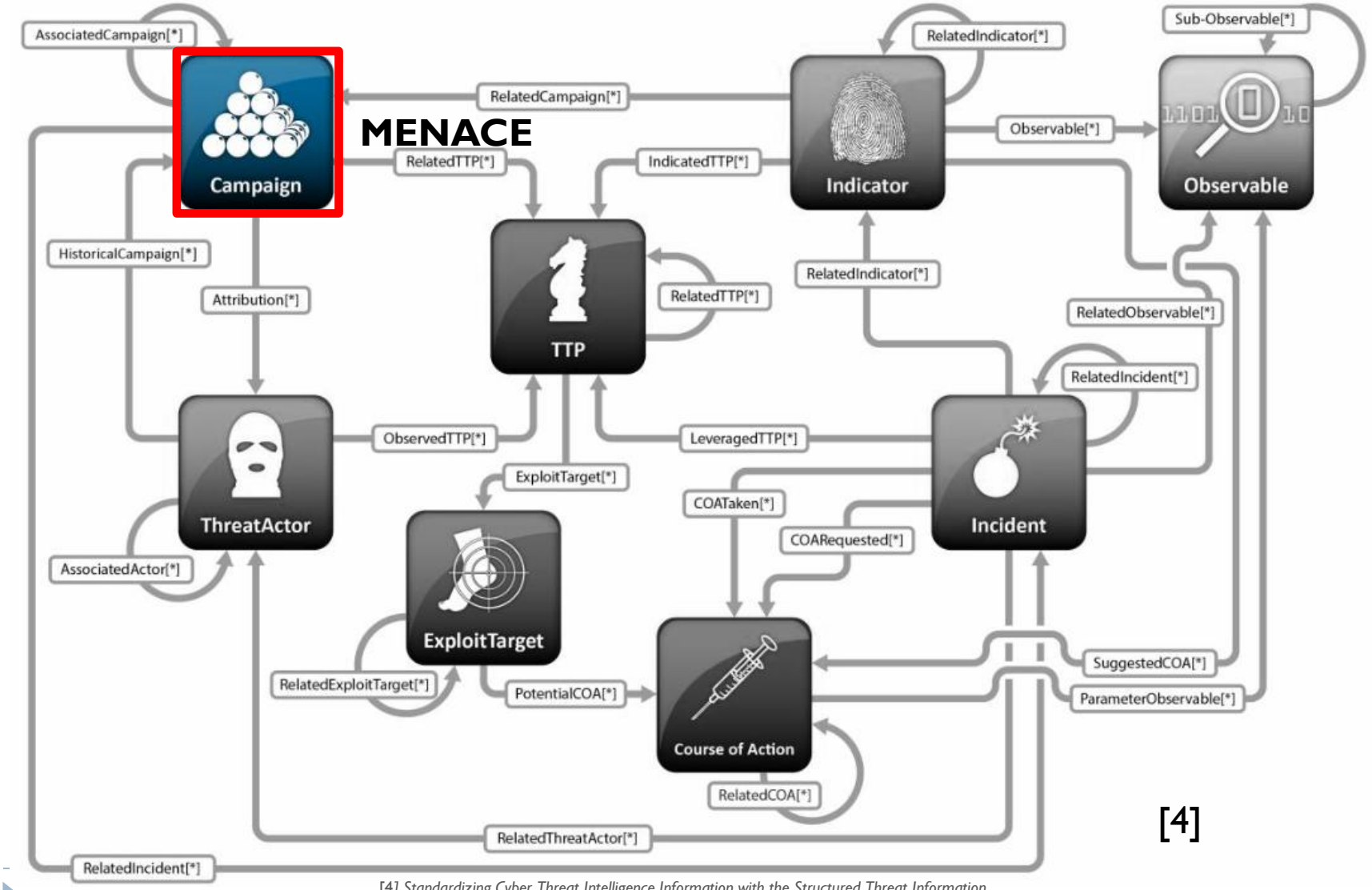
STIX



[4]

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

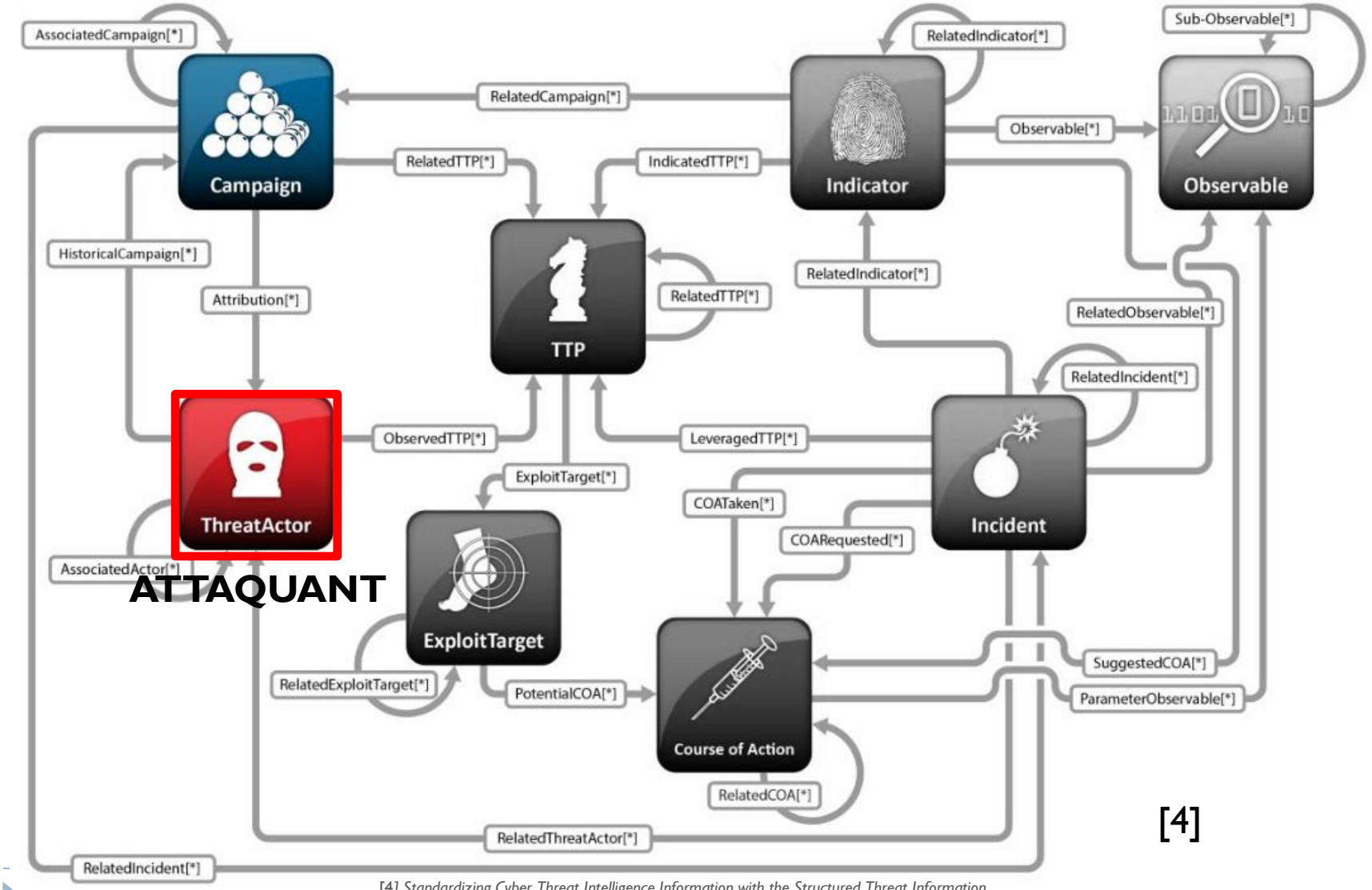
STIX



[4]

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

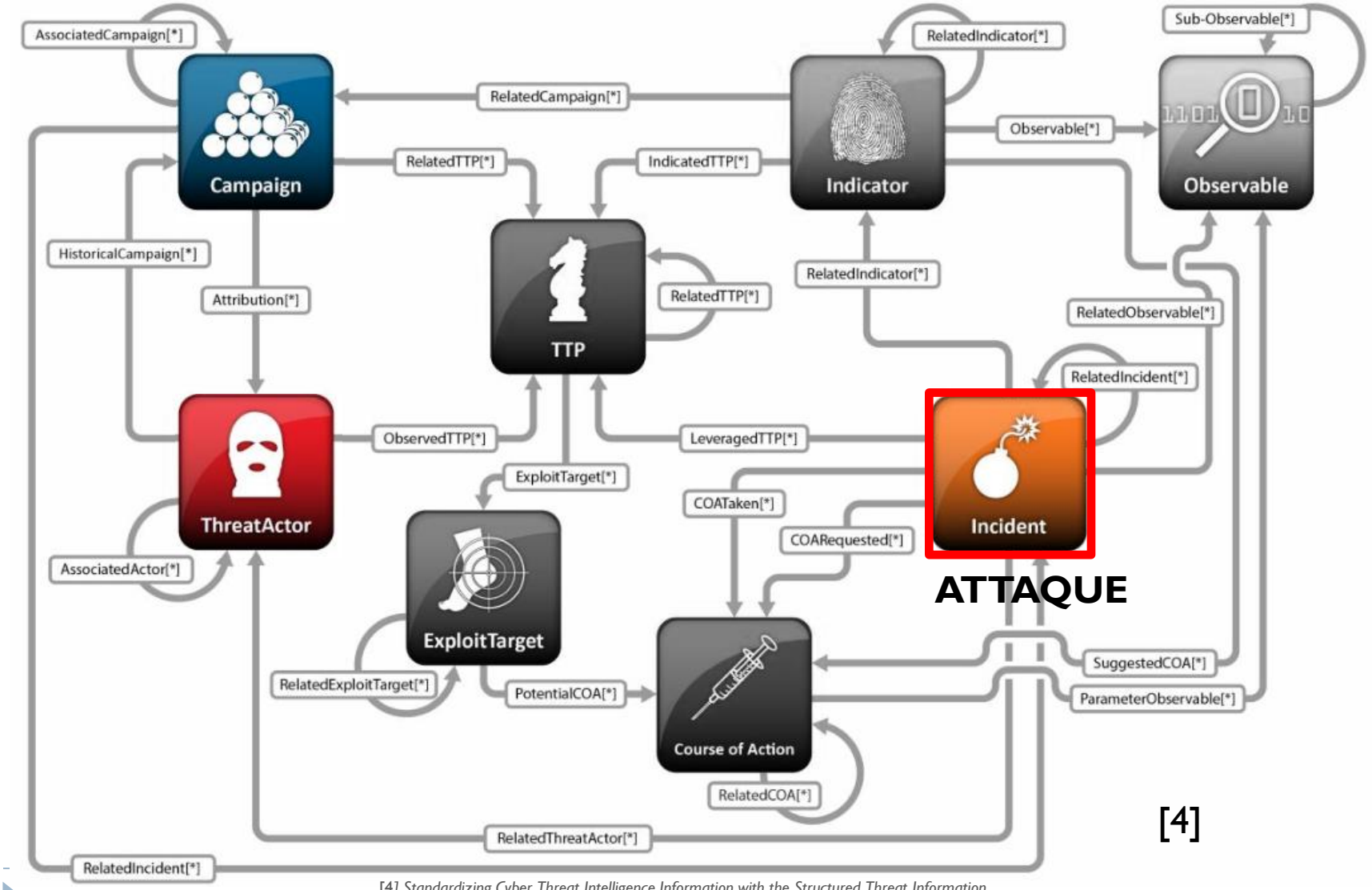
STIX



[4]

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

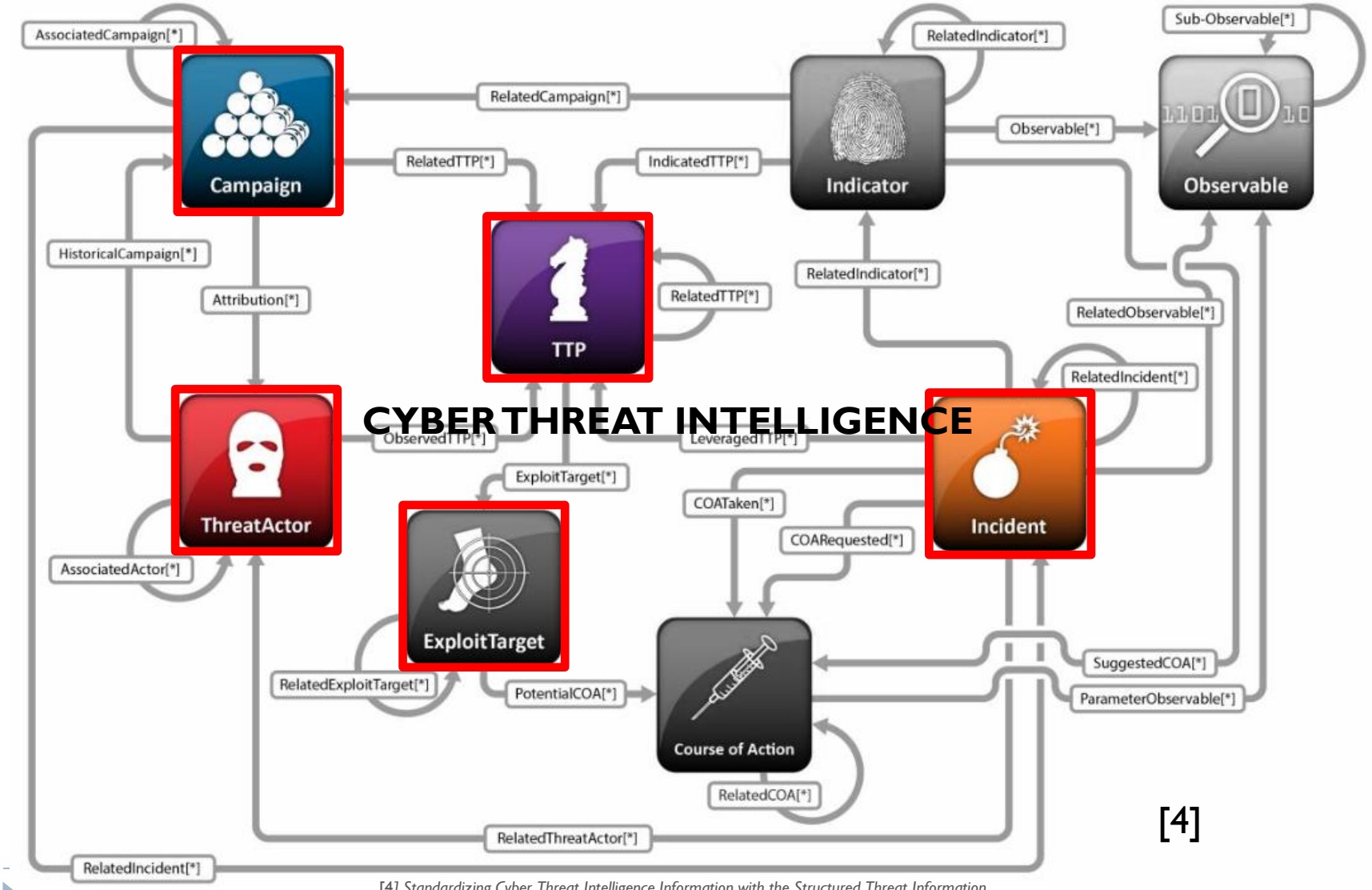
STIX



[4]

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

STIX

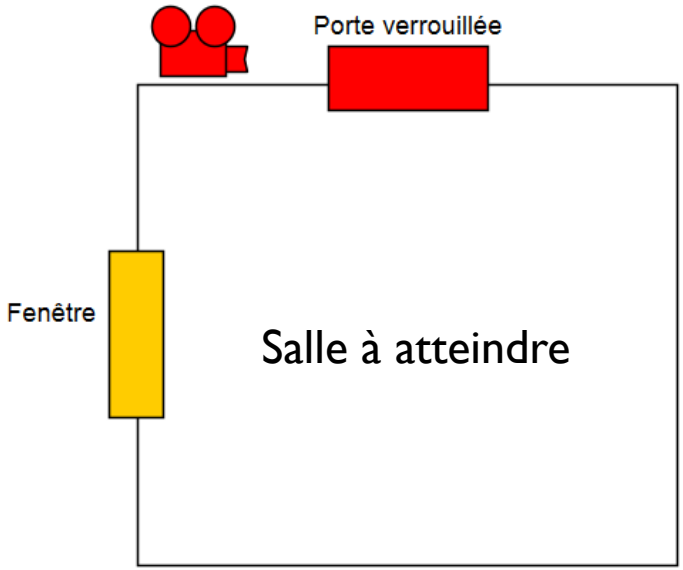


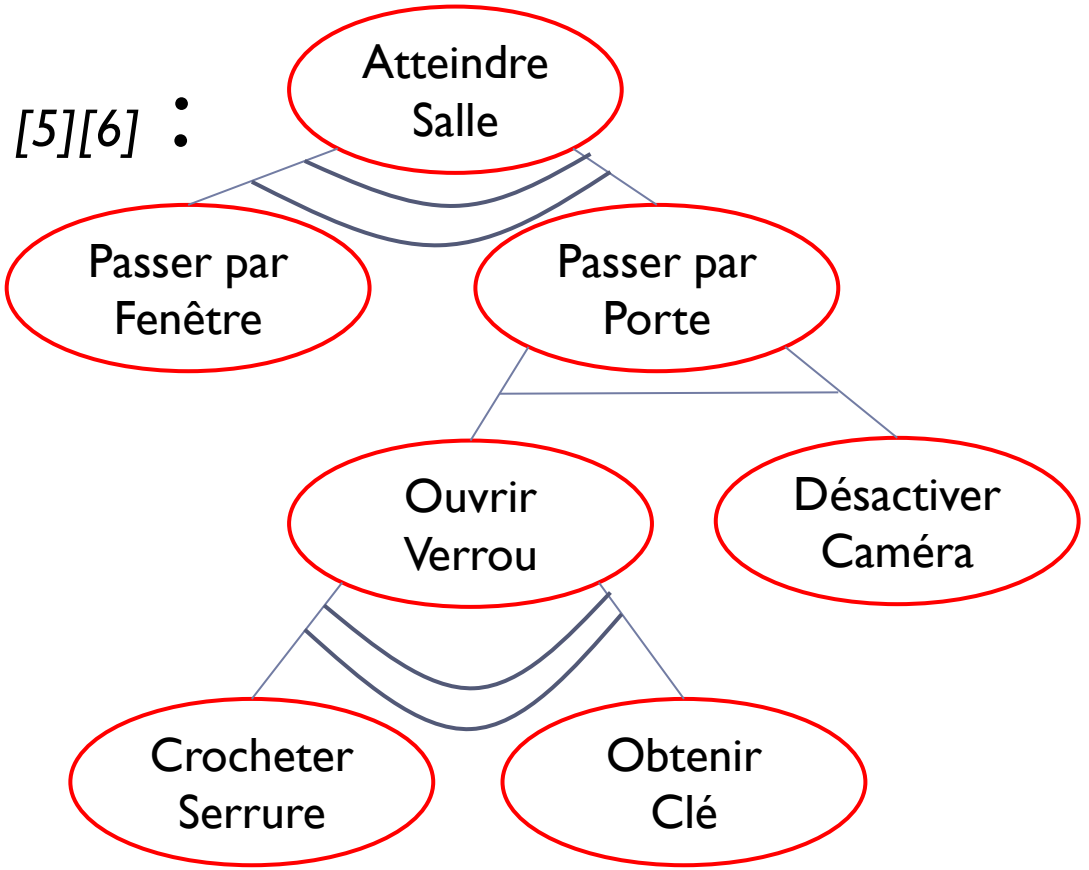
[4]

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

Avancement
Aspect dynamique

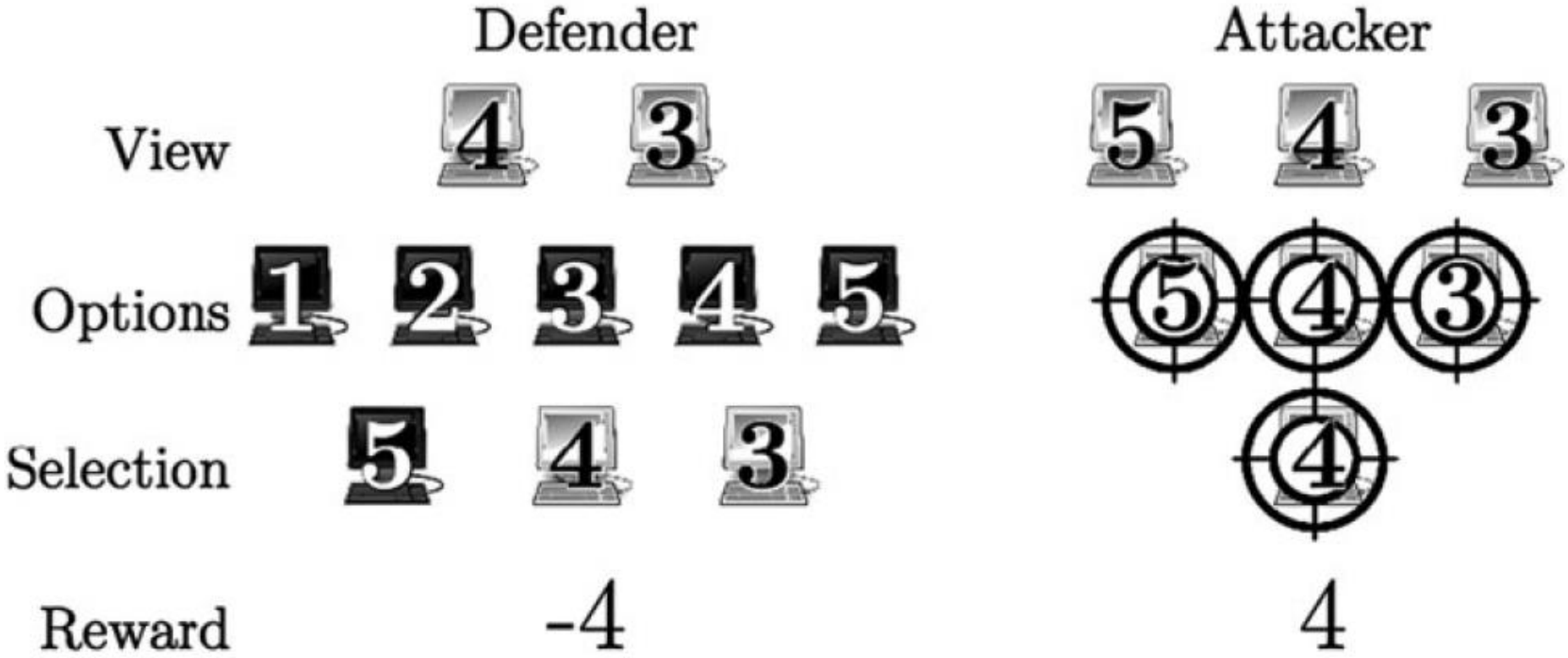
Arbres d'Attaque *[5][6]* :





[5] *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
[6] *Is my attack tree correct?* / Maxime Audinot, Sophie Pinchinat, & Barbara Kordy / IRISA Rennes, University Rennes 1, INSA Rennes, France / Août 2017

Théorie des jeux [7][8] :

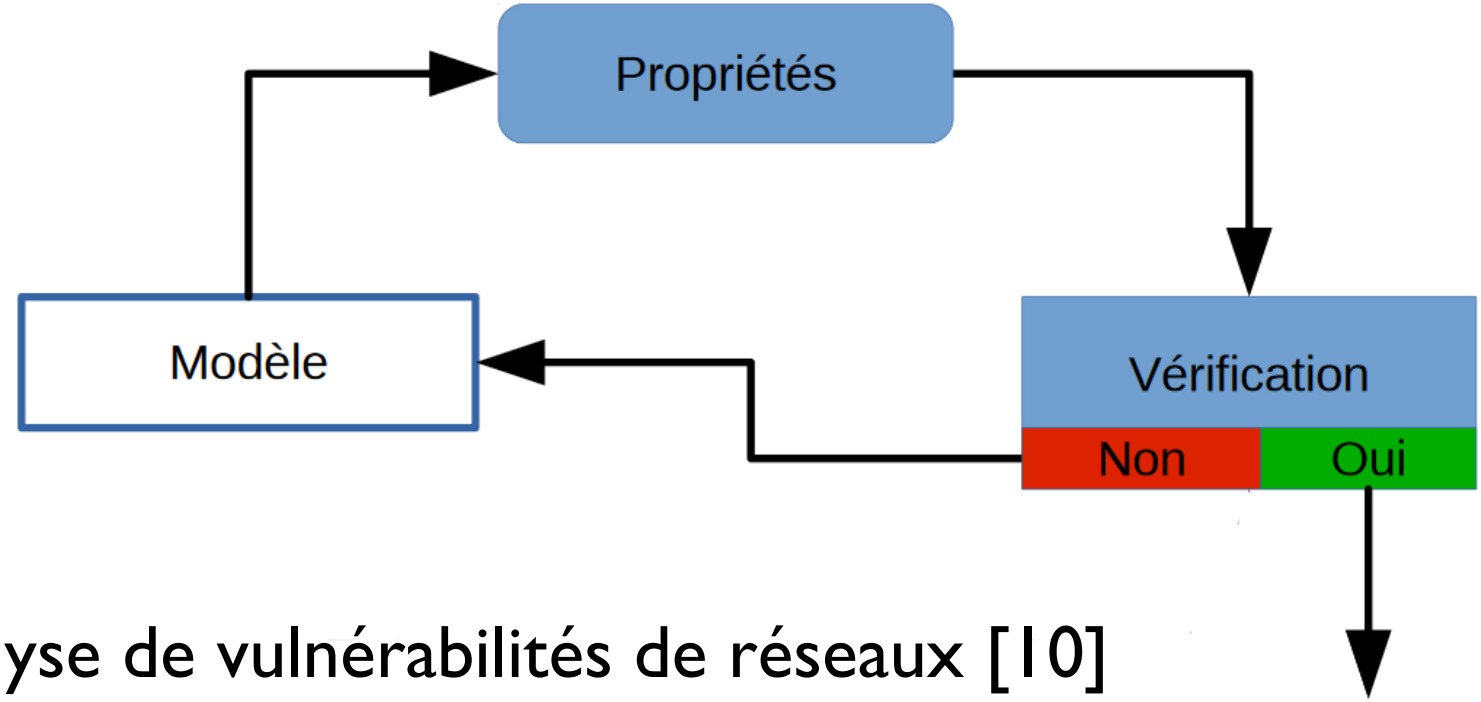


[7] *CyberWar Games: Strategic Jostling Among Traditional Adversaries* / Sanjay Goel, Yuan Hong / University of New York, New York, USA / 2015
[8] *Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security* / Christopher Kiekintveld, Viliam Lisý, Radek Píbil / University of Texas, El Paso, USA / Czech Technical University, Prague, Czech Republic / 2015

Model checking [9] :

Vérification formelle

Enumération exhaustive

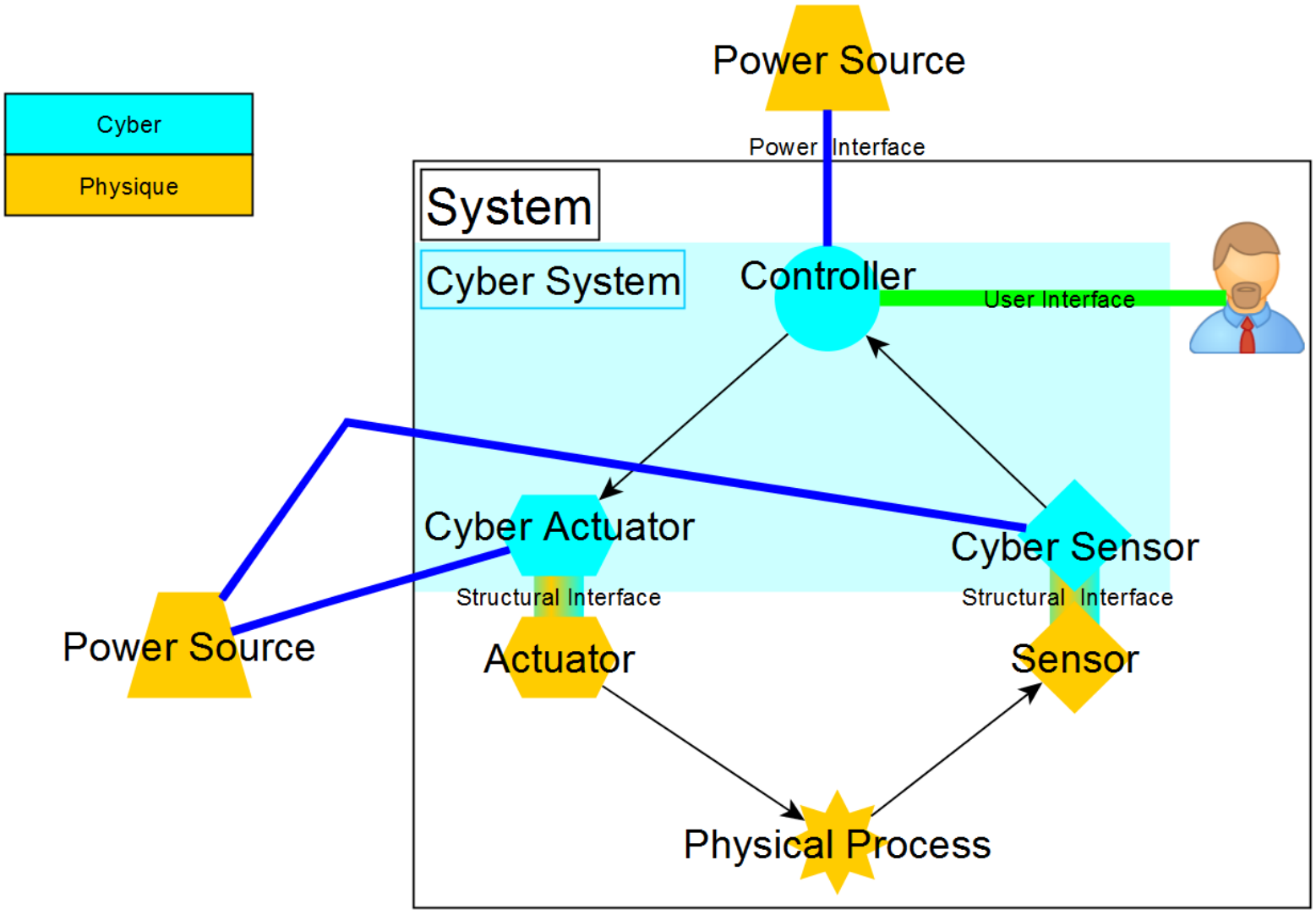


Analyse de vulnérabilités de réseaux [10]

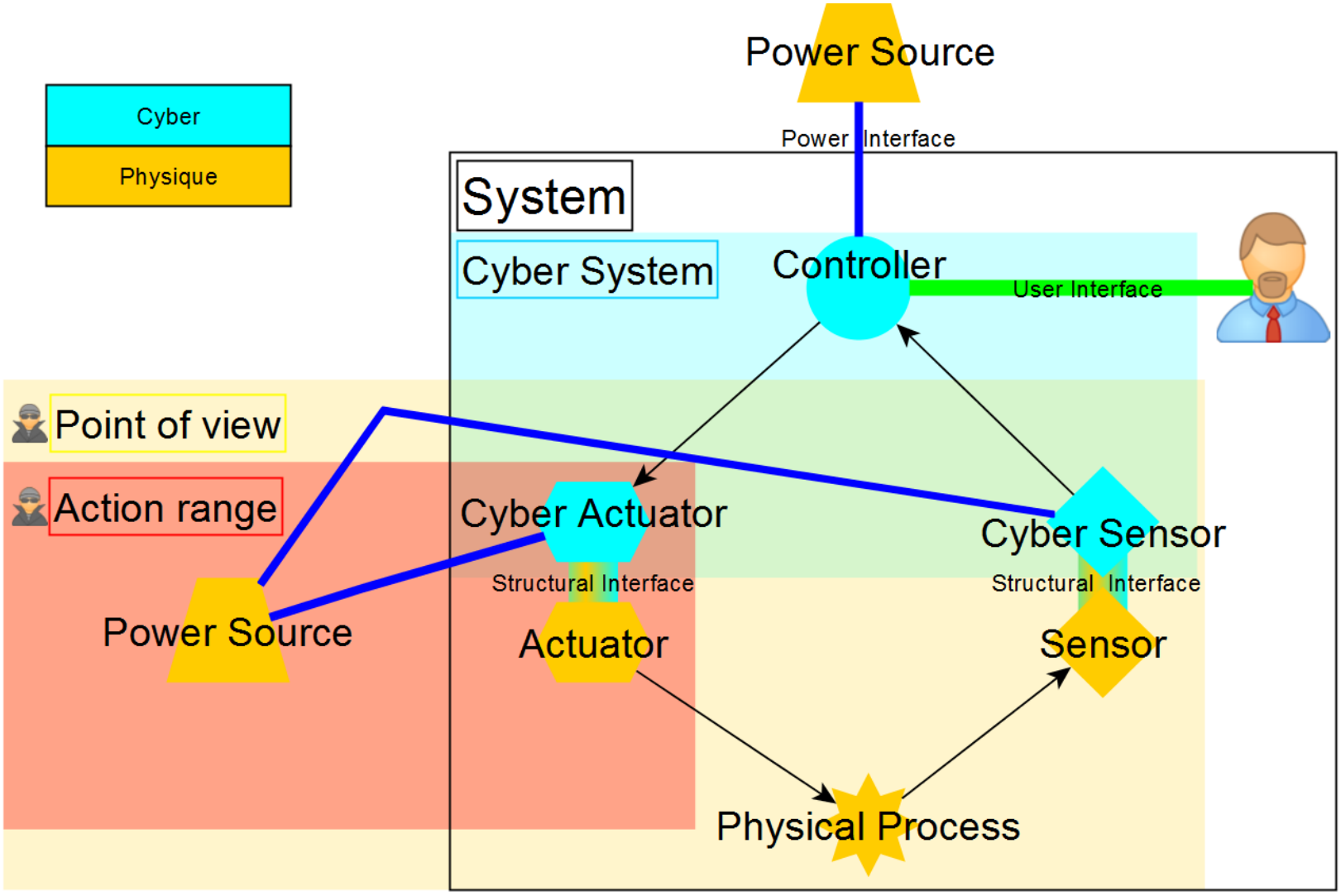
[9] *Contribution à la modélisation et la vérification formelle par model checking - Symétries pour les Réseaux de Petri temporels. Systèmes embarqués* / Pierre-Alain Bourdil / INSA de Toulouse / 2015.

[10] *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

Avancement
Premier modèle



Avancement
Premier modèle



Sommaire

- Sujet de thèse
  - Contexte
  - Problématique
  - Axes de recherches
- Avancement
  - Réification de la surface d'attaque
  - Aspect dynamique et évolution
  - Premier modèle
- **Conclusion**
  - **Bilan**
  - **Perspectives**

Conclusion
Bilan

- Etat de l'art
  - Réification de la surface d'attaque
  - Aspect dynamique
- Premier prototype
  - Modèle graphique
  - Théorie mathématique
  - Implémentation
- Article en préparation

Conclusion
Perspectives

- Maquette à raffiner
  - Machines à états
- Etude des systèmes cyber-physiques
- 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] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015

[2] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003

[3] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999

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

[5] *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

[6] *Is my attack tree correct?* / Maxime Audinot, Sophie Pinchinat, & Barbara Kordy / IRISA Rennes, University Rennes 1, INSA Rennes, France / Août 2017

Bibliographie

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

[8] *Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security* / Christopher Kiekintveld, Viliam Lisý, Radek Píbil / University of Texas, El Paso, USA / Czech Technical University, Prague, Czech Republic / 2015

[9] *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.

[10] *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