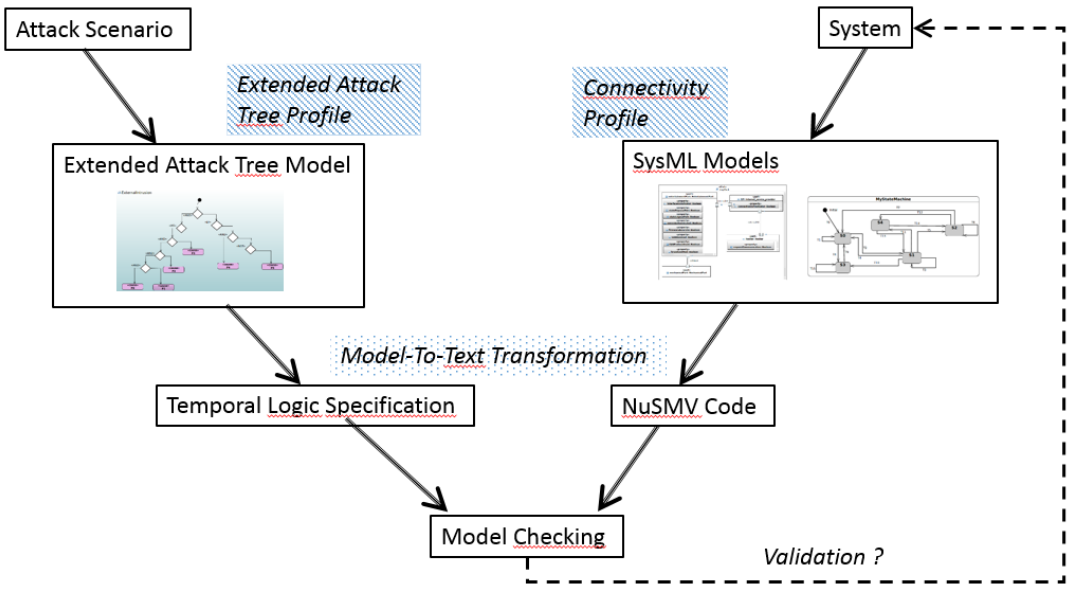
Modélisation et vérification des systèmes embarqués communicants

Nga Nguyen*, Saoussen Mili, Rachid Chelouah, Laboratoire Quartz, EISTI, Cergy, France

Avec l'émergence des nouvelles technologies, les systèmes embarqués sont devenus de plus en plus communicants. Il est primordial de prendre en compte la connectivité dans l'analyse de sécurité contre les cyber-attaques de tout système embarqué, et cela dès la phase de conception, ce qui permettra de réduire les coûts de développement et d'éviter des erreurs ultérieures. L'objectif de notre travail est de proposer des méthodes et des outils d'aide à la modélisation et à la validation via des méthodes formelles, ce qui permettra d'assurer la sécurité d'un système face à des perturbations extérieures qui peuvent se propager à l'intérieur du système. L'approche envisagée est composée de 3 étapes :

1) Modélisation des attaques sous forme d'un arbre d'attaque étendu en utilisant des opérateurs de la logique temporelle CTL. Un profil UML dédié (*Extended Attack Tree Profile*) et un diagramme d'activités sont utilisés afin de représenter la combinaison et la propagation d'erreurs dans un scénario d'attaque;
2) Modélisation du système, à la fois structurelle et comportementale en utilisant des diagrammes SysML, avec un profil UML dédié à la connectivité (*Connectivity Profile*) pour enrichir le modèle système avec des propriétés de protocoles de communication;
3) Validation formelle du système contre les vulnérabilités en utilisation un *model checker*, et celle-ci grâce à une génération automatique préalable du code. Une plate-forme de transformation de modèles développée sur Eclipse en utilisant des outils open-source Papyrus et Acceleo permet de générer du code NuSMV à partir des modèles SysML, ainsi qu'une spécification CTL à partir de l'arbre d'attaque étendu. En cas d'invalidité, le vérificateur de modèle renvoie un contre-exemple et la conception du système devrait être corrigée pour proposer un modèle plus sûr, en respectant l'approche *secure by design*.

Les étapes 1 et 2 peuvent être effectuées en parallèle, et l'approche est résumée dans la figure suivante.



Afin de consolider notre travail, une étude de cas sur le véhicule Jeep Cherokee a été choisie. Notre approche a été appliquée sur ce modèle pour prouver formellement la faille de conception, dans laquelle une intrusion provenant de l'extérieur via le composant Uconnect avec le port TCP 6667 ouvert a été propagée, permettant la réécriture du firmware du microcontrôleur V850, puis l'injection des paquets CAN contrôlant les composants mécaniques, provoquant la prise du contrôle à distance de la voiture. Plus de détails sur cet exemple, ainsi qu'un état de l'art et des comparaisons avec les autres travaux de recherche sont discutés dans les publications suivantes :

1. Saoussen Mili, Nga Nguyen and Rachid Chelouah. Transformation-based Approach to Security Verification for Cyber-Physical Systems, IEEE Systems Journal, acceptée en October 2018.
2. Saoussen Mili, Nga Nguyen and Rachid Chelouah. Attack Modeling and Verification for Connected System Security, IEEE 13th System of Systems Engineering Conference (SoSE 2018), Paris, France, June 2018.
3. Saoussen Mili, Nga Nguyen and Rachid Chelouah. Connected Systems Modeling and Validation, 2017 IEEE International Symposium on Systems Engineering, Vienna, Austria, October 2017.