|  |
| --- |
| **Sujet de thèse**  **Modélisation et analyse de la menace sur systèmes embarqués**  **11 Janvier 2016**  **Joel Champeau**  **Lab-STICC UMR 6285**  **ENSTA Bretagne** |

|  |
| --- |
| **Résumé** |
| Le travail de thèse se situe dans le contexte de la modélisation logicielle et système pour la découverte de systèmes embarqués pour des besoins d’analyse de la menace reposant sur des systèmes embarqués interconnectés.  L’objectif du travail est de constituer et fédérer des modèles de référence sur l’architecture système, les architectures logicielles et matérielles utilisées, incluant les aspects de sécurité inhérents à de tels systèmes. Cette fédération de modèles reposera sur les modèles précités mais aussi sur des informations issues de documentation et d’expérimentations menées conjointement. Cette capitalisation des informations relatives aux systèmes embarqués permettra d’aboutir à une carte d’identité du système numérique dans son contexte système. |

|  |
| --- |
| **Description du sujet de thèse** |
| La cybersécurité est aujourd’hui identifiée comme un enjeu critique tant d’un point de vue système d’information que sur différents les systèmes embarqués, les systèmes SCADA et les systèmes incluant des objets connectés. Par exemple sur les systèmes embarqués, de nombreux travaux sont menés sur le volet matériel (cryptographie, résilience, etc.) et aussi sur le volet logiciel (bonnes pratiques de programmation, etc.). En revanche, peu de travaux ciblent l’interface entre le matériel et le logiciel, pourtant essentielle dans le cadre des systèmes embarqués. Cette interface est effectivement cruciale, puisque à partir du logiciel, elle donne accès à la partie matérielle qui dans la majorité des cas traitent des données applicatives qui peuvent être sensibles. Ainsi maitriser cette interface matérielle logicielle offre la capacité de violer les propriétés d’intégrité ou de confidentialité des données traitées.  Renforcer la méthodologie d’analyse de la menace de cette interface matérielle logicielle permet de mieux maitriser les systèmes à sécurisés mais aussi de proposer une méthodologie de découverte de systèmes non connus de manière exhaustive, par exemple en vue d’une attaque. Pour se faire, manipuler plusieurs niveaux d’abstraction et multi-points de vue allant de modèles système jusqu’au code permet en effet de renforcer la capitalisation des connaissances de l’interface matériel - logiciel.  La phase d’analyse et de capitalisation de l'information s'appuie sur une modélisation hétérogène du système. En effet, il existe différents langages de description matériel sur différents niveaux d’abstraction mais aussi de modélisation au niveau système. La fédération de ces différents modèles reste à ce jour une problématique ouverte sans approche largement adoptée même si différentes initiatives cherchent à combler ce manque [3].  La modélisation par rôle qui repose sur de nombreux travaux tant théoriques que technologiques [4,5] se propose de fournir une alternative pour la définition d’interfaces adaptables pour outils et langages en allouant statiquement et dynamiquement des objets ou éléments de modèles à des rôles.  Dans le cadre cette thèse, nous nous proposons donc d’utiliser ce concept de rôle pour fédérer les différents modèles mis en jeu lors la capitalisation des connaissances des systèmes que nous cherchons à analyser dans un but de découverte de son architecture. Pour cela, nous nous baserons sur des travaux issus d’une précédente thèse (financement DGA – Région Bretagne) menée au sein de l’équipe qui a ouvert la voie de la définition de rôle dans le but de fédérer différents modèles systèmes [10,11,12,13]. Ce travail nous permet de disposer d’un prototype d’outillage, cependant il reste encore à formaliser et à étendre pour traiter le problème de fédération, de l’intégration de langages de programmation (matériel et logiciel) et ainsi que des données faiblement structurées. Les conclusions du document de thèse a identifié un certain nombre de ces perspectives de travail [14].  Ce travail de modélisation et fédération par rôles se basera sur les approches de conception descendante de circuits classiques, où les spécifications subissent des changements incessants et où les raffinements (introduction de détails architecturaux, etc) correspondent à autant d'explorations architecturales. Ces approches incrémentales sont particulièrement employées dans la conception  de SoC (system-on-chip), où deux à trois niveaux d'abstraction différents ont cours : comportemental, architectural et détaillé [1,2,9]. Dans ce cadre la synthèse de haut niveau permet la production de circuits matériels à partir de spécification modélisées. La maitrise de cette synthèse de haut niveau dans l’équipe de l’ENSTA Bretagne permet de se reposer sur une expertise éprouvée pour améliorer la modélisation des systèmes sur différents niveaux d’abstraction. En effet, l’équipe de l’ENSTA Bretagne a développé en propre et en collaboration avec ses partenaires du Lab-STICC des outils logiciels permettant la synthèse de haut niveau [6,7,8]. Cette maitrise technologique de la phase de synthèse de haut-niveau permet d’orienter à façon pour répondre à des problématiques ciblées comme l’évaluation d’architectures cibles.  L’enjeu de ces travaux se positionne au niveau de la gestion de la connaissance de l’interface matériel – logiciel et elle repose sur différents modèles hétérogènes fédérés servant de capitalisation de cette connaissance lors de l’analyse de systèmes en vue d’une sécurisation ou d’une attaque.   1. Z. J. Jia, A. Núñez, T. Bautista, and A. D. Pimentel. 2014. A two-phase design space exploration strategy for system-level real-time application mapping onto MPSoC. Microprocess. Microsyst. 38, 1 (February 2014). 2. Mark Thompson and Andy D. Pimentel. 2013. Exploiting domain knowledge in system-level MPSoC design space exploration. J. Syst. Archit. 59, 7 (August 2013), 351-360. 3. M. Seifert, C. Wende, and U. Aßmann, “Anticipating unanticipated tool interoperability using role models,” in Proceedings of the First International Workshop on Model-Driven Interoperability. ACM, 2010. 4. F. Steimann, “On the representation of roles in object-oriented and conceptual modelling,” Data & Knowledge Engineering, vol. 35, no. 1, pp. 83–106, 2000. 5. T. Kühn, M. Leutäuser, S. Götz, C. Seidl, and U. Aßmann, “A metamodel family for role-based modeling and programming languages,” in Software Language Engineering, ser. Lecture Notes in Computer Science. Springer International Publishing, 2014, 6. A Prototyping Platform for Virtual Reconfigurable Units. Lagadec L., Le Lann Jean-Christophe, Bollengier T. Recosoc 2014 - May, Montpellier France. 7. An experimental toolchain based on high-level dataflow models of computation for heterogeneous MPSoC. Julien Heulot, Karol Desnos, Jean-François Nezan, Maxime Pelcat, Mickaël Raulet, Hervé Yviquel, P.-L. Lagalaye, J-C Le Lann. DASIP'12 8. From system-level models to heterogeneous embedded systems, Jean-Christophe Le Lann, Joël Champeau, Papa Issa Diallo, Pierre-Laurent Lagalaye.RITF 2012 - Recherche et Innovation pour les Transports du Futur, Paris : France. 9. Modélisation algorithmique et synthèse d'architectures assistées par model-checking, Jean-Christophe Le Lann, Philippe Dhaussy, Pierre-Laurent Lagalaye.CAL 2012-, Montpellier : France. 10. MoPCoM Methodology: Focus on Models of Computation. Ali Koudri, Joël Champeau, Jean-Christophe Le Lann and Vincent Leilde. ECMFA'2010, Paris 11. Model federation in toolchains. J. Champeau, V. Leildé, and P. I. Diallo, in Workshop “[Semantic Information Modeling for Federation](http://models2013.lcc.uma.es/workshops.html#WTA17) “ in conjunction with MODELS 2013. 12. A Role Language to Interpret Multi-Formalisms System of Systems Models. Jean-Philippe Schneider, Joël Champeau, Ciprian Teodorov, Eric Senn and Loïc Lagadec. IEEE International System Conference, Vancouver, April 13-15, 2015. 13. Role Framework to Support Collaborative Virtual Prototyping of System of Systems. Jean-Philippe Schneider, Joël Champeau, Loïc Lagadec and Eric Senn. WETICE Conference June 15-17 2015. 14. Les rôles : Médiateurs dynamiques entre modèle système et modèles de simulation, , Jean Philippe Schneider, thèse de doctorat de l’Université de Bretagne Sud, Novembre 2015. |