Maîtrise des Correctifs de Sécurité pour les Systèmes Navals

Bastien Sultan[1], Fabien Dagnat[2] et Caroline Fontaine[3]

[1] Chaire de Cyber Défense des Systèmes Navals
École navale, Télécom Bretagne, DCNS, THALES
École navale – CC 600
F29240 Brest CEDEX 09
bastien.sultan@telecom-bretagne.eu
[2] IRISA, Télécom Bretagne
fabien.dagnat@telecom-bretagne.eu
[3] Lab-STICC, CNRS, Télécom Bretagne
caroline.fontaine@telecom-bretagne.eu

Résumé

Un navire est un système complexe, opéré dans le but d'accomplir un ensemble de missions. Les composants d'un tel système peuvent être affectés de vulnérabilités dont l'exploitation peut avoir des conséquences sur les missions en cours. Il est donc nécessaire d'appliquer des correctifs réduisant le risque lié à ces vulnérabilités. Mais il est important de s'assurer que ces correctifs n'ont pas eux-mêmes d'impact négatif sur les missions du navire. Nous proposons, dans cet article, l'architecture d'un processus de gestion des correctifs appliqué au contexte des systèmes navals. Nous extrayons de ce processus les problématiques principales qu'il pose : la modélisation d'un système complexe, et le calcul des impacts liés aux correctifs et vulnérabilités. Nous évoquons ensuite l'intérêt de la fédération de modèles pour représenter le système naval, puis nous proposons une mesure de l'impact des correctifs et vulnérabilités sur la sûreté de fonctionnement du système, basée sur l'utilisation d'automates temporisés.
Mots clés : mesures d'impact, fédération de modèles, systèmes navals, correctifs, cyberdéfense

Ships are complex systems operated to perform a given set of missions. Such systems can be affected by vulnerabilities which, when exploited, can impact their missions. Thus it is necessary to apply patches to mitigate these vulnerabilities, and fundamental to ensure that deployed patches does not negatively affect the system's dependability. This paper puts forward a patch management process architecture applied to naval systems. An analysis of this process allows us to evoke the two main issues of our research: complex systems modelling and impact assessment. Then we present models federation *as a tool for ships modelling, and an impact assessment approach based on trace analysis of timed automata.*
Keywords: *impact assessment, models federation, naval systems, patch management, cybersecurity*

Introduction

Répondant à l'objectif d'acquisition de compétences et de technologies en cybersécurité prônée par le Livre Blanc de la Défense 2013, la Chaire de Cyber Défense des Systèmes Navals est née de la coopération académique et industrielle entre Télécom Bretagne, l'École Navale, DCNS et Thales. L'application de la recherche en cybersécurité au domaine naval est, en effet, particulièrement importante à l'heure où les bâtiments – civils ou militaires – embarquent un grand nombre de systèmes informatiques contrôlant notamment des actionneurs mécaniques d'importance critique, ou permettant au navire de communiquer, se localiser, percevoir son environnement opérationnel.

Toute bénéfique qu'elle soit en termes d'efficacité et de précision, la présence de ces systèmes informatiques peut ouvrir des brèches à un attaquant sachant les exploiter. Ces failles peuvent être logicielles, matérielles, organisationnelles, humaines et posent le problème de leur détection et de leur comblement. Véritable processus critique du système naval, la maîtrise des correctifs palliant ces failles est au cœur des travaux dont la phase initiale est présentée dans cet article.

Il convient, dans la première partie du document, de définir les notions essentielles mobilisées par nos travaux. Nous nous attachons ensuite à présenter le modèle simplifié d'un processus de gestion de correctifs, dont l'étude nous permet de dégager les deux problématiques majeures du projet de recherche : *la représentation du système*, et *les calculs d'impact et de risque des correctifs et vulnérabilités*. La partie 3 permet d'exposer notre manière d'aborder ces deux thématiques et de mettre en évidence leurs liens. Enfin, la partie 4 présente une démarche d'estimation d'impact basée sur l'analyse de trace d'automates temporisés.

1 Le navire, un système complexe

Un navire, ou système naval, est un système complexe composé d'un ensemble de sous-systèmes, dont des systèmes cyber-physiques (CPS), opérés par un équipage dans le but d'accomplir des missions. Les fonctions d'un système naval impliquent de nombreux acteurs. Par exemple, la navigation repose sur des capteurs GNSS et/ou des centrales inertielles, des systèmes de traitement et d'analyse de leurs signaux, le choix de la route, l'opération des systèmes de propulsion... La sécurité de ces équipements est primordiale : si l'un d'entre eux ne remplit pas son rôle, cela peut mettre en péril le système ou ses missions. Or, dans l'exécution de telles fonctions, des faiblesses peuvent affecter des acteurs divers (capteurs, actionneurs, procédures, ...) et perturber ainsi les différentes étapes des missions. La mise en place d'un correctif, ayant pour but de tempérer ces faiblesses, peut également perturber le fonctionnement du navire. Il est donc nécessaire d'étudier les impacts des vulnérabilités et des correctifs sur le système. Cette étude implique de définir les notions de *système*, *vulnérabilité*, *correctif* et *impact*.

— **Système :** Un système est une entité composée d'opérateurs, de procédures, d'équipements matériels, de fonctions et de logiciels. Les composants de cette entité œuvrent conjointement dans leur environnement opérationnel dans le but d'accomplir des missions données [10]. Le système possède une politique de sécurité [1] garantissant notamment la sûreté de fonctionnement de ses éléments.

— **Vulnérabilité :** Une vulnérabilité, ou faille, est une faiblesse dans la conception, la configuration, l'opération ou la maintenance d'un système, qui peut être exploitée pour violer sa politique de sécurité. Une vulnérabilité suit un cycle de vie [5] ; on peut à chaque stade de ce cycle associer un niveau de risque à la vulnérabilité qui s'exprime en fonction de son impact et de la probabilité de son exploitation.

— **Correctif :** Un correctif est une mesure, ou un ensemble de mesures (action, dispositif matériel, logiciel, procédure, ...) qui réduit la possibilité d'exploiter une vulnérabilité [9]. Son application peut être temporaire ou permanente.

— **Impact :** L'impact de l'exploitation d'une vulnérabilité (resp. du déploiement d'un correctif, des opérations de déploiement de ce correctif) est l'ensemble des retombées de l'exploitation d'une vulnérabilité (resp. du déploiement d'un correctif, des opérations de déploiement de ce correctif) sur la capacité du système à accomplir ses missions de manière sûre. Ces impacts permettent de comparer les conséquences de chacun de ces événements, et donc de décider de la démarche la plus adaptée lors de la découverte d'une faille, en fonction des missions en cours (faut-il appliquer un correctif ? Si oui, lequel ?).

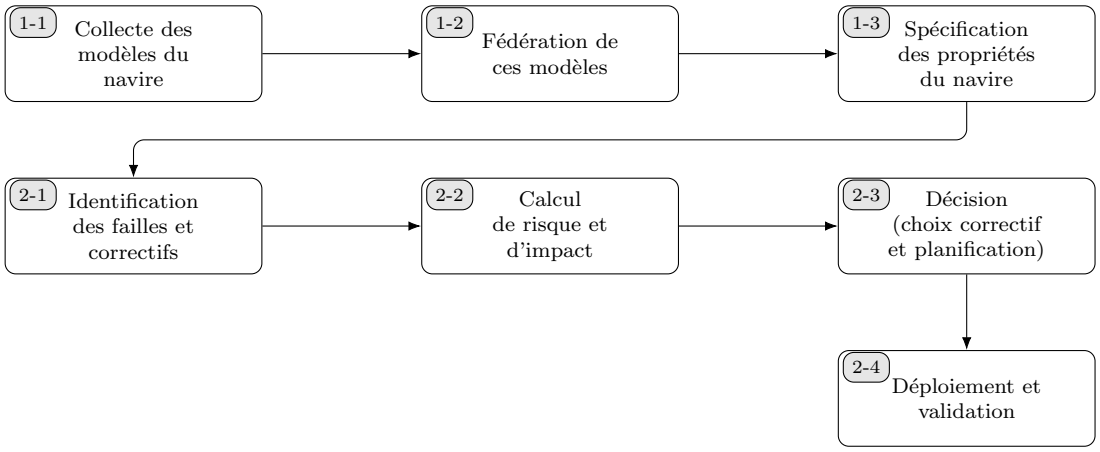

FIGURE 1 – Processus d'analyse du système (1) et de gestion des correctifs (2)

2 Le processus de gestion des correctifs de sécurité

La gestion des correctifs a été traitée par plusieurs articles [5, 7, 12, 11]. Nous pouvons proposer, en nous inspirant de ces travaux et notamment de [7], les grandes étapes d'un processus de gestion des correctifs adapté à notre contexte (*cf.* figure 1). Nous ajoutons toutefois une étape supplémentaire, moins traitée par les publications du domaine mais qui nous semble cruciale : le calcul de l'impact des opérations de déploiement d'un correctif. En effet, ces opérations peuvent suspendre temporairement certains processus critiques, ce qui peut être intolérable. Par exemple, la désactivation d'un automate de contrôle pendant un temps donné peut interrompre le cours de certaines missions.

Le processus proposé commence par la phase d'identification *des vulnérabilités* (2-1). Cette étape a pour but d'agréger les informations d'intérêt ayant trait aux failles des différents éléments du système. Or, de très nombreux sous-systèmes cohabitent au sein du navire : certains sont génériques et largement utilisés dans d'autres contextes, alors que d'autres sont très spécifiques et ont été conçus *ad hoc*. Cette tâche s'appuie donc sur l'analyse de sources diverses comme par exemple des flux d'information publics des producteurs de COTS, des informations plus confidentielles pour les composants « sur-mesure » ou des vulnérabilités non publiées.

De la même manière, la phase d'identification *des correctifs* (2-1) s'attache à passer en revue les contre-mesures permettant de combler chaque faille. Cette étape se rapproche de la précédente car des contre-mesures peuvent être publiées, notamment en ce qui concerne les vulnérabilités affectant les composants génériques. Parfois, aucune contre-mesure n'est connue. Il s'agit donc d'agréger les informations disponibles, mais aussi de concevoir des correctifs spécifiques (qui peuvent être des mesures temporaires simples, comme l'isolement physique d'un composant du système, sa mise hors-service ou son remplacement).

À partir des informations rendues disponibles par les deux premières étapes du processus, un ensemble de calculs d'impact et de risque vont pouvoir être menés (2-2). Les résultats de ces calculs guideront les choix des correctifs à appliquer, en permettant la comparaison des retombées des différents correctifs sur la capacité du système à réaliser ses missions (2-3).

Trois analyses distinctes sont proposées :

1. l'*analyse du risque associé aux vulnérabilités*, recouvrant le calcul d'impact de chaque ex-

ploitation possible des vulnérabilités et l'estimation de leur probabilité ;

2. le *calcul d'impact des correctifs*, ayant pour visée de déterminer l'impact de chaque correctif envisagé, une fois déployé au sein du système ;
3. le *calcul d'impact du déploiement des correctifs* : il s'agit ici de déterminer l'impact de l'opération de déploiement de chaque correctif sur le système.

Connaître ces impacts se révèle donc essentiel [1]. Les cinq tâches de ce processus sont nécessaires à la phase de *décision*, où le choix des correctifs et la planification de leur déploiement sont arrêtés. p Trois problématiques principales se révèlent à l'analyse de ce processus : la *collecte d'informations* et leur analyse sont le préalable indispensable au processus ; les *calculs d'impact et de risque* associés aux vulnérabilités et correctifs sont au cœur de nos travaux ; enfin, la *représentation du système* est une problématique transverse et critique, nécessaire à chaque étape du processus de gestion de correctifs.

Nous avons choisi pour le moment de nous concentrer sur les calculs d'impact et de risque et la représentation du système.

3 Fédération de modèles et calcul d'impact

Une représentation suffisamment complète du système est nécessaire. Sa taille en fait toutefois un problème non trivial : *comment modéliser un système de cette ampleur ?* Notre démarche doit s'appuyer sur l'acquisition de connaissances aussi complètes que possible des différentes facettes du système étudié. En effet, s'il est certain qu'une unique représentation ne peut pas rendre compte de la complexité d'un système naval, de nombreux modèles peuvent être établis et utilisés, chacun représentant un aspect différent. Par exemple, une décomposition systémique ou la description d'un processus ne contiendra pas les mêmes informations qu'un plan du bâtiment ou qu'un règlement intérieur, mais viendra les compléter. Ces modèles peuvent être obtenus par l'étude de systèmes existants, en s'appuyant sur l'expertise des acteurs impliqués dans la conception, la réalisation et l'opération des systèmes navals. Mais, du fait de la forte diversité de navires, constructeurs, cadres d'emploi, missions, ..., la nature de ces modèles est variable d'un système à l'autre. Un second problème se pose alors : *comment établir une méthode de représentation adaptable à des systèmes aussi divers ?*

Pour répondre à ces deux problématiques, notre angle d'approche est la *fédération de modèles* [8]. La fédération de modèles lie les différentes abstractions de l'objet modélisé, et s'adapte à chaque système : elle établit un méta-modèle [2] ≪sur-mesure≫ de chaque bâtiment en fonction des modèles disponibles et n'a donc pas pour but d'analyser tous les navires suivant un ensemble prédéfini de modèles.

Cette modélisation sert notamment la tâche centrale du processus de gestion des correctifs : les calculs de risque et d'impact. Une vulnérabilité ou un correctif affectant un (ou plusieurs) composant(s) du système, nous souhaitons déduire de notre fédération de modèles la dépendance composants / missions [3]. [13] propose une méthode d'estimation de l'impact d'une attaque sur une mission, en s'appuyant entre autres sur un graphe de dépendance représentant les

1. Dans l'état actuel de nos recherches, nous nous concentrons sur les impacts sur la sûreté de fonctionnement du système. Nous verrons en partie 4 comment ils peuvent être calculés à partir des modèles.
2. Méta-modèle signifie ici "ensemble des modèles fédérés". Ce méta-modèle n'est pas calculé : il ne s'agit pas de fusionner les modèles disponibles en une seule représentation. Chacun des modèles fédérés reste exprimé dans son formalisme d'origine.
3. Nous pouvons déduire de la fédération de modèles d'autres informations qui peuvent servir au calcul d'impact. La dépendance mission / composant est le seul aspect évoqué dans cet article.

liens mission / tâche [4] / composant. [4, 3, 6] analysent des navires militaires suivant le méta-modèle *Abstraction Hierarchy* de Jens Rasmussen, servant à lier les missions du système à ses composants à travers cinq niveaux d'abstraction croissante (composants, trois niveaux de fonctions et de processus, missions). La fédération des modèles disponibles peut donc aboutir à ce type d'abstraction qui permet d'exprimer les dépendances nécessaires aux calculs de risque et d'impact. Elle permet aussi de spécifier les propriétés de sûreté de fonctionnement du système, qui sont nécessaires au type de mesure d'impact présenté dans la partie suivante.

4 Calcul d'impact et automates temporisés

Pour exprimer un impact en termes de *sûreté de fonctionnement*, nous devons modéliser le *comportement* du système et ses *missions*, ce qui peut être fait grâce aux automates temporisés[2]. En effet, une mission peut être vue comme un enchaînement d'états ; par exemple, pour un navire de mesures océanographiques : *navire à quai* $\rightarrow_1$ *en transit vers zone* $\rightarrow_2$ *campagne de mesures* $\rightarrow_3$ *en transit vers port* $\rightarrow_4$ *mission achevée*. De même, le fonctionnement des sous-systèmes composant le bâtiment peut être modélisé par un ensemble d'automates. Ces automates, qui sont eux-mêmes des modèles comportementaux du système, sont constuits à partir de la fédération de modèles.

La dépendance composants / missions peut être illustrée grâce à cette représentation. Par exemple, nous pouvons construire nos automates pour qu'ils vérifient la propriété suivante : la transition $\rightarrow_1$ ne peut être tirée que si l'automate modélisant le comportement de la propulsion du bâtiment atteint un ensemble d'états indiquant que ce sous-système est : en fonctionnement, en mesure de recevoir les consignes des opérateurs, et en mesure d'exécuter ces consignes.

Notre objectif est donc de modéliser le système sous la forme de deux ensembles d'automates : les *automates système*, représentant le comportement des composants du navire, et les *automates mission*, représentant le déroulement des missions. La dépendance entre ces deux ensembles est exprimée par le lien entre les *automates système* et les *automates mission*. Nous ajoutons également une temporisation à nos automates, pour modéliser les délais de fonctionnement des sous-systèmes.

Dans son état de fonctionnement nominal, le système permet l'exécution des missions. Cela implique, au niveau des traces d'exécution des automates, la vérification de certaines propriétés : par exemple, *l'automate système* A *peut atteindre l'état* s *en un temps* t, ou *l'automate mission* M *peut atteindre l'état* mission achevée. Un correctif, ou une attaque issue de l'exploitation d'une vulnérabilité, peut mener à une modification du comportement du système. Nous pouvons donc représenter cette transformation par une ≪mutation≫ des automates système. Cette mutation peut être un ensemble d'ajouts/suppressions d'états et transitions, ou la modification des horloges (pour représenter une modification des temps de fonctionnement d'un composant donné). Nous vérifions ensuite ces propriétés sur les traces d'exécution des automates ≪mutés≫. Une mesure d'impact peut être déduite de cette vérification : par exemple, une mesure ≪simpliste≫ serait de considérer le nombre de propriétés qui ne sont plus satisfaites.

Conclusion

La gestion des correctifs de sécurité est un enjeu majeur des navires modernes. Ces navires sont des systèmes complexes, constitués de composants de nature diverse. De tels composants

4. Une mission est vue comme un ensemble de tâches.

peuvent être affectés par des vulnérabilités, qui sont tempérées par des correctifs. Or, les correctifs comme les vulnérabilités ont des impacts sur les missions du navire : un processus de gestion de correctifs doit permettre de comparer leurs conséquences, pour faire le choix qui aura un impact minimal sur les missions du bâtiment. Ce processus s'appuie sur une représentation – aussi complète que possible – du système, obtenue par fédération de modèles, et sur des calculs de risque et d'impact. L'analyse de traces d'exécution d'automates temporisés nous permet d'obtenir une mesure d'impacts sur la *sûreté de fonctionnement* du système naval. Ce ne sont toutefois pas les seuls impacts possibles liés à une vulnérabilité ou à un correctif : la suite de nos travaux s'attachera à envisager des modes de calcul intégrant ces autres aspects.

Références

[1] A. Abou El Kalam. *Security of critical infrastructures and Networks.* Habilitation à diriger les recherches, Institut National Polytechnique de Toulouse - INPT, December 2009.

[2] G. Behrmann, K. G. Larsen, O. Moller, A. David, P. Pettersson, and W. Yi. Uppaal - present and future. In *Decision and Control, 2001. Proceedings of the 40th IEEE Conference on*, volume 3, pages 2881–2886 vol.3, 2001.

[3] A. M. Bisantz, C. M. Burns, and E. Roth. Validating methods in cognitive engineering: A comparison of two work domain models. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 46(3):521–525, 2002.

[4] A. M. Bisantz, E. Roth, B. Brickman, L. L. Gosbee, L. Hettinger, and J. McKinney. Integrating cognitive analyses into a large scale system design process. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 45(4):434–438, 2001.

[5] B. Brykczynski and R. A. Small. Reducing internet-based intrusions: Effective security patch management. *IEEE Software*, 20(1):50–57, Janvier 2003.

[6] C. M. Burns, D. J. Bryant, and B. A. Chalmers. Boundary, purpose, and values in work-domain models: Models of naval command and control. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 35(5):603–616, Sept 2005.

[7] C.-W. Chang, D.-R. Tsai, and J.-M. Tsai. A cross-site patch management model and architecture design for large scale heterogeneous environment. In *Security Technology, 2005. CCST '05. 39th Annual 2005 International Carnahan Conference on*, pages 41–46, Octobre 2005.

[8] C. Guychard, S. Guerin, A. Koudri, F. Dagnat, and A. Beugnard. Conceptual interoperability through Models Federation. In *Semantic Information Federation Community Workshop*, 2013.

[9] L. M. Jaworski. Tandem threat scenarios : a risk assessment approach. In *16th National Computer Security Conference : Proceedings*, pages 155–164, 1993.

[10] Department of Defense. *Department of Defense Handbook : System Security Engineering – Program Management Requirements, MIL-HDBK-1785.* 1995.

[11] US Department of Homeland Security / National Cyber Security Division / Control Systems Security Program. *Recommended Practice for Patch Management of Control Systems.* Décembre 2008.

[12] J.-T. Seo, D.-S. Choi, E.-K. Park, T.-S. Shon, and J. Moon. Patch management system for multiplatform environment. In *Parallel and Distributed Computing: Applications and Technologies: 5th International Conference, PDCAT 2004, Singapore, December 8-10, 2004. Proceedings*, pages 654–661, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[13] X. Sun, A. Singhal, and P. Liu. Who touched my mission: Towards probabilistic mission impact assessment. In *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense*, SafeConfig '15, pages 21–26, New York, NY, USA, 2015. ACM.