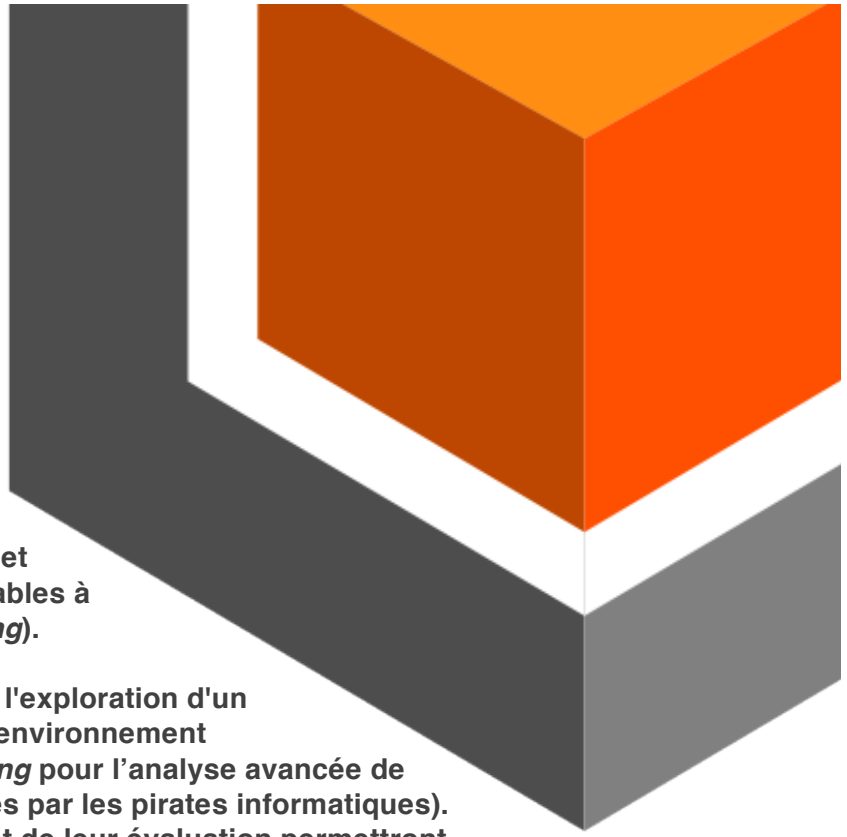
TETRANE – SECURITE ET FIABILITE DES OBJETS ET INFRASTRUCTURES NUMERIQUES SENSIBLES



En bref…

TETRANE apporte une réponse technologique innovante à la forte croissance des attaques informatiques ciblées et sophistiquées exploitant des failles logicielles. La technologie REVEN® (*REVerse ENgine*) conçue et développée par TETRANE depuis 2011, analyse les logiciels dans leur format exécutable, sans accès aux codes sources, et permet la détection et l'analyse de vulnérabilités logicielles dans des conditions semblables à celles des pirates informatiques, par rétro-conception du logiciel (ou *reverse-engineering*).

La technologie REVEN® est à l'informatique ce que l'IRM est à la médecine. Elle permet l'exploration d'un logiciel du processeur aux couches applicatives, de manière non intrusive et dans son environnement d'exécution. REVEN-Axion est aujourd'hui utilisée par des experts en *reverse-engineering* pour l'analyse avancée de code malveillant ou la compréhension de bugs techniques complexes (bugs exploitables par les pirates informatiques). Les prochains développements autour de la recherche automatisée des vulnérabilités et de leur évaluation permettront d'étendre l'usage des solutions de TETRANE aux éditeurs de logiciels, certificateurs ou conseils en sécurité.

Contexte

La multiplication des données échangées et stockées, la mobilité, l'Internet des Objets comme l'informatisation des systèmes critiques offrent un terrain de jeu de plus en plus grand aux cyber pirates. Les menaces sont désormais plus complexes et globalisées, les attaques sophistiquées et ciblées, entraînant des pertes financières considérables pour les entreprises ou administrations victimes.

L'enjeu pour les entreprises est de déterminer le bon équilibre entre sécurité, disponibilité de leur infrastructure et besoin utilisateur.

Les systèmes et produits de sécurité des systèmes d'information actuels, quoique indispensables, ne sont plus suffisants pour assurer un niveau satisfaisant de sécurité, pourtant nécessaire à l'adoption et l'usage des nouvelles technologies numériques.

Fort de ce constat, TETRANE travaille depuis plus de 4 ans à la mise au point d'une solution anticipative de la menace des attaques informatiques. Plutôt que de chercher à détecter les attaques dans les flux d'information, TETRANE cherche à identifier les vulnérabilités logicielles ciblées par les attaquants, dans des conditions semblables à celles des attaquants.

Qui sommes-nous ?

Créée en février 2011, TETRANE conçoit et développe des solutions de sécurité et fiabilité des logiciels sensibles par l'automatisation de la démarche de *reverse engineering* (retro conception des logiciels).
TETRANE compte actuellement 8 collaborateurs dont 7 ingénieurs en sécurité et développement logiciel.
TETRANE a reçu le prix spécial du Jury du Forum International de Cybersécurité 2015 (FIC 2015) pour sa technologie REVEN® et son produit REVEN-Axion.

Pourquoi la rétro conception du logiciel ?

Dans les milieux industriels, la rétro conception permet de comprendre et analyser un produit ou objet à partir de son état finalisé – sans accès aux informations de conception – afin d'en connaître ses propriétés, faiblesses ou spécificités techniques.
La rétro conception, appelée « *reverse* » dans le monde du logiciel, permet l'étude d'un logiciel sans avoir accès au code source.
Les plans d'un avion par exemple, comme le code source d'un logiciel, sont rarement disponibles car protégés pour des raisons évidentes de propriété intellectuelle ou de sécurité ; le code source des virus ou autres *malwares* n'est naturellement pas disponible non plus, pour d'autres raisons…

En réalisant le *reverse* d'un logiciel, l'expert en sécurité choisit de travailler sur le logiciel tel qu'il est exécuté sur une machine et non tel qu'il est « voulu » par le développeur lorsqu'il écrit le code source.
Entre ces deux états (code source / code exécutable), le logiciel est par ailleurs transformé par la compilation. Des failles invisibles dans le code source peuvent exister dans le logiciel « finalisé ».
Le *reverse* est La « méthode de travail » des meilleurs pirates informatiques pour trouver une vulnérabilité dans un logiciel afin de l'exploiter. En développant la technologie REVEN®, TETRANE automatise cette démarche manuelle afin de donner à ses clients la possibilité d'anticiper la démarche et la menace des hackers malveillants.

La technologie REVEN®

La technologie REVEN® permet l'accès et l'analyse des données d'exécution relatives à l'activité du processeur, de la mémoire et de l'ensemble des couches logicielles et matérielles nécessaires au fonctionnement d'un programme. Au-delà de l'automatisation de cette démarche traditionnellement effectuée à la main, REVEN® permet de « descendre » dans les couches d'un logiciel à un niveau inégalé aujourd'hui. Plus une vulnérabilité est proche du processeur, plus elle est difficile à détecter/corriger et plus elle est critique et dangereuse.

La technologie REVEN® s'appuie sur une innovation de rupture : la simulation symbolique du processeur physique. En exécutant tout ou partie d'un logiciel sur le processeur REVEN®, il est possible de « lire » et comprendre chaque octet manipulé, ses interactions avec le matériel, etc.
En développant ce processeur de manière « symbolique », TETRANE remplace des données numériques (1, 2, 3, etc.) par des symboles (x, y, z, etc.) et étend la couverture de son analyse.

L'équipe TETRANE a développé de nombreux algorithmes de haut niveau permettant la manipulation et l'interprétation des données. Les développements actuels ont pour objectif de poursuivre le niveau d'automatisation et d'interprétation de la technologie REVEN®.
L'analyse des binaires (0 et 1) permet l'analyse de n'importe quel logiciel fonctionnant sur un processeur, quelque soit son langage de programmation.

Actuellement, la technologie REVEN® peut analyser des logiciels fonctionnant dans des environnements Windows et Linux 32bit, les travaux en cours ont pour objectif d'étendre la couverture d'analyse au 64bit et aux environnements embarqués (Smartphones, domotique, etc.) tels que l'architecture ARM.

Le produit REVEN-Axion

La solution REVEN-Axion est le tableau de bord du moteur REVEN® dédié aux experts en *Reverse Engineering*. Interface de manipulation des données analysées et interprétées, il donne accès à l'analyse dynamique d'un logiciel.
Les premiers retours d'utilisateurs rapportent un temps d'analyse divisé par 8 par rapport à une démarche traditionnelle. Ce ratio ne cesse de croître au fur et à mesure des développements, laissant ainsi à l'utilisateur plus de temps à consacrer pour des tâches à forte valeur ajoutée : compréhension et remédiation d'un bug, évaluation du niveau de risque d'une faille, etc.

Caractéristique rare dans le monde des produits d'analyse de logiciels, REVEN-Axion est collaboratif. Plusieurs ingénieurs peuvent travailler simultanément et de manière coopérative sur un même projet, partageant ainsi leurs analyses, commentaires ou résultats.

Bénéfices utilisateurs et perspectives

Aujourd'hui utilisée par les experts du milieu de la Défense et d'entreprises reconnues en sécurité avancée des logiciels, la solution REVEN-Axion de TETRANE permet un gain de temps plus que significatif dans la compréhension d'un logiciel, l'analyse avancée de *malwares* ou la remédiation de bugs complexes. La profondeur d'analyse inégalée aujourd'hui est un atout considérable pour anticiper la démarche d'acteurs malveillants en identifiant avant eux les vulnérabilités potentielles d'un logiciel.

Dès les travaux relatifs à la couverture d'analyse terminés, TETRANE débutera le développement de REVEN-Impact qui assistera les éditeurs dans le développement de logiciels fiables et sécurisés. En analysant à tout moment du cycle de vie du logiciel, tout ou partie du code compilé, un développeur pourra identifier des bugs et les lier aux parties de codes sources correspondantes. Plus un bug est identifié tôt, moins sa remédiation est coûteuse. Ainsi, il pourra étendre les travaux d'assurance qualité à l'ensemble du logiciel développé en intégrant les dépendances (parties d'un logiciel développées par une entité tierce) et l'environnement d'exécution. Par ailleurs, le gain de temps dans la réalisation des travaux d'assurance qualité se traduit par une réduction des coûts de production du logiciel.

Contact

tetrane.com
+33 (0)3 39 25 00 45
contact@tetrane.com

TETRANE