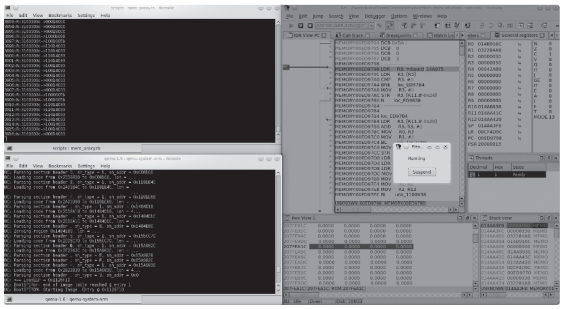
Méthodes d'émulations de systèmes embarqués inconnus

Domaine spécialisé: Sécurité Informatique
Chargé: Prof. Dr. Endre Bangerter
Expert: Prof. Dr. Pascal Junod

De nos jours, les systèmes embarqués font partie intégrante de la vie quotidienne. Nous ne savons par contre pas comment ils sont conçus, ni s'ils contiennent des failles de sécurité que l'on pourrait exploiter ou qui le sont déjà. Cette thèse décrit les méthodes permettant de développer un émulateur pour un système embarquée défini afin de faciliter l'analyse du firmware.

Contrairement aux ordinateurs personnels pour lesquels il existe une multitude d'outils permettant la recherche de vulnérabilités, les systèmes embarqués n'en n'ont que peu: la recherche se fait par analyse statique du firmware ou par l'utilisation d'un port de débogage hardware.

La technique proposée par cette thèse est d'émuler le système afin d'offrir toutes les possibilités qu'offre un ordinateur personnel en matière de recherche de vulnérabilités. En effet, l'émulation de systèmes embarqués permet une analyse dynamique du code et un contrôle total sur le système, ce qui simplifie la recherche de vulnérabilités.



Emulation et outils d'analyses

Nous décrivons dans cette thèse des méthodes d'analyses permettant d'émuler un système embarqué sans connaissance préalable et appliquons ces méthodes sur un système embarqué défini. Ces méthodes sont un mélange d'analyse statique et dynamique du firmware tout en observant les accès mémoire effectués entre le firmware et les périphériques, afin de comprendre le fonctionnement du système pour pouvoir implémenter un émulateur capable de faire fonctionner le firmware de la même manière que le système originel. Il n'est pas possible de connaitre le fonctionnement exact de tous les composants du système embarqué, mais nous simulons leur fonctionnement donnant au firmware les valeurs attendues. Nous obtenons ainsi un émulateur capable de faire fonctionner le firmware mais n'offrant pas toute les fonctionnalités disponibles du système réel, en raison de certains périphériques complexes dont le fonctionnement logique n'a pu être découvert à ce jour.

Boris Matti
matti_boris@yahoo.fr