Projet Vasoc

LIMOS – Université d'Auvergne

19/10/2018

S. Salva

OdJ

- Visite locaux Lab. Hubert Curien
- Bilan 1A Lab. LIMOS et perspectives
- Stages, projets ?
- Intégration Lab. Hubert Curien sur la 2A (besoins ?)
- Etude de cas, état des lieux (matériel, traces ?)

Bilan Limos

Audit / pentest

- Etapes générales
  - Audit: http://www.isefc.rnu.tn/downloads/Audit.pdf
  - Audit: https://www.bluekrypt.com/fr/audit-de-securite
  - pentesting *http://www.penteststandard.org/index.php/Main_Page*

  - Collecte d'information (audit de site, physique, technique)
  - MDL menace (suivant informations + bases CVE, CWE, CAPEC, etc.)
  - Exploitation (tests, pentest, tools, etc.)
  - Post-exploitation et résultats

Audit

- Besoin de matériel/réseaux/ passerelles/cloud auditables ?

  - Non auditable
  - -> messages, firmware chiffrés,
  - Déduction du traffic (ex:outil iotscanner), adresses, localité, nb entités
  - Résultats Limités (ex: traces Xiaomi fournies par Ageatis)

  - Auditable
  - Tout est déchiffré, besoin d'expertise suffisante pour formatage des données
  - Niveau d'accès : réseau, LOG, Debug, Code
  - -> mode auditable =>analyse plus approfondies, doit être prévu et limité dans le temps

Bilan

- Collecte d'information (mode auditable)
- 2 outils disponibles
  - Trace analyser -> formatage par regex, séparation en traces (temps, paramètres) et agrégation de messages
  - CONFECT générateur de mdls
- 3 publis

- Outil Confect : nécessite expertise métier importante sur les systèmes analysés

Perspectives

- Confect V2 (décembre)
  - Recherche d'identifiants de façon supervisées et séparation des composants (comportement) par ID
  - Plus simple, plus rapide

- Moyen terme : Collecte de données
  - Accès au code: intégration de nouvelles données ? Exploration par l'utilisation de l'outil SONARQUBE (données qualité et détection vulnérabilité)
  - Prise en compte mode DEBUG (appel fct), -> mdl plus complets, pl. Niveaux d'abstraction

Perspectives

- Moyen terme : analyse des MDL, rapports
  - Détection pb privacy, authentication via outil Tamarin depuis MDLs (étude en cours)
    - Génération de MDLs tamarins
    - Supervision par tag
  - Extraction auto d'information depuis MDL
  - Auditability (mode auditable et non auditable, différences entre les 2 ?), testability, privacy (envoi information vers ext.), entités,
- Autre ?
  - Gen. De Shield pour device ? Pour passerelles ?
  - Gen. De mdl de menaces, Gen. De squelettes de test , décomposition de MDL par protocoles ? Proposition d'outils de pentesting, configuration partielle de ces outils ?

Stages / projets

- Actuellement, un stagiaire licence (expériementations, Collecte de donnée avec Accès code source)

- Projets licence, DUT, ing. ?
- Stages Master?

- Le projet peut financer un stage
- Sujet ?

Intégration Lab. Hubert Curien sur la 2A (besoins ?)

Etude de cas, état des lieux (matériel, traces ?)

- Exploitation étude de cas sur esp8266
- Etude de cas proposée par Ageatis
- Plot ? Matériel ?
- ! Microsoft -> https://archive.codeplex.com/?p=labofthings
- ! IOT-lab

Industriels ?

- Qu'attendez vous du projet ?

- Transfert de savoir ?
  - Bases ? (CVE ? Etc.) méthodologie ?
- Etude / travail commun ? (stages ?)
- Outils ?