L'AUDIT DE SÉCURITÉ

Pour quels objectifs et par quels procédés ? Retour d'expérience.

Damien Cauquil

1er octobre 2018

digital.security

QUI SUIS-JE ?

- Responsable Recherche & Développement chez **digital.security** ;
- Chercheur en sécurité senior ;
- **Hardware Hacker** (et non pirate).

POURQUOI AUDITER ?

POURQUOI AUDITER ?

Plusieurs objectifs :

- **Connaître la situation réelle** et pouvoir la comparer à celle supposée ;

POURQUOI AUDITER ?

Plusieurs objectifs :

- **Connaître la situation réelle** et pouvoir la comparer à celle supposée ;
- Déterminer le **niveau de risque** ;

POURQUOI AUDITER ?

Plusieurs objectifs :

- **Connaître la situation réelle** et pouvoir la comparer à celle supposée ;
- Déterminer le **niveau de risque** ;
- **Éprouver les capacités** de détection, de réaction face à une menace.

CONNAÎTRE LA SITUATION RÉELLE

Il est important de savoir si **la vision** que l'on a correspond à la réalité :

- **Tout évolue** et certains changements peuvent avoir des conséquences non-anticipées ;

CONNAÎTRE LA SITUATION RÉELLE

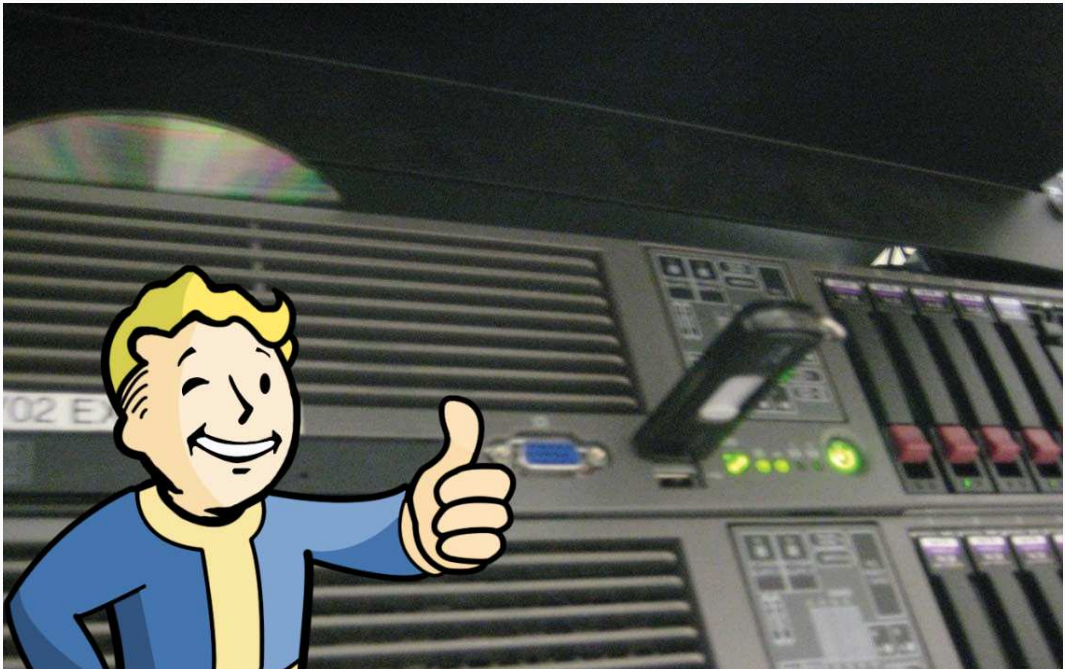
Il est important de savoir si **la vision** que l'on a correspond à la réalité :

- **Tout évolue** et certains changements peuvent avoir des conséquences non-anticipées ;
- Certaines tâches sont confiées à des **personnes ou organismes tiers qui assurent respecter les bonnes pratiques** (sans certitude) ;

CONNAÎTRE LA SITUATION RÉELLE

Il est important de savoir si **la vision** que l'on a correspond à la réalité :

- **Tout évolue** et certains changements peuvent avoir des conséquences non-anticipées ;
- Certaines tâches sont confiées à des **personnes ou organismes tiers qui assurent respecter les bonnes pratiques** (sans certitude) ;
- Des **évènements imprévus** peuvent avoir affecté la sécurité de l'ensemble.



Il s'agit notamment de répondre aux questions suivantes :

- Quelles sont le ou les **pires scénarios** qui puissent se produire ?
- Quelle est la **probabilité de réalisation** de chacun d'eux **selon les menaces et les vulnérabilités présentes** ?
- **Que va-t-on perdre** si ceux-ci se réalisent ?

Éprouver les capacités de détection et la réaction face à une menace

Il peut aussi s'agir d'évaluer :

- La **capacité** des équipes en charge de la sécurité **à détecter et réagir** à une ou plusieurs menaces ;
- **Le respect des consignes** de sécurité et des bonnes pratiques ;
- **L'adéquation des procédés et mécanismes de contrôle** de la sécurité face aux menaces actuelles.


PLEASE
CLOSE
GATE

A CHAQUE SITUATION SON AUDIT

Différents types d'audits pour différentes situations

Il existe une grande variété de types d'audit :

- Analyse et cartographie des risques ;
- Audit de configuration ;
- Test d'intrusion ;
- Détermination des points de présence sur Internet ;
- Test de réseau WiFi ;
- Test de systèmes connectés ;
- Campagne d'hammeçonnage ;
- Test Red Team ;
- etc...

AINSI QUE DIFFÉRENTS CONTEXTES DE RÉALISATION

- Différents **niveaux de connaissance** de la cible par l'attaquant (boîte blanche/grise/noire);
- **Types d'attaquants** (externe, interne);
- **Types d'actions** autorisées;

« Que souhaite-t-on vérifier ? »

Je veux savoir ce qu'il peut arriver de pire

Type de test Analyse de risque, cartographie
Contexte Connaissance complète (boîte blanche)

Avantages

- Exhaustif
- Permet de déterminer les **scénarios redoutés**

Inconvénients

- Prends du temps
- Collaboration requise

Je veux savoir ce qu'un pirate peut faire de pire

Type de test Test d'intrusion
Contexte Externe, sans information (boîte noire)

Avantages

- Donne **une bonne vision** de ce qu'un attaquant externe peut faire de pire
- Recommandations pour améliorer la sécurité

Inconvénients

- **Temps limité** contrairement à un attaquant
- **Non exhaustif**

Types de test Audit d'architecture

Contexte Connaissance complète (boîte blanche)

Avantages

- Vérification exhaustive
- Recommandations pour améliorer la sécurité

Inconvénients

- Prends du temps
- Collaboration requise

Types de test Red Team

Contexte Aucune connaissance préalable (boîte noire)

Avantages

- Vérification exhaustive
- Recommandations pour améliorer la sécurité

Inconvénients

- Prends du temps
- Collaboration requise

Types de test Audit de code

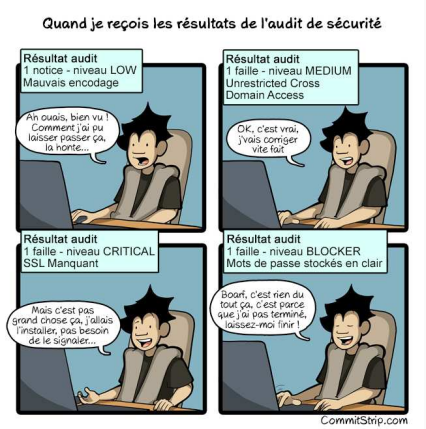
Contexte Connaissance complète (boîte blanche)

Avantages

- Vérification exhaustive
- Recommandations pour améliorer la sécurité

Inconvénients

- Prends du temps
- Collaboration requise



Audit PASSI

- Réalisé par des sociétés et auditeurs certifiés (**P**restataires d'**A**udit de la **S**écurité des **S**ystèmes d'**I**nformation)
- Déroulement encadré et conditions de réalisation strictes

Exhaustif ou non ?

- La **boîte blanche** est exhaustive ;
- Cela peut **accélérer les tests** ...
- ... ou prendre **plus de temps** car laborieux (analyse de risque) ;
- La **boîte grise est un compromis** permettant d'optimiser les tests.
- La **boîte noire** donne la vision d'un **attaquant externe**.

Etat des lieux ou vérification ?

- Le **test technique permet de vérifier** qu'un niveau de sécurité est atteint ;
- Les **audits d'architecture**, **audits de code** ou de **configuration** permettent de faire un **état des lieux**.

Comment réalise-t-on un audit ?

COMMENT RÉALISE-T-ON UN AUDIT ?

Étapes clés :

1. Plannification de l'audit ;

Étapes clés :

1. Plannification de l'audit ;
2. **Réunion de lancement ;**

Étapes clés :

1. Plannification de l'audit ;
2. Réunion de lancement ;
3. Réalisation de l'audit (tests, entretiens, etc.) ;

Étapes clés :

1. Plannification de l'audit ;
2. Réunion de lancement ;
3. Réalisation de l'audit (tests, entretiens, etc.) ;
4. Réunion de fin d'audit ;

Étapes clés :

1. Plannification de l'audit ;
2. Réunion de lancement ;
3. Réalisation de l'audit (tests, entretiens, etc.) ;
4. Réunion de fin d'audit ;
5. Restitution des livrables.

Méthodes et procédures

Les auditeurs **suivent des méthodes et des procédures** précises pour la réalisation de l'audit :

- EBIOS
- MEHARI
- Le guide de test de l'OWASP (version 4)
- Des méthodes définies en interne et partagées par l'ensemble des auditeurs et documentées dans les livrables

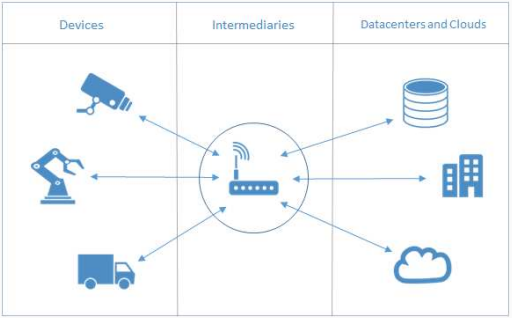
Les livrables sont des **documents de synthèse** détaillant :

- Ce qui **a été réalisé** durant l'audit ;
- Les **éléments positifs** qui ont été observés ;
- Les éléments qui sont **à améliorer** ;
- Des **recommandations** afin d'améliorer la sécurité.

CAS PARTICULIER DE L'IOT

Variétés des cibles :

- Plateformes Cloud, **serveurs applicatifs**;
- **Applications mobiles** iOS et Android;
- Applications embarquées;
- Équipements IoT spécifiques;
- **Protocoles de communication** variés (`Bluetooth Low Energy`, `WiFi`, `Zigbee`, `LoRaWAN`, `Sigfox`, etc.).



Audits matériels

- Nécessité d'avoir **au moins deux exemplaires** (destruction possible);
- **Temps d'analyse supérieur** à un audit technique classique
- **Attaques physiques** à envisager (électroniques et mécaniques)

Compétences différentes

- **Maîtrise de l'électronique**, des procédés de fabrication, des technologies;
- Mise en œuvre d'**attaques avancées** (contournement de protection, etc.);
- Rétro-ingénierie de **systèmes embarqués**;
- Recherche de vulnérabilités électroniques et mécaniques;
- Maîtrise des **protocoles de communication sans-fil** et de l'analyse radio.

TOP 10 DES ERREURS

Une **serrure connectée du marché**, 300 000 exemplaires déjà en magasin.

- L'application mobile demande une authentification pour récupérer le journal des ouvertures/fermetures ...

Une **serrure connectée du marché**, 300 000 exemplaires déjà en magasin.

- L'application mobile demande une authentification pour récupérer le journal des ouvertures/fermetures ...
- ... mais la serrure elle **n'en demande pas quand on communique directement** avec elle.

N°9 : FAIBLESSES MÉCANIQUES

N°9 : FAIBLESSES MÉCANIQUES

N°8 : ERREURS CRYPTOGRAPHIQUES

Default Trust Center Link Key

0x5A 0x69 0x67 0x42 0x65 0x65 0x41 0x6C 0x6C 0x69 0x61 0x6E 0x63 0x65 0x30 0x39

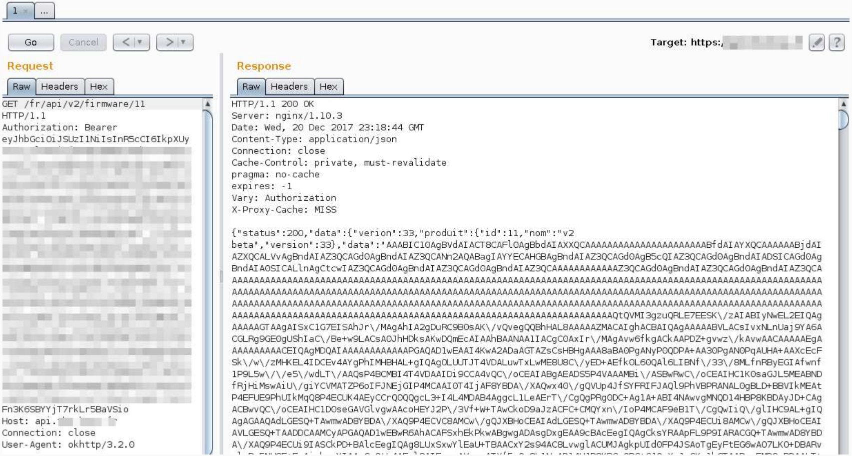
"ZigbeeAlliance09"

Note: The Link Key is listed in little-endian format.

Use Insecure Join

0x01 (True). This flag enables the use of insecure join as a fallback case at startup time.

N°6 : Mises-à-jour non-sécurisées

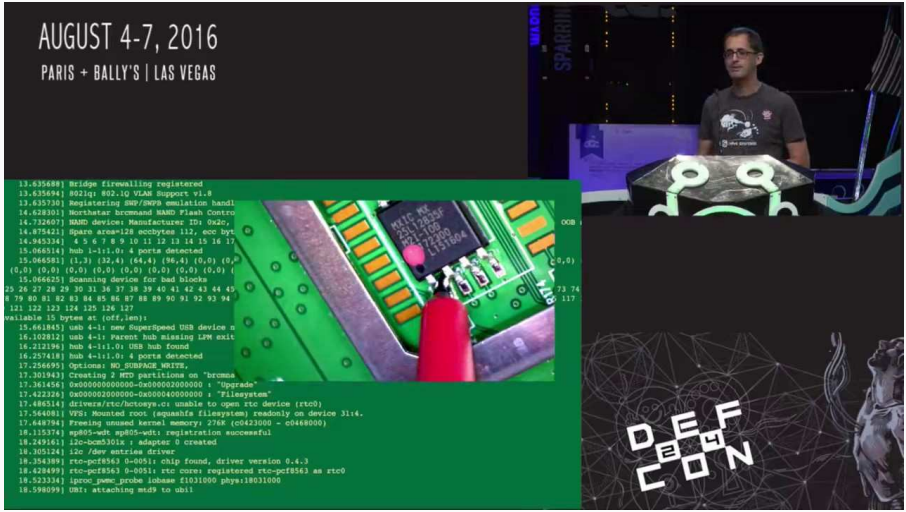


N°5 : MAUVAISE CONCEPTION ÉLECTRONIQUE

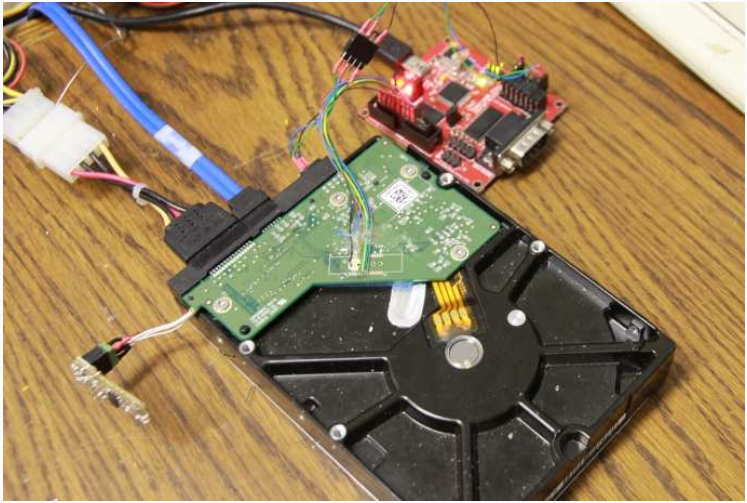
N°4 : MAUVAISE UTILISATION DE PROTOCOLES

N°3 : FUITES D'INFORMATION

N°2 : ABSENCE D'AUTHENTIFICATION



N°1 : INTERFACES DE DÉBOGAGE



Questions ?

Contact :

- @virtualabs
- damien.cauquil@digital.security