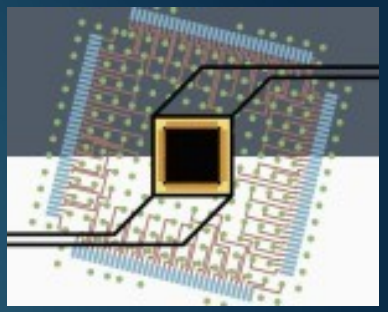
# IDRIX

## Cryptography and IT Security Experts



10/5/2016

Mounir IDRASSI

# Mounir IDRASSI

**Fondateur IDRIX / Consultant indépendant**

## Parcours Personnel

- Diplomé de l'Ecole Polytechnique (promotion X97)
- Ingénieur cryptographie chez Oberthur Card Systems entre 2000 et 2006

## IDRIX

- Project de création avec d'anciens collègues d'Oberthur
  - Cible: OS carte à puce et middleware
  - Recentrage sur middleware et développement d'applicatifs associés

# IDRIX aujourd'hui

| | |
|---|---|
| Forme juridique | SARL unipersonnelle |
| Siège | 7 rue de Civry, 75016 PARIS |
| Capital | 7,500 € |
| Chiffre d'affaire | ~200K € |
| Clients | Gemalto, Oberthur Technologies, Morpho |

# Axes d'activité d'IDRIX

## Sous-traitance

- Intervention sur divers projets autour de la carte à puce
- Solutions innovantes pour des problématiques d'authentification forte

## Conseil

- Missions de conseils chez divers fournisseurs de solutions PKI et cartes à puce
- Expertise en middleware (PKCS#11, CSP, minidriver) et développement JavaCard

# Produits et solutions

- Cryptoki Manager
  - Outil de référence pour la validation et le test de module PKCS#11 carte à puce
- Card Processor
  - Outil de script pour carte à puce
- ScardSpy
  - Module d'interception des échanges APDU entre applications et cartes à puce
- StoreExplorerPlus
  - Visualisation certificate store et extraction clef privée même non-exportable

# Open Source

- SCard4Wine : http://sourceforge.net/projects/scard4wine/
  - Implémentation Winscard.dll pour WINE
- CertRequestor : https://certrequestor.codeplex.com/
  - Requête de certificat avec CertEnroll
- VeraCrypt : https://veracrypt.codeplex.com/
  - Fork de TrueCrypt avec amélioration de la sécurité
- RSA Converter : http://sourceforge.net/projects/rsaconverter/
  - Factorisation rapide de clef RSA au format SFM
- SimCardManager : http://sourceforge.net/projects/simcardmanager/
  - Lecture information et données sur carte SIM

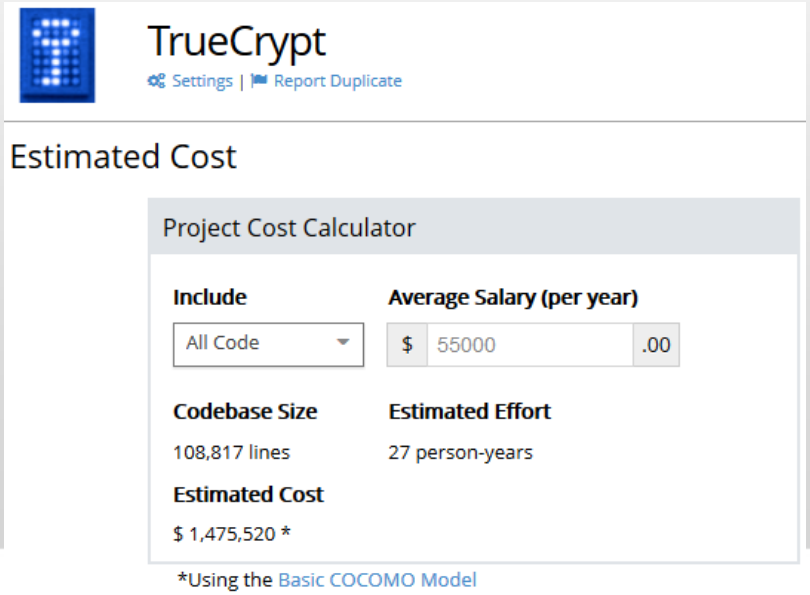
# VeraCrypt

- Analyse code source TrueCrypt en 2012
  - Aucune backdoor détectée.
  - Version personalisée pour besoin interne.

- Renforcement dérivation de clef et publication VeraCrypt le 22 Juin 2013
  - 17 jours après les révélations Snowden
  - Besoin d'un projet ouvert transparent et non anonyme
  - Construire une communauté open source
  - Harmonisation code source Linux/OSX/Windows
  - Simplification système de build

# VeraCrypt

- Mystérieux arrêt du projet TrueCrypt en Avril 2014
  - Développement arrêté depuis Mars 2012
  - Coincidence avec l'affaire Paul Le Roux et lien avec autoritées US
  - Explication source de financement
  - https://mastermind.atavist.com/he-always-had-a-dark-side
  -



# VeraCrypt

- Evolution VeraCrypt
  - ✓ De 300 t/j en 2014 à 3000 t/j en 2016
  - ✓ Static Code Analysis: Plusieurs problèmes corrigés
    - ✓ Klocwork, HP Fortify, Coverity
  - ✓ Résolution vulnérabilités
    - ◆(CVE-2015-7358 CVE-2015-7359 CVE-2016-1281)
  - ✓ SHA-2 pour chiffrement partition système
  - ✓ Support GPT et UEFI (Mai 2016)
  - ✓ Niveau sécurité dynamique (PIM)
  - ✓ Support mot de passe Unicode
  - ✓ Détection variante attaque “Evil Maid”

# VeraCrypt

- Roadmap
  - ✓ Finalisation boot UEFI
  - ✓ Montage volume par PKI carte à puce
  - ✓ Boot UEFI par carte à puce
  - ✓ Modularisation algorithme cryptographique
  - ✓ Modernisation code Linux et OSX
  - ✓
- Equipe dévelopment
  - Actuellement unique développeur
  - Plusieurs contributions externe mais non régulières
  - Manque d'experts technique Windows souhaitant contribuer
  - OSSIR peut aider sur ce point?

# VeraCrypt

- Financement
  - ✓ Temps libre personnel
  - ✓ Niveau dons PayPal insuffisant
  - ✓ Contact divers organisations
- OSTIF (US): don 25K$ de DuckDuckGo pour audit VeraCrypt
  - ✓ Exploration Crowdfunding
  - ✓ Recherche sponsoring
  - ✓ Business model Open Source?

# VeraCrypt

- Controverse et légalité
  - ✓ Mauvaise image du chiffrement (Terrorisme, Criminalité...)
  - ✓ Lois Renseignement
  - ✓ Status de l'Open Source pas claire.
  - ✓ Risque de délocalisation (Suisse?)
  - ✓ OSSIR: support possible?

# Merci

https://www.idrix.fr/