Gostcrypt

Analyse de code

Alexis Lefrançois Adrien Burel

Projet de fin d'études

27/01/2017

Sommaire

Introduction

Gostcrypt

- TrueCrypt
  - Logiciel de chiffrement de données
  - Arrêt du développement. Prétexte : fin du support windows XP
  - Affirmation des développeurs que TrueCrypt est compromis
  - Recommande Bitlocker
  - Bitlocker est connu pour ses backdoors accessibles par les services de renseignements
- Gostcrypt
  - Fork de TrueCrypt d'une version non compromise

Sommaire

Solutions intégrées à l'OS

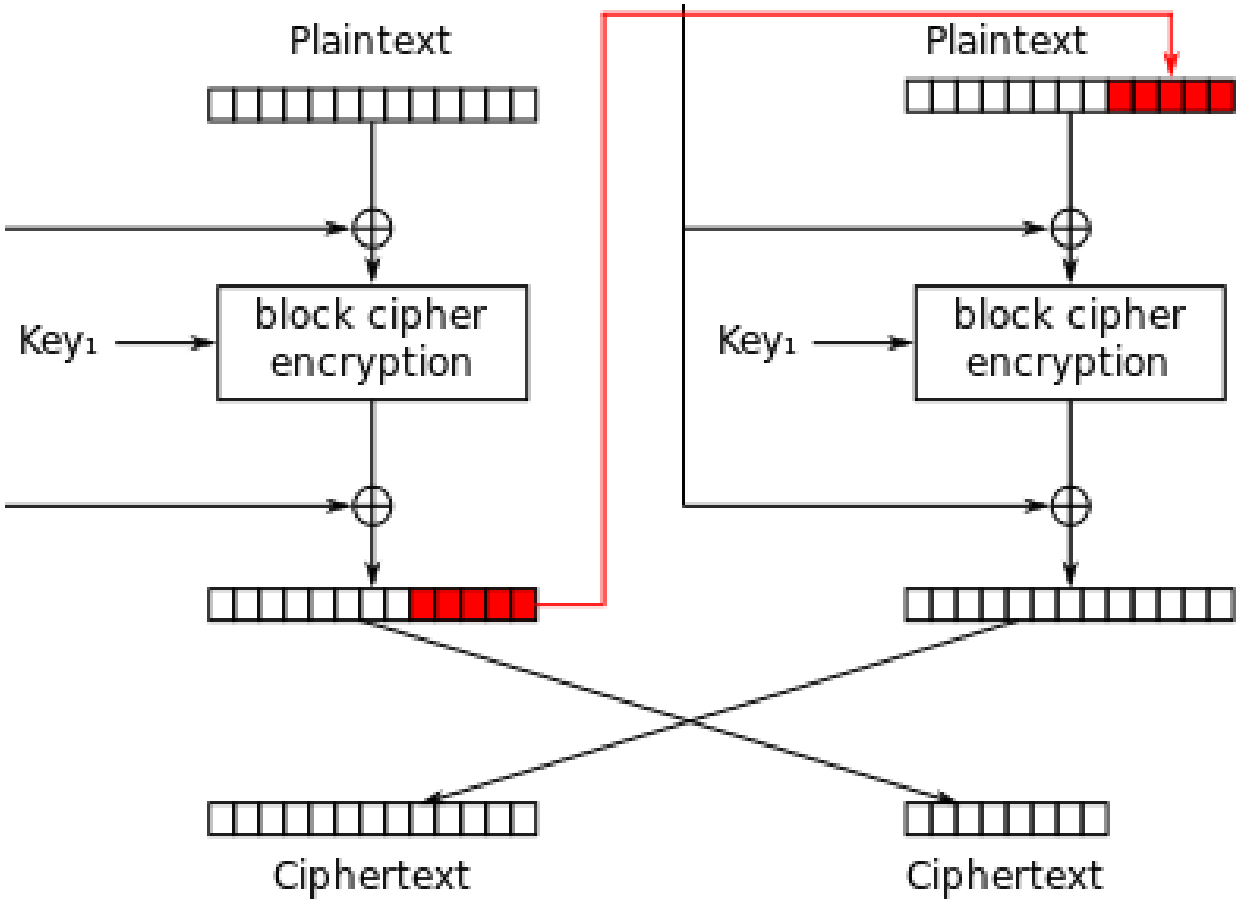
- Bitlocker (Windows)
  - Chiffrement AES-XTS AES 128-256bits
- FileVault (Apple)
  - Chiffrement AES-XTS of AES 128-256bits
  - Utilisation d'un chipset propriétaire pour le chiffrement (iOS uniquement Mai 2016)
- LUKS (Linux Unified Key Setup)
  - Chiffrement AES - Serpent - Cast5/6 - Twofish
  - Possibilité de choisir avec ou sans XTS.

Solutions intégrées à l'OS

XTS

XTS est une méthode de substitution lorsque la taille du secteur qui doit être chiffré n'est pas divisible par la taille du block de chiffrement.

Solutions intégrées à l'OS



Solutions intégrées à l'OS

Domination de AES

Ces systèmes utilisent principalement AES à part Linux. Les OS propriétaires ne permettent pas de vérifier le code de chiffrement.

Sommaire

Solutions logicielles

Autres solutions

Il existe des logiciels permettant de chiffrer de plus petites parties. Elles offrent des alternatives aux chiffrements intégrés aux OS, qui pourraient être compromis.

- Bestcrypt (Windows)
  - Chiffrement AES,Twofish et cast-128
- DiskCryptor (Windows)
  - Chiffrement AES-256,Twofish et serpent

Solutions logicielles

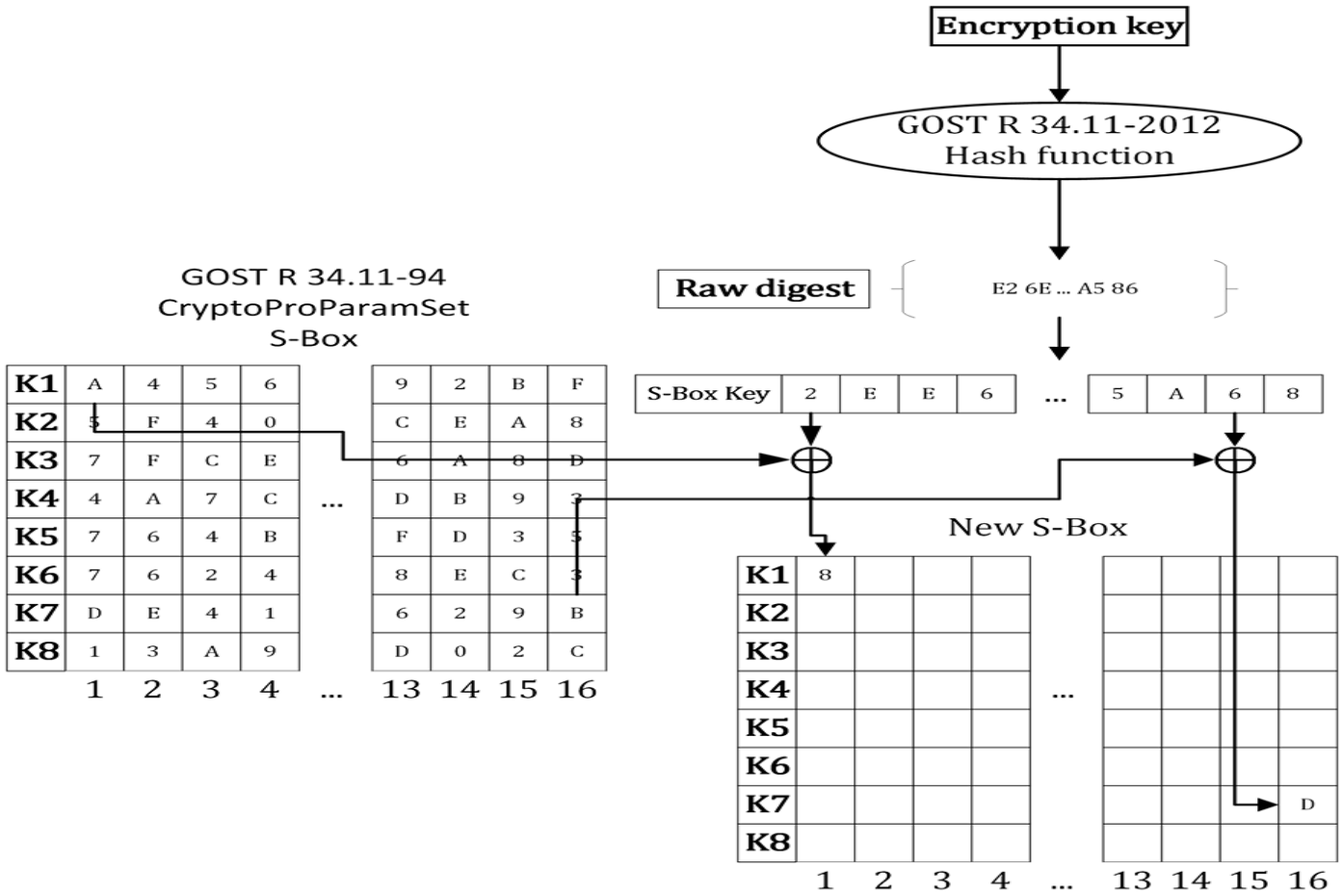
- Veracrypt
  - Chiffrement AES, Twofish, Serpent, Camellia, Kuznyechik et des combinaisons avec AES,Twofish,Serpent
- Goscrypt
  - Chiffrement Gost 28147-89,Gost Grasshopper.

Sommaire

S-BOX

S_5		Middle 4 bits of input														
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Algorithme


Encryption key
GOST R 34.11-2012
Hash function
Raw digest
E2 6E ... A5 86
GOST R 34.11-94
CryptoProParamSet
S-Box
S-Box Key
2 E E 6 ... 5 A 6 8
New S-Box
K1 A 4 5 6 ... 9 2 B F
K2 5 F 4 0 C E A 8
K3 7 F C E 6 A 8 D
K4 4 A 7 C D B 9 3
K5 7 6 4 B F D 3 5
K6 7 6 2 4 8 E C 3
K7 D E 4 1 6 2 9 B
K8 1 3 A 9 D 0 2 C
1 2 3 4 ... 13 14 15 16
K1 8
K7 D

Sommaire

Objectifs

- Comprendre Gostcrypt et faire la documentation avec doxygen
- Effacer le code inutile de l'ancien TrueCrypt
- Changer l'interface graphique pour la passer en Qt
- Faire l'analyse du code en statique et en dynamique
- Revoir l'algorithme Gost
- Ajout d'une fonctionnalité

Sommaire

Documentation du code

Pourquoi ?

Nous avons choisi de commenter le code pour aider à la compréhension du programme et faciliter l'arrivé de nouveaux acteurs au projet. Cela nous permet également d'apprendre plus sur le projet dans sa globalité.

- Les autres objectifs du sujet requiert une bonne compréhension du code.
- Une documentation avec Doxygen permet d'avoir une documentation structurée et lisible supportant une recherche de fonction.

Doxygen

Doxygen

Doxygen est un logiciel libre permettant de produire une documentation Latex et/ou HTML à partir d'un code source. Il peut être combiné avec graphviz pour générer des arbres d'appels.

- Réalisation d'un script générant la base de commentaires pour Doxygen.

Doxygen

Doxygen

Doxygen est un logiciel libre permettant de produire une documentation Latex et/ou HTML à partir d'un code source. Il peut être combiné avec graphviz pour générer des arbres d'appels.

- Réalisation d'un script générant la base de commentaires pour Doxygen.
- Compréhension et commentaires du code représentant près de 64 000 lignes.

Doxygen

Doxygen

Doxygen est un logiciel libre permettant de produire une documentation Latex et/ou HTML à partir d'un code source. Il peut être combiné avec graphviz pour générer des arbres d'appels.

- Réalisation d'un script générant la base de commentaires pour Doxygen.
- Compréhension et commentaires du code représentant près de 64 000 lignes.
- Réalisation de la documentation avec Doxygen. Réalisation de schémas.

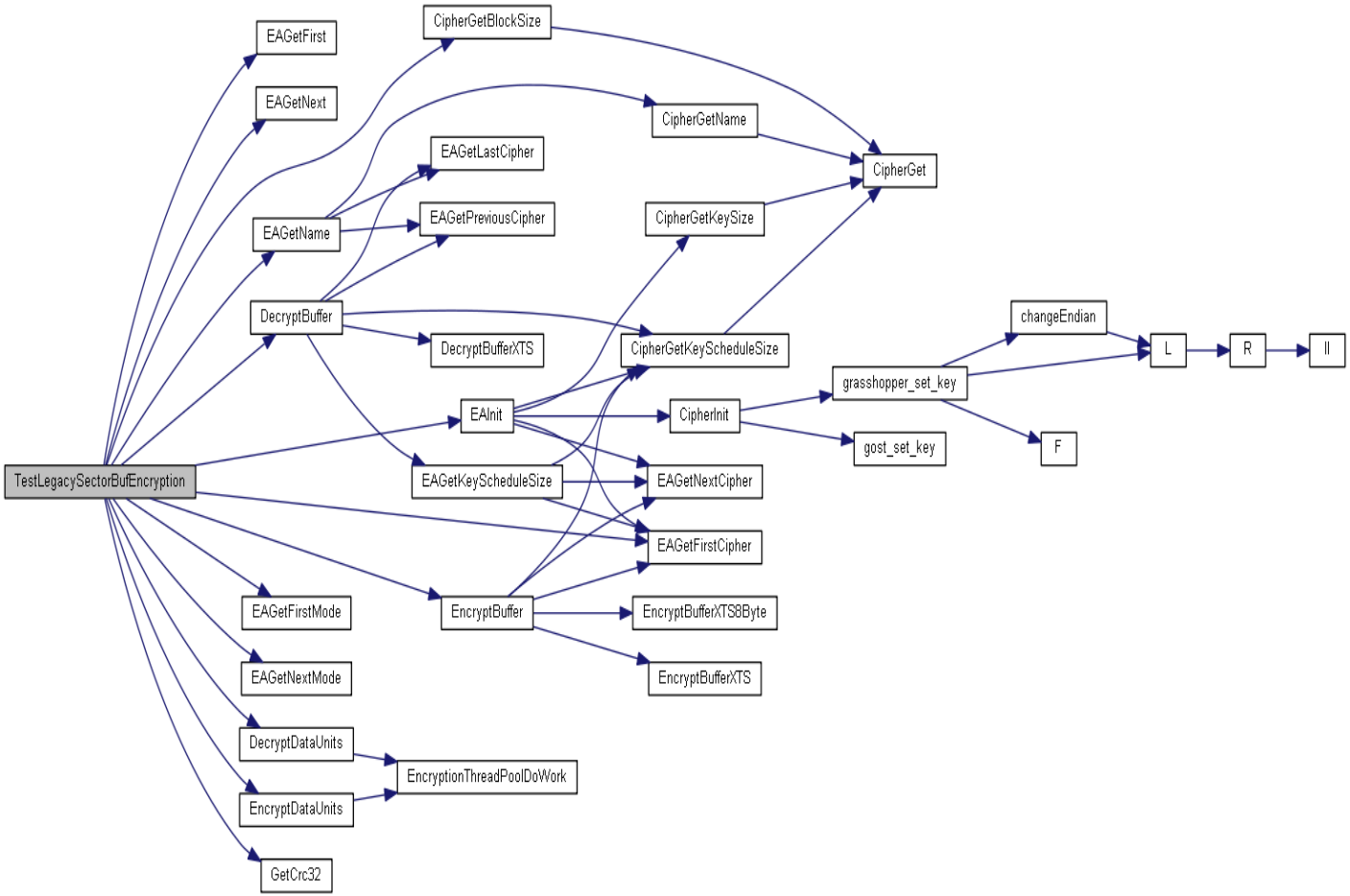
Doxygen

Doxygen

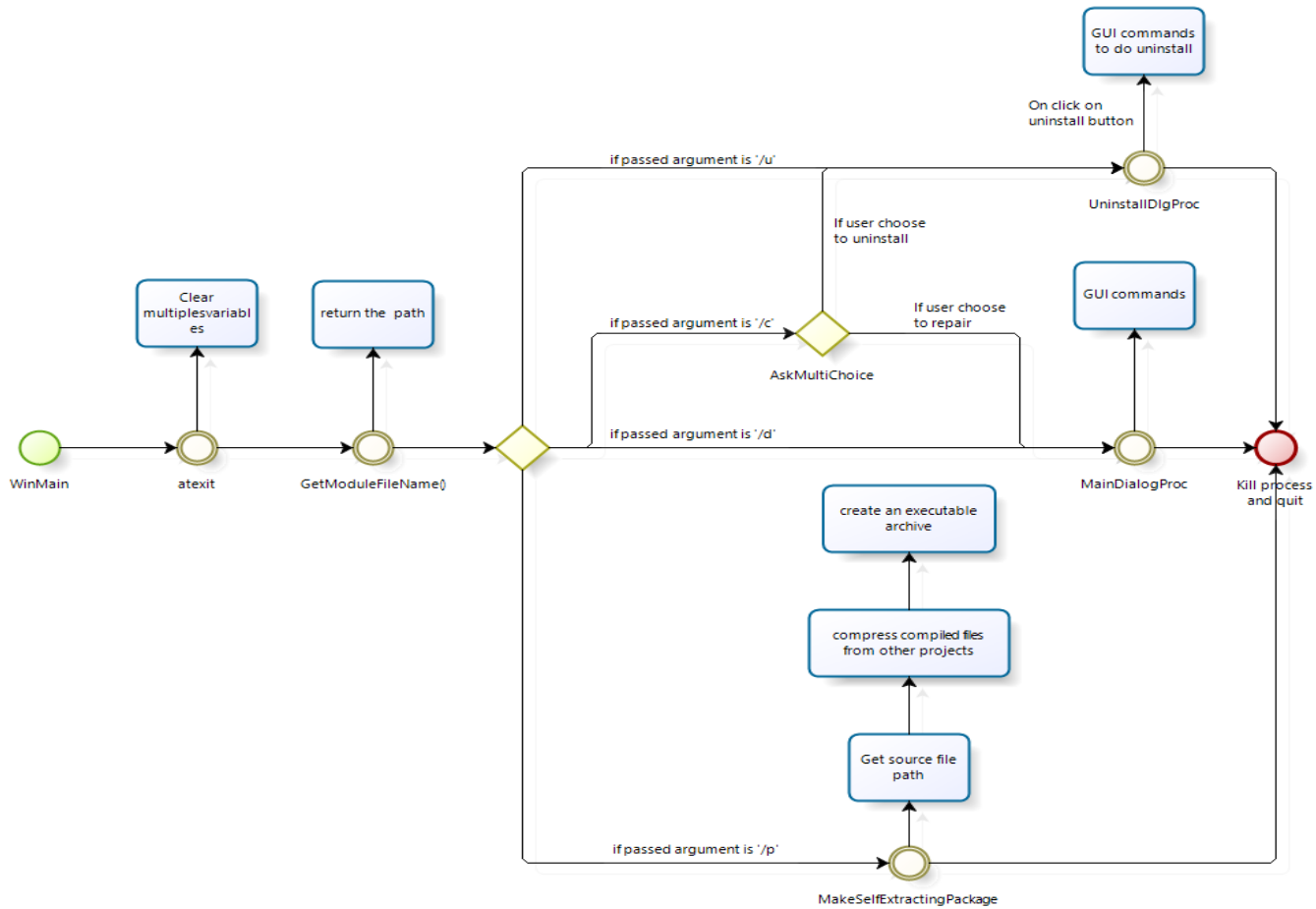
Doxygen est un logiciel libre permettant de produire une documentation Latex et/ou HTML à partir d'un code source. Il peut être combiné avec graphviz pour générer des arbres d'appels.

- Réalisation d'un script générant la base de commentaires pour Doxygen.
- Compréhension et commentaires du code représentant près de 64 000 lignes.
- Réalisation de la documentation avec Doxygen. Réalisation de schémas.
- Marquage du code inutile par des balises de commentaire.

Doxygen avec graphviz



Schémas réalisé



Sommaire

Marquage du code

- le code inutile est marqué par des balises de commentaire
- un fichier texte rappel les fonctions inutiles

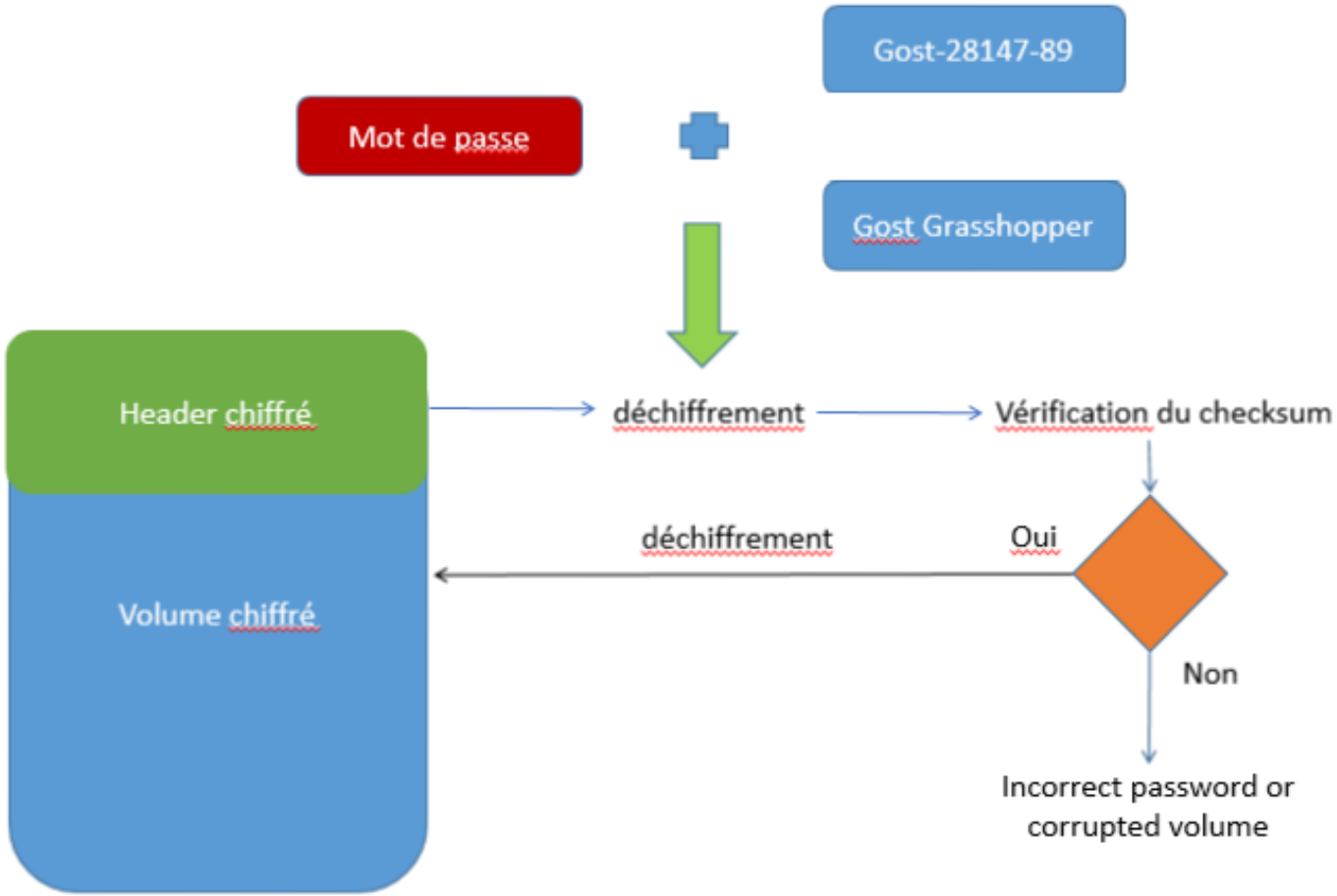
Sommaire

analyse statique du code

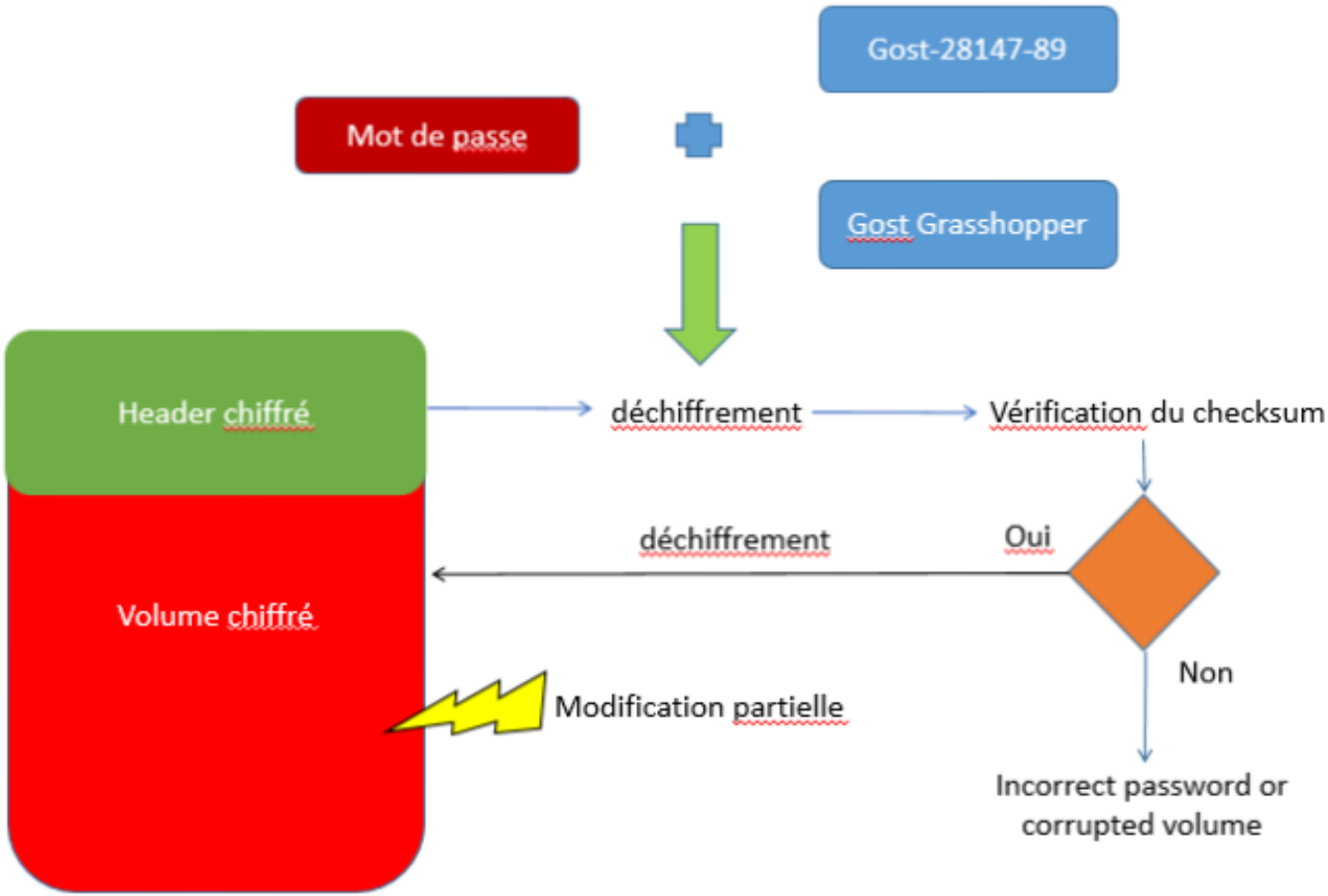
- Flawfinder nous à permis de générer le rapport d'analyse statique
- le rapport signale 1380 erreurs dont 299 erreurs de niveau 5.

Sommaire

Ouverture d'un volume



Zone sensible



Proposition de fonctionnalité

- Manque d'une alerte si les fichiers internes sont modifiés.
- Système de Checksum grâce à l'algorithme de hachage de Gost.

Proposition de fonctionnalité

- Manque d'une alerte si les fichiers internes sont modifiés.
- Système de Checksum grâce à l'algorithme de hachage de Gost.
- Proposition : système de hachage avant chiffrement pouvant vérifier l'intégrite des fichiers après déchiffrement.

Problèmes rencontrés

- Découverte du projet. Une semaine à comprendre le début du programme.
- Les appels récurrent aux fonctions windows.
- Les variables d'interface graphique windows.
- Langage Assembleur

Test sur Veracrypt

- Veracrypt est très actif dans son développement.

Test sur Veracrypt

- Veracrypt est très actif dans son développement.
- Etant plus avancé nous avons tester sur Veracrypt la même manipulation que sur Gostcrypt

Test sur Veracrypt

- Veracrypt est très actif dans son développement.
- Etant plus avancé nous avons tester sur Veracrypt la même manipulation que sur Gostcrypt
- Conclusion : Veracrypt ne vérifie pas non plus l'intégrité du message.

Conclusion

- Un objectif de Gostcrypt est de s'affranchir définitivement de la license Truecrypt et Veracrypt
- Nous pensons que l'ajout de cette fonctionalité peut être un pas dans la séparation avec Veracrypt.

Conclusion

Questions ?