

# Soutenance projet annuel - Audit des implantations SSL/TLS

Claire Smets – William Boisseleau – Pascal Edouard – Mathieu Latimier – Julien Legras

Master 2 Sécurité des Systèmes Informatiques

28/02/2014



# Sujet et problématique

Titre du bloc

Contenu

# Sommaire

- 1 Introduction
  - Sujet et problématique
- 2 Audit des clefs RSA des certificats
  - Récupération
    - Adresses
    - Certificats
  - Factorisation
  - Résultats
- 3 Audit d'OpenSSL
  - Entropie
  - Génération des clefs
  - Chiffrement et protocoles
  - Signature et authentification
  - Protocole SSL/TLS
  - Ouverture
- 4 Analyse dynamique du navigateur client
  - Faiblesses identifiées
  - Implémentation
  - Démonstration
- 5 Conclusion

# Récupération des adresses

# Récupération des certificats

# Factorisation

# Factorisation – Démonstration

# Résultats



# Introduction

# Entropie

# Entropie – Démonstration

# Génération des clefs

# Chiffrement et protocoles

# Signature et authentification

# Protocole SSL/TLS

# Ouverture



# Faiblesses identifiées

# Implémentation

# Démonstration

# Conclusion