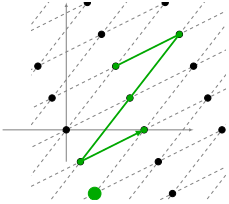

Surveillance

Relations entre la France et le Royaume-Uni

Matthias Minihold

13.06.2017 – 12.30 @ RUB

Cryptology and IT-Security, Ruhr-Universität Bochum

Introduction

Je suis Charly étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Introduction

Je suis Matthias étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Introduction

Je suis Matthias étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Mes thèmes de recherche sont :

étude et conception d'algorithmes (classique et quantiques) pour le décodage de codes linéaires, par exemple, ou pour des problemes combinatoires sur les réseaux.

Introduction

Je suis Matthias étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Mes thèmes de recherche sont :

étude et conception d'algorithmes (classique et quantiques) pour le décodage de codes linéaires, par exemple, ou pour des problemes combinatoires sur les réseaux.

- On peut résumer ma recherche par le mot «Cryptanalyse».

Introduction

Je suis Matthias étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Mes thèmes de recherche sont :

étude et conception d'algorithmes (classique et quantiques) pour le décodage de codes linéaires, par exemple, ou pour des problemes combinatoires sur les réseaux.

- On peut résumer ma recherche par le mot «Cryptanalyse».
- Mon thème aujourd'hui :

Introduction

Je suis Matthias étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Mes thèmes de recherche sont :

étude et conception d'algorithmes (classique et quantiques) pour le décodage de codes linéaires, par exemple, ou pour des problemes combinatoires sur les réseaux.

- On peut résumer ma recherche par le mot «Cryptanalyse».
- Mon thème aujourd'hui :
  - des agences de renseignements

Introduction

Je suis Matthias étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Mes thèmes de recherche sont :

étude et conception d'algorithmes (classique et quantiques) pour le décodage de codes linéaires, par exemple, ou pour des problemes combinatoires sur les réseaux.

- On peut résumer ma recherche par le mot «Cryptanalyse».
- Mon thème aujourd'hui :
  - des agences de renseignements
  - d'un récent projet de loi sur le renseignement

Introduction

Je suis Matthias étudiant en Cryptologie et Sécurité à la Ruhr-Universität Bochum.

Mes thèmes de recherche sont :

étude et conception d'algorithmes (classique et quantiques) pour le décodage de codes linéaires, par exemple, ou pour des problemes combinatoires sur les réseaux.

- On peut résumer ma recherche par le mot «Cryptanalyse».
- Mon thème aujourd'hui :
  - des agences de renseignements
  - d'un récent projet de loi sur le renseignement
  - un mot qui revient systématiquement dans ces débats : «métadonnées».

Métadonnées

En quoi consistent exactement ces métadonnées?

Les métadonnées permettent d'identifier et de décrire les documents par :

- le contenu (comme : titre, description, source, langue, ...),

Métadonnées

En quoi consistent exactement ces métadonnées?

Les métadonnées permettent d'identifier et de décrire les documents par :

- le contenu (comme : titre, description, source, langue, ...),
- la propriété intellectuelle (comme : créateur, éditeur, ...),

Métadonnées

En quoi consistent exactement ces métadonnées?

Les métadonnées permettent d'identifier et de décrire les documents par :

- le contenu (comme : titre, description, source, langue, ...),
- la propriété intellectuelle (comme : créateur, éditeur, ...),
- la matérialisation (comme : date, type, format, ...).

Métadonnées

En quoi consistent exactement ces métadonnées?

Les métadonnées permettent d'identifier et de décrire les documents par :

- le contenu (comme : titre, description, source, langue, ...),
- la propriété intellectuelle (comme : créateur, éditeur, ...),
- la matérialisation (comme : date, type, format, ...).

Métadonnées

En quoi consistent exactement ces métadonnées?

Les métadonnées permettent d'identifier et de décrire les documents par :

- le contenu (comme : titre, description, source, langue, ...),
- la propriété intellectuelle (comme : créateur, éditeur, ...),
- la matérialisation (comme : date, type, format, ...).

Pourquoi avoir les métadonnées?

Ces sont des éléments essentiels de l'architecture Web et elles sont necéssaires pour transmettre l'information élèctronique mais elles peuvent être supprimées après peu de temps.

La Situation

- Il y a de nombreux câbles sous-marins de communication Transatlantique qui partent des côtes françaises. Sur les côtes de la Méditerranée (au Sud) d'autres câbles arrivent d'Algérie par exemple, ou d'Afrique en général.

La Situation

- Il y a de nombreux câbles sous-marins de communication Transatlantique qui partent des côtes françaises. Sur les côtes de la Méditerranée (au Sud) d'autres câbles arrivent d'Algérie par exemple, ou d'Afrique en général.
- Ainsi, pour envoyer un courriel depuis l'Algérie vers les Etats-Unis, il est très probable que les données passent par la France.

La Situation

- Il y a de nombreux câbles sous-marins de communication Transatlantique qui partent des côtes françaises. Sur les côtes de la Méditerranée (au Sud) d'autres câbles arrivent d'Algérie par exemple, ou d'Afrique en général.
- Ainsi, pour envoyer un courriel depuis l'Algérie vers les Etats-Unis, il est très probable que les données passent par la France.
- Cette situation est très favorable pour la Direction Générale de la Sécurité Extérieure abrégée DGSE et les Cinq Yeux abrégés FVEY.

La Situation

- Il y a de nombreux câbles sous-marins de communication Transatlantique qui partent des côtes françaises. Sur les côtes de la Méditerranée (au Sud) d'autres câbles arrivent d'Algérie par exemple, ou d'Afrique en général.
- Ainsi, pour envoyer un courriel depuis l'Algérie vers les Etats-Unis, il est très probable que les données passent par la France.
- Cette situation est très favorable pour la Direction Générale de la Sécurité Extérieure abrégée DGSE et les Cinq Yeux abrégés FVEY.
- Les partenaires anglo-saxons ont approfondi les relations avec les services secrets français en adoptant un protocole d'échange de données massif.

La Situation

- Il y a de nombreux câbles sous-marins de communication Transatlantique qui partent des côtes françaises. Sur les côtes de la Méditerranée (au Sud) d'autres câbles arrivent d'Algérie par exemple, ou d'Afrique en général.
- Ainsi, pour envoyer un courriel depuis l'Algérie vers les Etats-Unis, il est très probable que les données passent par la France.
- Cette situation est très favorable pour la Direction Générale de la Sécurité Extérieure abrégée DGSE et les Cinq Yeux abrégés FVEY.
- Les partenaires anglo-saxons ont approfondi les relations avec les services secrets français en adoptant un protocole d'échange de données massif.

La Situation

- Il y a de nombreux câbles sous-marins de communication Transatlantique qui partent des côtes françaises. Sur les côtes de la Méditerranée (au Sud) d'autres câbles arrivent d'Algérie par exemple, ou d'Afrique en général.
- Ainsi, pour envoyer un courriel depuis l'Algérie vers les Etats-Unis, il est très probable que les données passent par la France.
- Cette situation est très favorable pour la Direction Générale de la Sécurité Extérieure abrégée DGSE et les Cinq Yeux abrégés FVEY.
- Les partenaires anglo-saxons ont approfondi les relations avec les services secrets français en adoptant un protocole d'échange de données massif.

Je vais continuer en anglais!

Five Eyes (FVEY)

Five Eyes comprising

- National Security Agency (NSA) of the United States

Five Eyes (FVEY)

Five Eyes comprising

- National Security Agency (NSA) of the United States
- Government Communications Headquarters (GCHQ) of the United Kingdom

Five Eyes (FVEY)

Five Eyes comprising

- National Security Agency (NSA) of the United States
- Government Communications Headquarters (GCHQ) of the United Kingdom
- Government Communications Security Bureau (GCSB) of New Zealand

Five Eyes (FVEY)

Five Eyes comprising

- National Security Agency (NSA) of the United States
- Government Communications Headquarters (GCHQ) of the United Kingdom
- Government Communications Security Bureau (GCSB) of New Zealand
- Communications Security Establishment of Canada (CSEC)

Five Eyes (FVEY)

Five Eyes comprising

- National Security Agency (NSA) of the United States
- Government Communications Headquarters (GCHQ) of the United Kingdom
- Government Communications Security Bureau (GCSB) of New Zealand
- Communications Security Establishment of Canada (CSEC)
- Defence Signals Directorate (DSD) of Australia

Lustre — Timeline

- 2006 cooperation between French DGSE and American NSA began

Lustre — Timeline

- 2006 cooperation between French DGSE and American NSA began
- 2010 extent of intelligence cooperation increased drastically

Lustre — Timeline

- 2006 cooperation between French DGSE and American NSA began
- 2010 extent of intelligence cooperation increased drastically
- 2011 formal memorandum and data exchange signed by France and Five Eyes

Lustre — Timeline

- 2006 cooperation between French DGSE and American NSA began
- 2010 extent of intelligence cooperation increased drastically
- 2011 formal memorandum and data exchange signed by France and Five Eyes
- 2013 existence of Lustre (and this timeline) revealed

Lustre — Timeline

- 2006 cooperation between French DGSE and American NSA began
- 2010 extent of intelligence cooperation increased drastically
- 2011 formal memorandum and data exchange signed by France and Five Eyes
- 2013 existence of Lustre (and this timeline) revealed
- aside of NSA's global surveillance disclosure efforts

Lustre — Timeline

- 2006 cooperation between French DGSE and American NSA began
- 2010 extent of intelligence cooperation increased drastically
- 2011 formal memorandum and data exchange signed by France and Five Eyes
- 2013 existence of Lustre (and this timeline) revealed
- aside of NSA's global surveillance disclosure efforts
- based on leaked documents collected by Edward Snowden

Lustre — Timeline

- 2006 cooperation between French DGSE and American NSA began
- 2010 extent of intelligence cooperation increased drastically
- 2011 formal memorandum and data exchange signed by France and Five Eyes
- 2013 existence of Lustre (and this timeline) revealed
- aside of NSA's global surveillance disclosure efforts
- based on leaked documents collected by Edward Snowden
- viewed & published by responsible journalists (unlike recently)

Lustre — Example

- Lustre = secret treaty between services: DGSE, the GCHQ, and the NSA

Lustre — Example

- Lustre = secret treaty between services: DGSE, the GCHQ, and the NSA
- France Télécom (= Orange S.A.) stores extensive customer call data

Lustre — Example

- Lustre = secret treaty between services: DGSE, the GCHQ, and the NSA
- France Télécom (= Orange S.A.) stores extensive customer call data

$\xrightarrow{shares}$ data with DGSE

Lustre — Example

- Lustre = secret treaty between services: DGSE, the GCHQ, and the NSA
- France Télécom (= Orange S.A.) stores extensive customer call data

$\xrightarrow{shares}$ data with DGSE
$\xrightarrow{shares}$ data with GCHQ

Lustre — Example

- Lustre = secret treaty between services: DGSE, the GCHQ, and the NSA
- France Télécom (= Orange S.A.) stores extensive customer call data

$\overset{shares}{\longrightarrow}$ data with DGSE
$\overset{shares}{\longrightarrow}$ data with GCHQ

Example: Scale of surveillance

shared > 70000000 meta-data records
only between Dec. 2012 and 8.1.2013.

Questions?

. . . thank you for your attention!