

- 1)  
tresses cryptographiques
- 2)  
Detection de Sniffer sur un réseau Ethernet
- 3)  
SHA  
"Near Collisions of SHA-0"
- 4)  
Les attaques par déni de service
- 5)  
Attaque RSA à clé partiellement révélée
- 6)  
Implémentation du chiffrement d'Elgamal et cryptanalyse
- 7)  
Craquage de mots de passe sous Windows et Linux
- 8)  
WEP
- 9)  
WPA
- 10)  
Injection SQL  
"SQLRand, preventing SQL injection Attacks"
- 11)  
AES, Implementation
- 12)  
Cryptanalyse du code de Vigenère et ses variantes
- 13)  
Rejeu  
"On Interactive Internet Traffic Replay".

14)  
Cryptographie et courbes elliptiques.

15)  
Https/SSL, Attaque Man-In-the-Middle

16)  
"Etude des protocoles AMP et EPA et implémentation de leurs failles"  
"Cryptanalysis of Two Password-Authenticated Key Exchange Protocols"

17)  
L'attaque temporelle(Timing Attack) sur les systèmes RSA.

18)  
Attaques de RSA à clé partiellement révélée.

19)  
SNMP

20)  
"Le protocole DNS du point de vue de l'intrus"

21)  
Generateur Pseudo-aleatoire de nombres premiers

22)  
AES  
"Modes d'opérations pour les chiffrements par blocs.  
Attaques par réinjection de paquets, exemples connus.  
Lutte contre les attaques par dictionnaire de codes.

[23\)](#)  
Application de la cryptographie aux réseaux VPN

24)  
"Cryptographie visuelle"

25)  
Débordement de buffer sur Mac OSX

- 26)  
AKS et RSA
- 27)  
Attaque par effet de bord
- 28)  
Tests d'intrusions externes.
- 29)  
Craquage Mot de passe Windows, compromis temps-memoire
- 30)  
Md5, collisions, attaque
- 31) UMTS et techniques de sécurité
- 32) Stéganalyse
- 33) failles dans la VOIP
- 34) sécurité du protocole Bluetooth
- 35)VPN et securite
- 36) Snort/Sguil et les attaques disponibles sur le site  
taosecurity
- 37) messagerie instantanee
- 38) zero-knowledge et e-donkey
- 39) ssl et attaques
- 40) Vigenere
- 41) attaques DDos
- 43)SNB Mac-Address Spoof detection

0)steganographie

AURELIE.BARRAT@bvra.etu.univ-lyon1.fr

GIRAUD J.B.

(2 envois faits)

Stéganographie pratique et stéganalyse.Ce sujet nous permettra de montrer spécifiquement comment mettre en place un programme de stéganographie en C, C++, ainsi qu'un autre de stéganalyse.Nous allons aussi tenter de réfléchir à des solutions résistant à une stéganalyse d'échange des bits poids forts / poids faibles.Il nous a donc semblé justifié de nous mettre en binôme car nous allons traiter spécifiquement deux sujets très liés (stéganographie et stéganalyse).

1)

page de l'auteur décrivant l'algorithme blowfish:

<http://www.schneier.com/paper-blowfish-fse.html>page

decrivant l'algorithme twoish:<http://www.schneier.com/paper-twofish-paper.html>

Tomasz Krajczynski 10305061Bartosz Kowalski 10301328

2)

générateur nonce "nomus".

Dieng Sidy

d\_sidy@hotmail.com

Annie Laure TCHIMKAP

ANNIE-LAURE.TCHIMKAP-DJIENG@bvra.etu.univ-lyon1.fr

(envoi sha-1+md5 collision)

3)

Cassage et durcissement des mots de passe unix

misc n°5 (en ma possession)

ysilog@gmail.com

jeremie.cieslak@etu.univ-lyon1.fr

4)

"Sécurité des transactions électroniques : le protocole SSL". je voudrais savoir si le sujet n'est pas déjà pris, si ce n'est pas le cas et si c'est possible d'avoir le rapport qui traite ce sujet(N°39) .

Sarah NAIT BAHLOUL 10708863

SARAH.NAIT-BAHLOUL@bvra.etu.univ-lyon1.fr

5)

**(- La machine Enigma**

- Le procédé
- Ses faiblesses (les différentes attaques)
- Développement de la machine en C

**- Le chiffre de vigenère**

- Le procédé
- Ses faiblesses (les différentes attaques)
- Développement de l'algorithme en C

**- RSA et ses attaques**

- L'attaque de Wiener
- L'attaque de Hastad
- L'attaque par chronométrage
- L'attaque par chiffrement choisi

**- La sécurité des cartes bancaires**

- Le procédé
  - authentification RSA en locale
  - authentification DES en ligne
- l'affaire Humpich et les autres méthodes de fraude

**- Une approche sur la cryptographie quantique)**

**choix: - Une approche sur la sécurité réseau**

- L'attaque sur RIP (MISC 30 pages 66 à 79)
- Sécurité des protocoles multicast (MISC 25 pages 56 à 63)

steve.roux@free.fr

Steve ROUX 10607327

Xiao Yang

6)

coincidence de Friedman en décrivant parallèlement des algorithmes de cryptage comme le codage de Cesar, de Vigenère...

J'attends votre accord pour commencer de constituer cet exposé

Guillaume Desloges

guillaume.desloges@gmail.com

7) SUPPRIME  
s.jourdan@yahoo.com  
MD5  
(envois faits)

8)  
PGP(Pretty Good Privacy) et sur le certificats de confiance.

Adrianna Roxane YOMBI

ADRIANNA.YOMBI@bvra.etu.univ-lyon1.fr

9)

SHA-0

akim.saidani@gmail.com

10)

IAN.OTANDO-OYEMBO@bvra.etu.univ-lyon1.fr

### **La machine Enigma**

- Le procédé
- Ses faiblesses (les différentes attaques)
- Developpement de la machine en C

11)

Rambaud Targuy  
vmsplice

12)

reseaux Bayesiens  
MAMADI.DIAKITE@bvra.etu.univ-lyon1.fr

13)

LAABI Raid  
Watermarking

14)

"failles dans les voip"

Souga Ghassen

ghassen\_rock2001@yahoo.fr

envoi fait

15)

degraevegreg

degraevegreg@hotmail.fr

ssl: backdoor cryptographique

(2 misc donnesbackdoor crypto, bluetooth hacking)

16) SUPPRIME

n.lacombe

n.lacombe@gmail.com

Voici un article wikipedia détaillant les procédé utilisé par Kevin

Mitnick:

[http://fr.wikipedia.org/wiki/Attaque\\_de\\_Mitnick](http://fr.wikipedia.org/wiki/Attaque_de_Mitnick)

Cette page contient également beaucoup d'information:

<http://www.gulker.com/ra/hack/>

Notamment une description de l'attaque par Shimomura:

<http://www.gulker.com/ra/hack/tsattack.html>

Je pourrais par exemple m'appuyer sur cette affaire pour parler des

failles du systeme de RSH permettant l'IP spoofing comparé au SSH, des

failles du UDP qui le permette aussi, ou encore des inondations de

requêtes SYN et des moyens de le contrer.

17)

Pratique spoofing -php

ACLEMENT Pierre

LIEVRE Thibault

18)

Diffie-Hellman-MD5 (a preciser)

Nejad DEGHAN

19)

JOURDAN Sylvain RC4 (article)

20)

ROUSSELOT Thibault

(Article Crypto. 2006 19)

Fly Authentication and Signature Schemes

21)

CONG Wei

"VPN et IPSec"

1.Introduction du réseau VPN

2.Principe de fonctionnement VPN

3.Le protocole IPSec (AH, Esp, Isakmp, IKE, etc.)

4.Les autres protocoles sous VPN

5.Comparaison des différents protocoles

6.Conclusion.

22)

keyloggers

Pierre Bourget, Guillaume Floret.

23)

algorithme Skipjack et notamment expliciter ses spécifications et parler des cryptanalyses réalisées.

Jérôme Belleman [JEROME.BELLEMAN@bvra.etu.univ-lyon1.fr](mailto:JEROME.BELLEMAN@bvra.etu.univ-lyon1.fr)

24)

t SQL Injection.

Nous le traiterons de la façon suivante:

Définition

Les risques

Attaquer une requête (les requêtes fragiles)

Comment se protéger (préformatage des requêtes et autre solution)

Les difficultés (compromis temps)

Exemple d'attaque (PHP ou autre)

Conclusion

-

Aubertin Philippe 10402657  
aubertinp@gmail.com  
Bouc Grégory  
gregory.bouc@gmail.com

25)  
CROSS SITE SCRIPTING ( INJECTIONS HTML)[ANDRIAMAROSOA Sariaka](#)

26) patrickkenfack@yahoo.fr PCI-DSS

27) ADFGVX et Playfair QUOC-VI.TRAN@bvra.etu.univ-lyon1.fr

28) Valtrine Mathieu Attaques IPV6

29)  
Chiffrements par blocs Lakehal Noureddine et ?

29) Pohlig-Hellman Nejad Deghan Alda

30)  
**Bouras Samy**  
attaques par dump mémoire

31)  
protocole d'authentification EPA  
Alberto Fanton

32)  
nmap (fonctionnement, analyse)  
Florian MOLÉ

33)  
canaux cachés  
Jules Dagnaud

