Sécurité des développements

ICAM – JP Gouigoux – 11/2012

Glossaire

- Virus / Backdoor / Troyen
- Vulnérabilité / Exploit / Faille / 0-day
- Injection / Déni de service / Canonicalisation
- Advanced Persistant Threat / Network scan
- Social Engineering / Malware / Scareware

Economie de la sécurité

- 66% des clés USB perdues sont piégées
- 17,7 M$: CA produits sécurité 2011
- Incident sécurité pour 60% des entreprises en 2011 (39% en 2010)
- Twitter, LinkedIn, Facebook : tous avec une attaque critique en 2012
- NASA : hacké
- FBI, CIA, NSA : 1000+ attaques / jour !

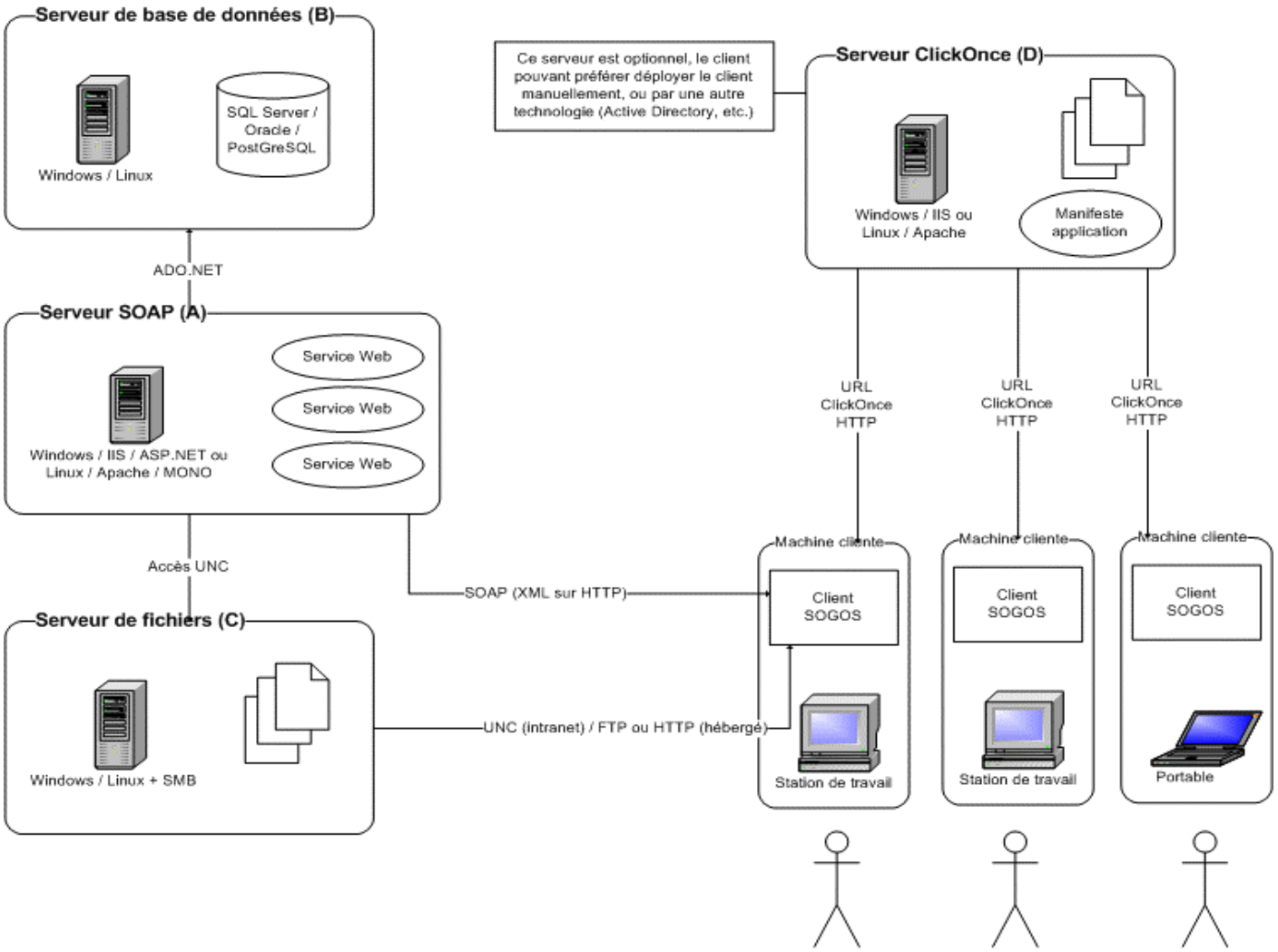
Les bases de la sécurité : pas une question technique, mais de méthode

- Modélisation des attaques
  - SD3 = Secure by Design / Default / Deployment
  - Analyse de risque : risque = occurrence x sévérité

- Savoir sortir la tête de la technique
  - Veille technologique
  - Mise en place de bonnes pratiques de programmation

- Ne pas trop en faire
  - Le bon niveau, c'est état de l'art + 1
  - Le problème final est entre le clavier et la chaise

Architecture applicative standard



Attaques classiques

Client	Zone internet	DMZ	Zone intranet	Intranet enfoui
Affichage en clair du mot de passe Analyse des DLL Lancement usurpé	Attaque MITM Session hijacking	Injection SQL ***Déni de service*** Accès non identifié	Client non autorisé ***Déni de service*** Attaque brut MDP Escalade de privilèges	Injection SQL ***Déni de service*** Escalade de privilèges
Zone de mot de passe invisible à VUPassword MDP invisible en mémoire Certificat client Authentification sur proxy	HTTPS (100% flux + déploiement) Tunnel VPN Sessions sans cookie	Validation par Schema XML Cryptage MDP Annuaire LDAP	Blocage des UserAgent externes par défaut Timeout aléatoire sur validation MDP Code Access Security (XML)	Paramétrisation complète + validation préalable Comptes dédiés

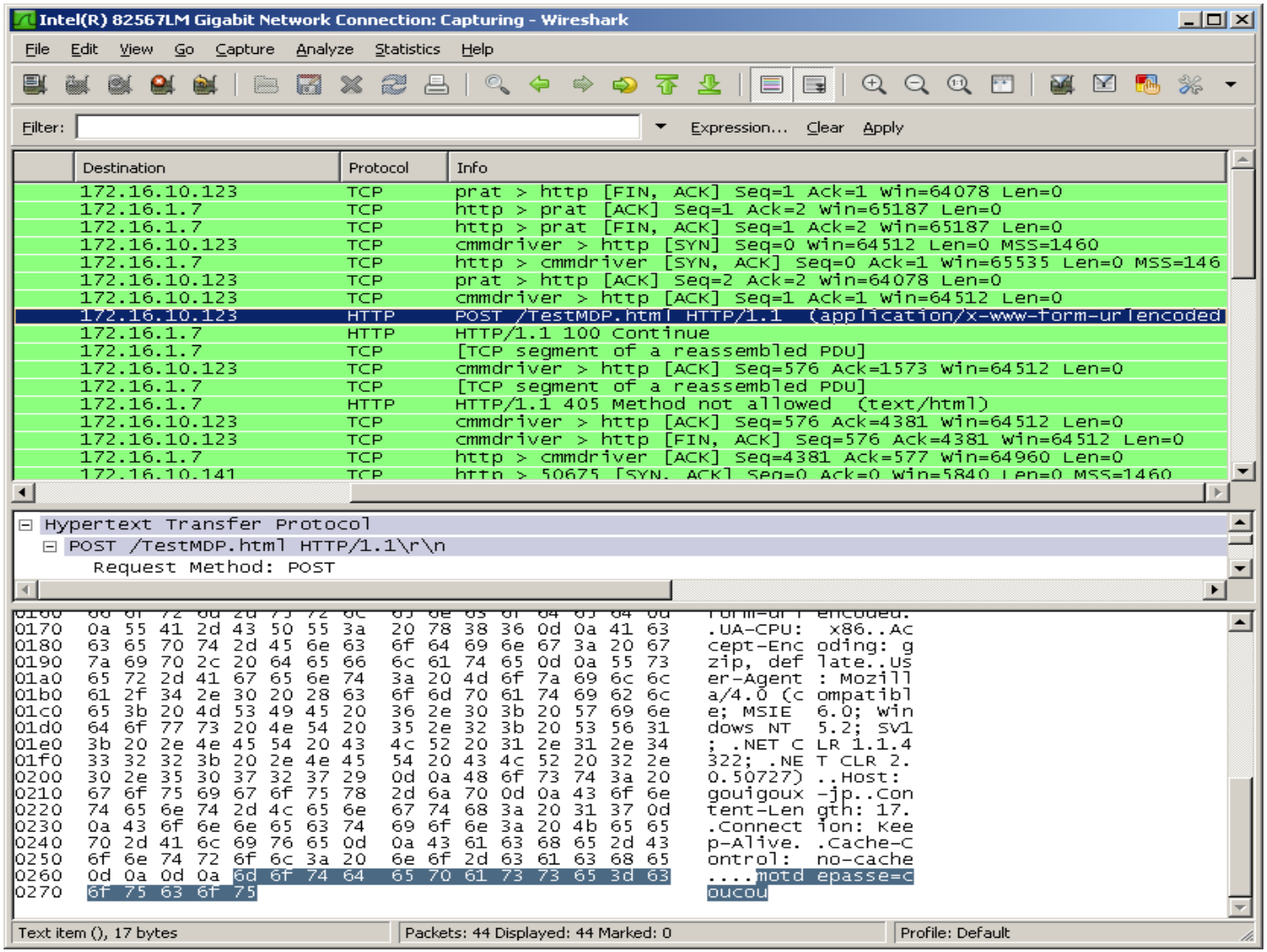
Attaques sur le client

- Affichage en clair du mot de passe
  - Principe de VUPassword
  - Lock de session
  - SecureString
- Référence invisible en mémoire
  - Analyse DLL par ILDASM
  - Protection par hash
  - Ne pas oublier le sel... (voir plus loin)
- Authentification client
  - Authentification intégrée / LDAP / propriétaire
  - Problème d'accessibilité internet
  - Chiffrage des crédentiels

Attaques sur internet

- Par défaut, le flux HTTP est en clair
  - Man In The Middle
  - Capture TCP d'un GET avec Wireshark
- Mise en place de HTTPS
  - Principe de fonctionnement
  - Limitation de sécurité des certificats
- Session Hijacking
  - Déconnecter proprement
  - Attention aux cookies
  - Gérer les timeouts

Trafic Ethernet

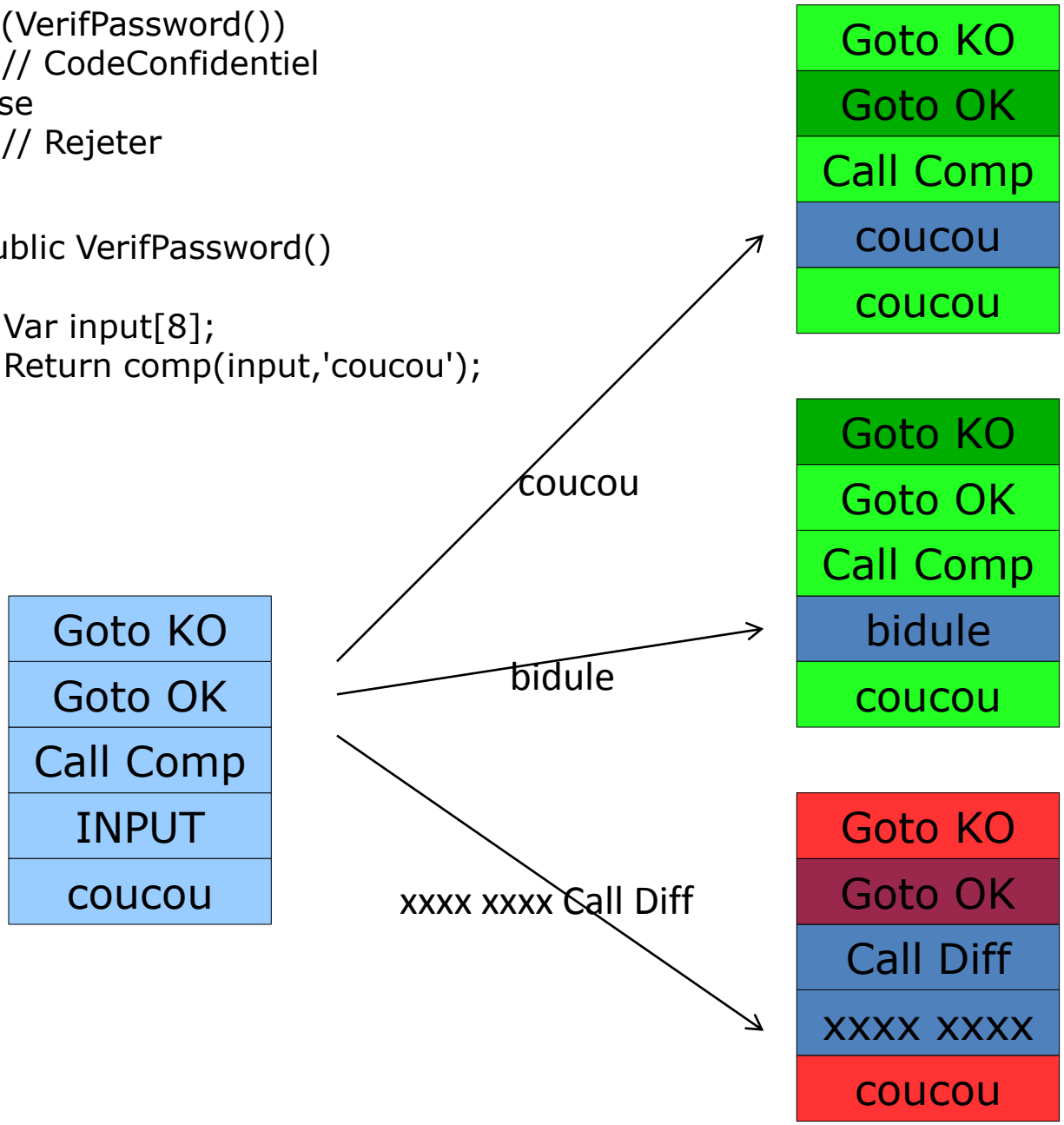


Attaques sur le métier

- Injection SQL
  - Démonstration
  - Sécurisation : simplement coder proprement
- Débordement de tampons
  - Principe
  - Une des raisons pour les L4G
- Fonctionnalité non autorisée
  - Défaut de programmation
  - Backdoor intentionnelle
  - Abus de licence

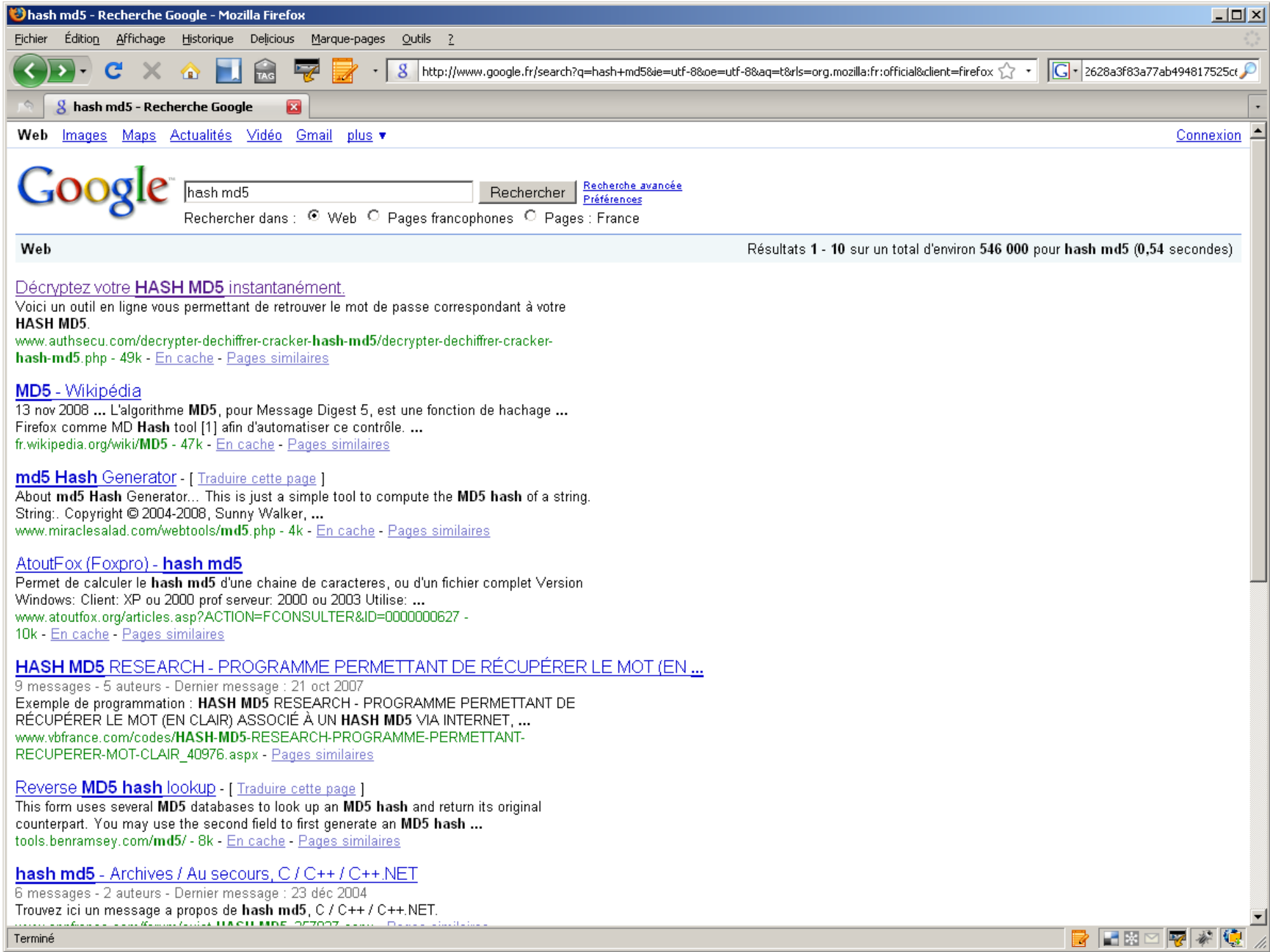
```
if (VerifPassword())
   // CodeConfidentiel
else
   // Rejeter


Public VerifPassword()
{
   Var input[8];
   Return comp(input,'coucou');
}
```



Failles de cryptographie

- Cryptographie symétrique / asymétrique
- Algorithmes de hash / signature
  - MD5 : terminé
  - SHA1 : collisions possibles
  - SHA256 : pas sans sel
  - SHA256 + sel : pas nécessairement suffisant (LinkedIn)
- On commence par la base : démo


hash md5 - Recherche Google - Mozilla Firefox
Fichier Édition Affichage Historique Delicious Marque-pages Outils ?
http://www.google.fr/search?q=hash+md5&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox
hash md5 - Recherche Google
Web Images Maps Actualités Vidéo Gmail plus ▼
Connexion
Google
hash md5
Rechercher
Recherche avancée
Préférences
Rechercher dans : Web Pages francophones Pages : France
Web
Résultats 1 - 10 sur un total d'environ 546 000 pour hash md5 (0,54 secondes)
Décryptez votre HASH MD5 instantanément.
Voici un outil en ligne vous permettant de retrouver le mot de passe correspondant à votre HASH MD5.
www.authsecu.com/decrypter-dechiffrer-cracker-hash-md5/decrypter-dechiffrer-cracker-hash-md5.php - 49k - En cache - Pages similaires
MD5 - Wikipédia
13 nov 2008 ... L'algorithme MD5, pour Message Digest 5, est une fonction de hachage ...
Firefox comme MD Hash tool [1] afin d'automatiser ce contrôle. ...
fr.wikipedia.org/wiki/MD5 - 47k - En cache - Pages similaires
md5 Hash Generator - [Traduire cette page]
About md5 Hash Generator... This is just a simple tool to compute the MD5 hash of a string.
String:. Copyright © 2004-2008, Sunny Walker, ...
www.miraclesalad.com/webtools/md5.php - 4k - En cache - Pages similaires
AtoutFox (Foxpro) - hash md5
Permet de calculer le hash md5 d'une chaine de caracteres, ou d'un fichier complet Version Windows: Client: XP ou 2000 prof serveur: 2000 ou 2003 Utilise: ...
www.atoutfox.org/articles.asp?ACTION=FCONSULTER&ID=0000000627 - 10k - En cache - Pages similaires
HASH MD5 RESEARCH - PROGRAMME PERMETTANT DE RÉCUPÉRER LE MOT (EN ...
9 messages - 5 auteurs - Dernier message : 21 oct 2007
Exemple de programmation : HASH MD5 RESEARCH - PROGRAMME PERMETTANT DE RÉCUPÉRER LE MOT (EN CLAIR) ASSOCIÉ À UN HASH MD5 VIA INTERNET, ...
www.vbfrance.com/codes/HASH-MD5-RESEARCH-PROGRAMME-PERMETTANT-RECUPERER-MOT-CLAIR_40976.aspx - Pages similaires
Reverse MD5 hash lookup - [Traduire cette page]
This form uses several MD5 databases to look up an MD5 hash and return its original counterpart. You may use the second field to first generate an MD5 hash ...
tools.benramsey.com/md5/ - 8k - En cache - Pages similaires
hash md5 - Archives / Au secours, C / C++ / C++.NET
6 messages - 2 auteurs - Dernier message : 23 déc 2004
Trouvez ici un message a propos de hash md5, C / C++ / C++.NET.
Terminé

AuthSecu
Le site de la Sécurité Réseau des Entreprises

Décryptez votre HASH MD5
par Sébastien FONTAINE (_SebF)

Mot de passe : toto HASH

HASH MD5 : Déchiffrer

1 - Fonction de décryptage MD5

Le HASH MD5 est une fonction irréversible, ce qui signifie qu'il n'existe pas d'algorithme ou de fonction permettant de retrouver la chaîne d'origine à partir de son HASH.

La seule méthode pour déchiffrer un HASH est de crypter un ensemble de chaînes de caractères. Ainsi, chaque chaîne cryptée sera comparée au HASH recherché jusqu'à trouver la correspondance. Il existe principalement 3 méthodes qui sont la comparaison par :

- Brut force, qui consiste à générer toutes les combinaisons possible d'une chaîne pour une longueur donnée. Cette méthode est très longue.

- Dictionnaire, qui consiste à utiliser les mots d'un dictionnaire. C'est beaucoup plus pertinent, mais ça demande beaucoup d'espace et de temps.

- Rainbow table, qui consiste à la recherche d'empruntes. c'est un bon compris entre le temps et l'espace, mais cela reste tout de même très long.

L'idée de l'outil en ligne proposé est de vous permettre de déchiffrer un HASH MD5 instantanément (inférieur à 3 secondes). Pour cela, nous avons générés 500 Millions de HASH stockés dans la base de AuthSecu.com. Ainsi, vous pourrez disposer d'une méthode qui outrepasse le problème de mémoire et de temps.

L'intérêt de cet outil est qu'il requête dans une base composée principalement de dictionnaire français où chaque mot à subit des variation brut force. Augmentant ainsi au maximum la pertinence et les chances de trouver votre HASH.

AuthSecu

Le site de la Sécurité Réseau des Entreprises

Décryptez votre HASH MD5 instantanément

Chaîne demandée : toto

Chaîne correspondante : f71dbe52628a3f83a77ab494817525c6

Google

f71dbe52628a3f83a77ab494817525c6 Rechercher Recherche avancée Préférences

Rechercher dans : Web Pages francophones Pages : France

Web Résultats **1** - **10** sur un total d'environ **254** pour **f71dbe52628a3f83a77ab494817525c6** (**0,11** secondes)

Réponse [WD12][eGroupWare] Vérification du mot de passe, entraide ...
6 messages - Dernier message : 29 oct
sPwdStocke est une chaîne = "**f71dbe52628a3f83a77ab494817525c6**" sHashPwd est une chaîne = HashChaîne(HA_MD5_128,sPwd) ...
www.generation-nt.com/reponses/wd12-egroupware-verification-mot-passe-entraide-3238031.html - Pages similaires

Tester la fiabilite de son mot de passe - Tux-planet
md5force to **f71dbe52628a3f83a77ab494817525c6** 4 ... md5force 0123456789abcdefghijklmnopqrstuvwxyz. **f71dbe52628a3f83a77ab494817525c6** 6 ...
www.tux-planet.fr/tester-la-fiabilite-de-son-mot-de-passe/ - 53k - En cache - Pages similaires

Mysql convertir mot de passe en md5 - Page 2 - Forum des développeurs
Et dans ta base tu devrais avec **f71dbe52628a3f83a77ab494817525c6** aussi car ... Et donc **f71dbe52628a3f83a77ab494817525c6=f71dbe52628a3f83a77ab494817525c6**, ...
www.developpez.net/forums/d402786-2/bases-donnees/mysql/administration/mysql-convertir-passe-md5/ - 218k - En cache - Pages similaires

phpBB-fr.com • Probleme Hebergeur : Installation - Page 2
sa pas lair de marcher, jai été dans mon phpmyadmin et Sql et mis la requete, UPDATE phpbb_users SET `user_password` = "**f71dbe52628a3f83a77ab494817525c6**" ...
forums.phpbb-fr.com/support-installation-phpbb3/sujet155813-15.html - Il y a 2 heures - Pages similaires

Contenu de la table `jacl2_group` -- INSERT INTO `jacl2_group` ...

\r\n', 0, 1209824147, 1, NULL, NULL, NULL, '2.jpg', 0, '', NULL), (3, 'juju', 'juju', '**f71dbe52628a3f83a77ab494817525c6**', 'h', '1986-10-19', ...
forge.jelix.org/svn/wechange/app/install/wechange_install_data.mysql.sql - 6k - En cache - Pages similaires

wechange - Changeset 76 - Jelix Forge - [Traduire cette page]
3, 3, UPDATE membres SET `password`='**f71dbe52628a3f83a77ab494817525c6**'; ... 98, (1, 'bastnic', 'bastnic', '**f71dbe52628a3f83a77ab494817525c6**', 'h', ...
forge.jelix.org/projects/wechange/changeset/76 - 99k - En cache - Pages similaires
Autres résultats, domaine forge.jelix.org »

planet.evolix.org
de hash MD5 au format hexadécimal, **f71dbe52628a3f83a77ab494817525c6** par exemple, ...

Google

f71dbe52628a3f83a77ab494817525c6 Rechercher Recherche avancée Préférences

Rechercher dans : Web Pages francophones Pages : France

Web Résultats **51** - **53** sur **53** pour **f71dbe52628a3f83a77ab494817525c6**. (**0,08** secondes)

password2md5 - password to md5 list(s) - [Traduire cette page]
toto **f71dbe52628a3f83a77ab494817525c6** touchstone
9ad528c46d6714991e0795e3671c5b77 tove a2649d165191e9a91e0e645fb6e18bc6 previous page next page **...**
md5.paniert.org/md5/page2420.php - 148k - En cache - Pages similaires

0b080119cbf1138edfa9132471e1a661 - [Traduire cette page]
f71dbe52628a3f83a77ab494817525c6 == md5("toto"). brīvas gribas cilvēks mūzikas skola pretstraume likumīgums iesoļot rindā labā stavoklī uzsūkšanās haniste **...**
savs.sytes.net/hash/md5/0b080119cbf1138edfa9132471e1a661/tot.htm - 67k - En cache - Pages similaires

phpMyAdmin SQL Dump -- version 2.6.3-pl1 -- http://www.phpmyadmin **...**
-- phpMyAdmin SQL Dump -- version 2.6.3-pl1 -- http://www.phpmyadmin.net -- -- Serveur: nt2r.sql.free.fr -- Généré le : Dimanche 28 Octobre 2007 à 01:12 **...**
nd2r.free.fr/nt2r.sql - Pages similaires

Pour limiter les résultats aux pages les plus pertinentes (total : 53), Google a ignoré certaines pages à contenu similaire.
Si vous le souhaitez, vous pouvez relancer la recherche en incluant les pages ignorées.

◄ Goooooogle
Précédent 1 2 3 4 5 6

f71dbe52628a3f83a77ab494817525c6 Rechercher

Rechercher dans ces résultats | Outils linguistiques | Conseils de recherche

```
  `adminname` varchar(255) collate latin1_general_ci NOT NULL default '',
  `password` varchar(255) collate latin1_general_ci NOT NULL default '',
  PRIMARY KEY  (`ID`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci AUTO_INCREMENT=1 ;

--
-- Contenu de la table `ch_admins`
--


-- --------------------------------------------------------

--
-- Structure de la table `ch_chatters`
--

CREATE TABLE `ch_chatters` (
  `ID` bigint(20) NOT NULL auto_increment,
  `chatter` varchar(255) collate latin1_general_ci NOT NULL default '',
  `password` varchar(255) collate latin1_general_ci NOT NULL default '',
  `email` varchar(255) collate latin1_general_ci NOT NULL default '',
  PRIMARY KEY  (`ID`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci AUTO_INCREMENT=4 ;

--
-- Contenu de la table `ch_chatters`
--

INSERT INTO `ch_chatters` VALUES (1, 'alexandre', '1d17ac8c385815c42f4c92718446dc5b', 'alexandre.baret@free.fr');
INSERT INTO `ch_chatters` VALUES (2, 'malex', 'f71dbe52628a3f83a77ab494817525c6', 'toto@free.fr');
INSERT INTO `ch_chatters` VALUES (3, 'toto', 'f71dbe52628a3f83a77ab494817525c6', 'toto@noos.fr');

-- --------------------------------------------------------

--
-- Structure de la table `ch_messages`
--

CREATE TABLE `ch_messages` (
  `ID` bigint(21) NOT NULL auto_increment,
  `poster` varchar(255) collate latin1_general_ci NOT NULL default '',
  `message` mediumtext collate latin1_general_ci NOT NULL,
  `registered` int(11) NOT NULL default '0',
  `time` bigint(21) default NULL,
```

Failles de cryptographie

- Force brute
  - Rarement utilisée seule
  - Exploit 0-day sur SSL = 16 000 $
- Déchiffrage intelligent
  - Analyse de la durée de l'algorithme
  - Rainbow tables
- Faille dans les algorithmes de cryptographie
  - SSL 1024 inutile si génération de clé incorrecte
  - Difficile d'obtenir du hasard d'un ordinateur
  - Ne surtout jamais créer des algorithmes propriétaires

Principe du moindre privilège

- Si l'application est compromise
  - Ne pas être administrateur
- Principe de la défense en profondeur
  - Moindre privilège multi-niveaux

Conclusion

- L’attaquant a toujours une longueur d’avance
  - Il invente les méthodes
  - Impossible d’être sécurisé à 100 %
- Ratio piratabilité / gain / risque
  - Besoin de l’état de l’art + 1
  - Si le gain est énorme, recours à l’assurance
  - Risque : pour les pirates avant tout
- La sécurité est un vrai métier
  - Mythe du pirate informatique en berne
  - Aujourd’hui : une mafia organisée