3ème année

Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo
CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Présentation du cours (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Présentation du cours (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Plan (1/2)

- **Généralités**
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés
  - Principes de conception et d'utilisation

Un large périmètre d'action

- Actions non-techniques
  - Habilitation des personnes
  - Délégation écrite
  - Contrats
  - Sensibilisation / Formation
  - Enseignement
- Protection
  - Réseau
  - Système
  - Applications
- Surveillance
  - Détection d'intrusion
  - Observation
- Connaissance des agressions
  - Attaques
  - Vulnérabilités / Audit
  - Tests d'intrusion
- Gestion des risques et évaluation

Technologies concrètes

- Firewall
- Détection d'intrusion
- Systèmes d'authentification
- VPN
- Protection des applications
- Administration
- Utilitaires « sécurité » (intégrité, chiffrement, etc.)
- Observation et surveillance réseau

Plan (1/2)

- Généralités
  - **Propriétés de sécurité**
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Propriétés de base - **Confidentialité**

- Propriété d'une information de ne pas être révélée à des utilisateurs non autorisés à la connaître
  - empêcher les utilisateurs de lire une information confidentielle, sauf s'ils y sont autorisés
  - empêcher les utilisateurs autorisés à lire une information confidentielle de la divulguer à des utilisateurs non-autorisés

Propriétés de base - **Intégrité**

- Propriété d'une information d'être exacte
  - empêcher une modification (création ou destruction) indue de l'information (incorrecte ou par des utilisateurs non autorisés)
  - faire en sorte qu'aucun utilisateur ne puisse empêcher une modification légitime

Propriétés de base - **Disponibilité**

- Propriété d'une information d'être accessible quand on en a besoin
  - fournir l'accès à l'information pour que les utilisateurs autorisés puissent la lire ou la modifier
  - faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information

L'information

- Données
  - saisies, générées, stockées, transmises, affichées, ...
- « Méta-données » : associées aux données et utilisées par les services de manipulation
  - identités, noms, adresses (utilisateur, machine, processus, périphériques, etc.)
  - temps (date de l'opération)
  - droits d'accès
  - etc.

Autres propriétés

- Anonymat = confidentialité de l'identité d'un utilisateur
- Protection de la vie privée = confidentialité de (données personnelles + identité de l'utilisateur)
- Authenticité d'un message = intégrité du (contenu + identité de l'émetteur + date + …)
- Authenticité d'un document = intégrité du (contenu + identité du créateur + date + …)
- Authenticité d'un utilisateur = intégrité de l'identité
- « Auditabilité » = disponibilité de (qui, quoi, quand, où, …) d'une action
- Non-répudiation d'origine = disponibilité de (identité de l'émetteur + …) + intégrité du contenu
- Non-répudiation de réception = disponibilité de (identité du récepteur + …) + intégrité du contenu
- Protection de la propriété intellectuelle = confidentialité du contenu (+ intégrité du contenant)

Besoins de sécurité selon les secteurs

- Défense, gouvernement :
  confidentialité ≫ intégrité, disponibilité
- Finance :
  intégrité ≫ disponibilité > confidentialité
- Autres : industrie, administrations, médecine
  ça dépend !

➔ Il faut définir les besoins spécifiques de l'application : Politique de sécurité

Axes d'action théoriques

- Prévention
  - La prévention des fautes vise à empêcher l'occurrence ou l'introduction de fautes.
- Tolérance
  - La tolérance aux fautes correspond à un ensemble de moyens destinés à assurer qu'un système remplit sa fonction en dépit des fautes.
- Élimination
  - L'élimination des fautes vise à réduire le nombre ou la sévérité des fautes.
- Prévision
  - La prévision des fautes vise l'estimation de la présence, la création et les conséquences des fautes.

Plan (1/2)

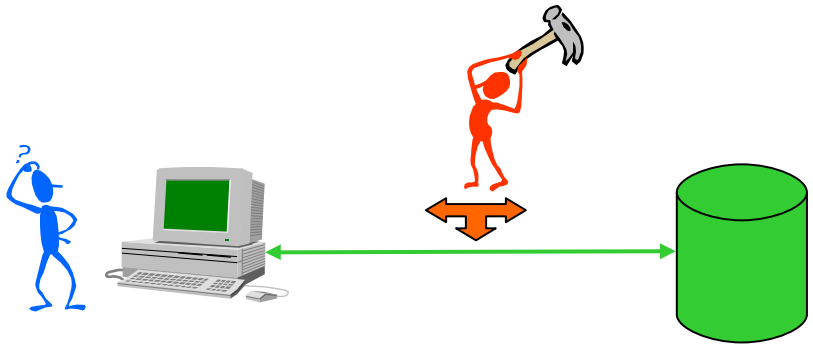
- Généralités
  - Propriétés de sécurité
  - **Attaques**
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Les attaquants et leurs motivations

- Jeu : explorer les limites, éprouver et étendre ses connaissances, découvrir de nouvelles failles, améliorer la sécurité : "hackers" (pirates = "crackers" en fait)
- Émulation, sectarisme : groupe de hackers : "exploits"
- Vandalisme : montrer sa force, punir : "web defacing", virus, vers…
- Politique, idéologie : ex. CCC
- Vengeance
- Profit : espionnage, extorsion de fonds : concurrence déloyale, crime organisé
- Guerre informatique, terrorisme ?
- Sensibilisation, lobbying
- Protection abusive : ex. SONY

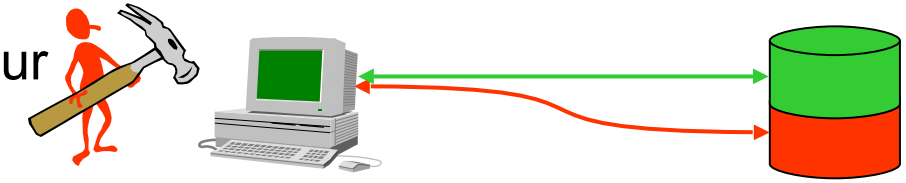
Qui sont les « intrus »?

1: Externe



☺ Authentification
☺ Autorisation

2: Utilisateur



☹ Authentification
☺ Autorisation

3: Utilisateur privilégié

☹ Authentification
☹ Autorisation

80% des fraudes sont "autorisées"

Caractériser des attaquants
[ITSEM 1993, §3.3.29-32, §6.C.28-34]

- compétence
  - profane
  - personne compétente
  - expert
- ressources
  - temps
    - quelques minutes
    - quelques jours
    - quelques mois
  - équipement
    - sans équipement
    - équipement disponible
    - équipement spécial
- opportunités
  - collusion
    - seul
    - avec un utilisateur
    - avec un administrateur
  - chance
  - détection

Niveau de résistance
- élémentaire
- moyenne
- élevée

Des classes d'attaques

- Ecoute passive
- Interception
- Canaux cachés
- Cryptanalyse
- Répudiation
- Inférence
- Déguisement
- Portes dérobées
- Bombe logique
- Cheval de Troie
- Virus
- Ver
- Déni de service
- et attaques complexes...

Bénéfices envisageables

- Gains financiers :
  - Utilisation de numéros de cartes de crédit
  - Chantage, extorsion de fonds, espionnage industriel, …
  - Connexion à des lignes téléphoniques payantes
  - Accès à des comptes (banques, *paypal*, FAI, opérateurs téléphoniques, hotspots, retraites…)
  - Vente d'adresses e-mails : ex. 28 000 $ pour 92 M@ (AOL)
  - Services payants (ex. porno, films piratés…) + *spammers*, …
  - *click fraud* (relais de publicité) : ex : 60 K$ avec 0,4 Mpc
  - Location de botnets, …2004: (IRC) #botz4sale

➔ Correction des failles pour protéger ses revenus

Exemple de phishing

Perfectionnement de Banque AGF en ligne

Cher Client,

Nous poursuivons le perfectionnement de notre site web. Comme vous le savez certainement, Banque AGF vous offre un mécanisme idéal pour une gestion optimisée de votre argent au quotidien.

Chaque jour, nous travaillons pour améliorer notre système et nous voulons vous communiquer les résultats de nos efforts :

- Maintenant, lorsque le solde de votre compte dépasse 750 €, l'exc édent est automatiquement transféré sur votre Compte sur Livret pour vous rapporter des intérêts en restant disponible à tout moment

- Si vous n'avez pas de contrat d'assurance avec Banque AGF, il est temps d'y penser, car vous bénéficierez de conditions privilégiées en passant par notre banque à distance. Découvrez la gamme Privalis maintenant!

- Banque AGF vous présente l'occasion de donner vie à vos projets – les crédits auto et immobiliers sont désormais disponibles 24h/24 et 7j/7. Pour les abonnés de Banque AGF à distance les prêts Reflexis commencent à 2.90% TEG fixe.

- Etez-vous néophite en bourse? Banque AGF en ligne vous présente un guide complet qui vous permettra de comprendre les mécanismes boursiers ainsi que les termes spécifiques. Vous saurez la différence entre les actions nominatives et les bons de souscription et pourrez même acheter des actions en ligne de votre domicile.

De plus, nous avons une offre spéciale pour ceux qui travaillent en situation de mobilité externe, c'est-à-dire avec des assistants numériques personnels (PDA) ou des téléphones portables multifonctions. Dès aujourd'hui vous pouvez consultez vos comptes en utilisant ces appareils.

Pour pouvoir profiter de toutes les nouvelles options, veillez confirmer vos données en passant par le lien en bas de cette page.

Veuillez agréer l'assurance de notre considération distinguée,

Banque AGF

Exemple de phishing (2)

De : PayPal <account.access@paypal.com>
Objet : **Update Your PayPal Account**
Date : 15 novembre 2005 04:38:35 HNEC
Répondre à : no.reply@paypal.com

Dear valued **PayPal®** member:

It has come to our attention that your **PayPal®** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.

Once you have updated your account records, your **PayPal®** session will not be interrupted and will continue as normal.

To update your **PayPal®** records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

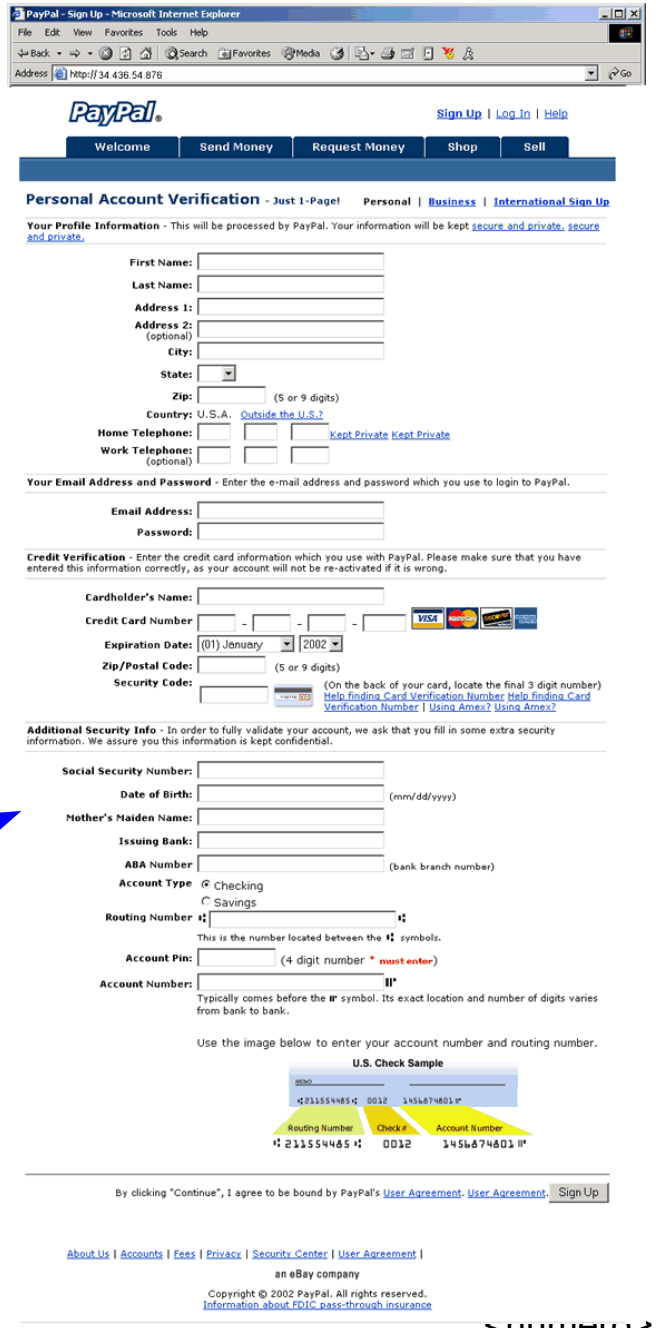
http://61.56.224.108/.cgi-bin/index.php

Thank You.
PayPal® UPDATE TEAM

PayPal®

Accounts Management As outlined in our User Agreement, **PayPal®** will periodically send you information about site changes and enhancements.

TIWECBLOYJFNPOLTYVKULKXJERUNLYISWDTDIR



Exemple de *scam*

DEAR SIR,

URGENT AND CONFIDENTIAL BUSINESS PROPOSAL

I AM MARIAM ABACHA, WIDOW OF THE LATE NIGERIAN HEAD OF STATE, GEN. SANI ABACHA. AFTER HE DEATH OF MY HUSBAND WHO DIED MYSTERIOUSLY AS A RESULT OF CARDIAC ARREST, I WAS INFORMED BY OUR LAWYER, BELLO GAMBARI THAT, MY HUSBAND WHO AT THAT TIME WAS THE PRESIDENT OF NIGERIA, CALLED HIM AND CONDUCTED HIM ROUND HIS APARTMENT AND SHOWED HIM FOUR METAL BOXES CONTAINING MONEY ALL IN FOREIGN EXCHANGE AND HE EQUALLY MADE HIM BELIEVE THAT THOSE BOXES ARE FOR ONWARD TRANSFER TO HIS OVERSEAS COUNTERPART FOR PERSONAL INVESTMENT.

ALONG THE LINE, MY HUSBAND DIED AND SINCE THEN THE NIGERIAN GOVERNMENT HAS BEEN AFTER US, MOLESTING, POLICING AND FREEZING OUR BANK ACCOUNTS AND EVEN MY ELDEST SON RIGHT NOW IS IN DETENTION. MY FAMILY ACCOUNT IN SWITZERLAND WORTH US$22,000,000.00 AND 120,000,000.00 DUTCH MARK HAS BEEN CONFISCATED BY THE GOVERNMENT. THE GOVERNMENT IS INTERROGATING HIM (MY SON MOHAMMED) ABOUT OUR ASSET AND SOME VITAL DOCUMENTS. IT WAS IN THE COURSE OF THESE, AFTER THE BURIAL RITE AND CUSTOMS, THAT OUR LAWYER SAW YOUR NAME AND ADDRESS FROM THE PUBLICATION OF THE NIGERIAN BUSINESS PROMOTION AGENCY. THIS IS WHY I AM USING THIS OPPORTUNITY TO SOLICIT FOR YOUR CO-OPERATION AND ASSISTANCE TO HELP ME AS A VERY SINCERE RESPONSIBLE PERSON. I HAVE ALL THE TRUST IN YOU AND I KNOW THAT YOU WILL NOT SIT ON THIS MONEY.

I HAVE SUCCEEDED IN CARRYING THE FOUR METAL BOXES OUT OF THE COUNTRY, WITH THE AID OF SOME TOP GOVERNMENT OFFICIAL, WHO STILL SHOW SYMPATHY TO MY FAMILY, TO A NEIGHBOURING COUNTRY (ACCRA-GHANA) TO BE PRECISE. I PRAY YOU WOULD HELP US IN GETTING THIS MONEY TRANSFERRED OVER TO YOUR COUNTRY. EACH OF THESE METAL BOXES CONTAINS US$5,000,000.00 (FIVE MILLION UNITED STATES DOLLARS ONLY) AND TOGETHER THESE FOUR BOXES CONTAIN US20,000,000.00(TWENTY MILLION UNITED STATESDOLLARS ONLY). THIS IS ACTUALLY WHAT WE HAVE MOVED TO GHANA.

THEREFORE, I NEED AN URGENT HELP FROM YOU AS A MAN OF GOD TO HELP GET THIS MONEY IN ACCRA GHANA TO YOUR COUNTRY. THIS MONEY, AFTER GETTING TO YOUR COUNTRY, WOULD BE SHARED ACCORDING TO THE PERCENTAGE AGREED BY BOTH OF US.PLEASE NOTE THAT THIS MATTER IS STRICTLY CONFIDENTIAL AS THE GOVERNMENT WHICH MY LATE HUSBAND WAS PART OF IS STILL UNDER SURVAILLANCE TO PROBE US.

YOU CAN CONTACT ME THROUGH MY FAMILY LAWYER AS INDICATED ABOVE AND ALSO TO LIAISE WITH HIM TOWARDS THE EFFECTIVE COMPLETION OF THIS TRANSACTION ON TEL/FAX NO:xxx-x-xxxxxxx AS HE HAS THE MANDATE OF THE FAMILY TO HANDLE THIS TRANSACTION.

THANKS AND BEST REGARD

MRS. MARIAM ABACHA

☺ Parfois: recel et blanchiment d'argent !

http://www.joewein.de/sw/spam.htm

Exemple : *Cross Site Scripting*

http://www.cert.org/advisories/CA-2000-02.html

- Un pirate crée un script caché dans un message (ex: HTML tags "`SCRIPT`" et "`/SCRIPT`").
- Il l'enregistre sur un serveur innocent (ex: blog, forum, …).
- La victime lit le message avec un browser configuré pour permettre l'exécution de scripts...
- La victime peut aussi s'auto-scripter (ex: par phishing) :

```
<A HREF="http://example.com/comment.cgi?
mycomment=<SCRIPT>malicious code</SCRIPT>"> Click here</A>
```

Gagner en crédibilité

1 comment:

Peter Parker 2 December 2014 02:53

Hello your blog is sharing great information. Thanks for share this blog, Scommesse Online providing best Trading Business in Italy

Scommesse

Reply

Exemples de patch/bug

- Origine : OpenBSD (2006, 2007)
- Correction du serveur httpd (patch)
  - Absence de nettoyage d'un header HTTP (Expect:)
  - Possibilité de XSS
  - CVE-2006-3918
- Correction de ld.so (patch)
  - Nettoyage de l'environnement
  - Exploitable ?
- Correction de la commande file (patch)
  - Débordement de pile
  - CVE-2007-1536

Exemples d'attaques

- Essais répétitifs (*brute force*) : script expect
- Interactions script système et bug (patch) : programme C
- Programme Windows (injection DLL)
- Fichier image

  http://www.determina.com/security.research/vulnerabilities/ani-header.html

Curseur ANImé sous Windows (1/3)
CVE-2007-0038 (CVE-2005-0416 bis)

```
struct ANIChunk
{
    char  tag[4];         // ASCII tag
    DWORD size;           // length of data in bytes
    char  data[size];     // variable sized data
}

int LoadCursorIconFromFileMap(struct MappedFile* file, ...)
{
    struct ANIChunk  chunk;
    struct ANIHeader header;        // 36 byte structure
    ...
    // read the first 8 bytes of the chunk
    ReadTag(file, &chunk);

    if (chunk.tag == 'anih') {

+       if (chunk.size != 36)       // added in MS05-002
+           return 0;

        // read chunk.size bytes of data into the header struct
        ReadChunk(file, &chunk, &header);
```

Curseur ANImé sous Windows (2/3)
CVE-2007-0038 (CVE-2005-0416 bis)

```
int LoadAniIcon(struct MappedFile* file, ...)
{
    struct ANIChunk  chunk;
    struct ANIHeader header;        // 36 byte structure
    ...
    while (1) {
        // read the first 8 bytes of the chunk
        ReadTag(file, &chunk);
        switch (chunk.tag) {
            case 'seq ':
                ...
            case 'LIST':
                ...
            case 'rate':
                ...
            case 'anih':
                // read chunk.size bytes of data into the header
  struct
                ReadChunk(file, &chunk, &header);
```

Curseur ANImé sous Windows (3/3)
CVE-2007-0038 (CVE-2005-0416 bis)

- LoadCursorIconFromFileMap appelle LoadAniIcon
- LoadCursorIconFromFileMap ne valide que le *premier* fragment `anih`
- Un fichier .ANI :

```
00000000   52 49 46 46  90 00 00 00  41 43 4F 4E  61 6E 69 68   RIFF....ACONanih
00000010   24 00 00 00  24 00 00 00  02 00 00 00  00 00 00 00   $...$...........
00000020   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000030   00 00 00 00  01 00 00 00  61 6E 69 68  58 00 00 00   ........anihX...
00000040   41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41   AAAAAAAAAAAAAAAA
00000050   41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41   AAAAAAAAAAAAAAAA
00000060   00 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41   .AAAAAAAAAAAAAAA
00000070   41 41 41 41  41 41 41 41  41 41 41 41  00 00 00 00   AAAAAAAAAAAA....
00000080   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000090   42 42 42 42  43 43 43 43                            BBBBCCCC
```

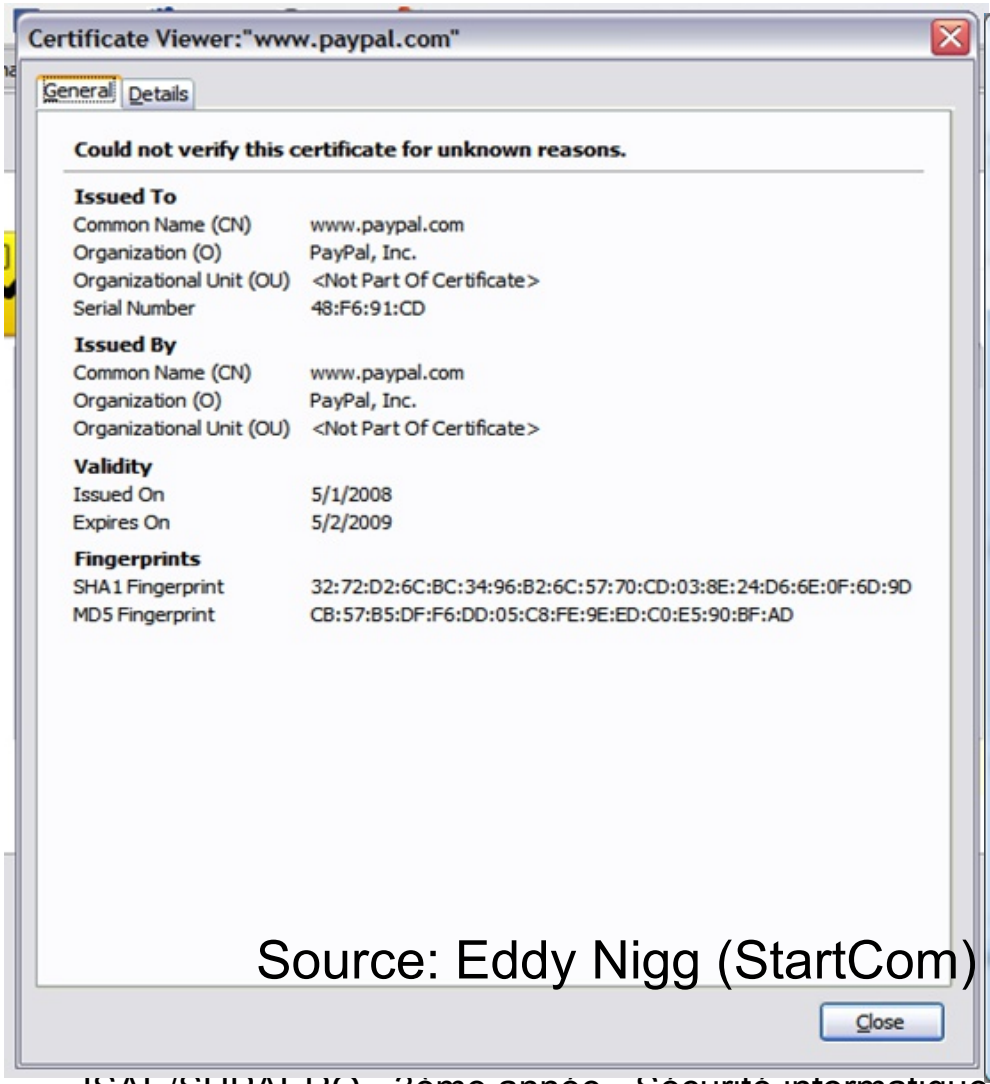
- NB: Evite les protections contre les débordements du compilateur Vista (/GS) centrées sur les tableaux (et non les struct). Bug situé dans un code tolérant les exceptions

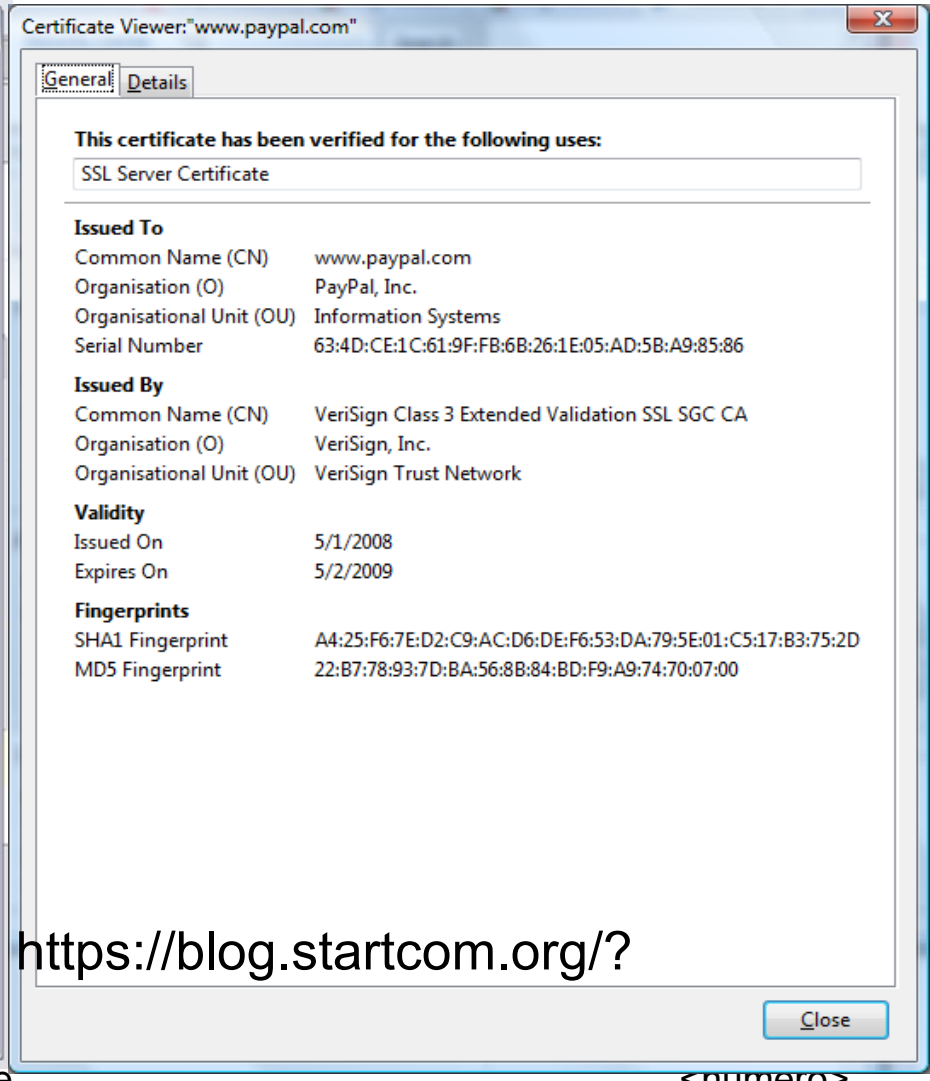
Falsification d'empreintes digitales

- Objectif : tromper un lecteur d'empreinte de PC
- Matériel
  - Verre propre
  - (Vapeur de) Colle cyanocrylate
  - Appareil photo numérique
  - PC, imprimante laser, transparent
  - Colle à bois

    http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en
- Et c'est là une méthode « sophistiquée » (par opposition à la pâte à modeler, la buée)

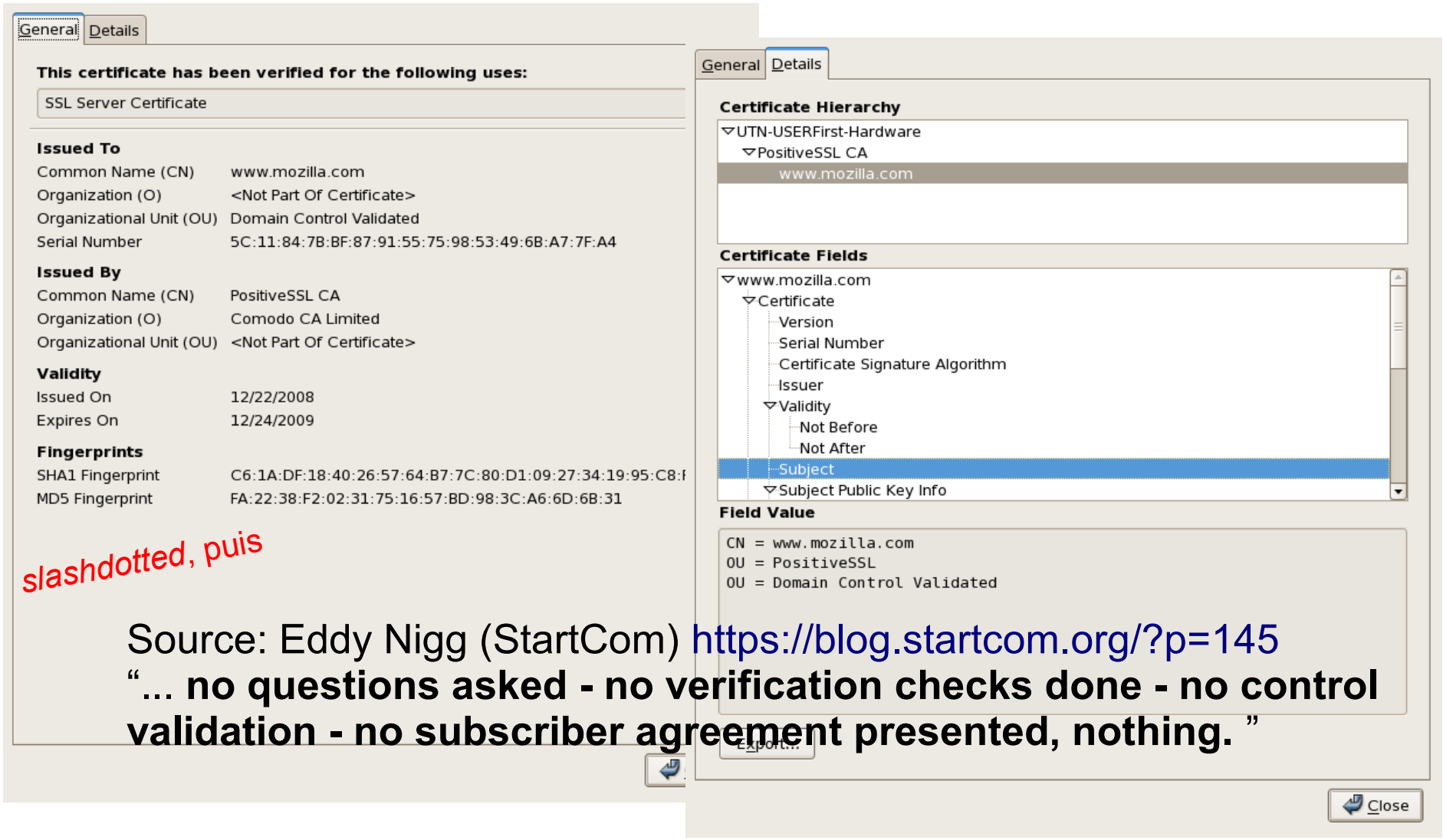
Présentation et certificats





Source: Eddy Nigg (StartCom) https://blog.startcom.org/?

Délivrance des certificats



slashdotted, puis

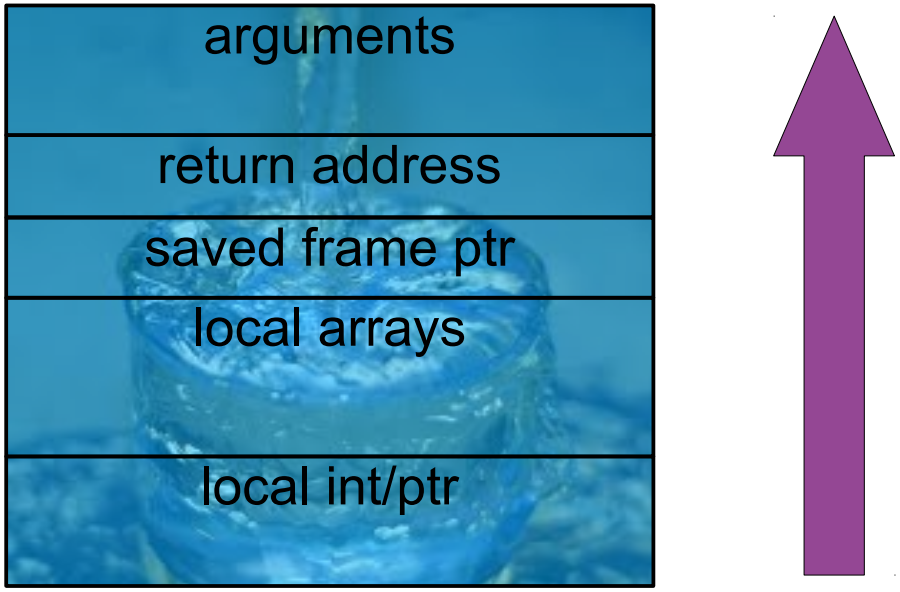
Source: Eddy Nigg (StartCom) https://blog.startcom.org/?p=145

“... no questions asked - no verification checks done - no control validation - no subscriber agreement presented, nothing. ”

Buffer Overflow – Un exemple

- Fonctionnement d'un appel de fonction (C)
  - Sauvegarde des registres généraux sur la pile
  - Calcul de l'adresse de retour et sauvegarde sur la pile
  - Empilement des paramètres d'appel de la fonction
  - Les variables locales et les tableaux sont également stockés sur la pile
- L'ordre exact dépend du contexte, mais l'idée générale est toujours la même

Disposition de la pile



Contrived example

```
void function(char* str) {
   char buffer[16] ;
   strcpy(buffer, str) ;
 }
int main(void) {
   /* lenght of str > 16 bytes */
   char* s = "Je ne fais pas moins de 16
   caractères.";
   function(s) ;
}
```

Vulnérabilité de ce type de code?

- Le résultat n'est pas toujours prévisible
- On écrit dans des zones mémoires non prévues pour cela
- Avons-nous écrasé l'adresse de retour ?
- Avec des valeurs d'entrées choisies très soigneusement, on peut fixer le point de retour de la suite du programme
- Cela peut se situer dans du code contrôlé par l'utilisateur, si celui-ci à réussi à la faire rentrer en mémoire.
  - Sinon, on se débrouille autrement

Format strings

```
int function(char* str) {
   fprintf(stdout, str) ;
}
```

- Que se passe t'il quand :
  `str = "%s%s%s%s%s";`

- Le plus probable : une erreur fatale
- Sinon : impression du contenu de la mémoire

- NB : forme correcte
  `fprintf(stdout, "%s", str);`

Prévention

- Attention en écrivant dans des tampons mémoire
  - Le contrôle de la longueur des entrées est obligatoire
- Ne jamais utiliser de trucs en C
- strcpy() et strcat() sont interdits
  - Utiliser strlcpy() et strlcat()
  - Si vous en disposez...

Hack1ng R0x

- Buffer overflows (exemple SSL, exemple)
- Format strings (exemple, exemple)
- Etc.

Lisez `Phrack`

- Une autre référence plus académique

How to 0wn the Internet in your Spare Time,
Staniford, Paxson, Weaver, 11th Usenix Security Symposium, 2002.

Fun with NULL pointers

- Linux 2.6.30 kernel local root exploit
- Brad Spengler
  - cheddar_bay.tgz
  - http://lwn.net/Articles/341773/
- Jonathan Corbet, LWN.net, 20&21 juillet 2009
  - Part 1 http://lwn.net/Articles/342330/
  - Part 2 http://lwn.net/Articles/342420/
- Comments from various readers

Actualités 2010

- Stuxnet (1° vue)
- Phishing visant la CAF
- Les états d'âmes de Linux
- Google part de Chine
- GSM et la sécurité

Some news 2010/2011
with 2012 update

- New or significant failures
  - Compromised, abused (Comodo, DigiNotar) or doubtful *Internet* certification authorities
    - *Business as usual or bankruptcy*
  - Intrusion at Bercy (G20 organization)
    - *nothing*
  - *Sony PlayStation Network*
    - Personal data of 77 millions users stolen
    - *« Welcome back » package, class action running*
  - STARS / Stuxnet
    - Very specific worm targeting critical industrial control systems
    - *NYT reports combined U.S./Israeli intelligence operation running under two different presidents (01/06/12)*

Some news 2010/2011

- State communication
  - *La sécurité dans le cyberspace, un enjeu stratégique,* Lettre du Secrétaire Général de la Défense et de la Sécurité Nationale (SGDSN), fin 2010
  - Communication du Premier ministre relative à la protection des systèmes d'information au Conseil des ministres du 25 mai 2011
    - *ANSSI hires, gets a new building and plays Antigone...*
    - *ANSSI does cryptanalysis research (!)*
  - In summer 2011, the *Department of Transport* launched a call for proposals with respect to cars (cyber) security
    - *Summer 2012 : WiFi linked vehicle test*

Hackers interests

- Latest hackers security conferences (ie. DEFCON & BlackHat 2011)
  - Home automation security (especially X10 over CPL systems)
  - Car alarms
  - Insulin pumps
  - Autonomous WiFi+GSM sniffing drone

DEFCON 2012

- *NFCs, anti-forensics, gen. Keith Alexander*

Some 2012 academic research

- I/O based attacks
  - Do not involve the CPU... at all
- PMAT security
  - Portable Maintenance Terminal (probably)
  - The problem domain starts to get interesting

(Old version)

2013, of course

IETF 88 Technical plenary: Hardening the Internet

http://www.nsa.gov/about/cryptologic_heritage/women/honorees/index.shtml

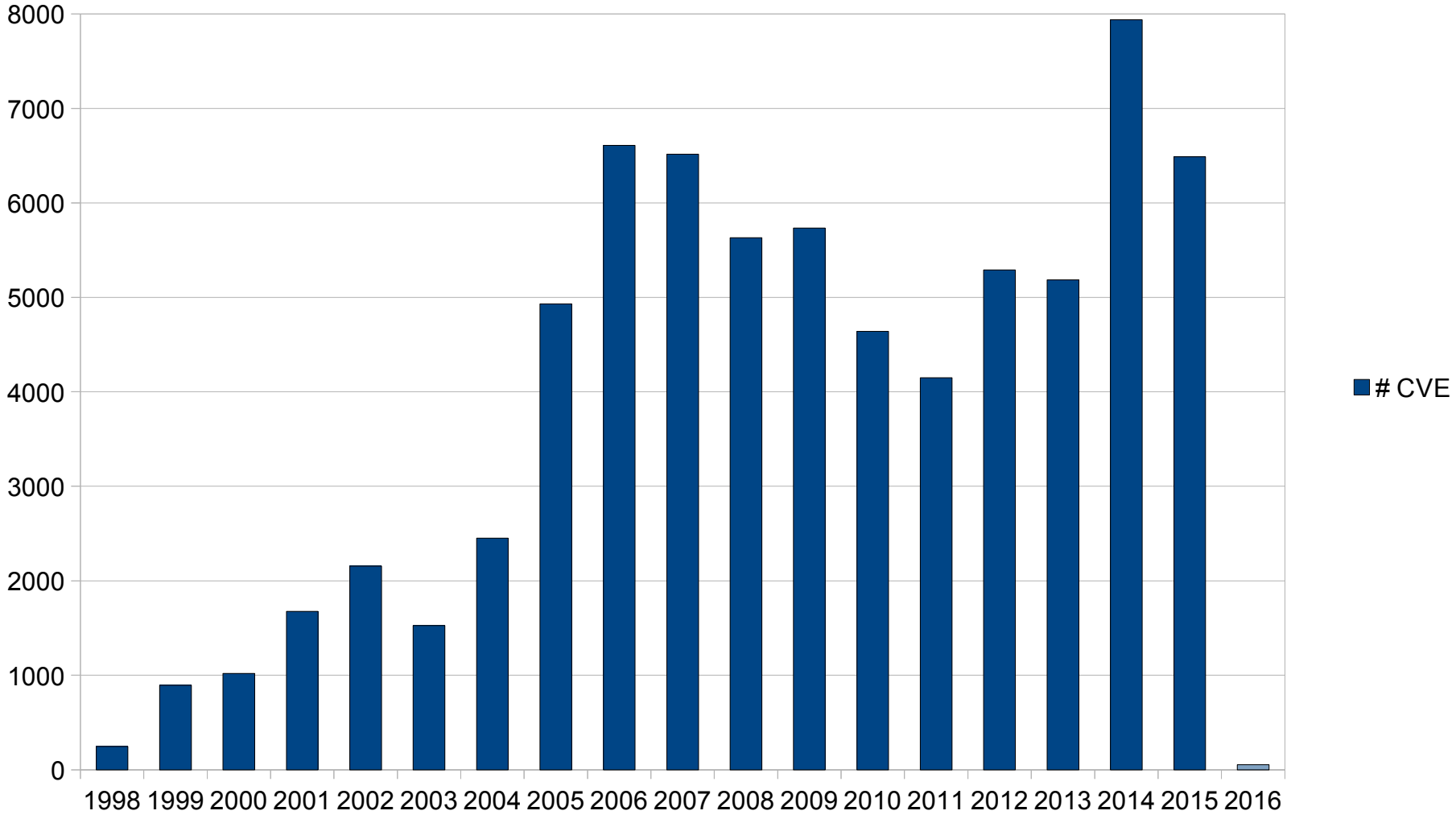
2014

- Microsoft OSes expose a significant vulnerability from Windows 95 onward
  - CVE-2014-6332
  - 19 years, some BSD code has already revealed things (probably) older in the past years
  - But where is the continuous improvement promised by commercial companies?
  - And why are there still older versions in production with no fixes (and possibly more bugs)?
- OpenSSL/LibreSSL fork
  and a record broken... (cf. infra)

2015

- Innovations (?) in the automotive industry
  - VW
  - Jeep
- Reminder
  - Physical security > Org. security > Logical security

Vulnerabilities



Source:

Une dernière...

« The final step (…) simply adds a second Trojan horse to the one that already exists. The second pattern is aimed at the C compiler. The replacement code is a (…) self-reproducing program that inserts both Trojan horses in the compiler. (…) First we compile the modified source with the normal C compiler to produce a bugged binary. We install this binary as the official C. We can now remove the bugs from the source of the compiler and the new binary will reinsert the bugs whenever it is compiled. Of course, the login command will remain bugged with no trace in source anywhere. »

Morale

« *You can't trust code that you did not totally create yourself.*
(Especially code from companies that employ people like [him].) »

Ken Thomson, Reflections on Trusting Trust, *Turing award lecture*, in *Communications of the ACM*, vol.27, no.8, pp.761-763, August 1984.