HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

# La sécurité par TLS, un voeu pieu ?

christophe.renard@hsc.fr

Hervé Schauer Consultants

20 mars 2014

# Agenda

Introduction

Les menaces

Couches de TLS

Que faire

Références

# Pourquoi

Cette présentation est née de la combinaison de deux expériences :

- Le constat d'une incertitude répandue quand à la fiabilité de SSL et TLS
- Des audits de code applicatif se comportant en client SSL

# Le doute

Le doute est à la mode :

- Révélations de E.Snowden sur la NSA
  - interception de quasiment tout traffic non chiffré,
  - efforts significatifs sont mis en oeuvre pour s'approprier des clés privées,
  - attaques en MitM courantes,
  - la NSA à fait une perçée importante en cryptanalyse en 2010,
  - quand possible, les mécanismes cryptographiques sont piégés.
- Cumul des annonces de failles
  - Failles protocolaires : BEAST, Lucky13, CRIME, TIME, BREACH
  - Apple - Goto fail
  - GnuTLS - type de retour

# Le doute

Le doute est à la mode :

- Révélations de E.Snowden sur la NSA
  - interception de quasiment tout traffic non chiffré,
  - efforts significatifs sont mis en oeuvre pour s'approprier des clés privées,
  - attaques en MitM courantes,
  - la NSA à fait une perçée importante en cryptanalyse en 2010,
  - quand possible, les mécanismes cryptographiques sont piégés.
- Cumul des annonces de failles
  - Failles protocolaires : BEAST, Lucky13, CRIME, TIME, BREACH
  - Apple - Goto fail
  - GnuTLS - type de retour

# Les audits

- Audits de source : implémentation défaillantes
- Recommandations de correction
  - Facile : corrigez la ligne 123 pour passer le paramètre 435
  - Complexe : activez toujours toutes les options correctes
- La systématisation est difficile.
- Les API en sont largement responsables
  (pour ne pas parler de CURL)

# Spoiler

- L'utilisation d'un TLS sécurisé en 2014 relève-t-elle du voeu pieu ?
- Non
- Mais elle est anormalement complexe.
- Surtout pour les développeurs.

# Spoiler

- L'utilisation d'un TLS sécurisé en 2014 relève-t-elle du voeu pieu ?
- Non
- Mais elle est anormalement complexe.
- Surtout pour les développeurs.

# Spoiler

- L'utilisation d'un TLS sécurisé en 2014 relève-t-elle du voeu pieu ?
- Non
- Mais elle est anormalement complexe.
- Surtout pour les développeurs.

# Les menaces

# Quelles sont les attaques ?

Deux types d'attaques bien distinctes :

- Attaques actives
  - ne se pratiquent qu'en temps réel
  - donc ciblées sur une communication particulière
  - impraticable sur des masses de communication.
- Attaques passives
  - en deux temps : collecte / traitement
  - le traitement peut être trivial : si on récupère les clés
    ce qui se prête bien aux aux attaques de masse
  - sinon trés calculatoire : cryptanalyse
    nécessite un mécanisme faible
    ou une porte dérobée

Toutes les attaques exploitent une vulnérabilité.

# Quelles sont les attaques ?

Deux types d'attaques bien distinctes :

- Attaques actives
  - ne se pratiquent qu'en temps réel
  - donc ciblées sur une communication particulière
  - impraticable sur des masses de communication.
- Attaques passives
  - en deux temps : collecte / traitement
  - le traitement peut être trivial : si on récupère les clés
    ce qui se prête bien aux aux attaques de masse
  - sinon trés calculatoire : cryptanalyse
    nécessite un mécanisme faible
    ou une porte dérobée

Toutes les attaques exploitent une vulnérabilité.

# Voie d'attaque royale

- Compromission d'une des extrémités de la communication
- Ce n'est pas l'objet de cette présentation
- Peut être de peu d'intérêt après la transmission d'une information.

# Une approche par couches

# Couches d'un système cryptographique

- Algorithmes
- Mécanismes cryptographiques
- Protocoles
- Implémentation
- Intégration
- Configuration
- Opération

(Basé sur une idée originale de Matthew Green)

# Couches d'un système cryptographique

- Algorithmes
- Mécanismes cryptographiques
- Protocoles
- Implémentation
- Intégration
- Configuration
- Opération

(Basé sur une idée originale de Matthew Green)

# Couches d'un système cryptographique

- Algorithmes
- Mécanismes cryptographiques
- Protocoles
- Implémentation
- Intégration
- Configuration
- Opération

(Basé sur une idée originale de Matthew Green)

# Couches d'un système cryptographique

- Algorithmes
- Mécanismes cryptographiques
- Protocoles
- Implémentation
- Intégration
- Configuration
- Opération

(Basé sur une idée originale de Matthew Green)

# Couches d'un système cryptographique

- Algorithmes
- Mécanismes cryptographiques
- Protocoles
- Implémentation
- Intégration
- Configuration
- Opération

(Basé sur une idée originale de Matthew Green)

# Couches d'un système cryptographique

- Algorithmes
- Mécanismes cryptographiques
- Protocoles
- Implémentation
- Intégration
- Configuration
- Opération

(Basé sur une idée originale de Matthew Green)

# Couches d'un système cryptographique

- Algorithmes
- Mécanismes cryptographiques
- Protocoles
- Implémentation
- Intégration
- Configuration
- Opération

(Basé sur une idée originale de Matthew Green)

# Algorithmes

- Briques de base,
- Essentiellement maitrisées par des cryptographes purs,
- Choix faisant l'objet de réflexions et vérifications lourdes,
- Failles rares, mais catastrophiques,
- Algorithmes obsolètes de TLS
  - DES, RSA-MD2, RSA-MD5, RC2, RC4
- Choix
  - Négociation de clé : ECDHE, DHE
  - Authentification : RSA-SHA-1, RSA-SHA-256
  - Chiffrement : AES, CAMELLIA
  - Intégrité : HMAC(SHA-1), HMAC(SHA-256)
  - Futur(TLS-1.3 ?) : Chacha20, Poly1305, Salsa20

# RC4 must die !

- RC4 est rapide.
- RC4 est facile d'implémentation.
- RC4 est plus vieux que HSC (27ans).
- RC4 est cassé :
  - 1995 - *Roos* - clés faibles
  - 2001 - *Fluhrer Mantin et Shamir* - Attaque FMS - Souvernirs de WEP
  - 2005 - *Klein* - Extension de l'attaque de Roos
  - 2013 - *AlFardan, Bernstein, Paterson et al.* - Attaque statistique pratique récupérant le clair

# Mécanismes cryptographiques

- Assemblages de confiance,
- Maitrisé par les spécialistes de cryptographie appliquée,
- Assure l'usage correct des algorithmes de base.
- Exemples : AES-CBC, signature RSA SSA-PKCS1-v1.5
- On preferera des modes authentifiants.
- Choix :
  - Chiffrement : AES-GCM, CAMELLIA-GCM

    (AES-CCM bon candidat est très peu supporté)
  - Futur (TLS-1.3 ?) : Salsa20+HMAC(SHA-256), Chacha20+Poly1305
  - Dilemne : Vieux navigateurs et quelques bibliothèques AES absent, CBC seul mode, restent DES3 et ... RC4

# Protocoles

- Combine des contraintes de fonction, de performance, compatibilité.
- Souvent conçu par des spécialistes réseau ou système.
- Choix basés sur les propriétés assumées des mécanismes.
- Choix fondamental de TLS
  - mac-then-encrypt : attaques à chiffré choisit possibles
- Exemples :
  - 2009 - Vulnerabilité sur les renégociations

    (CVE-2009-3555, RFC-5746)
  - Toutes les attaques sur CBC

    (CVE-2011-3389, CVE-2012-4929, CVE-2013-0169...)
  - 2014 - Vulnérabilité sur la reprise sécurisée (IETF89)

# Protocoles : Choix

- Compression dans SSL/TLS
  - Désactiver.
  - `SSLCompression off`
- Renégociation sécurisées
  - Exiger
  - `SSLInsecureRenegotiation off`
- *OCSP Stappling*
  - Actif (si votre AC fait de l'OCSP)
  - `SSLUseStapling on`

# Implémentation

- Implémente protocoles et mécanismes.
- Développeurs sensibilisés et/ou spécialistes.
- Code complexe à écrire et contre-intuitif.
- Peu de vérifications (surtout publiques).
- Des failles lourdes, comme les deux dernières en date :
  - Apple - *goto fail*

    CVE2014-1266
  - GnuTLS - *bool is not int*

    CVE-2014-0092 - `http://gnutls.org/security.html`

    Seconde entrée : Tous les certificats X509v1 étaient des AC potentielles....

# Intégration

- Les développeurs des bibliothèques sont censés être des spécialistes
- Pas ceux des applications
- Les développeurs de navigateurs sont les exceptions (depuis peu)
- 2012, *The most dangerous code in the world, validating SSL certificates in non-browser software*
- Et si vous développez en Java ?
  - Java 6 ?
  - Android ? (quelle version ?)

# Vérifier une signature

Vérifications :

- Signature
- Signature du certificat
- Validité
- Révocation
- Identité du signataire
- Usages
- Vérification des AC : itérativement identique
  En vérifiant profondeur et attribut d'AC

# Vérifier une signature

Vérifications :

- Signature
- Signature du certificat
- Validité
- Révocation
- Identité du signataire
- Usages
- Vérification des AC : itérativement identique
  En vérifiant profondeur et attribut d'AC

# Vérifier une signature

Vérifications :

- Signature
- Signature du certificat
- Validité
- Révocation
- Identité du signataire
- Usages
- Vérification des AC : itérativement identique
  En vérifiant profondeur et attribut d'AC

# Vérifier une signature

Vérifications :

- Signature
- Signature du certificat
- Validité
- Révocation
- Identité du signataire
- Usages
- Vérification des AC : itérativement identique
  En vérifiant profondeur et attribut d'AC

# Vérifier une signature

Vérifications :

- Signature
- Signature du certificat
- Validité
- Révocation
- Identité du signataire
- Usages
- Vérification des AC : itérativement identique
  En vérifiant profondeur et attribut d'AC

# Vérifier une signature

Vérifications :

- Signature
- Signature du certificat
- Validité
- Révocation
- Identité du signataire
- Usages
- Vérification des AC : itérativement identique
  En vérifiant profondeur et attribut d'AC

# Vérifier une signature

Vérifications :

- Signature
- Signature du certificat
- Validité
- Révocation
- Identité du signataire
- Usages
- Vérification des AC : itérativement identique
  En vérifiant profondeur et attribut d'AC

# Les APIs

- Les librairies SSL/TLS sont peu ou mal documentées.
- Leur code est complexe à lire.
- Besoin :
  - Choisir la meilleure suite cryptographique dans une liste ordonnée,
  - Spécifier la liste des AC utilisées,
  - Vérifier le certificat et la signature de requête par défaut,
  - Communiquer sur une socket TLS
- Difficile de trouver une API satisfaisante.

# Configuration

- Le sujet commence à être maitrisé
- 3 cibles principales : Apache, Nginx, IIS
- Problème des serveurs d'application
  - moins bien maitrisés,
  - dépendant de la version de Java.
- A configurer sur un serveur
  - Chaine de certification
  - Options de renegociation (sécurisée uniquement)
  - Options de compression (désactivée)
  - Suites cryptographiques acceptées
  - Paramètres Diffie-Hellman
  - *OCSP stapling*

# Opérations

- Fiabilité des autorités de certification
  - Diginotar
  - Comodo
- Gestion des certificats sur les serveurs
- Architectures réseau complexes
- Certificats autosignés légitimes
  - particuliers : plus aujourd'hui
  - interfaces de configuration d'appliances
- Problème lourd d'Interface Homme Machine

# Que faire

# Failles/Mesures 1/2

Par difficulté d'exploitation croissante

- Mécanisme nuls ou trés faibles
  - Configuration des serveurs
- Autorités de certification peu fiables
  - AC interne ou voir les éditeurs
- Certificats invalides
  - Vérificateur
- Certificats révoqués
  - Vérificateur
- Certificat usurpés (cryptographiquement valides)
  - Vérificateur/DANE/Notaries/AC interne

# Failles/Mesures 1/2

Par difficulté d'exploitation croissante

- Mécanisme nuls ou trés faibles
  - Configuration des serveurs
- Autorités de certification peu fiables
  - AC interne ou voir les éditeurs
- Certificats invalides
  - Vérificateur
- Certificats révoqués
  - Vérificateur
- Certificat usurpés (cryptographiquement valides)
  - Vérificateur/DANE/Notaries/AC interne

# Failles/Mesures 1/2

Par difficulté d'exploitation croissante

- Mécanisme nuls ou trés faibles
  - Configuration des serveurs
- Autorités de certification peu fiables
  - AC interne ou voir les éditeurs
- Certificats invalides
  - Vérificateur
- Certificats révoqués
  - Vérificateur
- Certificat usurpés (cryptographiquement valides)
  - Vérificateur/DANE/Notaries/AC interne

# Failles/Mesures 1/2

Par difficulté d'exploitation croissante

- Mécanisme nuls ou trés faibles
  - Configuration des serveurs
- Autorités de certification peu fiables
  - AC interne ou voir les éditeurs
- Certificats invalides
  - Vérificateur
- Certificats révoqués
  - Vérificateur
- Certificat usurpés (cryptographiquement valides)
  - Vérificateur/DANE/Notaries/AC interne

# Failles/Mesures 1/2

Par difficulté d'exploitation croissante

- Mécanisme nuls ou trés faibles
  - Configuration des serveurs
- Autorités de certification peu fiables
  - AC interne ou voir les éditeurs
- Certificats invalides
  - Vérificateur
- Certificats révoqués
  - Vérificateur
- Certificat usurpés (cryptographiquement valides)
  - Vérificateur/DANE/Notaries/AC interne

# Failles/Mesures 2/2

- Versions obsolètes du protocole
  - Désactiver
- Récupération des clés privées
  - ECDHE, DHE, HSM
- Suites cryptographiques faibles
  - Désactiver, si possible
- Autorités de certification piratées
  - DANE/Notaries/AC interne
- Générateur aléatoire piègé ou défaillant
  - Voir avec l'éditeur (arcfour, IOS7 ?)

# Failles/Mesures 2/2

- Versions obsolètes du protocole
  - Désactiver
- Récupération des clés privées
  - ECDHE, DHE, HSM
- Suites cryptographiques faibles
  - Désactiver, si possible
- Autorités de certification piratées
  - DANE/Notaries/AC interne
- Générateur aléatoire piégé ou défaillant
  - Voir avec l'éditeur (arcfour, IOS7 ?)

# Failles/Mesures 2/2

- Versions obsolètes du protocole
  - Désactiver
- Récupération des clés privées
  - ECDHE, DHE, HSM
- Suites cryptographiques faibles
  - Désactiver, si possible
- Autorités de certification piratées
  - DANE/Notaries/AC interne
- Générateur aléatoire piègé ou défaillant
  - Voir avec l'éditeur (arcfour, IOS7 ?)

# Failles/Mesures 2/2

- Versions obsolètes du protocole
  - Désactiver
- Récupération des clés privées
  - ECDHE, DHE, HSM
- Suites cryptographiques faibles
  - Désactiver, si possible
- Autorités de certification piratées
  - DANE/Notaries/AC interne
- Générateur aléatoire piégé ou défaillant
  - Voir avec l'éditeur (arcfour, IOS7 ?)

# Failles/Mesures 2/2

- Versions obsolètes du protocole
  - Désactiver
- Récupération des clés privées
  - ECDHE, DHE, HSM
- Suites cryptographiques faibles
  - Désactiver, si possible
- Autorités de certification piratées
  - DANE/Notaries/AC interne
- Générateur aléatoire piégé ou défaillant
  - Voir avec l'éditeur (arcfour, IOS7 ?)

# Perspectives

- Prise de conscience chez les éditeurs de navigateur
  réactions au attaques de 2011 lors des élections iraniennes
  - Durcissement de la politique à l'égard des AC
  - Décollage des initiatives de confirmation de certificats (notaries, DANE)
- Evolution vers TLS 1.2
  - Pas vue comme urgente
  - Jusqu'a CRIME
  - Et les révélations de Snowden
- Le futur : HTTP 2.0 et TLS 1.3
- Quid des vieux navigateurs ?

# Références

# Références : Failles 1/2

- Insecure resumption IETF89
  - `https://secure-resumption.com/`
- *Matthew Green, How does NSA break TLS ?*
  - `http://blog.cryptographyengineering.com/2013/12/how-does-nsa-break-ssl.html`
- Diginotar - *Fox-IT - Black Tulip repport*
  - `http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf`

# Références : Failles 2/2

- Bugs GnuTLS
  - `http://blog.existentialize.com/the-story-of-the-gnutls-bug.html`
- Bug Apple
  - `https://www.imperialviolet.org/2014/02/22/applebug.html`

# Références : Futur

- TLS 1.3
  - `http://www.ietf.org/proceedings/89/slides/slides-89-tls-5.pdf`
- Salsa20 dans TLS
  - `http://tools.ietf.org/html/draft-josefsson-salsa20-tls-04`
- Chacha20 et Poly1305 pour TLS et implémentation
  - `https://www.imperialviolet.org/2013/10/07/chacha20.html`
  - `https://tools.ietf.org/html/draft-agl-tls-chacha20poly1305-04`
- OpenBSD Dec. 2013 *Belopuhov - Where is crypto headed*
  - `http://www.openbsd.org/papaers/rubsd2013-mikeb-en.pdf`

# Références : A lire

- MISC
  - *Dossier SSL et TLS : La crypto peut elle vous protéger ?* Num. 71 01-02/2014
  - *Bonnes pratiques SSL ou comment configurer son serveur HTTPS de la meilleur des façons* Num. 72 03-04/2014
- Ristic - *Bulletproot SSL TLS and PKI* - Feisty Duck
  - `https://www.feistyduck.com/books/bulletproof-ssl-tls-and-pki/`
- Ristic - *SSL Threat Model*
  - `http://blog.ivanristic.com/downloads/SSL_Threat_Model.png`
- Rescorla - *SSL and TLS : Designing and Building Secure Systems* - Addison Wesley
  - `http://www.rtfm.com/sslbook/`

# Références : pour rester au courant

- Blog de Matthew Green
  - `http://blog.cryptographyengineering.com/`
- Blog de Ivan Ristic
  - `http://blog.ivanristic.com/`
- Blog de Adam Langley
  - `https://www.imperialviolet.org/`

# Hervé Schauer Consultants

http://www.hsc.fr

Formations HSC liées :

Défense : PKI, SANS-SEC401, SANS-DEV522

Intrusion : SANS-SEC560, SANS-SEC660, SANS-SEC542