



Breizh C@mp
Mix de technologies

Security matters

#sm

Mathieu POUSSE - @m_pousse

Security matters

Works @ZenikaOuest

Usually Java Dev / Ops ASAP

OSS committer when needed

TOOCOMPLEX



SSL, Handsake, Algorithm,
Hash, X.509, Signature,
Certificate, PGP, TLS, CSR,
CA, private key, Elliptic
Curves, POODLE, Extended
Validation, RSA, SHA256,
still reading?, RC4, Bob and
Alice, ^{broken by}
_{design} openssl, 3DES,
hacking, sha256, self-signed

THE NEED



bob & carol & ted & alice

ELLIOTT GOULD

DYAN CANNON





POLICE
FORCE OUVRIERE

NICOLAS COMTE
SYNDICAT UNITÉ SGP POLICE

SOLUTION



7

Negotiate
the
protocol

2

Verify
tiers
identities

3 Agree
on the
secret

4

Exchange
ciphered
data

PRACTICALLY

Cet énoncé, dû à Tunnell est le suivant que n est l'aire d'un triangle rectangle en nombres entiers si et seulement si $y^2 - n^2x$ a

Dans un tout autre ordre d'idées, certaines méthodes analytiques permettent d'estimer l'ordre d'annulation au centre de la borne critique de familles de courbes elliptiques. Ces estimations se transposent en informations sur le rang des familles de courbes elliptiques correspondantes. Par exemple²⁰ :

Théorème — En admettant l'hypothèse de Riemann généralisée et la conjecture de Birch et Swinnerton-Dyer, le rang moyen des courbes elliptiques

a conjecture de Shimura-Taniyama-Weil et son application au théorème de Fermat

[modifier] [modifier le code]

La conjecture de Shimura-Taniyama-Weil, encore connue sous le nom de « conjecture modulaire », affirme que toute courbe elliptique sur \mathbb{Q} est modulaire, c'est-à-dire qu'il existe une forme modulaire de poids 2 et de niveau N , où N est le conducteur de la courbe elliptique E (un entier divisible par les mêmes nombres premiers que le discriminant). Autrement dit, si, pour $\Re(s) > 3/2$, on écrit la fonction L sous la forme

$$L(E/\mathbb{Q}, s) = \sum_{n>0} a(n)n^{-s},$$

alors l'expression $\sum a(n)q^n$, avec $q = e^{2i\pi z}$, définit une forme modulaire (parabolique, nouvelle) de poids 2 et de niveau N . Pour les nombres premiers premiers l distincts de 37, on peut vérifier la propriété sur les coefficients. Ainsi pour $l = 3$, les solutions de l'équation modulo 3 sont $(0, 0), (0, 1), (0, 2)$.

La conjecture qui date du milieu des années 1950 a été finalement démontrée complètement en 1999, à partir des idées d'Andrew Wiles, qui l'avait déjà partiellement résolue. Il existe plusieurs formulations de cette conjecture ; prouver leur équivalence n'était pas facile et a fait l'objet de travaux importants dans la seconde moitié du XXe siècle.

Le conducteur N s'exprime aussi par le fait qu'il existe un morphisme non constant, défini sur \mathbb{Q} , de la courbe modulaire $X_0(N)$ dans E . En particulier, les courbes modulaires.

Par exemple, un paramétrage modulaire de la courbe elliptique $y^2 + y = x^3 - x$ est donné par²¹

$$\begin{cases} x(z) &= q^{-2} + 2q^{-1} + 5 + 9q + 18q^2 + 29q^3 + \dots \\ y(z) &= q^{-3} + 3q^{-2} + 9q^{-1} + 21 + 46q + 92q^2 + \dots \end{cases}$$

Client

Server

→ ClientHello

ServerHello ←

Certificate ←

Generate secret key

→ Encrypt secret w/ public key

→ Agreement

Agreement ←

Ciphered w/AES

+ Summary (hash ~ sha256)

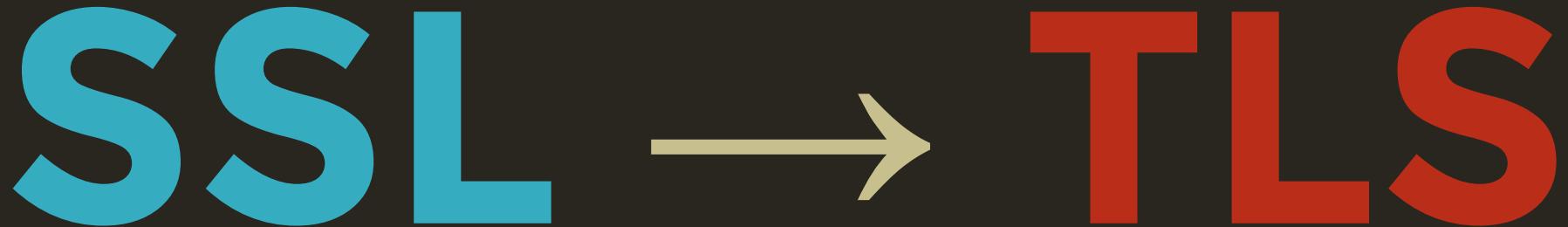
+ Signature

2 extra roundtrips

keep alive / session

Hides data in the wire

Does not hide the wire



SSLv1 (draft) - **VULNERABLE**

SSLv2 (1995) - **VULNERABLE**

SSLv3 (1996) - **VULNERABLE**

TLSv1.0 (1999)

TLSv1.1 (2006 - yesterday)

TLSv1.2 (2008 - today)

TLSv1.3 (TBD - tomorrow)

TLSv1.0

not supported by

Java 6 (2006)

Internet Explorer 6 (2001)

Page quatre-vingt.

Ce livret est de 32 pages.
Ce livret est de 32 pages.
Ce livret est de 32 pages.

Signalement.

Connotati.

14. März 1874

125 - Centimètres

Centimeter
Centimetri

sehr lang, mächtig
hoch

Schwarz

Mäuse

Nas.

normal

sehr hell

Nase

Naso

Menton

Menton

Kinn

Mento

normal

oval

Age: Né le
Alter: geb. den
Uhr: nato il

Stature

Gestalt

Corporatura

Faible

Höhe

Statura

Cheveux

Haire

Capelli

Front

Sirène

Fronte

Scoucys

Augenbrauen

Sopracciglia

Yeux

Augen

Occhi

Bouche

Mund

Bocca

Visage

Gesicht

Viso

Signes particuliers

Besondere Kennzeichen

Segni particolari

Signature du porteur:

Unterschrift des Inhabers: — Firma del titolare:

A. Müller

Dieses Büchlein umfasst 32 Seiten.
Questo libretto consta di 32 pagine.

Seite.
quarta



Authenticate
Sign
Cipher

chained

CA / Certificate Authority (GlobaSign, ...)

 └ *.mydomain.org

 └ my-server.mydomain.org

1 private key

2 CSR

3 certificate

Self-signed
is not evil

Extended Validation





APPLAUSE