

R4.02 - QUALITÉ DE DÉVELOPPEMENT

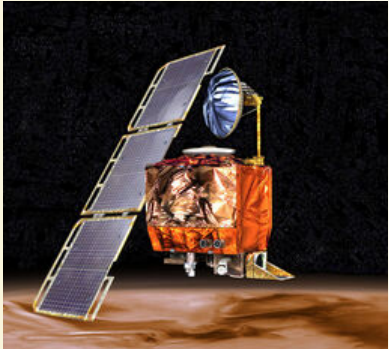


Institut Universitaire de Technologie de Bayonne et du Pays Basque

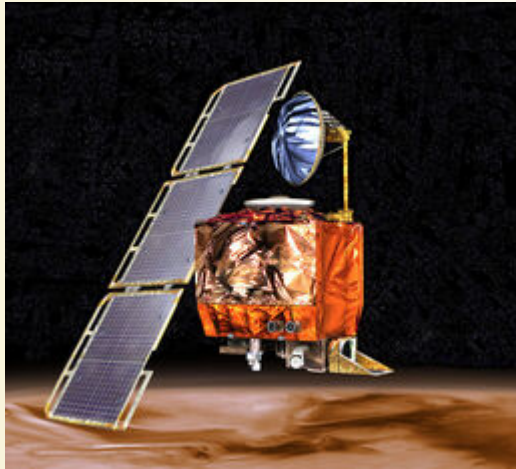
Pantxika Dagorret - Damien Urruty

BUT Informatique 2022 / 2023 - Semestre 4

QUEL EST LE POINT COMMUN ENTRE



MARS CLIMATE ORBITER



- Sonde écrasée sur Mars en 1999
- Erreur causée par un problème d'unité (système métrique vs anglo-saxon)
- Coût total : \$327 millions



FAILLE DE SÉCURITÉ APPLE

```

if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(ctx,
                   ctx->peerPubKey,
                   dataToSign,
                   dataToSignLen,
                   signature,
                   signatureLen);
/* plaintext */
/* plaintext length */

if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
               "returned %d\n", (int)err);
    goto fail;
}

fail:
SSLFreeBuffer(&signedHashes);
SSLFreeBuffer(&hashCtx);
return err;

```

SAUREZ-VOUS TROUVER LA FAILLE ?


APPLE "GOTO FAIL"

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(ctx,
                  ctx->peerPubKey,
                  dataToSign,
                  dataToSignLen,
                  signature,
                  signatureLen);
/* plaintext */
/* plaintext length */

if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
               "returned %d\n", (int)err);
    goto fail;
}

fail:
SSLFreeBuffer(&signedHashes);
SSLFreeBuffer(&hashCtx);
return err;
```



APPLE GOTO FAIL

- Faille dans la validation de certificats HTTPS (iOS et OS X)
- Double goto court-circuitant des validations
- Des millions de machines vulnérables
- Volontaire ou involontaire ?



GANDHI DANS LE JEU



- Censé être le personnage le plus pacifique du jeu
- A cause d'un bug devient le plus agressif

GANDHI DANS LE JEU

PSEUDO CODE

```
uint8 agressivite // entier non signé, [0, 255], 1 pour Gandhi
si (forme de gouvernement est democratie) {
    agressivite -= 2 // integer underflow, agressivité = 255
}
// => nuclear gandhi!
```

BUG, BUG, BUG...

- Ce ne sont que 3 exemples parmi des millions (voir M2204 et M3301 pour d'autres cas)
- Il y aura toujours des comportements non prévus et des bugs...

MODERN RESOLUTION FOR ALL PROJECTS

	2011	2012	2013	2014	2015
SUCCESSFUL	29%	27%	31%	28%	29%
CHALLENGED	49%	56%	50%	55%	52%
FAILED	22%	17%	19%	17%	19%

The Modern Resolution (OnTime, OnBudget, with a satisfactory result) of all software projects from FY2011-2015 within the new CHAOS database. Please note that for the rest of this report CHAOS Resolution will refer to the Modern Resolution definition not the Traditional Resolution definition.

CHAOS REPORT (2015)

BON ALORS, ON FAIT QUOI ?

