Information Security Drivers and Challenges for High Assurance Applications

Glyn Jones – Security Research Team Leader
Adrian Waller – Chief Technical Consultant

Thales UK Research & Technology

Open

THALES

Collective intelligence for a safer world

Whenever critical decisions need to be made, Thales has a role to play.
In all its markets — aerospace, space, ground transportation, defence and security — **Thales solutions help customers to make the right decisions at the right time and act accordingly**.

World-class technology, the combined expertise of **65,000 employees** and operations in **56 countries** have made **Thales a key player in keeping the public safe and secure**, guarding vital infrastructure and protecting the national security interests of countries around the globe.

Employees

65,000 (workforce under management at 31 Dec. 2012)

Global presence

56 countries

Research and development

2.5 billion euros (approx. 20% of revenues)

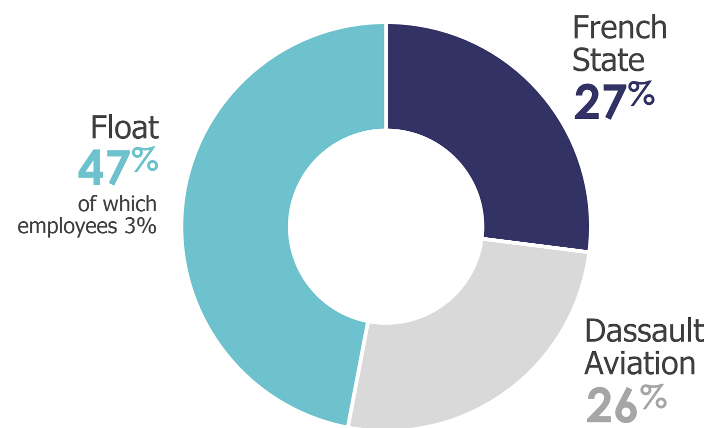
A balanced revenue structure

Revenues in 2012

€ **14.2** billion euros

Shareholders

(at 31 May 2013)



Open

THALES

Dual markets
Military & Civil

AEROSPACE

SPACE

GROUND TRANSPORTATION

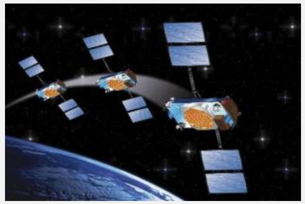
DEFENCE

SECURITY

TRUSTED PARTNER FOR A SAFER WORLD

Global Leadership

N°1 worldwide



Payloads
for telecom satellites

Air Traffic Management

Sonars

Security for interbank transactions

N°2 worldwide

Rail signalling systems

In-flight entertainment and connectivity

Military tactical radiocommunications

N°3 worldwide

Avionics

Civil satellites

Surface radars

€14 billion in revenues

Open

THALES

Safety and security are the common denominators of all our markets and the ultimate purpose of our technologies.

- Security is a prerequisite for sustainable development, and all of our key markets – aerospace, space, ground transportation, security and defence – play a vital role in our societies and economies.
- Thales solutions are deployed in critical environments where safety and security are of the utmost importance. They need to be reliable, adaptable and resilient.
- Our solutions help to address the major security issues of today and tomorrow, from cybersecurity to the growth in air traffic volumes, from urbanization to environmental protection.
- Thales provides a safe working environment and has a proven track record as a reliable partner, a loyal employer and a secure investment for shareholders.

Serving governments, institutions and civil operators

- **Providing access to relevant, reliable information - at all times**
- **Developing integrated solutions and services:**
  - Critical infrastructure protection
  - Border control
  - Critical information systems

N°1
Worldwide in security for interbank electronic transactions

N°3
Worldwide in hardware-based encryption systems

N°1
In europe in information systems security

Strong growth in critical infrastructure security and border protection

A comprehensive approach to national security and citizen protection

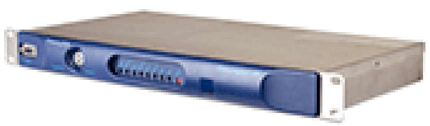
High-end hardware cryptographic devices - not software

- **Hardware Security Module Examples:**
  - nShield Connect
    - Crypto: Asymmetric - RSA (1024, 2048, 4096), Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH. Symmetric - AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, Triple DES.
    - Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512bit)
    - Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC) including Brainpool and custom curves

  - payShield 9000
    - Crypto: Symmetric - DES and Triple DES (key lengths 112 bit, 168 bit), AES (key lengths 128 bit, 192 bit, 256 bit). Asymmetric - RSA (key lengths up to 2048 bit)
    - Hashing: MD1, SHA-1,SHA-2

- **Network Encryptor Examples:**
  - Layer 2 Gigabit Ethernet Encryptor
    - Encryption: AES (256 bit key)
    - Key Management: ECDSA and SHA-384

  - Layer 3 Datacryptor IP Network Encryptor Platform
    - Triple DES, AES(128, 192, 256-bit key lengths)
    - Government and custom algorithms also available



Motivating Example - Satellites

- **The satellite industry is strategically important for Europe, and generates significant revenue as well as employing many tens of thousands of people in Europe.**
  - European space manufacturing industry employs 34,000 people, generating €6 billion sales revenue
  - Offers significant opportunities for growth
    - Global Monitoring for Environment and Security (GMES) forecasts of €30 billion in benefits by 2030
    - Europe's GNSS system, Galileo, forecast €90 billion over the next twenty years
- **Make use of cryptography in several areas**
  - Bulk data encryption on satellite link
  - Protection of command and control protocols
  - Protection of customer specific data

Why PQC?

- **Satellites are provided with fixed algorithms and key material at launch, and it is generally impossible to change these from the ground**
  - Commonly ASIC based
- **Long lifespan of satellites (e.g. 20 years for a communications satellite)**
- **Compromise of the key material and/or algorithms would have devastating consequences to the security of data and/or the satellite itself**
  - Could lead to it becoming unusable
  - Consequences of compromise would be considerable – money and reputation

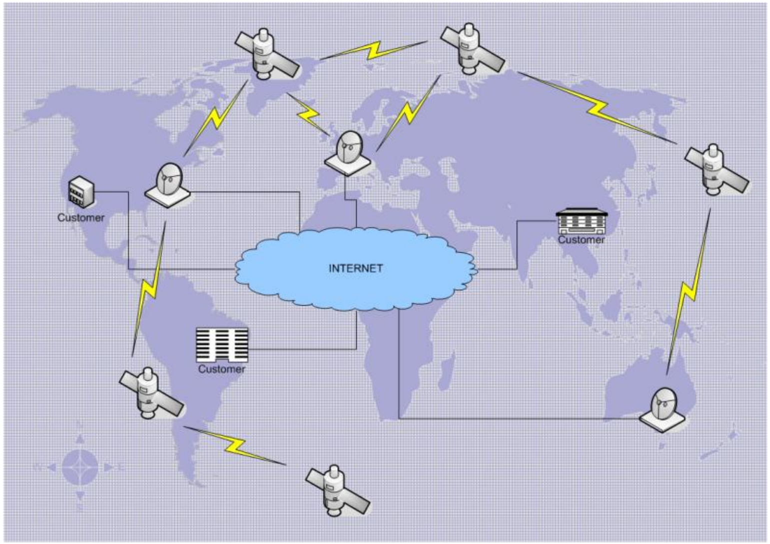
Thales interest in PQC

Key management

- Currently symmetric algorithm based, hence not vulnerable to Quantum Computing (i.e. don't panic)
- Appropriate for isolated, and particularly single mission, satellite infrastructures
- More complex satellite scenarios are starting to be deployed spacecraft constellations, and will become of central importance in future space missions
- BOOZ&CO report identifies the following as one of four key R&D areas for Europe
  - "Integration and convergence of networking: to further facilitate integration of satellites into terrestrial networks".

Future requirements

- In terms of key management, each spacecraft, ground station, Operational Control Centre and user may potentially need to establish keys
- A public-key based solution is needed and the subject of current research and development
- Anything developed now may still be in service in 2040



Requirements in more detail

Hardware cryptos are long term products

- Take time to develop
- Stay deployed for a long time

Main areas of concern:

- Key management
  - E.g. DCAPS Network Encryptor uses PK to set up Security Associations (up to 400)
  - Key exchange - Encryption AND authentication needed (QKD not particularly useful)
  - Algorithms in most products can be updated (software loadable crypto), but long term device key is more of an issue
- Digital Signatures
  - Offered to customer as a crypto service (e.g. nShield HSM)
  - More problematic for long-term is code signing for software loadable crypto
    - Relies on long-term root key for verification

Drivers and Challenges – Assurance

"the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software" – US DoD

Security functionality implementation is a small part in overall security. *Assurance* is the hard part.

- **Making sure it does what it says it does, and only that**
  - E.g. Heartbleed in OpenSSL (buffer over-read)
- **Can't be achieved by testing alone**
- **Requires removal of complexity and indirection**
- **Semi-formal, or even formal, design and implementation process**

Drivers and Challenges – Assurance

www.openssl.org/news/vulnerabilities.html

OpenSSL
Cryptography and SSL/TLS Toolkit

Newsflash | State | News | ChangeLog | Vulnerabilities

Title
FAQ
About
News
Documents
Source
Contribution
Support
Related

OpenSSL vulnerabilities

This page lists all security vulnerabilities fixed in released versions of OpenSSL since 0.9.6a was released on 5th April 2001.

2014

CVE-2014-0160: 7th April 2014

A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64kB of memory to a connected client or server. This issue did not affect versions of

Heartbleed

Fixed in OpenSSL 1.0.1g (Affected 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

CVE-2014-0076: 14th February 2014

Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack" Reported by Yuval Yarom and Naomi Benger.

Fixed in OpenSSL 1.0.1g (git commit) (Affected 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)
Fixed in OpenSSL 1.0.0m-dev (git commit) (Affected 1.0.0l, 1.0.0k, 1.0.0j, 1.0.0i, 1.0.0g, 1.0.0f, 1.0.0e, 1.0.0d, 1.0.0c, 1.0.0b, 1.0.0a, 1.0.0)

CVE-2013-4353: 6th January 2014

A carefully crafted invalid TLS handshake could crash OpenSSL with a NULL pointer exception. A malicious server could use this flaw to crash a connecting client. This issue only affected OpenSSL 1.0.1 versions. Reported by Anton Johansson.

Fixed in OpenSSL 1.0.1f (git commit) (Affected 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

2013

CVE-2013-6450: 13th December 2013

A flaw in DTLS handling can cause an application using OpenSSL and DTLS to crash. This is not a vulnerability for OpenSSL prior to 1.0.0. Reported by Dmitry Sobinov.

Fixed in OpenSSL 1.0.1f (git commit) (Affected 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)
Fixed in OpenSSL 1.0.0l (Affected 1.0.0k, 1.0.0j, 1.0.0i, 1.0.0g, 1.0.0f, 1.0.0e, 1.0.0d, 1.0.0c, 1.0.0b, 1.0.0a, 1.0.0)

CVE-2013-6449: 14th December 2013

A flaw in OpenSSL can cause an application using OpenSSL to crash when using TLS version 1.2. This issue only affected OpenSSL 1.0.1 versions. Reported by Ron Barber.

Fixed in OpenSSL 1.0.1f (git commit) (Affected 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

CVE-2013-0169: 4th February 2013

A weakness in the handling of CBC ciphersuites in SSL, TLS and DTLS which could lead to plaintext recovery by exploiting timing differences arising during MAC processing. (original advisory). Reported by Nadhem J. AlFardan and Kenneth G. Paterson of the Information Security Group Royal Holloway, University of London.

Fixed in OpenSSL 1.0.1d (Affected 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)
Fixed in OpenSSL 1.0.0k (Affected 1.0.0j, 1.0.0i, 1.0.0g, 1.0.0f, 1.0.0e, 1.0.0d, 1.0.0c, 1.0.0b, 1.0.0a, 1.0.0)
Fixed in OpenSSL 0.9.8y (Affected 0.9.8x, 0.9.8w, 0.9.8v, 0.9.8u, 0.9.8t, 0.9.8s, 0.9.8r, 0.9.8

Reported by Nadhem J. AlFardan and Kenneth G. Paterson

CVE-2013-0166: 5th February 2013

A flaw in the OpenSSL handling of OCSP response verification can be exploited in a denial of service attack. (original advisory). Reported by Stephen Henson.

Open

THALES

Drivers and Challenges – Assurance

Commonly demonstrated through:

- **Certification –** "comprehensive evaluation of a process, system, product, event, or skill typically measured against some existing norm or standard"
  - E.g. Common Criteria, CPA/CAPS
- **Accreditation –** "process of accepting the residual risks associated with the continued operation of a system and granting approval to operate for a specified period of time"

Drivers and Challenges – Standards

Standards are crucial, for acceptance/compliance and assurance

- **Device**
  - FIPS 140-2 Level 3
  - HMG UK CAPS (CESG Assisted Products Service)
- **Industry segment**
  - EMV
  - PCI DSS (HSM)
- **Compliance (e.g. PCI DSS) is a major customer driver**

Potential approaches – Lattice-based

Potentially solves all our requirements

- Encryption
- Digital Signatures

Change of algorithm, not of device

Allows new and interesting crypto applications:

- Fully Homomorphic Encryption
- Multi-Party Computation (based on Homomorphic Encryption)
- UK MoD CDE projects looked at scenarios and practicality
  - MPC looks particularly interesting. E.g. Splitting crypto keys onto multiple servers for defence in depth

Could even be faster and more efficient than current primitives

Potential approaches – QKD

Thales was an early innovator with several patents

- **Interest within Thales in satellite applications in response to calls from ESA. e.g. Space-QUEST project, which aims to demonstrate in space:**
  - fundamental quantum physics principles beyond the distance capabilities of earth-bound laboratories
  - absolute secure global distribution of cryptographic keys from Space to the ground

QKD issues:

- **Provides key exchange with no authentication**
- **Fine in theory, but assurance in practice is always the hard part**
  - Practice of QKD is different, and seems hard to do securely
- **Doesn't provide digital signatures**

Assured lattice-based implementations appear to offer many advantages

Thank you

Glyn.Jones@uk.thalesgroup.com
Adrian.Waller@uk.thalesgroup.com