Suite B: Strong Cryptography for Worldwide e-Commerce

IBLS Strategic Global Summit for E-Commerce

17 March 2006

Robert R. Jueneman
Chief Scientist
SPYRUS, Inc.

Personal Background

- "I Am Not a Lawyer" (but sometimes I play one on the Internet)
  - I've been involved in cryptography and information security for over 30 years
  - I've been a member of the American Bar Association's Information Security Committee for many years, and helped draft some of the early digital signature legislation and best practices documents
    - Utah, California, Oregon, Washington, Illinois, and several foreign countries
  - SPYRUS, Inc. is a California-based, privately-held company specializing in cryptographic and PKI solutions
    - We manufacture smart cards, USB tokens, HSMs, and complete PKI and token management solutions, with an emphasis on high assurance systems for government and commercial use
    - As Chief Scientist, I am responsible for our overall cryptographic modernization plan and security architecture.

Overview

- I'm going to review the current state of the cryptographic algorithms used for eCommerce and the Internet
  - The legacy algorithms: RSA, DES, and the hashing functions
  - The most recent attacks against these algorithms, and what they imply
  - Projected performance — speed vs. strength trade-offs
- We'll discuss the latest suite of unclassified algorithms being adopted within the US, NATO, and elsewhere: "Suite B"
  - Elliptic Curve Cryptography (public key algorithms)
  - AES symmetric key algorithms
  - "SHA-2" hash algorithms
- We'll review strategies and options for very long-term privacy and integrity
  - Health care records, land records, patents and invention disclosures, etc.
- Don't worry — I'm not going to get into any mathematics!

The Problem of Aging Algorithms

- 40-bit cryptography used to be required for export control
  - It is now considered almost trivial to break
- 56-bit DES was broken several years ago, for less than $300K
- 128-bit MD-4 hash is the equivalent of a 64-bit symmetric key algorithm, and has been broken with a paper-and-pencil attack!
- 128-bit MD-5 has been broken by the Chinese team, and should no longer be used.
  - Unfortunately it is still in wide use on many web servers.

The Problem of Aging Algorithms

- 80-bit crypto has a limited lifetime
  - SHA-1 has only 2^{69} strength, and is expected to be broken soon
  - Two-key triple DES has only 2^{80} strength, assuming the attacker can obtain 2^{40} cipher pairs
  - RSA-1024 is considered the equivalent of 2^{80} strength
  - The handwriting is on the wall
- NIST recommends phasing out 80-bit crypto by 2010
  - SPYRUS believes that it should be phased out sooner than that, if possible.
  - Enterprises need to initiate policies and architectures now for eventual migration to stronger cryptography

Stronger (But Slower) Keys Can Be Used

- RSA-2048 is somewhat stronger than RSA-1024, but requires substantially more processing power
  - RSA-2048 is equivalent to a 112-bit symmetric key algorithm
  - SHA-1 still has only 2^{69} strength, but very few applications support the new “SHA-2” algorithms yet
  - Three-key triple DES has only 2^{112} strength, again due to time-memory tradeoffs
- NIST recommends phasing out 112-bit crypto by 2030
- **Significantly stronger and faster alternatives are available today, and should be adopted much sooner than that.**

Is All This Strength Really Necessary?

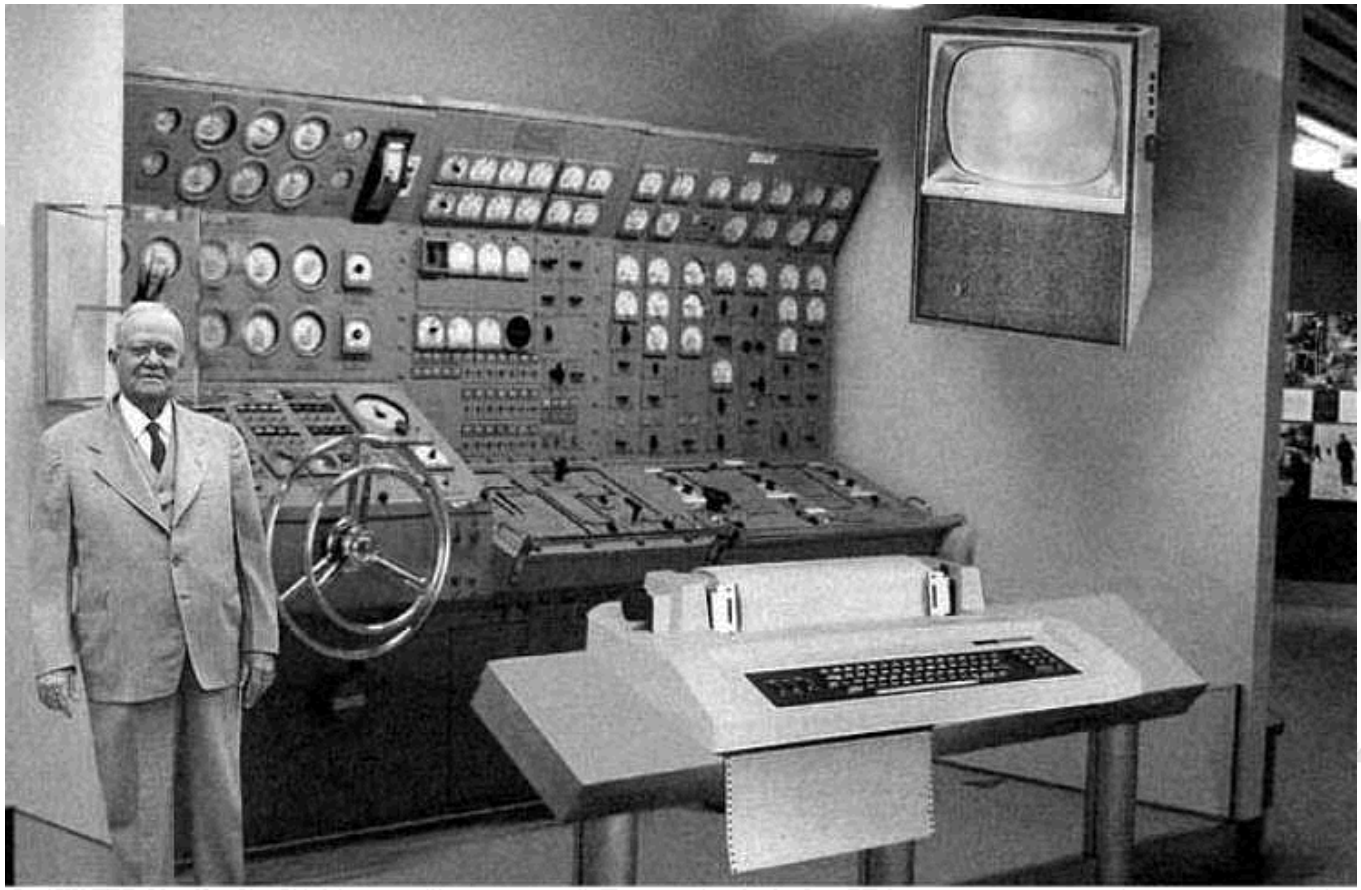
"Making predictions is very difficult — especially about the future."

Yogi Berra

Is All This Strength Really Necessary?

- Predictions of cryptographic strength are seldom too conservative
  - When DES was first announced, IBM and NIST predicted that it would take centuries of computer power to break it.
    - Now it can be broken in less than a day, with only a modest investment
  - Similar claims were initially made about RSA-512
  - The original Secure Hash Algorithm was designed by NSA lasted 2 years before it was replaced by SHA-1.

Popular Mechanics 1954 Prediction: The Home Computer of 2004



Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 50 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.

What Does This Mean for eCommerce?

- A high-assurance worldwide standard is needed for businesses with extended security requirements
  - E.g., for pharmaceutical companies, financial institutions, international trading partners
- "But eCommerce has only a relatively near-term security requirement."
  - The goods are ordered, paid for, delivered, and consumed within a few years, after which no one cares about the security of the transaction, right?
  - It depends on what you mean by eCommerce.

Health Industry Requirements

- Medical and public health records may require confidentiality and integrity for the life of the individual — conceivably 100 years or more
  - A pediatric patient might sue a doctor or a hospital for malpractice many years after the treatment
  - Psychiatric, adoption, and other privileged records must be kept private for the life of the individual
  - Public health records may be important many years later
    - Victims of the 1918 influence pandemic have been exhumed and their records analyzed in conjunction with Bird Flu
  - DNA records could exonerate (or convict) someone decades later
  - Census records must be sealed for 100 years
  - Genealogy records go back even further – 1000's of years in some cases

Land Recordation Requirements

- Land lasts forever, and court cases can drag on nearly as long
  - Colorado and New Mexico are still adjudicating land usage claims by the descendants of those granted rights by the Spanish Crown in the late 1500's
  - One of my ancestors, Don Louis Lorimier, a French-Canadian fur trapper, founded the river town of Cape Girardeau, Missouri in 1806, and in his will donated 400 acres for a court house.
    - Lorimier's son(?) Jacques LaRamee(?), may have been the shadowy figure for whom Ft. Laramie and many other places in Wyoming were named, during the Lewis and Clark expedition of 1804, but the records are conflicting.
    - In the 1930s, my grandmother sued the town for not complying with the terms of the deed of grant, seeking the return to the "heirs and successors" of most of downtown Cape Girardeau!

What's The Point?

- If information will be valuable for *N* years, you can't wait until year *N-1* to protect it adequately!
  - Data at rest or intercepted may be decrypted and valuable many decades later
  - You have to protect data *now*, using methods that will still be secure *then*
- Today, data is accumulating at the rate of about one gigabyte per year per person
  - Yet I have nearly a terabyte of hard disk storage on my home computer — 3 billion 5-1/4" floppy disks worth!

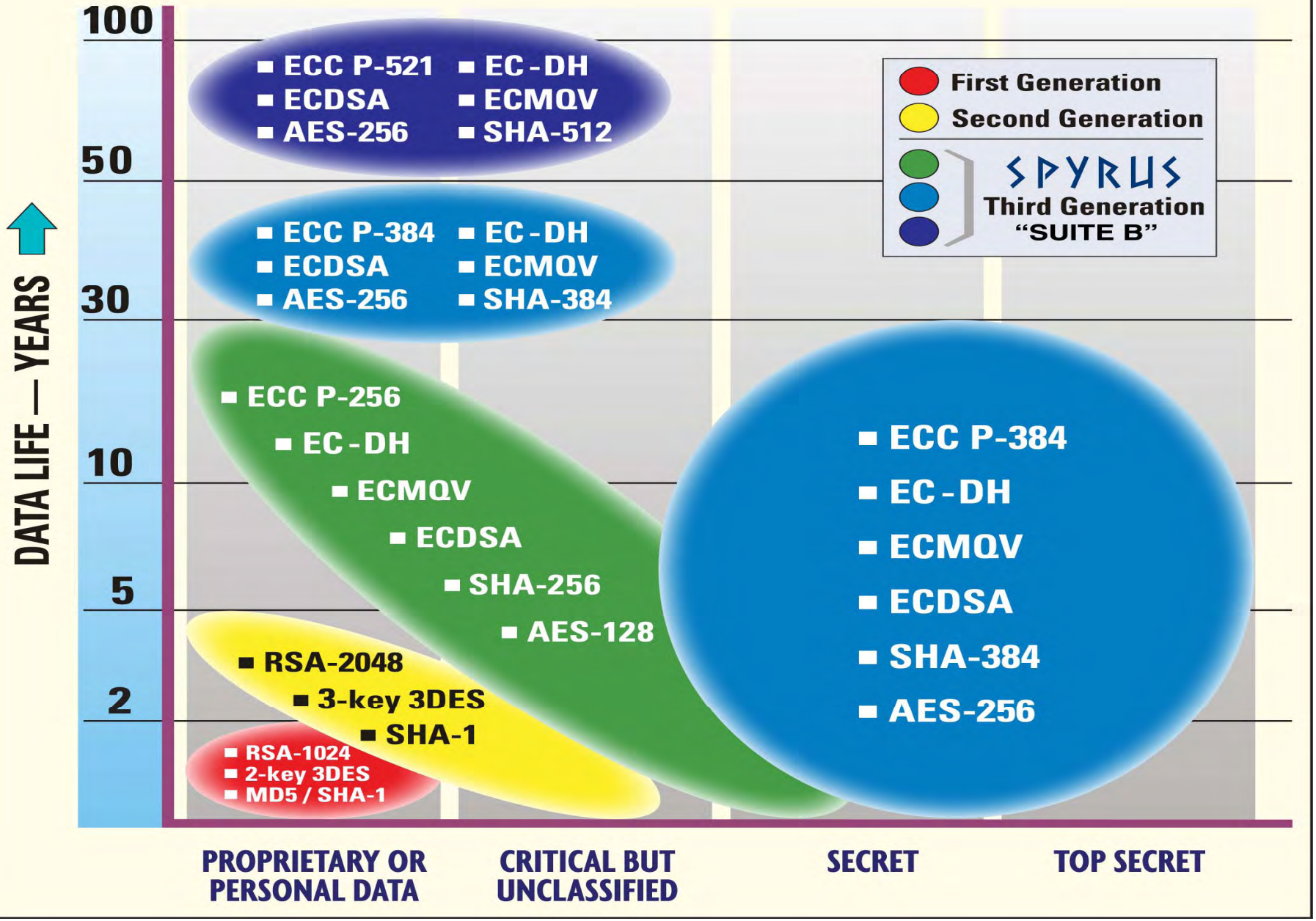
Information is Very Slippery

- Google has effectively replaced the Library of Congress
  - Some of my mother's genealogy correspondence can be found on the Internet — and she has never used a computer in her life!
- It is unrealistic to assume that "someone" will periodically re-encrypt or re-sign all of this data
  - Ergo, it has to be protected adequately from the very beginning, and for a very long time.

A Regulatory Perspective

- Corporations risk a huge consumer backlash over privacy and identity theft
  - California's SB-1386 privacy law has been replicated in many other states
  - Other countries have even stricter regulations
- Putting it simply, not protecting consumer data with encryption 24x7 is unconscionable
  - This includes everything from databases to backup tapes to personal memory devices.

Recommended Crypto Algorithms for Information Assurance



Back to RSA: Key Length vs. Strength

- RSA is inefficient — it gains strength very slowly
  - RSA-1024 is equivalent to an 80-bit symmetric key
  - RSA-2048 is equivalent to a 112-bit key (3DES)
  - RSA-3072 is equivalent to a 128-bit key (AES)
  - RSA-7,680 is equivalent to an 192-bit AES key
  - RSA-15,380 is required to equal an AES-256 key!
    - That's bad news for high strength keys
- But that's not all — the performance is terrible.

RSA Key Length vs. Performance

- The time required for larger keys increases rapidly
  - The time required for signing is proportional to the CUBE of the key length
  - RSA-2048 operations require 8 times as long as RSA-1024
    - Example: 60 milliseconds for RSA-1024 sign, 600 ms for RSA-2048
    - RSA-15,360 would take 3375 times RSA-1024, or 200 seconds!
- Fortunately, there a better alternative — the “Suite B” algorithms.

“Suite B”

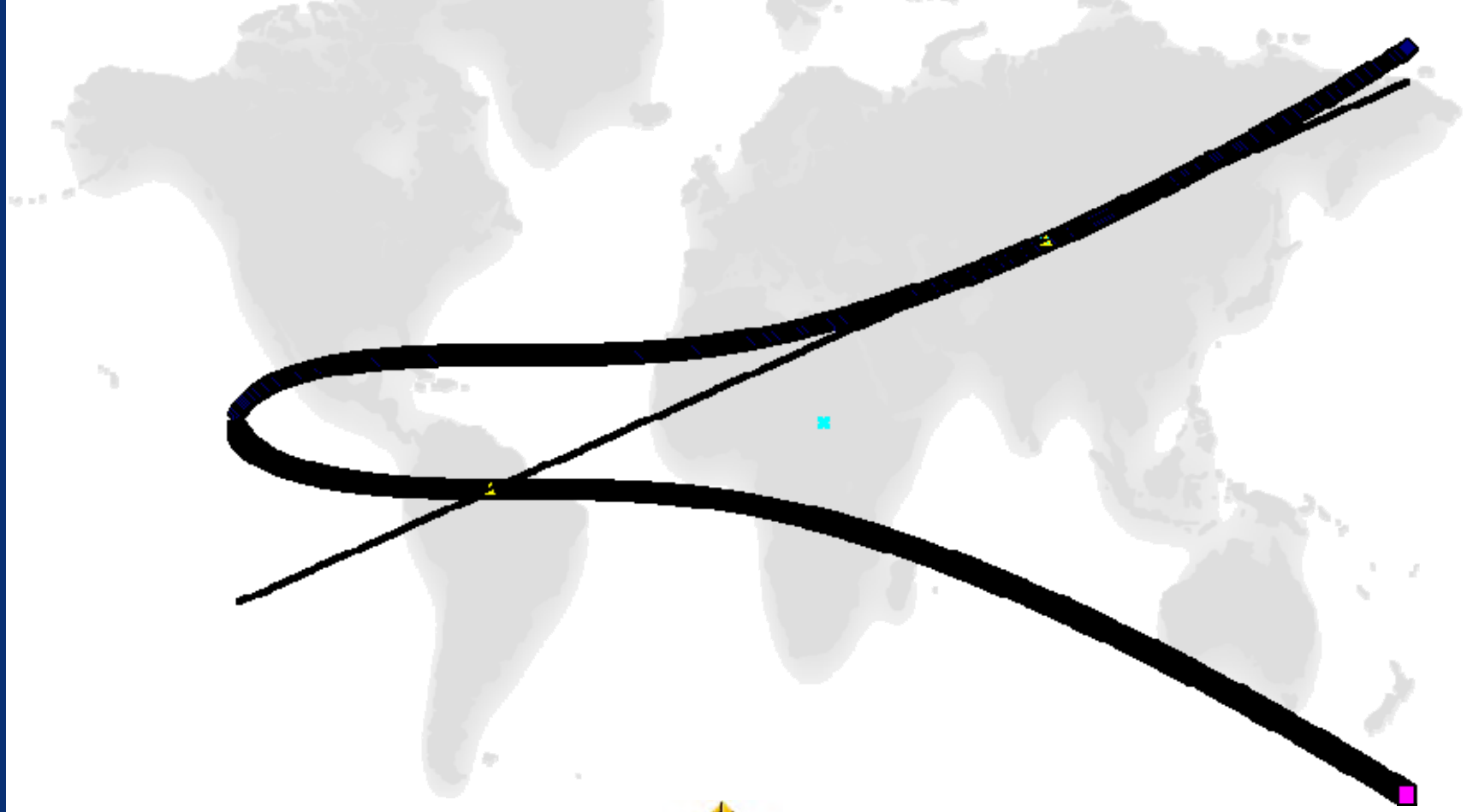
- NSA and NATO have adopted the “Suite B” algorithms for use in multinational information sharing environments up to TOP SECRET
  - Although approved for classified data, the algorithms themselves are unclassified and approved for worldwide use
- There are three components: Elliptic Curve Cryptography (ECC), the Advanced Encryption Standard (AES), and the “SHA-2” hash algorithms.

Elliptic Curve Cryptography

- ECC was invented by Neil Koblitz and Victor Miller in 1985, eight years after the RSA algorithm
  - Personal note — Victor Miller worked for me at IBM in 1969 and 1970, and I encouraged him to go back and get his Ph.D. in mathematics. I'm glad I did!
- ECC has been studied extensively for 20+ years, and is well-recognized and accepted world-wide for its strong number-theoretic foundation.
- ECC has been standardized internationally by ISO and the IETF, and within the US by ANSI and NIST.

Elliptic Curve Cryptography

- An elliptic curve is NOT an ellipse!



Elliptic Curve Cryptography

- NIST has defined several sets of curves, the most important of which are generated by equations of the form

$$y^2 = x^3 - 3x + b \text{ modulo } p$$

- Three curves in *GF(p)* are particularly important:
  - P-256, with a 256-bit key, equivalent to AES-128
  - P-384, with a 384-bit key, equivalent to AES-192, and
  - P-521, with a 521-bit key, equivalent to AES-256
- These three curves and key sizes form the heart of the “Suite B” algorithms.

ECC Performance

- Elliptic Curve Cryptography is much stronger per bit than RSA, and is less computationally intensive
  - P-256 is equivalent to RSA-3,072
  - P-384 is equivalent to RSA-7.680
  - P-521 is equivalent to RSA-15,380
- The performance of ECC is also proportional to the cube of the key size, but the keys are much smaller and more efficient in strength
  - P-256 is faster than RSA-2048, and much faster than RSA-3072. After that, there is no contest.

ECC Algorithms

- ECDSA is the elliptic curve equivalent of the DSA signature algorithms, and is standardized in FIPS 186-2
- EC Diffie-Hellman is a key establishment algorithm with five different variations
- ECMQV is another, stronger, key establishment algorithm that is patented by Certicom
- ECIES is an ECC encryption algorithm that is standardized by ISO, but has been rejected by NIST.

AES, and SHA-2

- The Advanced Encryption Standard (AES) was selected by NIST after an extensive competition and trials.
  - Initially called Rijndahl, it was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
  - AES-128 is significantly faster and stronger than triple-DES, and AES-256 is only slightly slower
  - AES-256 is rapidly becoming the *de facto* standard.
- The SHA-224/256/384/512 hash functions are significantly stronger than SHA-1, although somewhat slower.

ECC, AES, and SHA-2

- Suite B adoption timelines (US):
  - AES was approved in 2001
  - ECDSA with recommended curves was approved in 2001
  - SHA-224/256/384/512 was approved in 2002
  - NIST's SP 800-56A, dealing with ECC key establishment, has been available in various drafts since 2003, with a final version published this month
  - NSA announced the term "Suite B" at the RSA Conference in February 2005.

SPYRUS' Involvement

- We began a corporate-wide investment in Cryptographic Modernization in early 2004
  - We had been watching ECC technology for 10 years, waiting for a consensus to emerge as to fields, curves, and key lengths
  - When NSA announced that they purchased the rights to 26 patents from Certicom, we decided the time was ripe
- We have implemented the Suite B algorithms on all our Rosetta and LYNKS tokens and HSMs
- Our latest product, the Hydra Privacy Card, Series II, provides high-assurance protection to a pocket mass storage device.

Any Questions?

SPYRUS®

For more information:

rjueneman@spyrus.com

www.spyrus.com

1-408-953-0107