iMinds
CONNECT.INNOVATE.CREATE

KU LEUVEN

Strengths and Weaknesses of Cybersecurity Standards

Bart Preneel

COSIC KU Leuven and iMinds, Belgium

firstname.lastname@esat.kuleuven.be

April 7, 2014

What is cybersecurity?

Liddell and Scott, Greek-English Lexicon

Cyber- is a prefix derived from "cybernetic," which comes from the Greek adjective κυβερνητικός meaning *skilled in steering or governing*

Oxford Dictionary

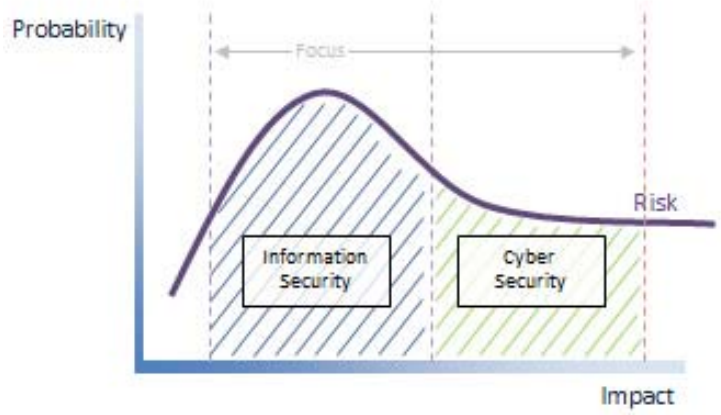
The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

UMUC

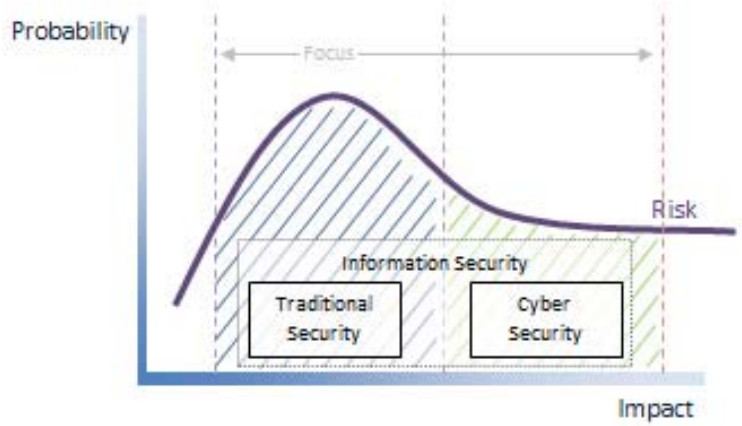
Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

What is cybersecurity?

ISACA



or



What is cybersecurity?

Cyber security strategy – the Netherlands (2011)

Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the **availability** and **reliability** of the ICT, breach of the **confidentiality** of information stored in ICT or damage to the **integrity** of that information."

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013

Cyber-security commonly refers to the safeguards and actions that can be used to protect the **cyber domain**, both in the **civilian** and **military** fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the **availability** and **integrity** of the networks and infrastructure and the **confidentiality** of the information contained therein.

What is cybersecurity?

ITU-T X.1205 (2008) Overview of cybersecurity

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the **cyber environment** and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

Security standards: a taxonomy

- **Base standards**
  - Cryptographic algorithms
  - Modes of use
  - Application Program Interfaces (APIs)
- **Functional standards**
  - procurement, product certification, services
  - TLS, IPsec, X.509, EMV specifications
- **Evaluation Criteria**
  - Common Criteria ISO/IEC 15408 (*Evaluation Criteria for IT Security)*
  - FIPS 140-2 (*Security Requirements for Cryptographic Modules*)
- **Interpretative documents and best practices:**
  - ISO/IEC 27002 (*Code of Practice for Information Security Management)*

A.S. Tanenbaum: “The nice thing about standards is there's so many to choose from”

- International
  - ISO: International Organization for Standardization
  - IEC: International Electrotechnical Commission
  - ITU: International Telecommunications Union
  - IETF: Internet Engineering Task Force
  - IEEE: Institute of Electrical and Electronic Engineers
- European
  - CEN: Comité Européen de Normalisation
  - ETSI: European Telecommunications Standards Institute – Cyber Security Coordination Group
  - ICTSB: ICT Standards Board – NISSG (‘04-’08)
- National
  - ANSI: American National Standards Institute
  - NIST: National Institute of Standards and Technology
- Industry
  - W3C, OASIS, Liberty Alliance, FIDO, Wi-Fi Alliance, BioAPI, WS-Security, TCG
  - GP, PC/SC, Open Card Framework, Multos
  - PKCS, SECG

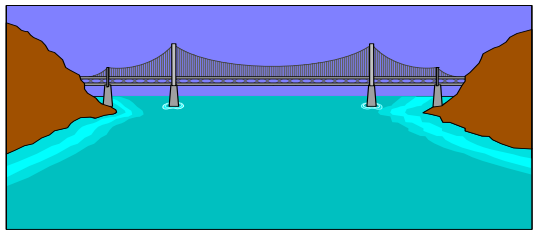
Are security standards different?

- Selection for inclusion in standard: needs an independent security evaluation
- Required security depends on threat analysis – may be strongly application dependent
- Security level changes over time:
  - ad hoc security
  - heuristic analysis based on unproven assumptions
  - formal analysis based on “hard problems”

J.L. Massey: *“A hard problem is a problem that nobody works on”*

Role of evaluation

academic research

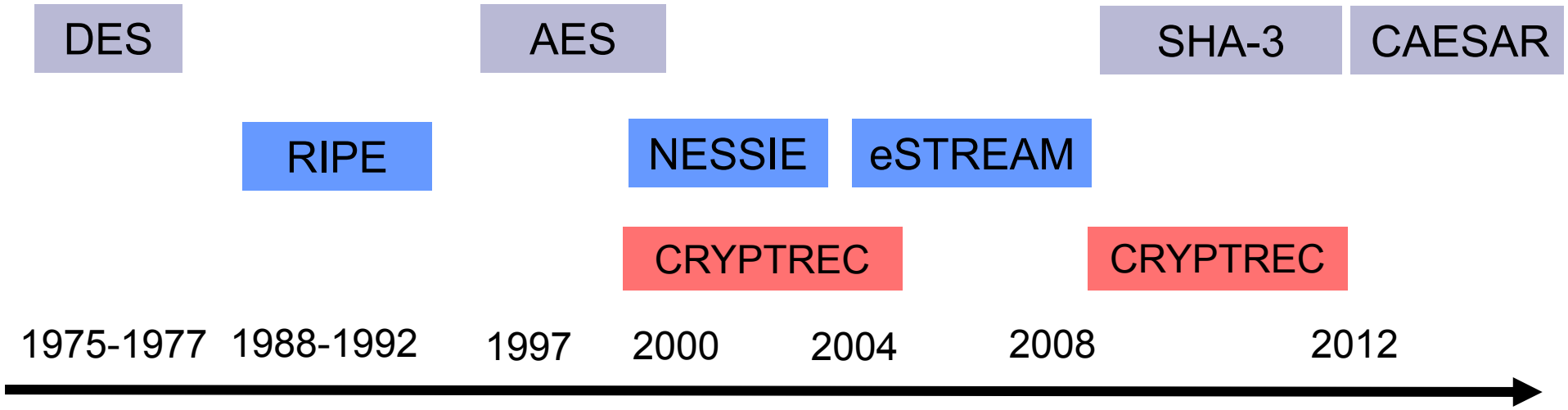


Standard ization bodies

- Broad spectrum of solutions, variants
- Not always fully specified
- Ignore “small” technical problems

- Not in sync with academic developments
- No evaluation effort
- Need clear specs

Open competitions



So far only in cryptology….

Dual_EC_DRBG or Dual Elliptic Curve Deterministic Random Bit Generator

- 1 of the 4 PRNGs in NIST SP 800-90A
- draft Dec. 2005; published 2006; revised 2012
  - in spite of negative comments and Crypto 2007 rump session attack
- 6 Sept. 2013 [Snowden]: backdoored by NSA
- 9 Sept. 2013: NIST **“strongly recommends" against the use of dual_EC_DRBG**, as specified in the January 2012 version of SP 800-90A.

Why was the slowest and least secure of the 4 NIST PRNGs chosen as the default algorithm in BSAFE?

Secure mechanisms are not sufficient

- incorrect specifications or requirements
- implementation errors

Evaluation criteria

Functionality and assurance

- security management

Guidelines and codes of practice

Evaluation criteria

- Expensive
- Slow
- Only high assurance levels count
- National security interests
- Can you trust the protection profile?
- Criteria seem sometimes “ad hoc”
- Are evaluations up to date?
  - Crypto, side channel attacks,…

The maintenance problem

- Context changes
- New technical vulnerabilities
- Cite a broken standard
- Is fixing it better than doing nothing?

- Fast changes incompatible with slow consensus-based procedures

The complexity problem

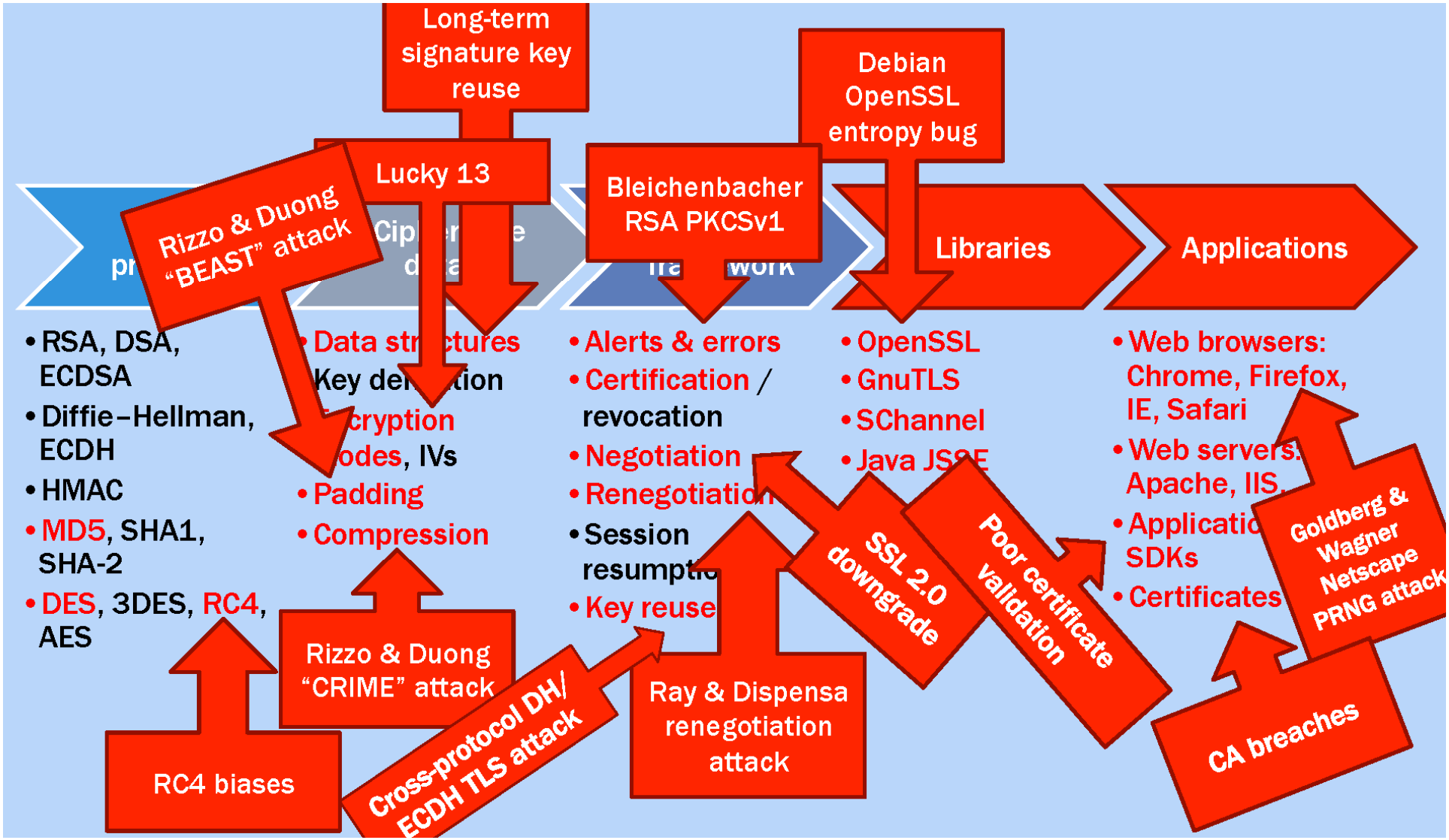
- Committee designs
- Backwards compatibility
- Optimizations for various cases
- High complexity
  - barrier for evaluation
  - barrier for market entry
  - makes secure implementation very difficult

TLS overview [Stebila'14]

Crypto primitives	Ciphersuite details	Protocol "Framework"	Libraries	Applications
RSA, DSA, ECDSA	Data structures	Alerts and errors	OpenSSL	Web browsers
DH, EC-DH	Key derivation	Certification/re-vocation	GnuTLS	Web servers
HMAC	Encryption modes and IVs	(Re-)Negotiation	SChannel	Application SDKs
MD5, SHA-1, SHA-2	Padding	Session Resumption	Java JSSE0	Certificates
DES, 3DES, RC4, AES	Compression	Key reuse		

Theoretical analysis

TLS attack overview [Stebila'14]



Conclusion

- Secure standards essential for security
  - standards are a tool, and not a goal
- Developing and maintaining security standards is perhaps more complex than general standards
- Plenty of fora and liaisons, but not enough real coordination
- Open evaluation procedures essential
- KISS principle
- Stimulate market through procurement?