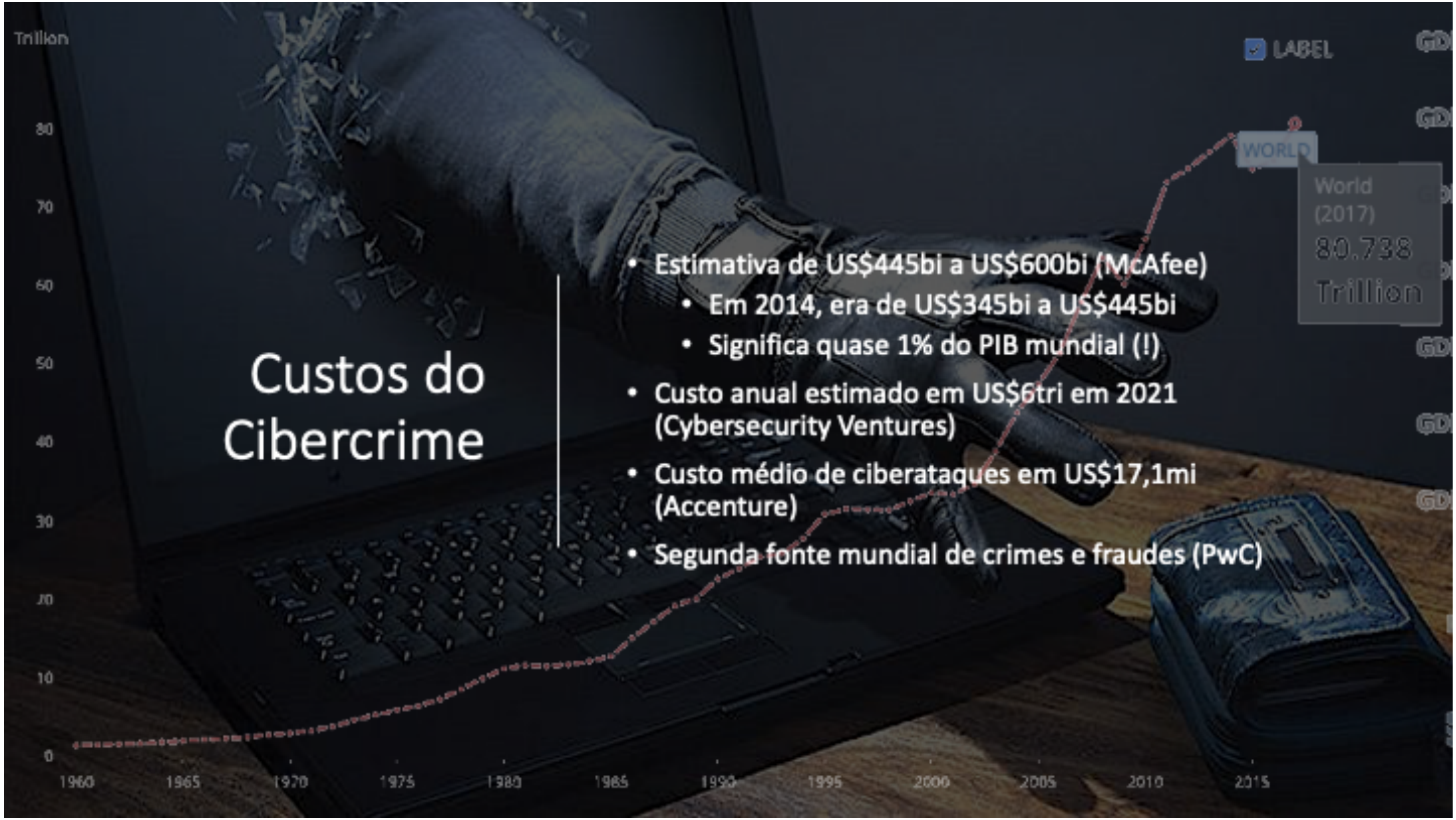
Segurança da Informação

1.1: Motivação e Conceitos Básicos

Motivação

Um pouco sobre a importância da segurança cibernética...


CYBERSECURITY VENTURES
HERJAVEC GROUP
2017 Cybercrime Report
Cybercrime damages will cost the world $6 trillion annually by 2021.
Steve Morgan, Editor-in-Chief
Cybersecurity Ventures
$90M
80M
70M
60M
50M
40M
30M
20M
10M
0
BBC NEWS
Technology
'Bad Rabbit' ra
and Russia
Business
PlayStation
Sony $171m
And counting
By Dan Goodin 24 May 2011 at 05:00
Breach Nears $300
volume em
23


Trillion
80
70
60
50
40
30
20
10
0
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
LABEL
WORLD
World
(2017)
80.738
Trillion
Custos do Cibercrime
• Estimativa de US$445bi a US$600bi (McAfee)
• Em 2014, era de US$345bi a US$445bi
• Significa quase 1% do PIB mundial (!)
• Custo anual estimado em US$6tri em 2021 (Cybersecurity Ventures)
• Custo médio de ciberataques em US$17,1mi (Accenture)
• Segunda fonte mundial de crimes e fraudes (PwC)

What are the most common types of reported economic *crime* and *fraud?*

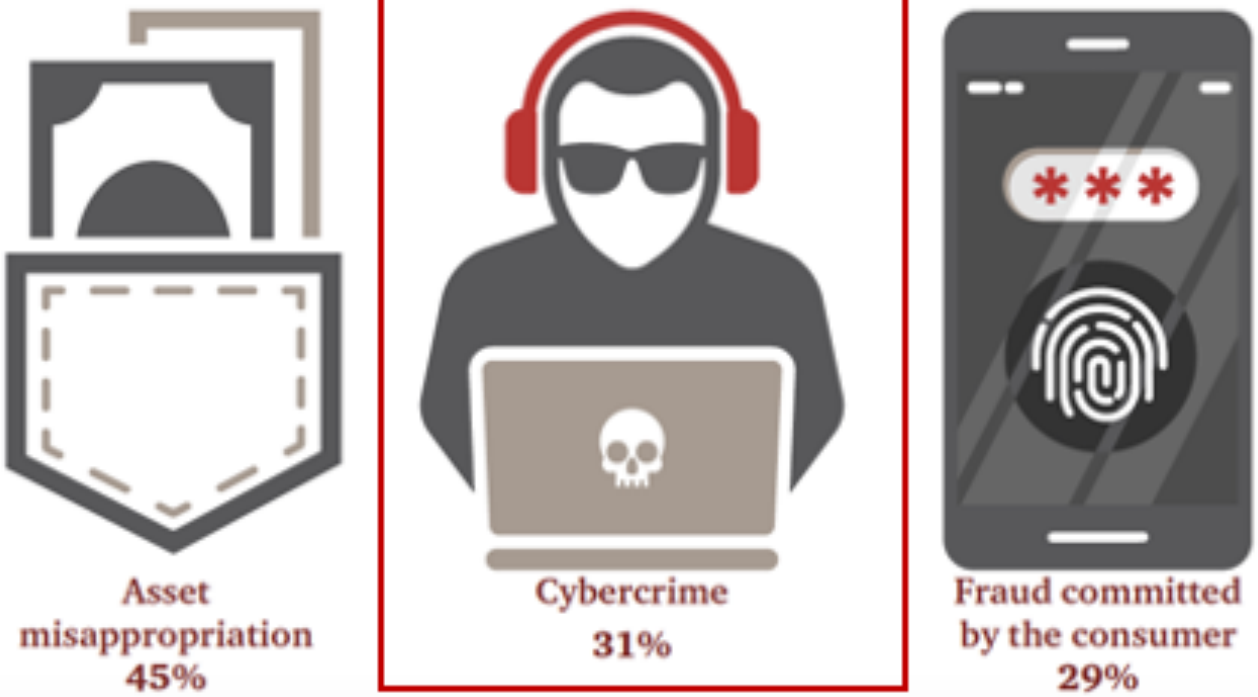
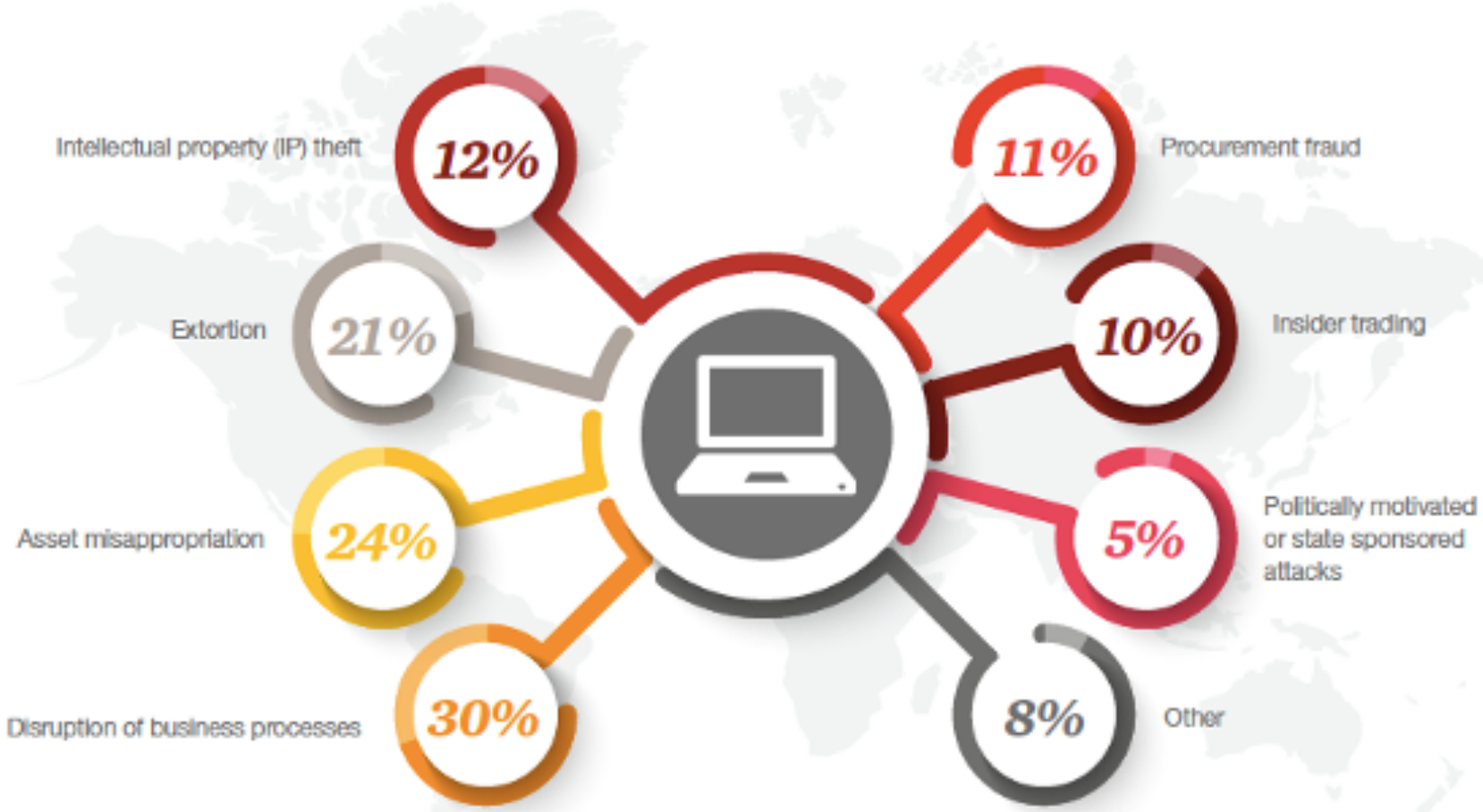


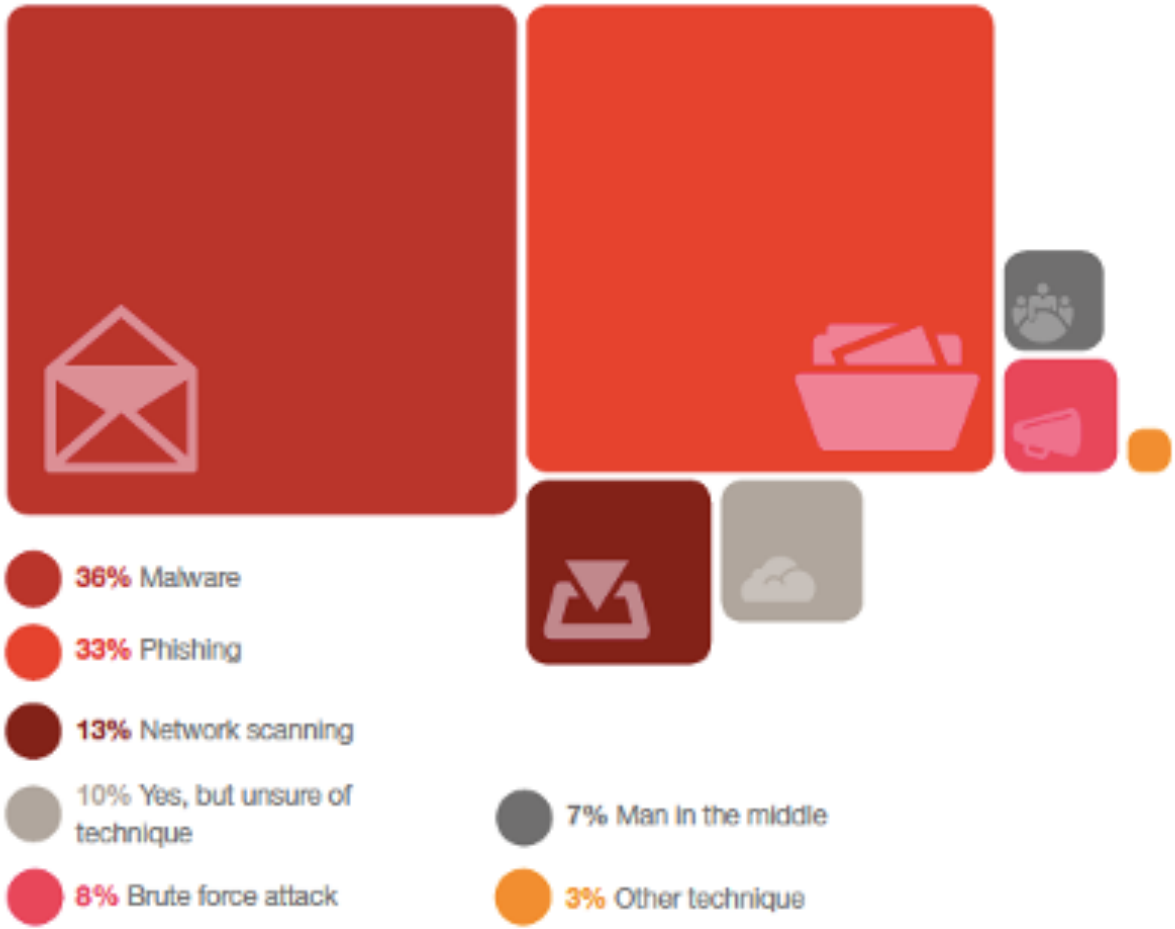
Exhibit 17: Types of fraud that organisations were a victim of through a cyber-attack



Q. Which of the following types of fraud and/or economic crime was your organisation victim of through a cyber-attack?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 18: Cyber-attack techniques used against organisations



Q. In the last 24 months, has your organisation been targeted by cyber-attacks using any of the following techniques?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Over a third of all respondents have been targeted by cyber-attacks, through both malware and phishing. Most of these attacks, which can severely disrupt business processes, also lead to substantive losses to companies: 24% of respondents who were attacked suffered asset misappropriation and 21% were digitally extorted.

pwc

Contents

Não apenas o mundo corporativo sofre com ataques...

Sibéria, 1982

"Com a cumplicidade dos vizinhos do norte, a CIA inseriu um código malicioso no software da empresa canadense."[1]
"...o software fez com que uma extremidade da bomba trabalhasse na taxa máxima, enquanto que na extremidade oposta outra válvula fechasse... maior explosão não nuclear já registrada..."[1]

Cyberwar

War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

Jul 1st 2010 | From the print edition

AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, "was the most monumental non-nuclear explosion and fire ever seen from space."

"…the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden "backdoor" inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar."[2]

ANNALS OF WAR

SEPTEMBER 17, 2012 ISSUE

THE SILENT STRIKE

How Israel bombed a Syrian nuclear installation and kept it secret.

BY DAVID MAKOVSKY

The Mossad extracted evidence of the nuclear site from the computer of a Syrian official.
PHOTOILLUSTRATION BY DAN WINTERS.

In the first days of March, 2007, agents from the Mossad, the Israeli intelligence agency, made a daring raid on the Vienna home of Ibrahim Othman, the head of the Syrian Atomic Energy Commission. Othman was in town attending a meeting of the International Atomic Energy Agency's board of governors, and had stepped out. In less than an hour, the Mossad operatives swept in, extracted top-secret information from Othman's computer, and left without a trace.

Irã, 2010

The attackers appeared to be searching for computers that had one of two Siemens proprietary software programs installed—either Siemens SIMATIC Step 7 software or its SIMATIC WinCC program. Both programs are part of an industrial control system (ICS) designed to work with Siemens programmable logic controllers (PLCs)—small computers, generally the size of a toaster, that are used in factories around the world to control things like the robot arms and conveyor belts on assembly lines.

Cyberwar

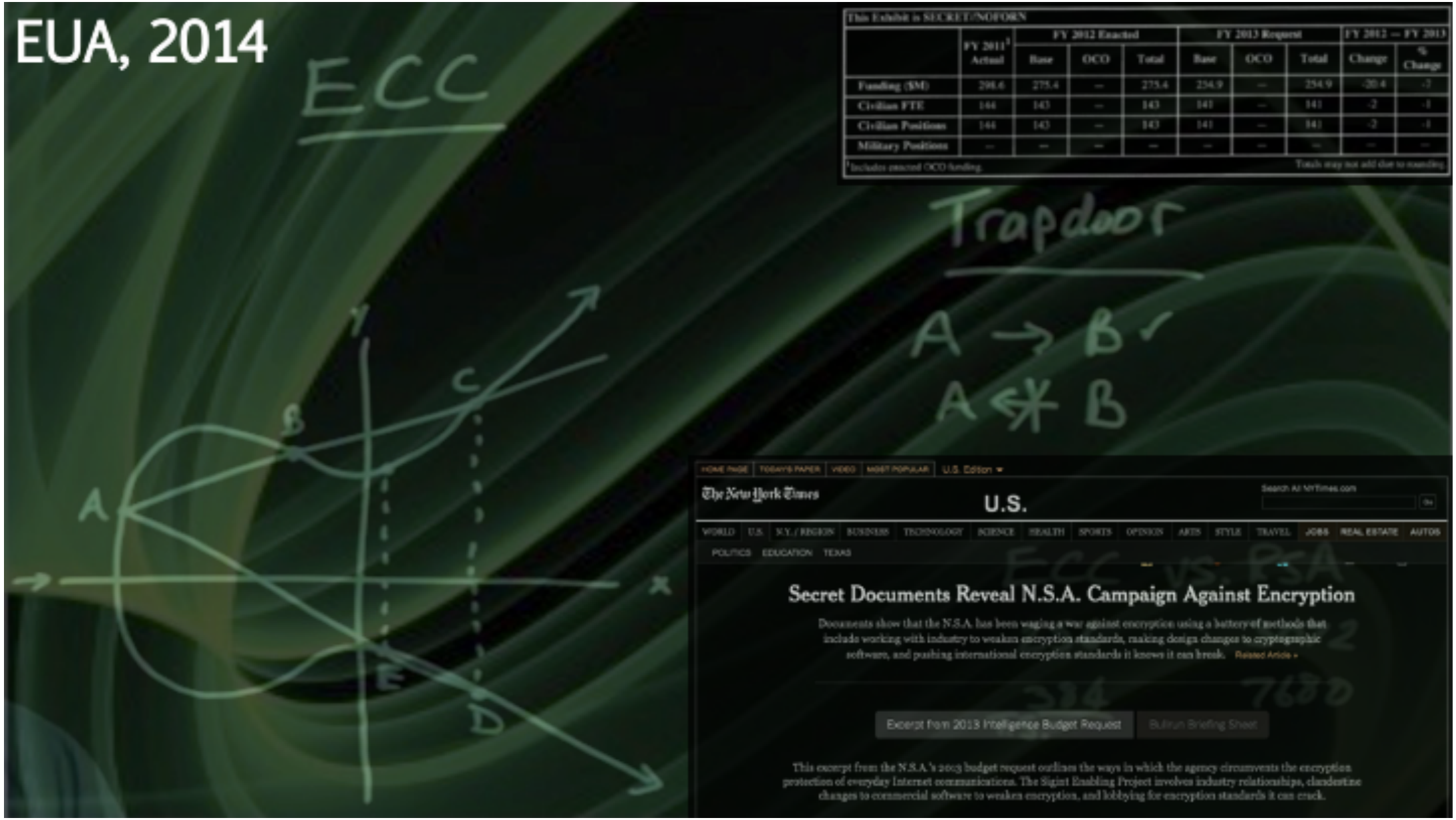
The meaning of Stuxnet

A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar

Sep 30th 2010 | From the print edition

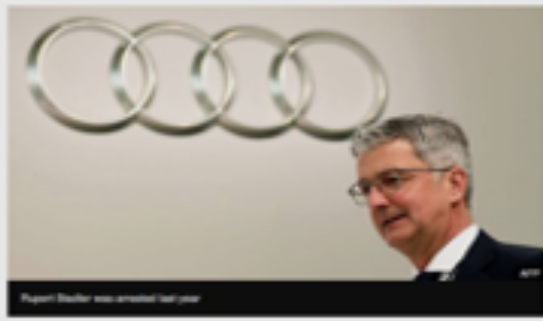
IT HAS been described as "amazing", "groundbreaking" and "impressive" by computer-security specialists. The Stuxnet worm, a piece of software that infects industrial-control systems, is remarkable in many ways. Its unusual complexity suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals (see article). It is designed to infect a particular configuration of a particular type of industrial-control system—in other words, to disrupt the operation of a specific process or plant. The Stuxnet outbreak has been concentrated in Iran, which suggests that a nuclear facility in that country was the intended target.

EUA, 2014


ECC
Trapdoor
A → B ✓
A ⇐✱ B
A
B
C
D
E
X
Y
This Exhibit is SECRET//NOFORN
FY 2012 Enacted
FY 2013 Request
FY 2012 — FY 2013
FY 2011[1] Actual
Base
OCO
Total
Change
% Change
Funding ($M)
Civilian FTE
Civilian Positions
Military Positions
[1] Includes enacted OCO funding.
Totals may not add due to rounding.
The New York Times
U.S.
Search All NYTimes.com
WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION ARTS STYLE TRAVEL JOBS REAL ESTATE AUTOS
POLITICS EDUCATION TEXAS
Secret Documents Reveal N.S.A. Campaign Against Encryption
Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, rushing design changes to cryptographic software, and pushing international encryption standards it knows it can break.
Related Article »
Excerpt from 2013 Intelligence Budget Request
Bullrun Briefing Sheet
This excerpt from the N.S.A.'s 2013 budget request outlines the ways in which the agency circumvents the encryption protection of everyday Internet communications. The Sigint Enabling Project involves industry relationships, clandestine changes to commercial software to weaken encryption, and lobbying for encryption standards it can crack.

EUA/Alemanha, 2009-2015

Former Audi boss charged in VW dieselgate scandal



German authorities have charged the former boss of Audi with fraud as part of an investigation into the VW emissions-cheating scandal.

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

EUA, 2016

BIZ & IT —

DoS attack on major DNS provider brings Internet to morning crawl [Updated]

Dyn's US East region hit hardest in attack that affected Twitter, Reddit.

SEAN GALLAGHER - 10/21/2016, 11:59 AM

Brasil, 2017

Os esquemas de fraude acompanharam o avanço da tecnologia, tornando-se mais sofisticados. Especialistas em informática violam o lacre da bomba e instalam um microprocessador (chip) que altera o seu giro e, consequentemente, o valor a ser pago.
O Globo, 27-jun-17

Quadrilhas usam chips para alterar volume em bombas de combustível

Fiscalizações apontam aumento de fraudes

Ramona Ordoñez

O GLOBO ECONOMIA

O que estes exemplos nos mostram...

- Existem adversários altamente motivados e com enormes recursos para ataques de grande complexidade
  - Adversários: estados-nação, fabricantes, criminosos, ativistas
  - Motivação: guerra, espionagem, lucro, motivação política
- Entidades "acima de qualquer suspeita" podem ser agentes de ataque
  - "Intencionalmente ou não..."
- Impactos de um ataque cibernético no mundo real
  - Centrífugas explodem, carros derrapam, sistemas críticos falham, economias colapsam

Conceitos

Definição de segurança de computadores

- Segurança de computadores: A proteção oferecida a um sistema de informação automatizado para atingir os **objetivos** apropriados de preservação da integridade, disponibilidade e confidencialidade de ativos de sistemas de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).
- Origem: An Introduction to Computer Security: the NIST Handbook (SP 800-12), de 1995, versão anterior ao "An Introduction to Information Security"
- É apenas uma das definições possíveis...

Objetivos fundamentais

- Confidencialidade
  - Confidencialidade de dados: informação confidencial não é disponibilizada a indivíduos não-autorizados
  - *Privacidade: indivíduos podem controlar a maneira como informações pessoais são coletadas, armazenadas, processadas e distribuídas
- Integridade
  - Integridade de dados: informações são modificadas apenas de maneira autorizada.
  - Integridade de sistemas: sistemas computacionais executam suas funções de maneira íntegra
- Disponibilidade
  - Recursos são disponibilizados prontamente/tempestivamente aos usuários autorizados

Outros objetivos

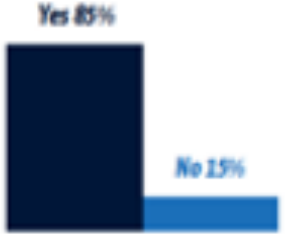
- Autenticidade
  - Entradas de usuários e sistemas são genuínas e podem ser verificadas e confiadas.
- Responsabilidade (Accountability)
  - Ações são rastreadas unicamente a uma entidade

Desafios da Segurança de Computadores

- Complexidades inerentes à área
  - Projetista de segurança deve considerar "todos" os possíveis ataques
  - Não há provas absolutas de corretude – comparar com tarefa "clássica" de engenharia
  - Ao atacante, basta um sucesso – defensor deve fechar "todas as portas"
- Baixo "apelo/atratividade" da segurança
  - Segurança não constitui recurso ou funcionalidade interessante
  - Importância da segurança só é percebida após um ataque
- Custos da segurança
  - Controles de segurança frequentemente têm custo elevado
  - Segurança tipicamente opõe-se a usabilidade
  - Segurança demanda custos constantes em monitoramento
- Dificuldade de comunicação técnico->gestor

More than three in five board members say they are both significantly or very "satisfied" (64%) and "inspired" (65%) after the typical presentation by IT and security executives about the company's cyber risk,

yet the majority (85%) of board members believe that IT and security executives need to improve the way they report to the board.



Board reconhece importância da Cibersegurança...
...mas reports precisam melhorar

Even though **70% of board members surveyed report that they understand everything** that they're being told by IT and security executives in their presentations

more than half (54%) agree or strongly agree that the data presented is too technical.

How Boards of Directors Really Feel About Cyber Security Reports

Based on an Osterman Research survey

OSTERMAN RESEARCH

The information that IT and security executives provide to the board is too technical

Agree/Strongly Agree	54%
Neutral Or Nearly So	42%
Disagree/Strongly Disagree	4%

Despite 70% of board members indicating that they understand everything that they're being told by IT and security executives in their presentations, more than half (54%) also agree or strongly agree that reports are too technical. The contradiction shows while some board members think they understand the data presented to them, that may not necessarily be the case.

IT and security executives should not be surprised by the finding. Based on our previous survey, only one-third of IT and security executives believe the board comprehends the cyber security information they provide.

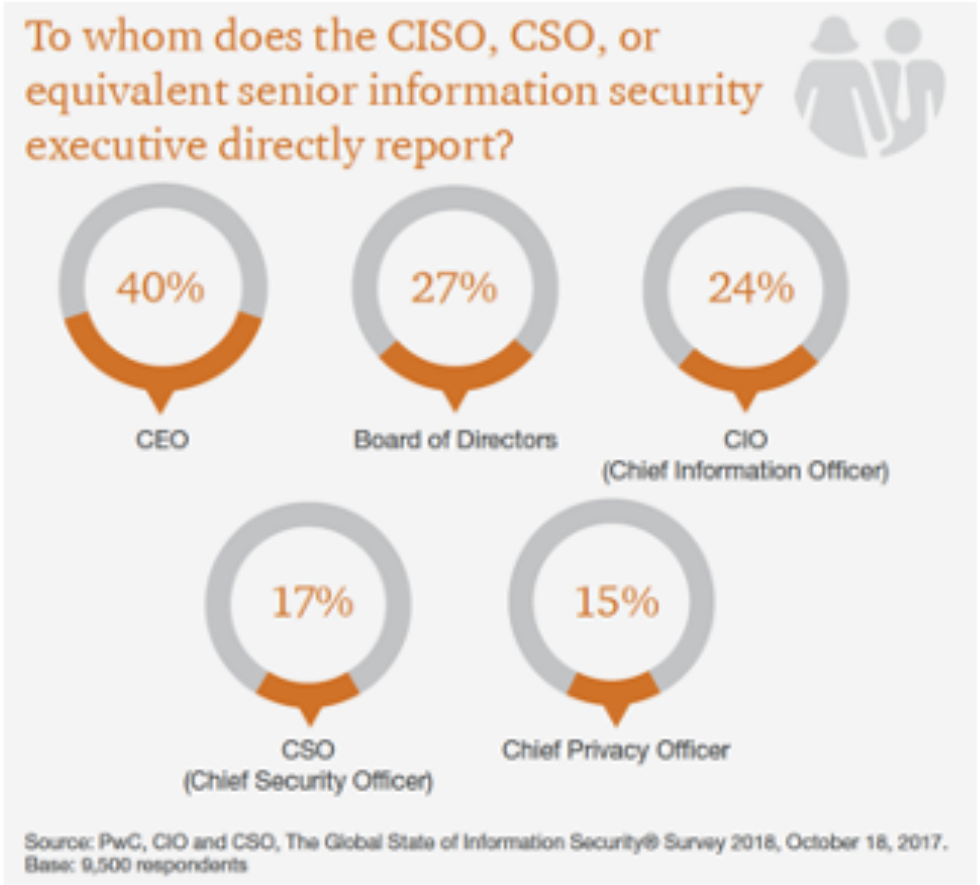
Some of the information that could be "too technical" for board members could be the top two featured in the most common types of information they say IT and security executives report. **According to board members, the top three common types of information reported include:**

1. A complete list of vulnerabilities within the organization,

2. Details on data loss, and

3. Downtime caused by data breach incidents.

Ciber-segurança é questão de negócio



Riscos, riscos, riscos...

On a scale of 1 to 7, what is the priority in addressing each of the following risks for the company, where 1 is "lowest priority" and 7 is "highest priority"?

Cyber risks	*5.60*
Financial risks	*5.54*
Regulatory risks	*5.40*
Competitive risks	*5.36*
Legal risks	*5.36*

Ciber-segurança significa "negócios"

Board Engagement, Comprehensive Data Policies Distinguish High-Performing Information Security Programs

Based on our analysis, there are two critical success factoes present in organizations that adhere to security and privacy best practices:

- High levels of engagement and understanding by the board of directors regarding information security risks
- Having all five "core" information security policies in place

In other Protiviti research, we have observed this correlation between board engagement in information security and the overall security posture of the organization, including in our 2015 IT Security and Privacy Survey report.[2] Similarly, our results this year show a notable difference between organizations that have all "core" information security policies in place — specifically, a records retention/destruction policy, a written information security policy, an acceptable use policy, a data encryption policy, and a social media policy — and those that do not; the former organizations demonstrate stronger information security practices overall.

Throughout our report, we compare the results from these two groups of companies that exhibit the above success factors (which we categorize as "top-performing organizations") with companies that do not exhibit them, and pinpoint notable gaps.

Ciber-segurança significa "negócios"

- *How engaged is your board of directors with information security risks relating to your business?*

	All respondents		Large Companies (≥ $1B)		Small Companies (< $1B)	
	Current	2015	Current	2015	Current	2015
High engagement and level of understanding by the board	33%	28%	37%	32%	26%	24%
Medium engagement and level of understanding by the board	37%	32%	37%	33%	39%	33%
Low engagement and level of understanding by the board	12%	15%	9%	11%	20%	19%
Don't know	18%	25%	17%	24%	15%	24%

- *Which of the following policies does your organization have in place? (Multiple responses permitted)*

	All respondents		Large Companies (≥ $1B)		Small Companies (< $1B)	
	Current	2015	Current	2015	Current	2015
Acceptable use policy	80%	77%	82%	82%	77%	72%
Record retention/destruction policy	78%	74%	81%	80%	72%	71%
Data encryption policy	70%	67%	77%	79%	60%	58%
Written information security policy (WISP)	69%	66%	72%	72%	65%	60%
Social media policy	59%	55%	61%	61%	53%	50%

Terminologia e Conceitos Fundamentais

Principais Padrões (e Órgãos de Padronização)

- IETF RFC 2828: Internet Security Glossary
- Modelo de Redes e Segurança de Redes
  - ISO/IEC 7498-1:1994 e ITU-T Recommendation X.200. INFORMATION TECHNOLOGY -- OPEN SYSTEMS INTERCONNECTION -- BASIC REFERENCE MODEL: THE BASIC MODEL
  - ISO/IEC 7498-2:1989 e Recommendation X.800. INFORMATION PROCESSING SYSTEMS -- OPEN SYSTEMS INTERCONNECTION -- BASIC REFERENCE MODEL -- PART 2: SECURITY ARCHITECTURE
- NIST SP 800-12 Rev. 1: An Introduction to Information Security

Nomenclaturas diversas para a própria área

- Segurança da Informação
  - Nome histórico, associado ao primeiro objeto protegido por meio de técnicas "criptográficas" – a informação
  - Ainda é o termo mais usado - podemos entender que extrapola para Segurança de Sistemas de Informação
- Segurança de Sistemas de Informação
  - Usado explicitamente por algumas agências (e.g. ANSSI)
- Segurança de Computadores
  - Remete não apenas à Informação mas aos aspectos "computacionais" a serem protegidos
- Segurança Cibernética
  - Geralmente usado no ambiente de Defesa, remete ao "espaço cibernético" como um ambiente a ser protegido e explorado
- Segurança da Informação e Criptografia (SIC)
  - Termo frequentemente usado pela Inteligência e Forças Armadas no Brasil

O que é “Segurança”

- Segurança de Computadores

  The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.

  (A proteção oferecida a um sistema de informação automatizado para atingir os **objetivos** apropriados de preservação da integridade, disponibilidade e confidencialidade de ativos de sistemas de informação)
  *tais ativos incluem hardware, software, firmware, informações/dados e telecomunicações

- Origem: An Introduction to Computer Security: the NIST Handbook, de 1995 (versão anterior ao ”An Introduction to Information Security”)

Definição da SP 800-12 R1

› *Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.*

(A proteção da informação e de sistemas de informação contra acesso, uso, divulgação, disrupção, modificação ou destruição não-autorizados de forma a garantir confidencialidade, integridade e disponibilidade)

Definição da RFC 2828

- $ computer security (COMPUSEC)
  - (I) Measures that implement and assure security services in a computer system, particularly those that assure access control service.
  - (C) Usually understood to include functions, features, and technical characteristics of computer hardware and software, especially operating systems.

"I" identifies a RECOMMENDED Internet definition.

"N" identifies a RECOMMENDED non-Internet definition.

"O" identifies a definition that is not recommended as the first choice for Internet documents but is something that authors of Internet documents need to know.

"D" identifies a term or definition that SHOULD NOT be used in Internet documents.

"C" identifies commentary or additional usage guidance.

RFC 2828

- $ security service
  - (I) A processing or communication service that is provided by a system to give a specific kind of protection to system resources.

    (See: access control service, audit service, availability service, data confidentiality service, data integrity service, data origin authentication service, non-repudiation service, peer entity authentication service, system integrity service.)
  - (O) "A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or the data transfers." [I7498 Part 2]
  - (C) Security services implement security policies, and are implemented by security mechanisms.

"I" identifies a RECOMMENDED Internet definition.

"N" identifies a RECOMMENDED non-Internet definition.

"O" identifies a definition that is not recommended as the first choice for Internet documents but is something that authors of Internet documents need to know.

"D" identifies a term or definition that SHOULD NOT be used in Internet documents.

"C" identifies commentary or additional usage guidance.

RFC 2828

› $ security service
  - (I) A processing or communication service that is provided by a system to give a spec
    (Se
    inte
    aut
  - (O)
    ade
  - (C)
    mec

"I" identifie

"N" identif

"O" identif
but is som

"D" identif

"C" identifies commentary or additional usage guidance.

service, data
ntity

ich ensures

by security

t documents

nts.

In most of the cases where this Glossary provides a definition to supersede one from a non-Internet standard, the substitute is intended to subsume the meaning of the superseded "O" definition and not conflict with it. For the term "security service", for example, the "O" definition deals narrowly with only communication services provided by layers in the OSI model and is inadequate for the full range of ISD usage; the "I" definition can be used in more situations and for more kinds of service. However, the "O" definition is also provided here so that ISD authors will be aware of the context in which the term is used more narrowly.

X.800 (e ISO 7498-2)

- Não propõe definição para segurança de computadores
  - Trata o conceito central de *serviços de segurança* e o conceito relacionado de *mecanismos de segurança*
- 3.3.51 security service.
  - A service, provided by a **layer of communicating open systems**, which ensures adequate security of the systems or of data transfers.
  - Curiosamente, o padrão não define "formalmente" o termo *segurança* ou *mecanismo* (embora trate estes assuntos)

Serviços e Mecanismos de Segurança X.800

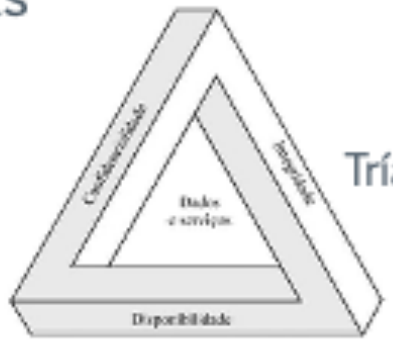
- 5.1 Overview
  - **Security services that are included in the OSI security architecture and mechanisms which implement those services** are discussed in this section. The security services described below are basic security services. In practice they will be invoked at appropriate layers and in appropriate combinations, usually with non-OSI services and mechanisms, to satisfy security policy and/or user requirements. Particular security mechanisms can be used to implement combinations of the basic security services. Practical realizations of systems may implement particular combinations of the basic security services for direct invocation.
- 5.2 Security services
  - The following are considered to be the security services which can be provided optionally within the framework of the OSI Reference Model. The authentication services require authentication information comprising locally stored information and data that is transferred (credentials) to facilitate the authentication.
- 5.3 Specific security mechanisms
  - The following mechanisms may be incorporated into the appropriate (N)-layer in order to provide some of the services described in § 5.2.

Serviços e Mecanismos de Segurança X.800

Service \ Mechanism	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	·	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

Analisando as definições

- Todas elas remetem a um conjunto de ”objetivos” ou ”requisitos” de segurança que permitem proteger recursos: **confidencialidade**, **integridade** e **disponibilidade**
- Especialistas convergem para um conjunto básicos de objetivos/requisitos de segurança:
  - Essa abordagem é bem clara nos padrões NIST, e reverberada por vários especialistas



Tríade CID (CIA)

Outros Termos (1)

- Ativos
  - Recursos que usuários de um sistema desejam proteger
    Ex.: Hardware, software, dados,...
- Vulnerabilidades
  - Fraquezas presentes em um sistema – seja pela sua implementação ou pela sua operação
- Política de Segurança
  - Conjunto de regras e práticas que especificam como um sistema provê serviços de segurança para proteger ativos
- Ameaças
  - Potencial violação da política de segurança por meio da exploração de uma vulnerabilidade

Outros Termos (2)

- Ataque
  - Concretização intencional de uma ameaça; um ataque bem-sucedido leva à violação de política de segurança.
    - Ataque ativo: ocorre interação do atacante com o sistema atacado.
    - Ataque passivo: não ocorre interação com o sistema atacado.
    - Ataque interno: realizado por usuário com acesso legítimo ao sistema atacado.
    - Ataque externo: realizado por usuário sem acesso ao sistema atacado.
- Controle (contramedida)
  - Medida para lidar com ameaças/ataques, minimizando riscos
    - Controles de prevenção, detecção, resposta e recuperação

Outros Termos (3)

- Ação de Ameaça
  - Ação que concretiza uma ameaça, tal como um ataque
- Agente de Ameaça
  - Entidade que concretiza uma ameaça ao sistema, tal comoum atacante
- Consequência de Ameaça
  - Violação de segurança resultada de uma ação de ameaça.
    - Unauthorized Disclosure: exposure, interception, inference, intrusion
    - Deception: masquerade, falsification, repudiation
    - Disruption: incapacitation, corruption, obstruction
    - Usurpation: misappropriation, misuse

Adversário e Ameaça

- $ adversary
  - (I) An entity that attacks, or is a threat to, a system.
- threat
  - (I) A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
  - (C) That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).
  - (C) In some contexts, such as the following, the term is used narrowly to refer only to intelligent threats:

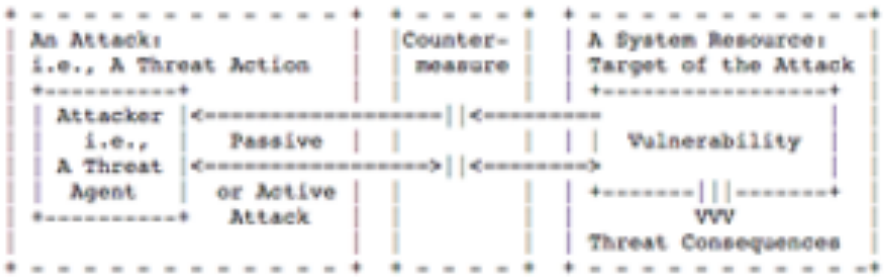
Ações e Consequências de Ameaças

- $ threat action
  - (I) An assault on system security. (See: attack, threat, threat consequence.)
- $ threat consequence
  - (I) A security violation that results from a threat action. Includes disclosure, deception, disruption, and usurpation. (See: attack, threat, threat action.)

* Ler RFC2828 para uma lista de ações e consequências

Ataque

- $ attack
  - (I) An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. (See: penetration, violation, vulnerability.)
    - - Active vs. passive: An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.)
    - - Insider vs. outsider: An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.
  - (C) The term "attack" relates to some other basic security terms as shown in the following diagram:



Ataque ativo vs passivo

- Passivo: não há interação, interferência ou efeito no sistema atacado
  - Exemplo: Leitura de mensagem em um canal de comunicação
- Ativo: baseia-se na interação, interferência ou efeito no sistema atacado
  - Exemplo: Modificação de uma mensagem em um canal de comunicação
  - Exemplo: Exploração de uma vulnerabilidade (exemplo, injeção de SQL) em uma aplicação web

Ataque interno vs externo

- Externo: realizado por indivíduo desprovido de credenciais ou informações privilegiadas em relação aos sistemas atacados; realizado a partir de redes públicas
  - Exemplo: invasão de uma rede corporativa a partir da Internet.
- Interno: realizado a partir de redes restritas ou beneficiado por credenciais e informações privilegiadas
  - Exemplo: invasão de um sistema corporativo por empregado a partir de uma Intranet
  - Exemplo (interno-equivalente): ataque realizado por visitante com acesso físico a um ponto de rede de uma empresa
  - Exemplo (interno-equivalente): acesso a uma VPN usando credenciais obtidas por meio de engenharia social

Paradigma de Alice e Bob (e “outros”)

Alice

Canal de Comunicação

Bob

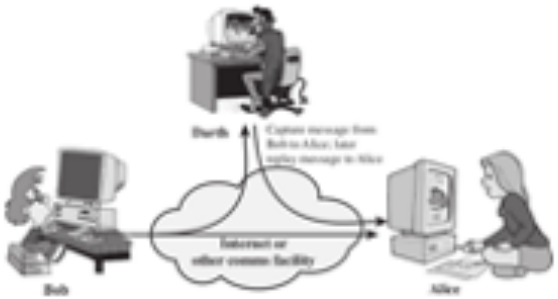
Atacante

Exemplos/Tipos de Ataque

Vazamento de Conteúdo de Mensagem

Análise de Tráfego

Masquerade (ou Impersonation)



Ataque de Replay

Ataque de Modificação de Conteúdo

Ataque de Negação de Serviço

Vulnerabilidade

- $ vulnerability
  - (I) A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
  - (C) Most systems have vulnerabilities of some sort, but this does not mean that the systems are too flawed to use. Not every threat results in an attack, and not every attack succeeds. Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use. If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable. However, if the attacks are well understood and easily made, and if the vulnerable system is employed by a wide range of users, then it is likely that there will be enough benefit for someone to make an attack.

Risco

- $ risk
  - (I) An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

*Conceito com muitas outras definições.
Ex. (ISO): Efeito da incerteza nos objetivos.

Contramedida (controle)

- $ countermeasure
  - (I) An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
  - (C) In an Internet protocol, a countermeasure may take the form of a protocol feature, an element function, or a usage constraint.

Contramedidas (abordagens)

- Prevenção
  - Ataque não é bem-sucedido
  - Exemplo: cifrar dados em trânsito
- Detecção
  - Ataque é detectado
  - Exemplo: detecção de presença de usuário não-autorizado
- Redução de Impacto
  - Ataque gera impacto reduzido
  - Exemplo: destruição automática de dados críticos
- Resposta
  - Sistema reage contra ataque
  - Exemplo: shutdown de sistema violado
- Recuperação
  - Sistema se recupera após ataque
  - Exemplo: sistema de backup

Arquitetura de Segurança

Arquitetura de Segurança

- Abordagem sistemática para definir requisitos de segurança e soluções que satisfaçam tais requisitos
- ITU-T Recommendation X.800, Security Architecture for OSI
  - Visão abstrata das principais questões de segurança
  - Conceitos-chave: mecanismos e serviços
  - Foco em redes de computadores e sistemas de comunicação
  - Conceitos podem ser (e são) generalizados para segurança de sistemas de informação
- ISO 7498-2: essencialmente igual ao X.800
- Padronização de Segurança
  - ITU-T: International Telecommunication Union, Telecommunication Standardization Sector
  - ISO: International Organization for Standardization

Conceitos Fundamentais de Arq. de Seg.

- Camada de comunicação (X.200 e 7498-1)
  - Abstração em um sistema de comunicações: uma camada consome serviços da camada imediatamente inferior e fornece serviços para a camada imediatamente superior, comunicando-se virtualmente com a camada em mesmo nível de outros hosts
- Serviço de Segurança (X.800 e 7498-2)
  - Serviço relacionado a Segurança da Informação oferecido por uma camada de comunicação
- Mecanismo de Segurança (X.800 e 7498-2)
  - Mecanismo implementado em uma camada e responsável por oferecer determinado(s) serviço(s) de segurança

INTERNATIONAL STANDARD

ISO/IEC 7498-1

Second edition
1994-11-15

Corrected and reprinted
1996-06-15

Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model

Technologies de l'information — Modèle de référence de base pour l'interconnexion de systèmes ouverts (OSI): Le modèle de base

Contents

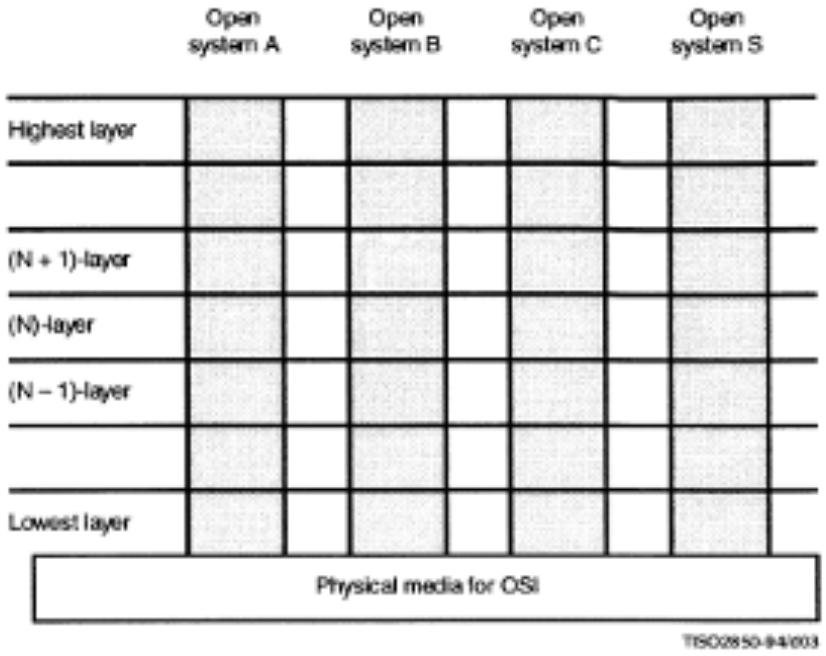


Figure 3 – Layering in cooperating open systems

INTERNATIONAL STANDARD

ISO 7498-2

First edition
1989-02-15

Information processing systems — Open Systems Interconnection — Basic Reference Model —

Part 2 :
Security Architecture

Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base —

Partie 2 : Architecture de sécurité

Information processing systems — Open Systems Interconnection — Basic Reference Model —

Part 2 :
Security Architecture

0 Introduction

ISO 7498 describes the Basic Reference Model for Open Systems Interconnection (OSI). That part of ISO 7498 establishes a framework for coordinating the development of existing and future standards for the interconnection of systems.

The objective of OSI is to permit the interconnection of heterogeneous computer systems so that useful communication between application processes may be achieved. At various times, security controls must be established in order to protect the information exchanged between the application processes. Such controls should make the cost of obtaining or modifying data greater than the potential value of so doing, or make the time required to obtain the data so great that the value of the data is lost.

This part of ISO 7498 defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required. It establishes, within the framework of the Reference Model, guidelines and constraints to improve existing standards or to develop new standards in the context of OSI in order to allow secure communications and thus provide a consistent approach to security in OSI.

A background in security will be helpful in understanding this document. The reader who is not well versed in security is advised to read annex A first.

This part of ISO 7498 extends the Basic Reference Model to cover security aspects which are general architectural elements of communications protocols, but which are not discussed in the Basic Reference Model.

1 Scope and field of application

This part of ISO 7498:

a) provides a general description of security services and related mechanisms, which may be provided by the Reference Model; and

b) defines the positions within the Reference Model where the services and mechanisms may be provided.

This part of ISO 7498 extends the field of application of ISO 7498, to cover secure communications between open systems.

Basic security services and mechanisms and their appropriate placement have been identified for all layers of the Basic Reference Model. In addition, the architectural relationships of the security services and mechanisms to the Basic Reference Model have been identified. Additional security measures may be needed in end-systems, installations and organizations. These measures apply in various application contexts. The definition of security services needed to support such additional security measures is outside the scope of this standard.

OSI security functions are concerned only with those visible aspects of a communications path which permit end systems to achieve the secure transfer of information between them. OSI Security is not concerned with security measures needed in end systems, installations, and organizations, except where these have implications on the choice and position of security services visible in OSI. These latter aspects of security may be standardized but not within the scope of OSI standards.

This part of ISO 7498 adds to the concepts and principles defined in ISO 7498; it does not modify them. It is not an implementation specification, nor is it a basis for appraising the conformance of actual implementations.

Conteúdo da 7498-2

DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

INTERNATIONAL TELECOMMUNICATION UNION

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

CCITT

THE INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE

X.800

3.3.51 **security service**

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

5 General description of security services and mechanisms

5.1 *Overview*

Security services that are included in the OSI security architecture and mechanisms which implement those services are discussed in this section. The security services described below are basic security services. In practice they will be invoked at appropriate layers and in appropriate combinations, usually with non-OSI services and mechanisms, to satisfy security policy and/or user requirements. Particular security mechanisms can be used to implement combinations of the basic security services. Practical realizations of systems may implement particular combinations of the basic security services for direct invocation.

Serviços de Segurança

- Autenticação
  - Autenticação de Entidade e Autent. de Origem de Dados
- Controle de acesso
- Confidencialidade de dados
  - Confidencialidade com conexão, sem conexão, seletiva por campos e de fluxo de tráfego
- Integridade de dados
  - Integridade com conexão com recuperação, sem recuperação e seletiva por campos; sem conexão e sem conexão seletiva por campos
- Irretratabilidade
  - Com prova de origem e com prova de entrega
- Disponibilidade

Mecanismos de Segurança Específicos

Associados a uma camada para oferecer serviços específicos

- Criptografia
- Assinatura Digital
- Controle de acesso
- Integridade de dados
- Troca de autenticações
- Preenchimento de tráfego
- Controle de roteamento
- Notarização

Mecanismos de Segurança Pervasivos

Não associados a nenhuma camada em particular

- Funcionalidade confiável
- Rótulo de segurança
- Detecção de evento
- Trilha de auditoria de segurança
- Recuperação de segurança

Relação entre serviços e mecanismos

Mechanism / Service	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	-	-	Y	-	-	-
Data origin authentication	Y	Y	-	-	-	-	-	-
Access control service	-	-	Y	-	-	-	-	-
Connection confidentiality	Y	-	-	-	-	-	Y	-
Connectionless confidentiality	Y	-	-	-	-	-	Y	-
Selective field confidentiality	Y	-	-	-	-	-	-	-
Traffic flow confidentiality	Y	-	-	-	-	Y	Y	-
Connection Integrity with recovery	Y	-	-	Y	-	-	-	-
Connection integrity without recovery	Y	-	-	Y	-	-	-	-
Selective field connection integrity	Y	-	-	Y	-	-	-	-
Connectionless integrity	Y	Y	-	Y	-	-	-	-
Selective field connectionless integrity	Y	Y	-	Y	-	-	-	-
Non-repudiation. Origin	-	Y	-	Y	-	-	-	Y
Non-repudiation. Delivery	-	Y	-	Y	-	-	-	Y

Posicionamento dos serviços

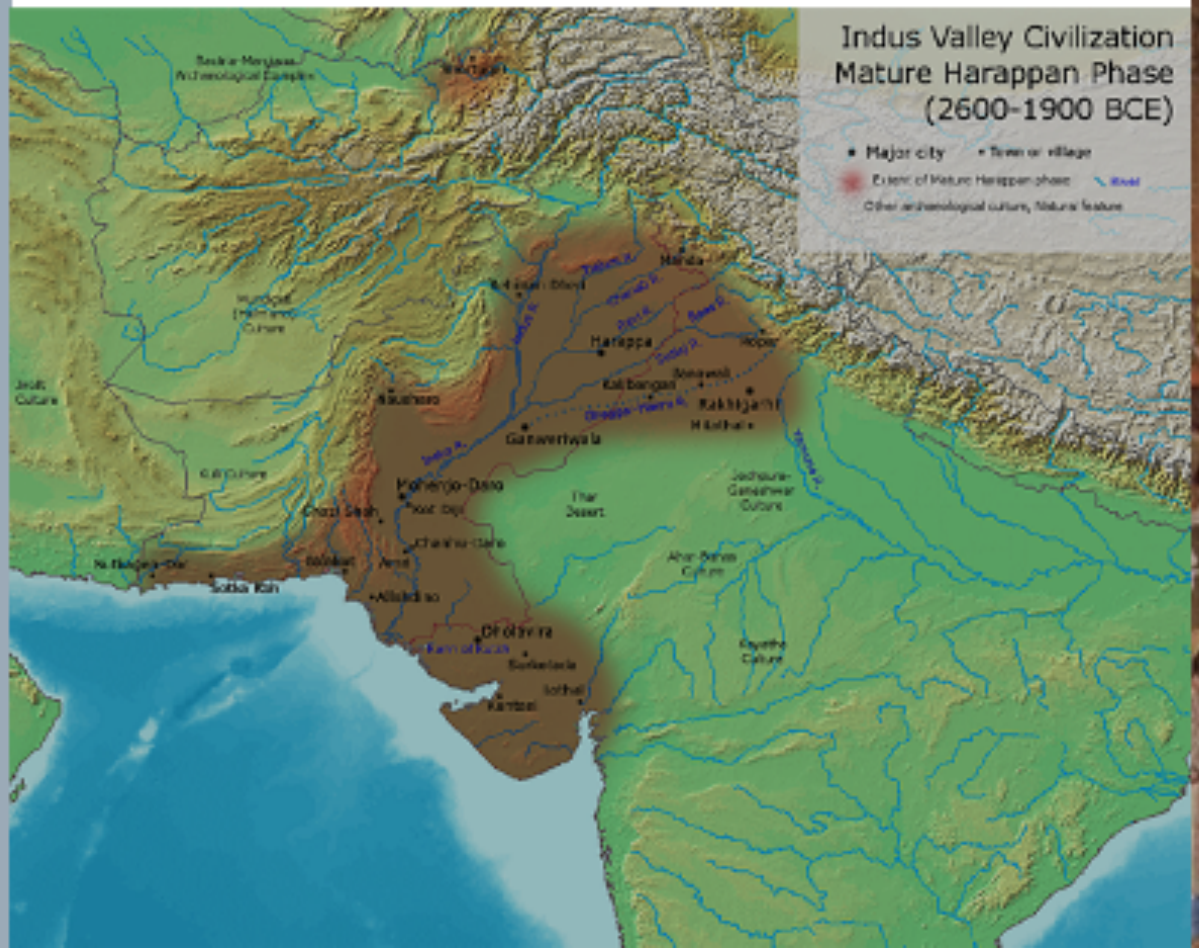
Service	Layer						
	1	2	3	4	5	6	7*
Peer entity authentication	·	·	Y	Y	·	·	Y
Data origen authentication	·	·	Y	Y	·	·	Y
Access control service	·	·	Y	Y	·	·	Y
Connection confidentiality	Y	Y	Y	Y	·	Y	Y
Connectionless confidentiality	·	Y	Y	Y	·	Y	Y
Selective field confidentiality	·	·	·	·	·	Y	Y
Traffic flow confidentiality	Y	·	Y	·	·	·	Y
Connection Integrity with recovery	·	·	·	Y	·	·	Y
Connection integrity without recovery	·	·	Y	Y	·	·	Y
Selective field connection integrity	·	·	·	·	·	·	Y
Connectionless integrity	·	·	Y	Y	·	·	Y
Selective field connectionless integrity	·	·	·	·	·	·	Y
Non-repudiation Origin	·	·	·	·	·	·	Y
Non-repudiation. Delivery	·	·	·	·	·	·	Y

Padronização de Segurança

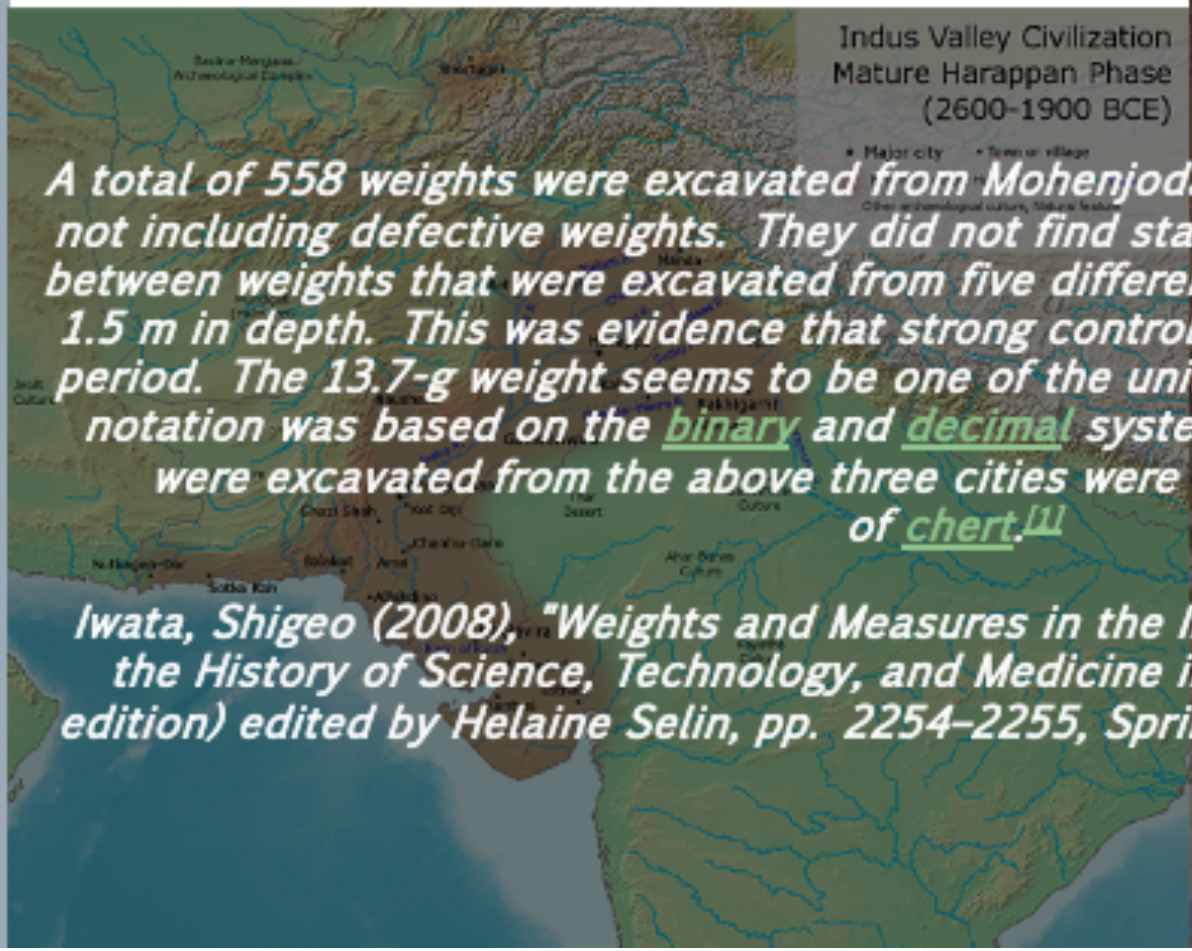
Padrões e Conformidade

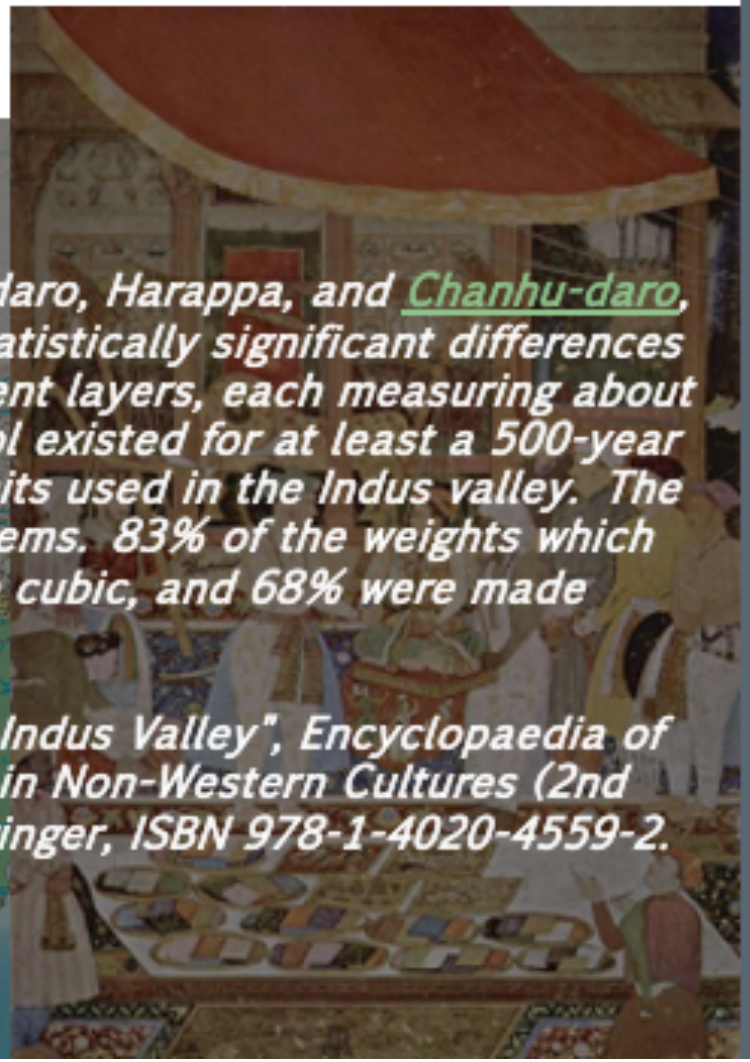
Padronização e Avaliação da Conformidade na Área de Segurança

Padrões, pesos e medidas: origens da metrologia científica



Padrões, pesos e medidas: origens na metrologia científica





A total of 558 weights were excavated from Mohenjodaro, Harappa, and Chanhu-daro, not including defective weights. They did not find statistically significant differences between weights that were excavated from five different layers, each measuring about 1.5 m in depth. This was evidence that strong control existed for at least a 500-year period. The 13.7-g weight seems to be one of the units used in the Indus valley. The notation was based on the binary and decimal systems. 83% of the weights which were excavated from the above three cities were cubic, and 68% were made of chert.[1]

Iwata, Shigeo (2008), "Weights and Measures in the Indus Valley", Encyclopaedia of the History of Science, Technology, and Medicine in Non-Western Cultures (2nd edition) edited by Helaine Selin, pp. 2254–2255, Springer, ISBN 978-1-4020-4559-2.

Tópicos Históricos da Padronização

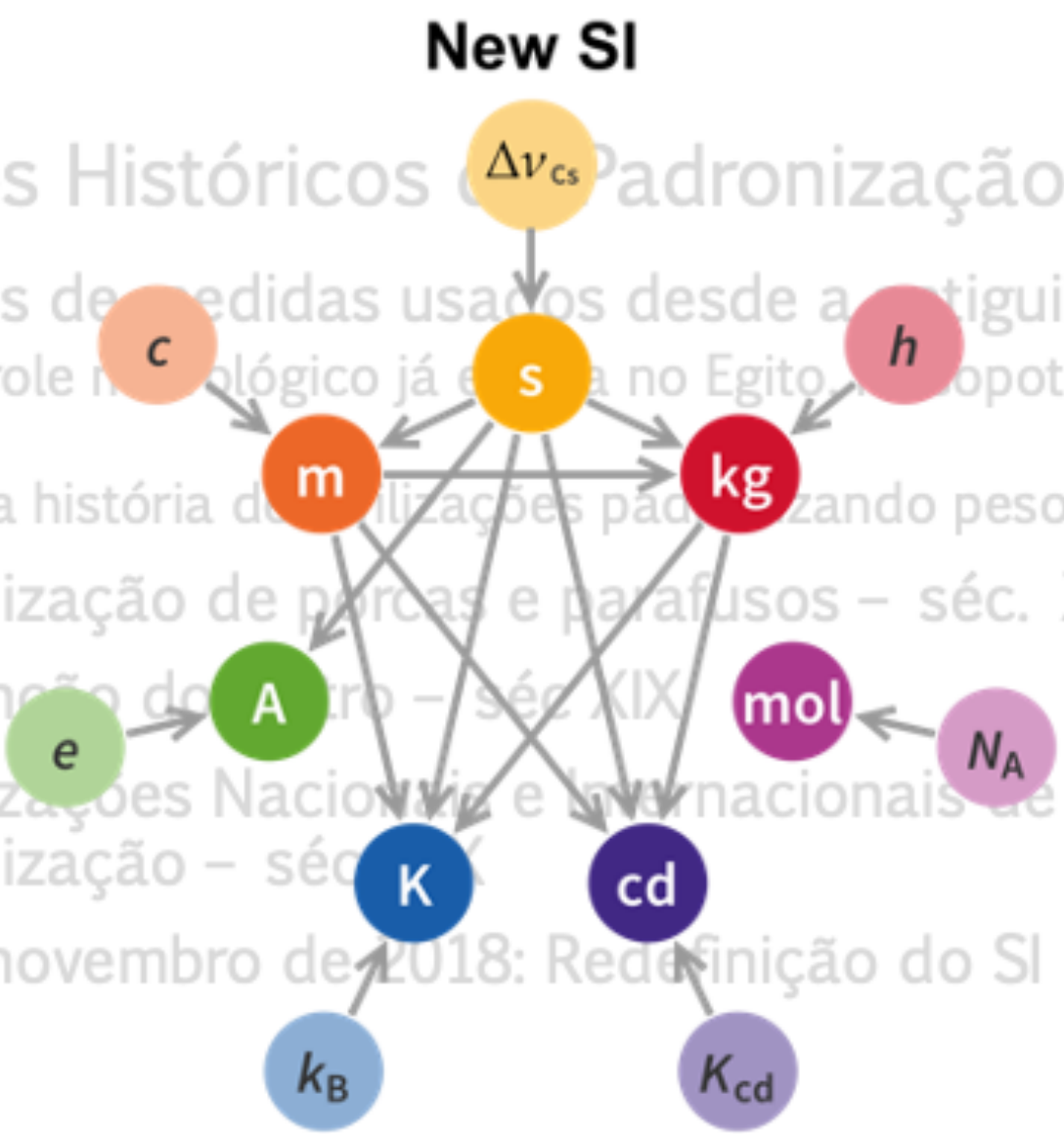
- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no Egito, Mesopotamia e Vale Indu
  - Longa história de civilizações padronizando pesos e medidas
- Padronização de porcas e parafusos – séc. XVIII
- Convenção do Metro – séc XIX
- Organizações Nacionais e Internacionais de Padronização – séc. XX
- 16 de novembro de 2018: Redefinição do SI

Histórico da Padronização

- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no vale indu
- Padronização de porcas e parafusos – séc. XVIII
- Organizações Nacionais de Padronização – séc. XX
  - 1901: Engineering Standards Committee (Inglaterra)
  - 1917: Deutsches Institut für Normung (Alemanha)
  - 1918: American National Standard Institute (EUA)
  - 1918: Commission Permanente de Standardisation (França)
- Padronização internacional:
  - formação da IEC (International Electrotechnical Commission) em 1906
  - fundação da ISA (depois ISO) em 1926 (resp. 1946)

Tópicos Históricos de Padronização

- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no Egito, Mesopotamia e Vale Indu
  - Longa história de utilizações padronizando pesos e medidas
- Padronização de porcas e parafusos – séc. XVIII
- Convenção do Metro – séc XIX
- Organizações Nacionais e Internacionais de Padronização – séc XX
- 16 de novembro de 2018: Redefinição do SI



Ex.: Padronização de Tempo (UTC)

BUREAU INTERNATIONAL DES POIDS ET MESURES

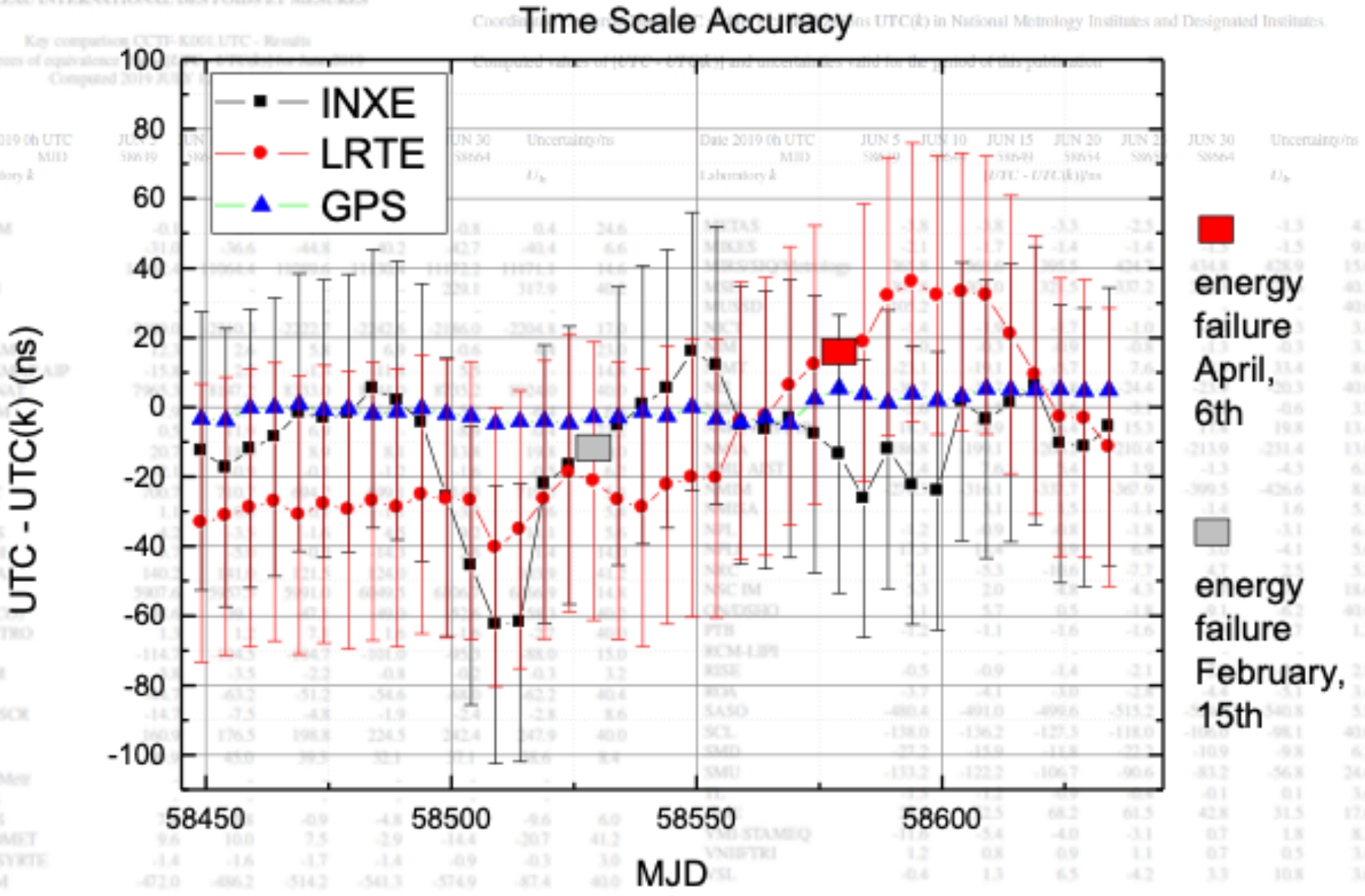
Key comparison CCTF-K001.UTC - Results
Degrees of equivalence $D_k = [UTC - UTC(k)]$ for June 2019
Computed 2019 JULY 12, 08h UTC

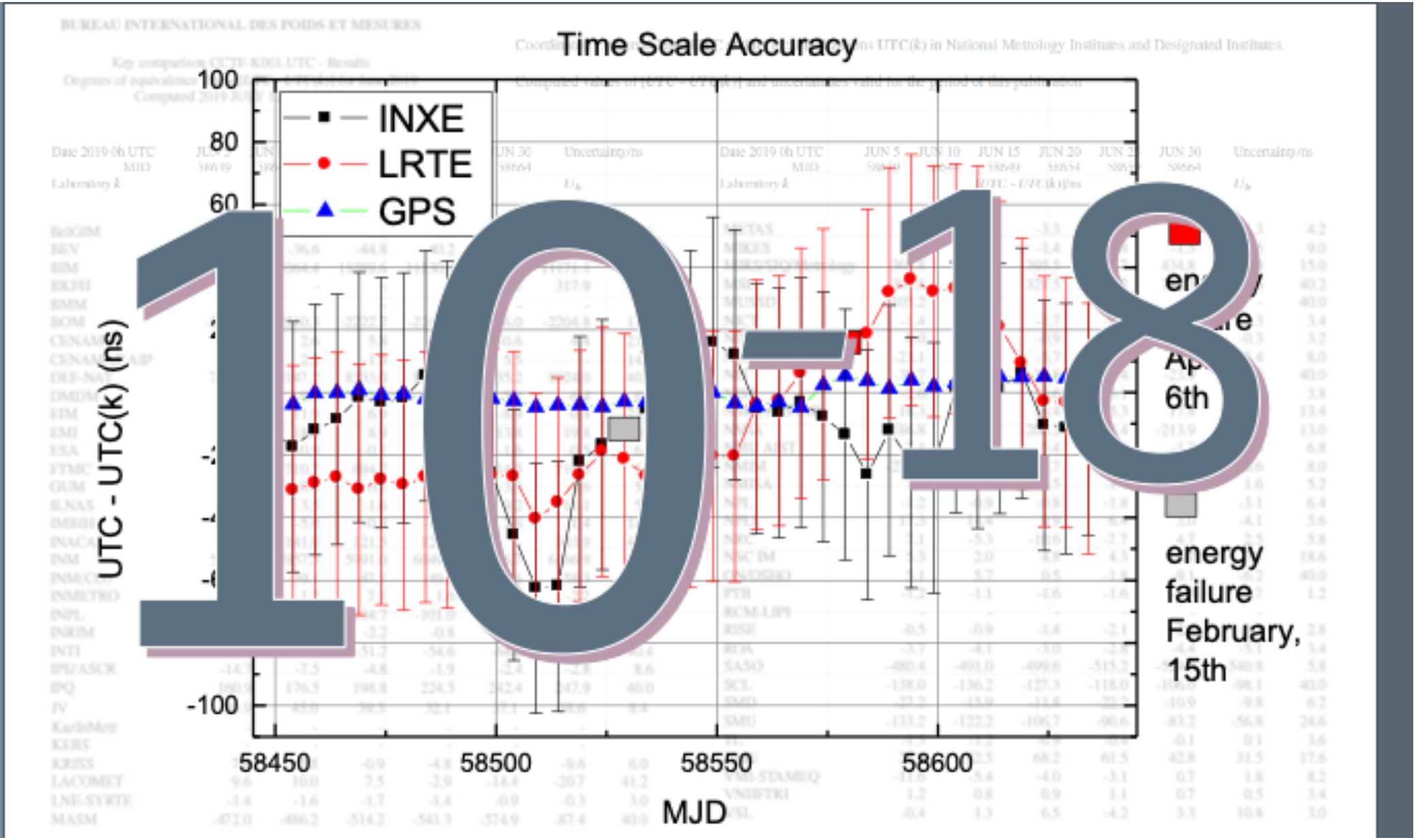
Coordinated Universal Time **UTC** and its local realizations **UTC(k)** in National Metrology Institutes and Designated Institutes.

Computed values of $[UTC - UTC(k)]$ and uncertainties valid for the period of this publication

Date 2019 0h UTC MJD Laboratory *k*	JUN 5 58639	JUN 10 58644	JUN 15 58649	JUN 20 58654	JUN 25 58659	JUN 30 58664	Uncertainty/ns U_k
	$[UTC - UTC(k)]$/ns						
BelGIM	-0.1	-0.8	-1.3	-1.5	-0.8	0.4	24.6
BEV	-31.0	-36.6	-44.8	-40.2	-42.7	-40.4	6.6
BIM	11052.4	11064.4	11089.6	11130.4	11172.2	11171.1	14.6
BKIH	-	-	-	-	229.1	317.9	40.2
BMM	-	-	-	-	-	-	
BOM	-2189.0	-2210.3	-2222.7	-2242.6	-2186.0	-2204.8	17.0
CENAM	12.3	2.6	5.8	6.9	-0.6	4.4	23.0
CENAMAP AIP	-15.8	2.2	-1.3	11.8	5.5	-	14.8
DEF-NAT	7965.3	8147.2	8333.0	8544.0	8735.2	8924.0	40.0
DMDM	-7.9	-9.7	-11.2	-14.5	-5.2	-6.4	6.6
EIM	0.5	11.9	6.9	-	-8.9	-0.4	23.2
EMI	20.7	18.0	8.9	8.1	13.8	19.8	19.0
ESA	-2.1	-0.9	-0.1	-1.2	-1.6	-0.5	6.2
FTMC	700.7	710.7	694.7	699.1	714.5	719.5	5.4
GUM	1.1	0.8	0.1	-1.1	-3.3	-5.6	5.4
ILNAS	-4.2	-3.5	-1.6	4.5	9.2	11.1	5.6
IMBIH	-5.7	-5.0	-0.3	-14.3	2.6	1.4	14.0
INACAL	140.2	141.0	121.5	124.0	-	103.9	41.2
INM	5907.6	5957.5	5991.0	6049.5	6106.7	6166.9	14.8
INM(CO)	-38.6	-39.1	-47.1	-49.0	-52.6	-58.3	40.2
INMETRO	1.3	1.2	7.1	1.6	-1.6	-2.7	40.0
INPL	-114.7	-104.5	-104.7	-101.0	-95.3	-88.0	15.0
INRIM	-3.8	-3.5	-2.2	-0.8	-0.2	-0.3	3.2
INTI	-44.7	-63.2	-51.2	-54.6	-68.0	-62.2	40.4
IPIT/ASCR	-14.7	-7.5	-4.8	-1.9	-2.4	-2.8	8.6
IPQ	160.9	176.5	198.8	224.5	242.4	247.9	40.0
JV	39.9	45.0	39.3	32.1	37.1	38.6	8.4
KazInMetr	-	-	-	-	-	-	
KEBS	-	-	-	-	-	-	
KRISS	7.8	3.8	-0.9	-4.8	-8.1	-9.6	6.0
LACOMET	9.6	10.0	7.5	-2.9	-14.4	-20.7	41.2
LNE-SYRTE	-1.4	-1.6	-1.7	-1.4	-0.9	-0.3	3.0
MASM	-472.0	-486.2	-514.2	-541.3	-574.9	-87.4	40.0

Date 2019 0h UTC MJD Laboratory *k*	JUN 5 58639	JUN 10 58644	JUN 15 58649	JUN 20 58654	JUN 25 58659	JUN 30 58664	Uncertainty/ns U_k
	$[UTC - UTC(k)]$/ns						
METAS	-3.8	-3.8	-3.3	-2.5	-1.6	-1.3	4.2
MIKES	-2.1	-1.7	-1.4	-1.4	-1.5	-1.5	9.0
MIRS/SIQ/Metrology	365.8	368.6	395.5	424.7	434.8	428.9	15.0
MSL	307.8	304.0	321.5	337.2	342.3	337.6	40.2
MUSSD	105.2	-	-	-	-	-	40.0
NICT	-1.4	-1.9	-1.7	-1.0	-0.7	-1.3	3.4
NIM	0.0	-0.3	-0.9	-0.8	-1.3	-0.3	3.2
NIMT	-23.1	-19.1	-5.7	7.6	28.3	33.4	8.0
NIS	-30.7	-37.7	-34.8	-24.4	-23.9	-20.3	40.0
NIST	-2.6	-3.5	-3.6	-3.1	-1.9	-0.6	3.8
NMC, A*STAR	18.3	20.9	16.4	15.3	17.4	19.8	13.4
NMIA	-186.8	-199.1	-206.2	-210.4	-213.9	-231.4	13.0
NMIJ AIST	7.4	7.6	5.4	1.9	-1.3	-4.3	6.8
NMIM	-278.3	-316.1	-337.7	-367.9	-399.5	-426.6	8.0
NMISA	-	3.1	1.5	-1.1	-1.4	1.6	5.2
NPL	-1.2	-0.9	-0.8	-1.8	-2.3	-3.1	6.4
NPLI	17.3	14.4	9.9	6.4	3.0	-4.1	5.6
NRC	7.1	-5.3	-10.6	-7.7	4.7	2.5	5.8
NSC IM	5.3	2.0	4.8	4.3	1.7	7.1	18.6
ONBDSHO	5.1	5.7	0.5	-1.8	-9.1	-6.2	40.0
PTB	-1.2	-1.1	-1.6	-1.6	-1.8	-1.7	1.2
RCM-LIPI	-	-	-	-	-	-	
RISE	-0.5	-0.9	-1.4	-2.1	-2.8	-3.1	2.8
ROA	-3.7	-4.1	-3.0	-2.8	-4.4	-5.1	3.4
SASO	-480.4	-491.0	-499.6	-515.2	-529.6	-540.8	5.8
SCL	-138.0	-136.2	-127.3	-118.0	-106.0	-98.1	40.0
SMD	-27.2	-15.9	-11.8	-22.2	-10.9	-9.8	6.2
SMU	-133.2	-122.2	-106.7	-90.6	-83.2	-56.8	24.6
TL	-1.5	-1.2	-0.9	-0.4	-0.1	0.1	3.6
UME	35.5	52.5	68.2	61.5	42.8	31.5	17.6
VMI-STAMEQ	-11.6	-5.4	-4.0	-3.1	0.7	1.8	8.2
VNIIFTRI	1.2	0.8	0.9	1.1	0.7	0.5	3.4
VSL	-0.4	1.3	6.5	-4.2	3.3	10.8	3.0


Time Scale Accuracy
INXE
LRTE
GPS
UTC - UTC(k) (ns)
MJD
100
80
60
40
20
0
-20
-40
-60
-80
-100
58450
58500
58550
58600
energy failure April, 6th
energy failure February, 15th

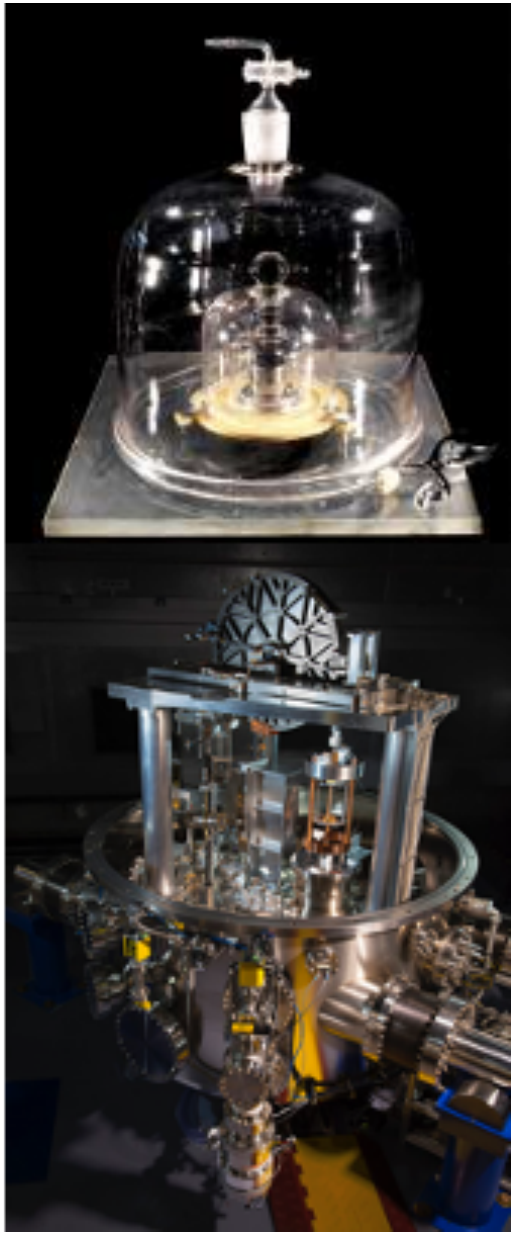

Time Scale Accuracy
INXE
LRTE
GPS
UTC - UTC(k) (ns)
100
80
60
-100
58450
58500
58550
58600
MJD
10-18
energy
failure
February,
15th

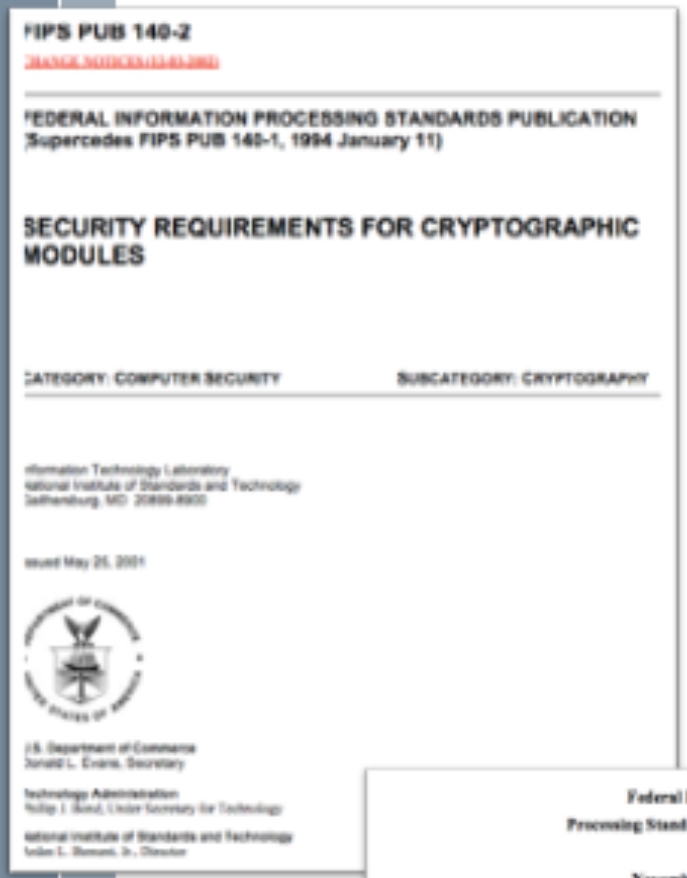
Importância dos padrões metrológicos

- Comércio
  - Muitos negócios baseiam-se em massa, área, volume – e até grandezas mais "inesperadas" (umidade, poder calorífico,...)
- Tributação
  - Governos também precisam saber das "quantidades" negociadas para aplicar taxação
- Indústria
  - Peças produzidas em diferentes países precisam "se encaixar"
  - Propriedades químicas de insumos para processos industriais
- Ciência
  - "*Metrology is key to reproducing results*" - Nature 547 (jul-2017)

Que padrões...?

- Padrões de referência de grandezas físicas
  - Metrologia científica "clássica" (SI)
  - Materiais de referência (inclusive biológicos)
  - Peças e ferramentas, processos industriais,...
- Padrões de software e segurança cibernética
  - Definições claras e rigorosas das "referências"
  - Padrão *versus* norma
- Exemplos de padrões de software/segurança
  - Algoritmo criptográficos (ex. AES)
  - Segurança de Hardware (ex. FIPS 140-2)
  - Metodologia de gestão de riscos (ex. NIST CSF)
  - Esquemas de validação de software (ex. CC)
  - Sistema de Gestão (ex. ISO/IEC 27001)
  - Auditoria de Labs (NVLAP Handbooks 150-17)





FIPS PUB 140-2

CHANGE NOTICES (12-03-2002)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

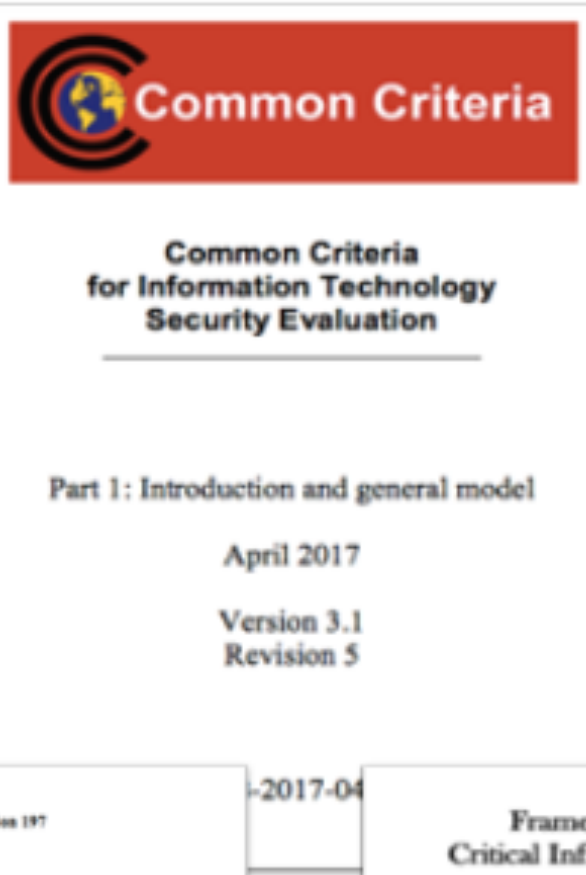
nformation Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

ssued May 25, 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Philip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director



Common Criteria

Common Criteria
for Information Technology
Security Evaluation

Part 1: Introduction and general model

April 2017

Version 3.1
Revision 5

-2017-04

INTERNATIONAL STANDARD ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005

Federal Information
Processing Standards Publication 197

November 26, 2001

Announcing the

ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 199 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235)

Framework for Improving
Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

January 10, 2017

Importância da Padronização

- Padrões representam a convergência técnica entre os maiores especialistas em um assunto
  - Descrevem as melhores práticas em relação àquele assunto
- Definem uma base conceitual e nomenclatura comum
  - Facilitam comunicação, medição, comércio e interoperabilidade
- Promovem boas práticas para a economia:
  - facilitam a interação entre empresas
  - facilitam a conformidade a leis e regulações
  - aceleram a introdução de inovações
  - promovem a interoperabilidade entre produtos, serviços e processos – novos e existentes

Princípios para desenvolvimento de padrões

- Padrões devem ser uma resposta a uma necessidade do mercado ou da sociedade
  - Para serem efetivos, padrões devem ser criados como uma resposta a uma necessidade de um setor do mercado ou da sociedade.
- Padrões devem ser baseados na opinião de especialistas
  - Bons padrões envolvem uma forte participação e liderança de especialistas, os quais negociam todos os detalhes técnicos dos padrões
- Padrões devem ser desenvolvidos numa base "multi-stakeholder"
  - Comitês técnicos responsáveis pelo desenvolvimento de padrões devem incluir especialistas do Governo, Indústria, Academia, Consumidores, Organizações Não-Governamentais e Sociedade, em geral.
- Padrões devem ser baseados em consenso
  - Comentários de todos os stakeholders devem ser levados em consideração

Padronização de Telecom

- ITU-T (ITU Telecommunication Standardization Sector)
  - 17-mai-1865: assinatura da Convention Télégraphique Internationale de Paris
    - Padrões elétricos e operacionais de telefones e telégrafos
    - Posteriormente, comunicações por rádio
  - Início do Século XX: CCIF, CCIR CCIT
  - 1956: CCITT (Comité Consultatif International Téléphonique et Télégraphique)
  - 1993: ITU-T
- Histórico: padronização de aspectos físicos e elétricos de equipamentos de telecom

Padronização em TIC

- Organizações internacionais formais
  - ISO/IEC, ITU-T
- Outros fóruns internacionais
  - IETF
- Organizações regionais relevantes
  - IEEE, ETSI
- Instituições de Governos Nacionais relevantes
  - NIST, BSI, ANSSI, NCSC
- Instituições setoriais relevantes
  - PCI SSC, NERC

IEEE-SA

- Institute of Electrical and Electronics Engineers Standards Association
- Padrões em diversas áreas: TI, telecom, energia,...
- Exemplos:
  - 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee
  - tecnologias de rede: wifi (802.11), Bluetooth, Wimax,...

IETF

- Internet Engineering Task-Force
- Evolução da arquitetura da internet e operação da internet
- Publicação de RFCs (Requests for Comments)
- Exemplos:
  - Domain Name System (DNS) security, authentication protocols, routing protocol security, Internet Protocol (IP) version 6, public key infrastructure, e-mail security, event logging, network traffic encryption

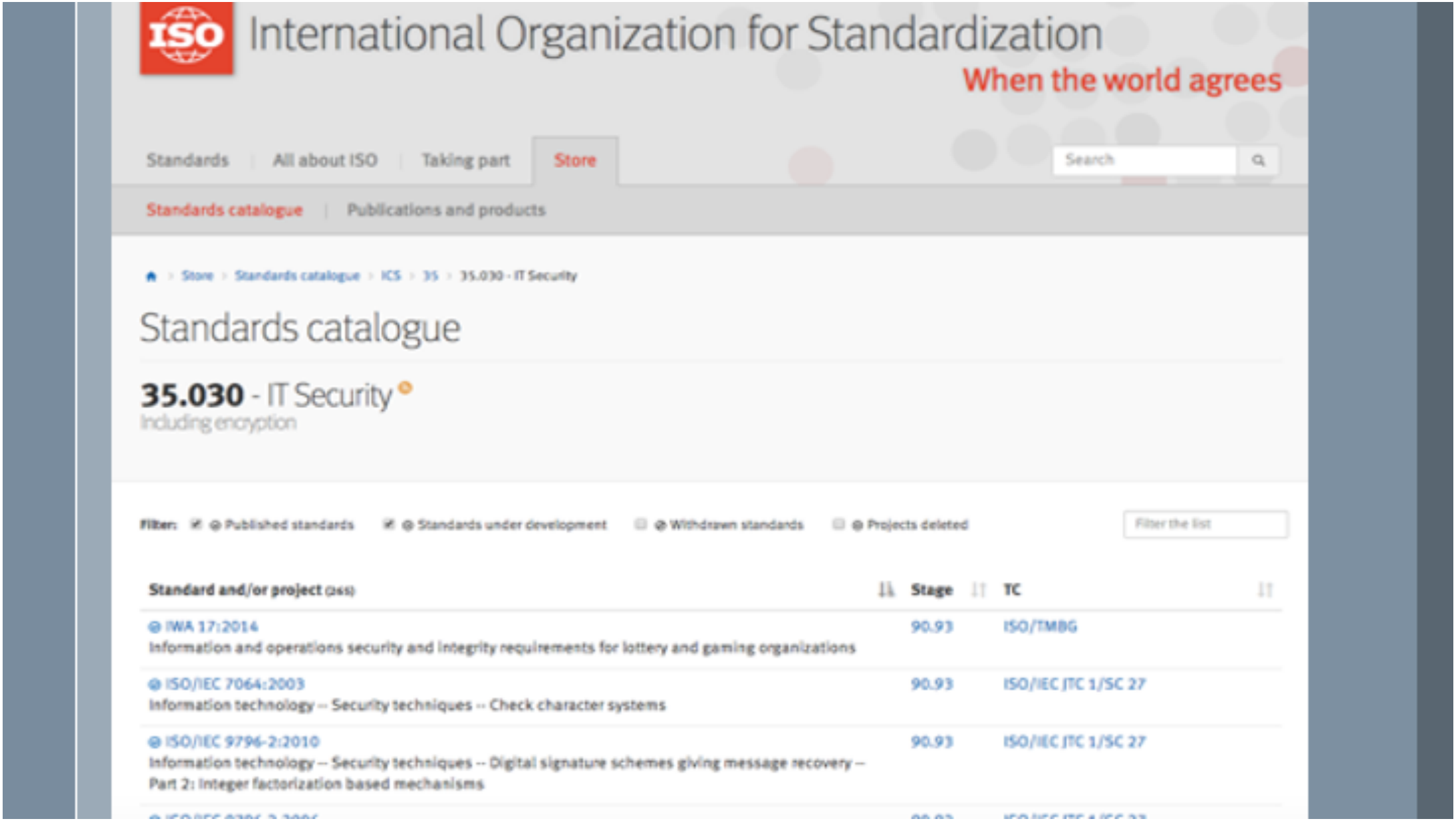
ISO

- International Organization for Standardization
- Mais de 150 países membros
- Aborda padrões de todas as áreas
- Padrões de elétrica/eletrônica são desenvolvidos em conjunto com IEC (JTC1)
- Exemplos:
  - Grupo SC17: cartões de identificação e identificação pessoal
  - Grupo SC27: técnicas de segurança de TI
  - Grupo SC31: identificação automática e captura de dados
  - Grupo SC37: padrões biométricos

LIST OF TECHNICAL COMMITTEES

FILTER BY TECHNICAL SECTOR: ALL SECTORS (248)

REFERENCE	TITLE	ISOTC WORKING AREA	PUBLISHED STANDARDS	STANDARDS UNDER DEVELOPMENT
ISO/IEC JTC 1	Information technology	Working area	3241	560
ISO/TC 22	Road vehicles	Working area	932	272
ISO/TC 34	Food products	Working area	866	126
ISO/TC 184	Automation systems and integration	Working area	854	48
ISO/TC 61	Plastics	Working area	687	118
ISO/TC 20	Aircraft and space vehicles	Working area	676	112
ISO/TC 29	Small tools	Working area	462	28
ISO/TC 45	Rubber and rubber products	Working area	439	77
ISO/TC 38	Textiles	Working area	402	60
ISO/TC 23	Tractors and machinery for agriculture and forestry	Working area	375	100
ISO/TC 8	Ships and marine technology	Working area	357	114
ISO/TC 44	Welding and allied processes	Working area	325	37
ISO/TC 147	Water quality	Working area	325	32
ISO/TC 138	Plastics pipes, fittings and valves for the transport of fluids	Working area	319	59
ISO/TC 17	Steel	Working area	311	37


International Organization for Standardization
When the world agrees
Standards
All about ISO
Taking part
Store
Search
Standards catalogue
Publications and products
Store › Standards catalogue › ICS › 35 › 35.030 - IT Security
Standards catalogue
35.030 - IT Security
Including encryption
Filter: Published standards Standards under development Withdrawn standards Projects deleted
Filter the list
Standard and/or project (255)
Stage
TC
IWA 17:2014
Information and operations security and integrity requirements for lottery and gaming organizations
90.93
ISO/TMBG
ISO/IEC 7064:2003
Information technology -- Security techniques -- Check character systems
90.93
ISO/IEC JTC 1/SC 27
ISO/IEC 9796-2:2010
Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
90.93
ISO/IEC JTC 1/SC 27

ITU-T

- ITU Telecommunication Standardization Sector
- Produz padrões chamados *Recommendations*, para redes de comunicação
- O grupo de estudo 17 (SG17) coordena os trabalhos relacionados a segurança entre todos os grupos de estudo do ITU-T.
- Exemplos:
  - X.800: Security architecture for Open Systems Interconnection for CCITT applications
  - Recommendation ITU-T X.509 for electronic authentication over public networks

Padronização e Avaliação da Conformidade

- Padrões frequentemente têm foco nos ”requisitos”
  - Mas é importante saber avaliar se os padrões estão sendo alcançados
- Testes de conformidade permitem avaliar o atendimento aos requisitos de um padrão
  - Realizados através de ensaios, inspeções, auditorias etc.
- Avaliação da Conformidade têm seus próprios padrões (ISO série 17000)

Padronização versus Obscurantismo

Obscurantismo

- Princípio através do qual se protege a Segurança de um sistema por meio do Segredo/Sigilo dos seus detalhes de implementação
- Conceito predominante até o século XIX por meio da esteganografia
- O tratamento cada vez mais "científico" da Segurança Cibernética - apoiado por disciplinas como Criptografia, Complexidade Computacional, Especificação Formal,... - tem relegado o obscurantismo a uma posição bastante restrita.
- O conceito ainda é bastante difundido em setores como Governo, Diplomacia, Militar/Defesa...

Padronização versus obscurantismo

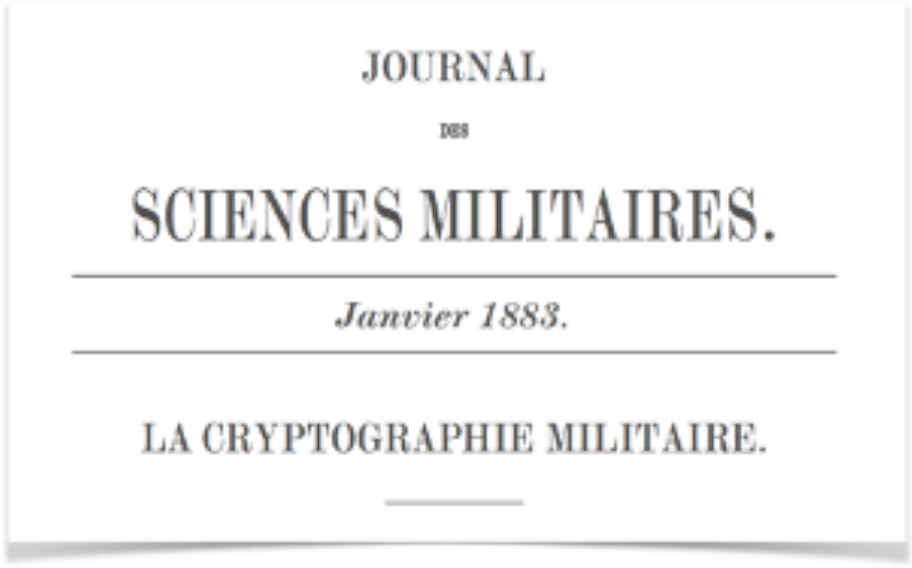
- Padronização versus obscurantismo: uma decisão técnica e política
  - Obscurantismo tem seu lugar em aplicações específicas
  - Mas para a maioria das aplicações, não é prático ou realístico
- Desvantagens do obscurantismo
  - Não pode ser garantida ao longo do tempo
    - Equipamentos criptográficos podem ser capturados por inimigo
    - Desenvolvedores de software mudam de empresa (para o concorrente!)
  - Reduz a visibilidade pelos usuários a respeito das funcionalidades do sistema
    - Como se ter certeza de que um equipamento sensível não está sujeito a manipulações?

Desvantagens do Obscurantismo

- Não pode ser garantida ao longo do tempo
  - Equipamentos criptográficos podem ser capturados por inimigo
  - Desenvolvedores de software mudam de empresa (para o concorrente!)
- Reduz a visibilidade pelos usuários a respeito das funcionalidades do sistema
  - Como o cidadão pode ter certeza de que um equipamento sensível (por exemplo, uma urna eletrônica ou um medidor inteligente) não está sujeito a manipulações?

Princípios de Criptografia de Kerckhoff

› DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE



JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Princípios de Criptografia de Kerckhoff

1. O sistema deve ser materialmente, se não matematicamente, indecifrável;
2. É necessário que o sistema em si não requeira sigilo, e que não seja um problema se ele cair nas mãos do inimigo;
3. Deve ser possível comunicar e lembrar da chave sem a necessidade de notas escritas, e os interlocutores devem ser capazes de modificá-la a seu critério;
4. Deve ser aplicável à correspondência telegráfica;
5. O sistema deve ser portátil, e não deve exigir a participação de múltiplas pessoas na sua operação e manuseio;
6. Por fim, o sistema deverá ser simples de usar e não exigir conhecimentos profundos ou concentração dos seus usuários nem um conjunto complexo de regras.

Por que padrões...

- Permitem ”refletir” para soluções locais as referências e boas práticas internacionais
- Padrões forçam o exercício do método científico
  - Descrição rigorosa de conceitos, requisitos e métodos
  - Compreensão plena e domínio técnico
- Padrões facilitam a propagação de informação
  - Estimulam a implantação de soluções de segurança
  - Caso do DES (Data Encryption Standard) – prox. slide

Requisitos do Data Encryption Standard

- The algorithm must provide a high level of security.
- The algorithm must be completely specified and easy to understand.
- The security of the algorithm must reside in the key; the security should not depend on the secrecy of the algorithm.
- The algorithm must be available to all users.
- The algorithm must be adaptable for use in diverse applications.
- The algorithm must be economically implementable in electronic devices.
- The algorithm must be efficient to use.
- The algorithm must be able to be validated.
- The algorithm must be exportable.

Impacto do Data Encryption Standard

- *These standards were unprecedented. Never before had an NSA-evaluated algorithm been made public. [...] DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure.*

Bruce Schneier, Applied Cryptography

Padronização, Avaliação da Conformidade e Auditibilidade

- Possibilidade de analisar todas as características e os detalhes de implementação de um sistema
- A estrutura de Padronização Técnica e Avaliação da Conformidade leva o conceito de auditibilidade a um novo patamar
  - Modelos avaliação de riscos e especificação de requisitos são padronizadas
  - Metodologias de avaliação da conformidade - ensaios e testes de segurança - são claramente especificados
  - Até mesmo os procedimentos de auditoria são claramente descritos

Padronização de um Algoritmo Criptográfico (AES)

Exemplo de transição
Academia -> Governo -> Indústria

Chamada por algoritmos

Federal Register / Vol. 62, No. 177 / Friday, September 12, 1997 / Notices 48051

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 970725180–7180–01]

RIN No. 0693–ZA16

Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; Request for candidate encryption algorithm nomination packages.

SUMMARY: A process to develop a Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES) specifying an Advanced Encryption Algorithm (AEA) has been initiated by the National Institute of Standards and Technology (NIST). This notice requests submission of candidate algorithms for *consideration for inclusion in the* AES and specifies how to submit a nomination package. The requirements for candidate algorithm submission packages and minimum acceptability requirements that must be satisfied in order to be deemed a "complete and proper" submission are presented. the evaluation criteria which will be used to appraise the candidate algorithms are also described.

Cinco Finalistas

Volume 104, Number 5, September–October 1999
Journal of Research of the National Institute of Standards and Technology

[J. Res. Natl. Inst. Stand. Technol. **104**, 435 (1999)]

Status Report on the First Round of the Development of the Advanced Encryption Standard

Volume 104 Number 5 September–October 1999

James Nechvatal, Elaine Barker, Donna Dodson, Morris Dworkin, James Foti, and Edward Roback

National Institute of Standards and Technology,
Gaithersburg, MD 20899-0001

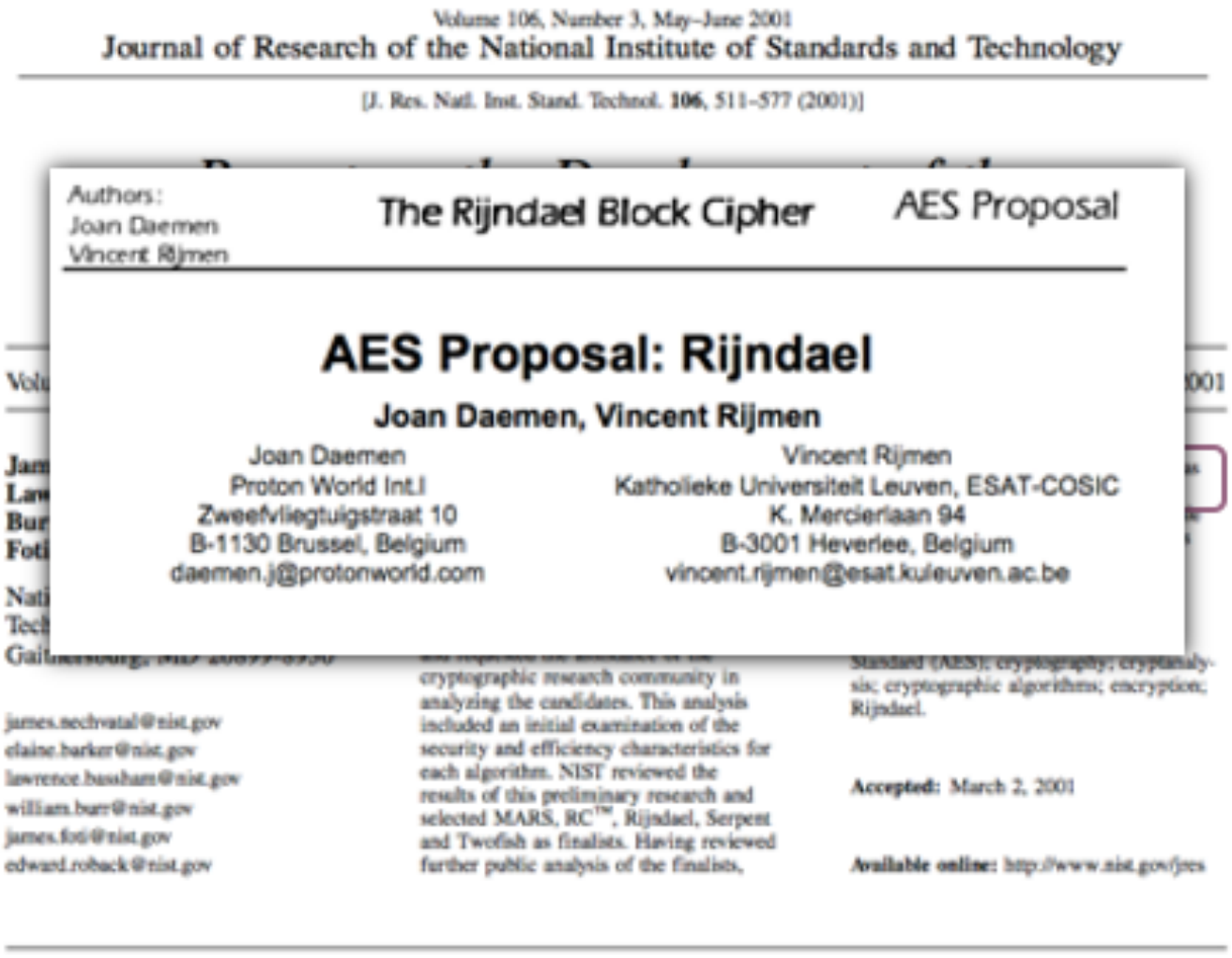
In 1997, the National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information in furtherance of NIST's statutory responsibilities. In 1998, NIST announced the acceptance of 15 candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. This analysis included an initial examination of the security and efficiency characteristics for each algorithm. NIST has reviewed the results of this research and selected five algorithms (MARS, RC6™, Rijndael, Serpent and Twofish) as finalists. The research results and rationale for the selection of the finalists are documented in this report. The five finalists will be the subject of further study before the selection of one or more of these algorithms for inclusion in the Advanced Encryption Standard.

Key words: Advanced Encryption Standard (AES); cryptography; cryptanalysis; cryptographic algorithms; encryption.

Accepted: August 11, 1999

Available online: http://www.nist.gov/jres

O escolhido: Rijndael



Volume 106, Number 3, May–June 2001
Journal of Research of the National Institute of Standards and Technology

[J. Res. Natl. Inst. Stand. Technol. **106**, 511–577 (2001)]

Authors:
Joan Daemen
Vincent Rijmen

The Rijndael Block Cipher AES Proposal

AES Proposal: Rijndael

Joan Daemen, Vincent Rijmen

Joan Daemen
Proton World Intl
Zweefvliegtuigstraat 10
B-1130 Brussel, Belgium
daemen.j@protonworld.com

Vincent Rijmen
Katholieke Universiteit Leuven, ESAT-COSIC
K. Mercierlaan 94
B-3001 Heverlee, Belgium
vincent.rijmen@esat.kuleuven.ac.be

Vol … 001

Jam…
Law…
Bur…
Foti…

Nati…
Tech…
Gai…

james.nechvatal@nist.gov
elaine.barker@nist.gov
lawrence.bassham@nist.gov
william.burr@nist.gov
james.foti@nist.gov
edward.roback@nist.gov

cryptographic research community in analyzing the candidates. This analysis included an initial examination of the security and efficiency characteristics for each algorithm. NIST reviewed the results of this preliminary research and selected MARS, RC™, Rijndael, Serpent and Twofish as finalists. Having reviewed further public analysis of the finalists,

Standard (AES); cryptography; cryptanalysis; cryptographic algorithms; encryption; Rijndael.

Accepted: March 2, 2001

Available online: http://www.nist.gov/jres

Federal Information

Processing Standards Publication 197

November 26, 2001

Announcing the

ADVANCED ENCRYPTION STANDARD (AES)

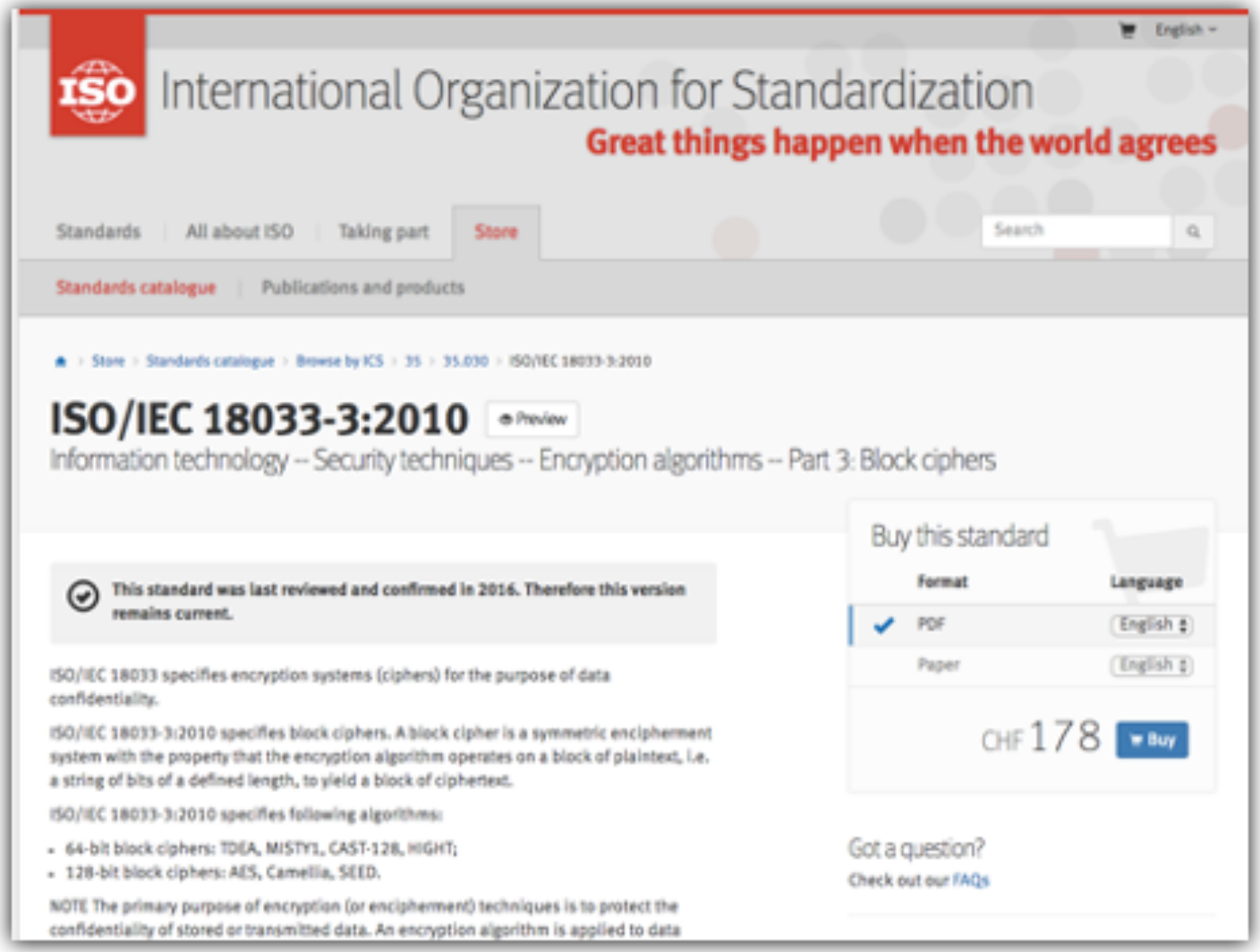
Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS PUB 197).

6. **Applicability.** This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection.

Other FIPS-appeoved cryptographic algorithms may be used in addition to, or in lieu of, this standard. Federal agencies or departments that use cryptographic devices for protecting classified information can use those devices for protecting sensitive (unclassified) information in lieu of this standard.

In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.


English
International Organization for Standardization
Great things happen when the world agrees
Standards
All about ISO
Taking part
Store
Search
Standards catalogue
Publications and products
Store › Standards catalogue › Browse by ICS › 35 › 35.030 › ISO/IEC 18033-3:2010
ISO/IEC 18033-3:2010
Preview
Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
This standard was last reviewed and confirmed in 2016. Therefore this version remains current.
ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality.
ISO/IEC 18033-3:2010 specifies block ciphers. A block cipher is a symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext.
ISO/IEC 18033-3:2010 specifies following algorithms:
64-bit block ciphers: TDEA, MISTY1, CAST-128, HIGHT;
128-bit block ciphers: AES, Camellia, SEED.
NOTE The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data
Buy this standard
Format
Language
PDF
English
Paper
English
CHF 178
Buy
Got a question?
Check out our FAQs

Avaliação da Conformidade

A medida realizada é válida?
O produto atende ao padrão??

Importância da conformidade

- Padrões só são úteis se forem aderidos/seguidos
- Como induzir o atendimento ao padrão
  - Conceito de regulação
- Como demonstrar o atendimento ao padrão
  - Conceito de avaliação da conformidade

Avaliação da conformidade

- Definição: conjunto de técnicas e atividades que têm por objetivo evidenciar que um produto, processo, serviço, sistema de gestão, pessoa ou organização atende a um conjunto de requisitos.
  - Exemplos dessas técnicas e atividades incluem estimação, auditoria, calibração, avaliação, exame, inspeção, e teste
  - Podem resultar numa declaração de conformidade pelo fornecedor, numa certificação ou numa acreditação

Padrões de Avaliação da Conformidade

- A ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) possuem publicações internacionais sobre avaliação da conformidade
  - Essas publicações internacionais são amplamente reconhecidas e usadas nos mais diversos setores e atores para atividades de avaliação da conformidades

Regulação, padrões e avaliação da conformidade

- Avaliação da conformidade baseada em padrões internacionais
  - favorece o reconhecimento do processo como bem-fundamentado e legítimo.
  - evita que regulações adicionem custos desnecessários e questionamentos quanto a barreiras técnicas ao comércio

Técnicas de avaliação da conformidade

- **Avaliação (assessment)** da competência técnica de uma organização;
- **Auditoria** de um sistema de gestão de uma organização;
- **Avaliação (evaluation)** de um produto, processo ou serviço em relação a um conjunto de requisitos;
- **Exame** da competência de uma pessoa;
- **Inspeção** de uma instalação, produto ou serviço;
- **Teste** de uma característica de produto.

Padrões de AC mais relevantes

- ISO/IEC DIS 17000 [Under development]
  - Conformity assessment -- Vocabulary and general principles
- ISO/IEC 17011:2017
  - Conformity assessment -- Requirements for accreditation bodies accrediting conformity assessment bodies
- ISO/IEC 17020:2012
  - Conformity assessment -- Requirements for the operation of various types of bodies performing inspection
- ISO/IEC 17021 (várias partes)
  - Conformity assessment -- Requirements for bodies providing audit and certification of management systems
- ISO/IEC 17025:2017
  - General requirements for the competence of testing and calibration laboratories

Padrões mais relevantes

- ISO 17034:2016
  - General requirements for the competence of reference material producers
- ISO/IEC 17040:2005
  - Conformity assessment -- General requirements for peer assessment of conformity assessment bodies and accreditation bodies
- ISO/IEC 17043:2010
  - Conformity assessment -- General requirements for proficiency testing
- ISO/IEC 17065:2012
  - Conformity assessment -- Requirements for bodies certifying products, processes and services
- ISO/IEC 17067:2013
  - Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes

Declarações de Conformidade

- Declarações a respeito do "objeto" de uma avaliação (produto, processo, serviço, sistema de gestão ou organismo)
  - feitas após aplicação de uma ou mais técnicas de avaliação
- Declarações de conformidade podem ser feitas por:
  - **Primeira parte** – pessoa ou organização que fornece o objeto e que é responsável pelo atendimento aos requisitos (exemplo, fabricante);
  - **Segunda parte** – pessoa ou organização que tem interesse no objeto (exemplo, uma cadeia de varejo comprando para revender; um órgão público validando um lote de produtos de uma compra pública);
  - **Terceira parte** – pessoa ou organização que é independente de quem fornece ou consome ou objeto (exemplos: laboratório de testes e organismo de certificação imparciais).

Exemplo de certificação: equip. ICP-Brasil

Cartão utilizado para assinar documento
e leitora usada para ler o cartão...

Atendem a requisitos definidos
por padrões internacionais

Bureau International des Poids et Mesures

ISO

IAF INTERNATIONAL ACCREDITATION FORUM

INMETRO

Equipamentos

Processos/qualidade

Pessoas

Avaliados por
laboratórios acreditados