Redes, Segurança e IoT

Programa de Pós-Graduação em Metrologia
Professor Raphael Machado

Objetivos do Curso

- Compreender riscos e modelos de ataque associados às diferentes aplicações de tecnologia da informação
- Conhecer as ferramentas e métodos de ataque e de defesa
  - Não é um curso de Criptografia – embora a Criptografia seja uma ferramenta fundamental para a construção de arquiteturas de segurança.
- Conhecer as diversas áreas da segurança nos setores corporativo, de estado e em pesquisa.

Objetivos... Em outras palavras

- Convencer o aluno de que Segurança da Informação...
  - é uma questão real (e que ataques cibernéticos são um problema capaz de grande impacto ”real”)
  - é um tema transversal, perpassa todas as áreas de negócio (e da sociedade)
  - dá origem a interessantes temas de pesquisa e desenvolvimento
- Apresentar ao aluno os fundamentos e conceitos que o permitirão trabalhar no tema de segurança – ou, pelo menos, compreendê-lo
- Apresentar ao aluno, temas de trabalho, desenvolvimento tecnológico e pesquisa científica na área de segurança

Abordagem do Curso

- Diferentes visões e aplicações de segurança
  - Governo, Mercado, Academia,...
- Curso fortemente orientado a ataques.
  - Muito além de Alice e Bob
- Curso fortemente orientado a padrões.
  - Buscar conhecimento na fonte
- Curso alterna momentos "informativos" e "formativos"
  - Predominantemente informativo: transmissão de informações (ex.: histórico de ransomware)
    - Pode ser considerado um curso "fácil"
  - Alguns tópicos formativos: conceitos/fundamentos (ex.: criptografia)

Avaliação

- Provas
  - 50% da nota
- Projeto
  - 30% da nota
- Atividades Complementares
  - 20% da nota

Temas de projetos de pesquisa

- Segurança de software (vulnerabilidades)
  - Implementar programa/aplicação simples com vulnerabilidade listada no SANS/CWE Top 25 (ou outra de relevância)
- Segurança de redes (ferramentas)
  - implementar rede (possivelmente, usando virtualização) contendo ferramentas básicas de segurança (IDS, IPS, FW, SIEM,...)
- Honeypot/honeynet
  - implementar host vulnerável, deixa-lo acessível e coletar dados de atacantes
- Números aleatórios
  - identificar três fontes distintas de números aleatórios e estudar a aleatoriedade

Temas de projetos de pesquisa

- Análise Estática de Código
  - demonstrar casos de uso das seguintes técnicas: grafo de controle de fluxo, grafo de chamada, tainting, value set analysis
- Análise Estática de Código - identificação de vulnerabilidades
  - Comparar pelo menos duas ferramentas com relação à identificação de vulns
- Ataques a sistemas industriais em rede
  - Desafio: dado objetivo (ex.: aumento de 45% a 55% de threshold) identificar sistema e minimizar número de perdas de pacotes para atingir o objetivo
- Padrões de cybersecurity em setores específicos
  - quais são as organizações e os padrões? existem regulamentos? Em que países? existe certificação? Como funciona?
- Projeto de pesquisa específico alinhado com professor

Questões práticas

- Grupo (email)
  - https://groups.google.com/d/forum/xxx
- Site
  - https://siccciber.com.br/ensino/xxx

Material Didático

- Livros didáticos
  - Stallings, Computer Security
  - (Stallings, Cryptography and Network Security)
- Material apresentado a cada aula
  - Artigos científicos
  - Estudos, reportagens, white papers
  - Vídeos, Webinars, Podcasts
  - Livros de divulgação
  - Normas, Guias e Manuais

Conteúdo do curso

› PARTE 1: APRESENTAÇÃO

- 1. Apresentação: O Impacto da (In)Segurança
- 2. Conceitos e Nomenclatura Básica
- 3. Padronização de Segurança
- 4. Segurança de Sistemas de Informação
- 5. Riscos, Ameaças, Ataques e Atacantes

Conteúdo do curso

- PARTE 2: AMEAÇAS
  - 6. Vulnerabilidades de software
  - 7. Malware: Software Malicioso
  - 8. Ataques de Negação de Serviço
  - 9. Engenharia Social
  - 10. Ameaças Avançadas e Persistentes

Conteúdo do curso

- PARTE 3: FERRAMENTAS DE SEGURANÇA
  - 11. Identificação e Autenticação de Usuário
  - 12. Controle de Acesso
  - 13. Criptografia
  - 14. Sistemas de Detecção de Intrusão
  - 15. Segurança de Redes com Firewalls

Conteúdo do curso

› PARTE 4: PADRÕES DE SEGURANÇA

- 16. Padronização
- 17. Avaliação da Conformidade
- 18. Segurança de Software e o Common Criteria
- 19. Segurança de Módulos Criptográficos e o FIPS 140-2
- 20. Sistemas de Gestão de Segurança da Informação e a ISO/IEC 27001
- 21. Padrões Nacionais de Segurança

Conteúdo do curso

- PARTE 5: DESENVOLVIMENTO SEGURO E AVALIAÇÃO DE SEGURANÇA
  - 22. SDLC
  - 23. Desafios e Importância de Avaliar Segurança
  - 24. Riscos, requisitos, soluções aceitáveis e caracterização do Ativo
  - 25. Criptografia e Arquitetura de Segurança
  - 26. Análise de Código, Vulnerabilidades de Software e Aspectos de Implementação
  - 27. Testes Operacionais e Testes de Penetração
  - 28. Auditoria de Sistemas de Gestão

Conteúdo do curso

› PARTE 6: Sociedade, Governo e Setor Produtivo

- 29. Gerenciamento de Riscos Cibernéticos
- 30. Infraestruturas Críticas e Defesa Cibernética
- 31. Regulação do Setor Cibernético

Atividades complementares

Trabalhos e Projetos

- Permitem aprofundar e consolidar temas do curso
- Valem pontos na média
  - Graduação: até um ponto (a mais) na média final
  - Pós-Graduação: valem metade da média
- Estratégia (programa de milhagem): ”acumular pontos” ao longo do curso
- Regra de outro: plágio é inaceitável e injustificável
- Cada entrega deverá vir acompanhada de:
  - relatório curto explicando a ”teoria” sobre o assunto estudado
  - documento e vídeo (screencast) explicando o funcionamento do ambiente/programa/aplicação e a exploração da vulnerabilidade

Segurança de software (vulnerabilidades) - até 3 pontos

- Implementar programa/aplicação simples com vulnerabilidade listada no SANS/CWE Top 25
- Poderão ser implementados até 3 programas/aplicações
  - não pode haver sobreposição de vulnerabilidades entre diferentes alunos
  - preferencialmente, explorar ambientes diversos (SO, C/C++, appweb,...)

Segurança de redes (ferramentas) - até 2 pontos

- implementar rede (possivelmente, usando virtualização) com ferramentas básicas de segurança (IDS, IPS, FW, SIEM,...)
  - pode ser feito em grupo pontuação é dividida pelo número de participantes do grupo
  - 1 ponto por tipo de ferramenta identificada
- 0,2 a 1 ponto por cenário de uso (dependendo da complexidade
- Exemplo
  - topologia com filtro de pacotes (FW), bastião, IDS, SIEM (4 pontos)
  - cenário de scan interno detectado por IDS (+0,2 ponto)
  - Cenário de scan externo filtrado por IDS (+0,2 ponto)
  - cenário de ataque: exploração de vulnerabilidade do FW, bypass do bastião, acesso a hosts internos, alerta SIEM (+1 ponto)
- Pontuação adicional se implementar honeypot (até 2 pontos)
  - 1 ponto pela implementação, 1 ponto pelo estudo dos ataques

Números aleatórios – até 2 pontos

- Identificar fontes distintas de números aleatórios e estudar a aleatoriedade
  - descrever como os números aleatórios são gerados
  - executar suítes do NIST, Dieharder, TestU01, PractRand e o gjrand
  - medir entropia com 800-90B
- 0,5 ponto por fonte ”pronta”
- 1,0 ponto por fonte ”construída”
- discutir com professor o que caracterizaria as fontes como ”prontas” e ”construídas”

Análise Estática de Código - até 1 ponto

- - demonstrar casos de uso das seguintes técnicas
  - grafo de controle de fluxo
  - grafo de chamada
  - tainting
  - value set analysis
- - os códigos analisados devem ser desenvolvidos pelo aluno

Análise Estática de Código - identificação de vulnerabilidades - até 1 ponto

- Comparar pelo menos duas ferramentas com relação à identificação de vulns
- Os códigos analisados devem ser desenvolvidos pelo aluno
- 0,05 ponto por vuln identificada por todas as ferr.
- 0,2 ponto por vuln não-identificada por alguma ferr.

Padrões de cybersecurity em setores específicos - até 1 ponto (individual)

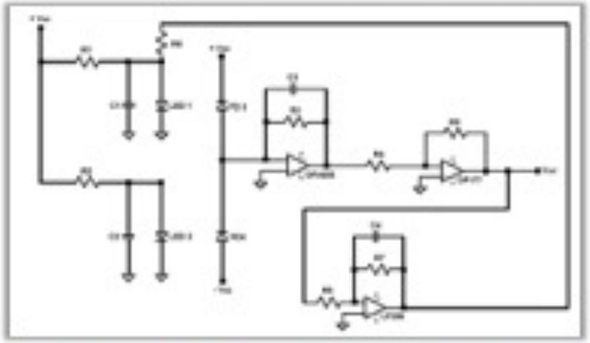
- Quais são as organizações e os padrões? Existem regulamentos? Existe certificação? Como funciona?
- - setores
  - marítimo
  - energia
  - nuclear
  - veículos autônomos
  - saúde
  - segurança pública
  - governo
- O aluno deve apresentar "proposta" de setor antes de executar pesquisas aprofundadas. Isso para garantir que existe quantidade adequada de material a ser estudado.

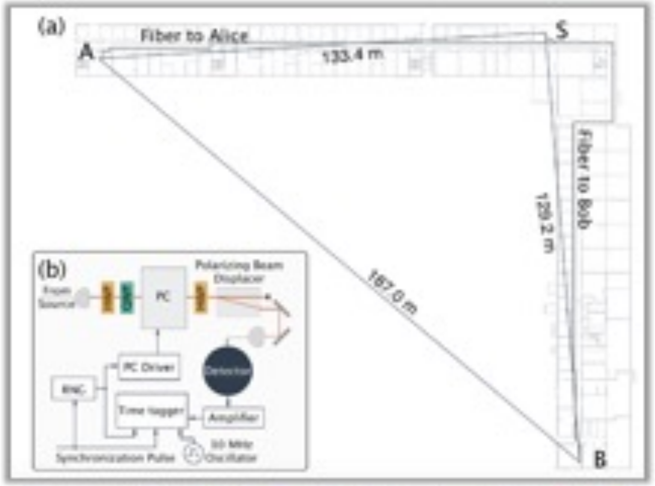
Temas de Pesquisa e Desenvolvimento

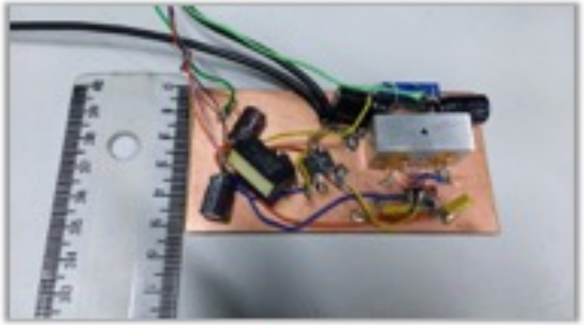
(Temas para projetos)

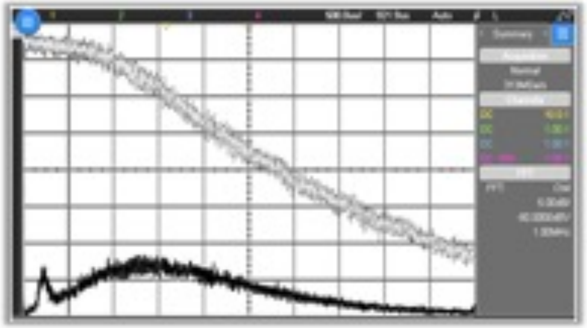
Testes de Aleatoriedade

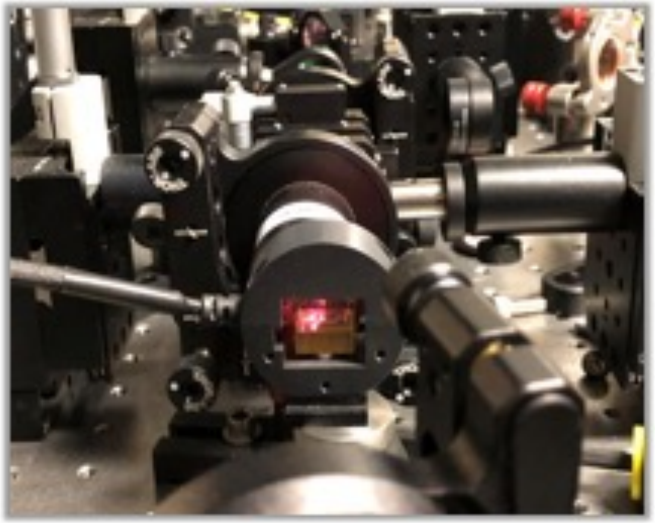
Estudo de Fontes de Aleatoriedade



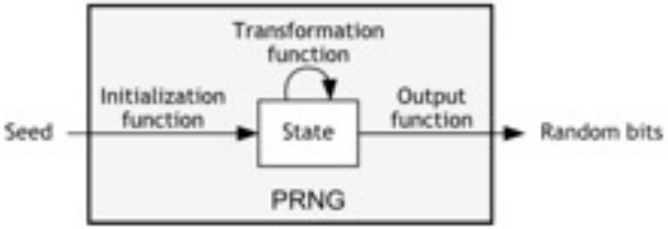


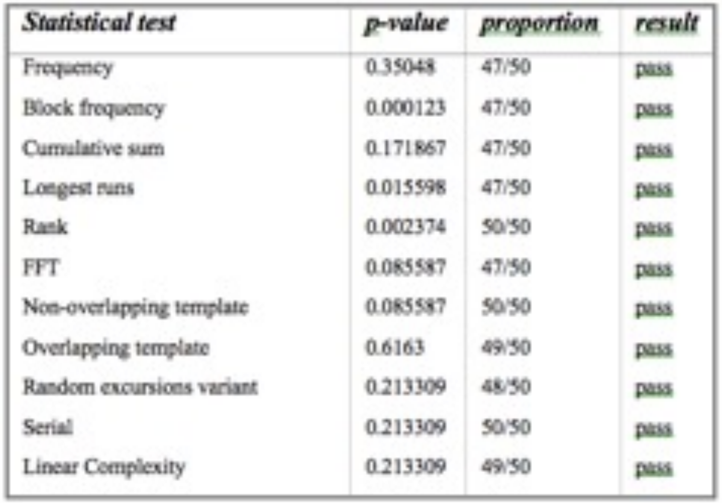




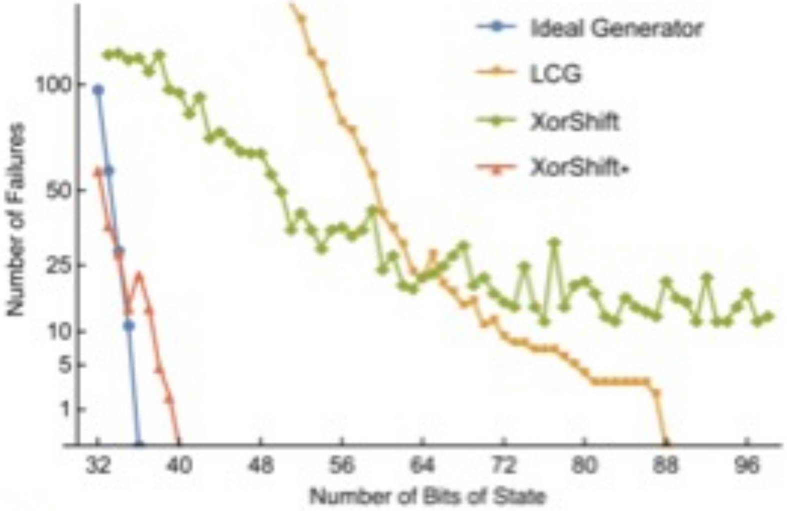


Caracterização da Aleatoriedade





Statistical test	*p-value*	*proportion*	*result*
Frequency	0.35048	47/50	pass
Block frequency	0.000123	47/50	pass
Cumulative sum	0.171867	47/50	pass
Longest runs	0.015598	47/50	pass
Rank	0.002374	50/50	pass
FFT	0.085587	47/50	pass
Non-overlapping template	0.085587	50/50	pass
Overlapping template	0.6163	49/50	pass
Random excursions variant	0.213309	48/50	pass
Serial	0.213309	50/50	pass
Linear Complexity	0.213309	49/50	pass



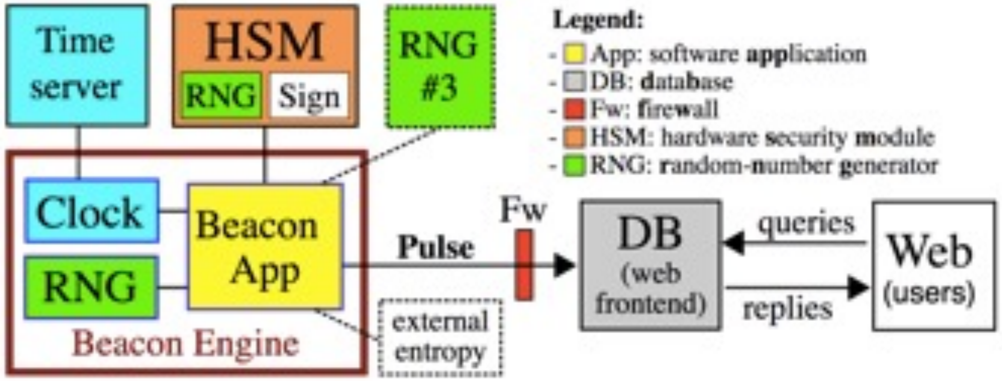
Randomness beacon: Disseminação e Aplicações

- Caracterização de fontes de entropia e RNGs
- Desenvolvimento de um sistema para distribuição beacons de aleatoriedade
- Pesquisa de protocolos de segurança baseados em beacons de aleatoridade

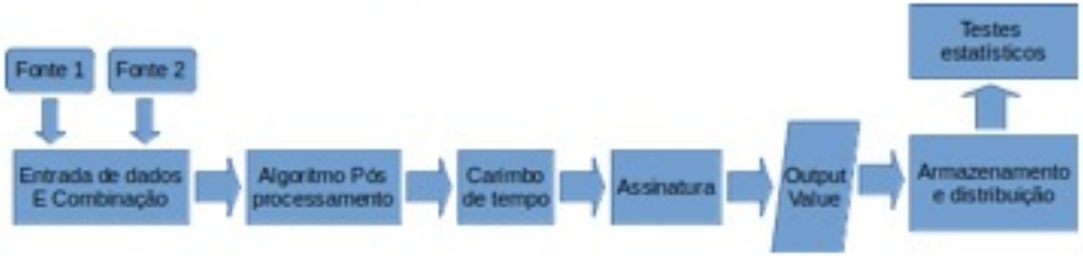
INMETRO

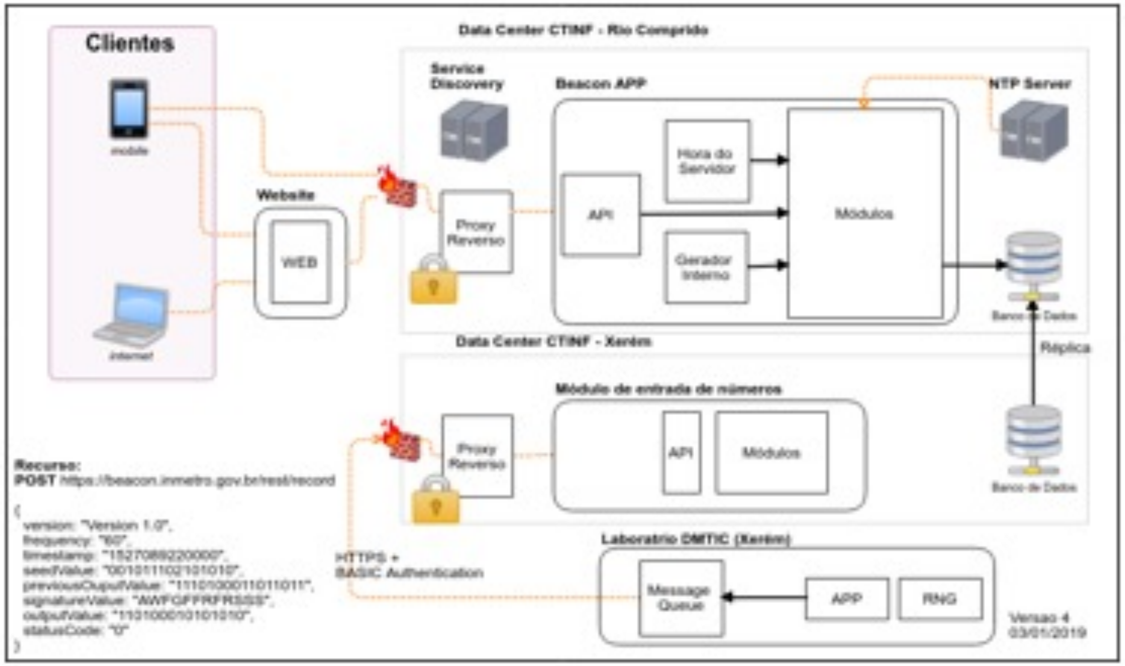
uff

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



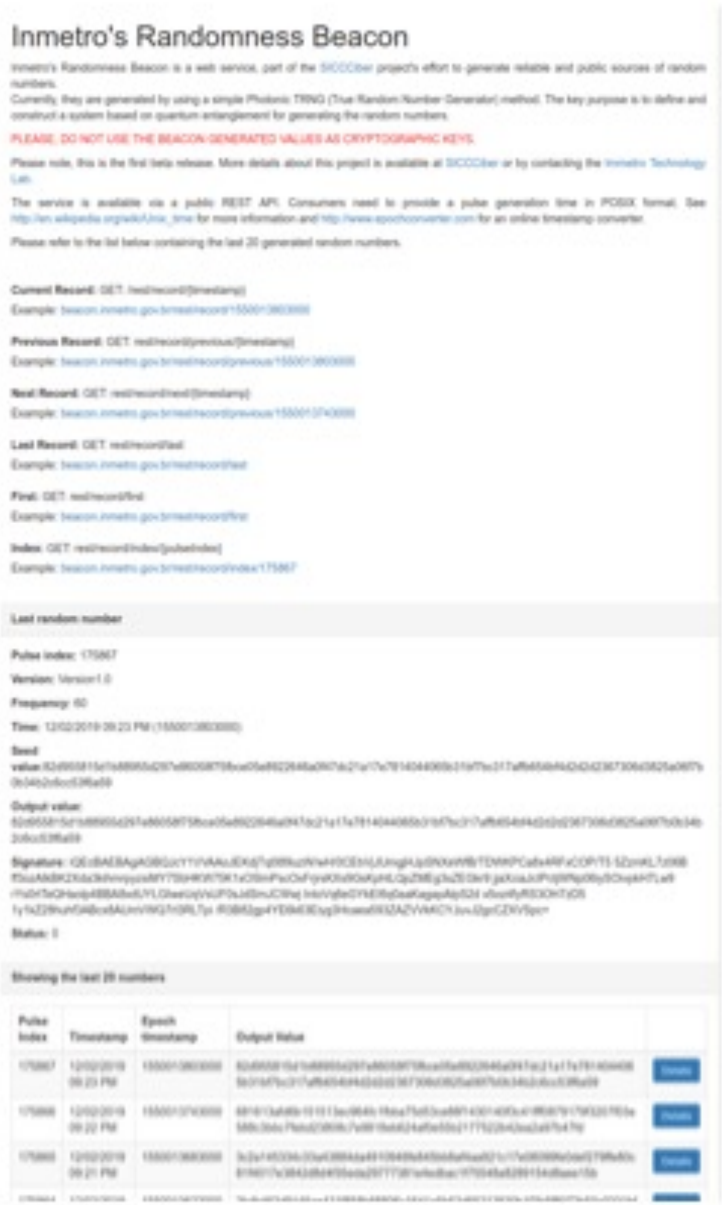
Randomness beacon: Disseminação e Aplicações


Fonte 1
Fonte 2
Entrada de dados E Combinação
Algoritmo Pós processamento
Carimbo de tempo
Assinatura
Output Value
Armazenamento e distribuição
Testes estatísticos



Recurso:
POST https://beacon.inmetro.gov.br/rest/record

```
{
  version: "Version 1.0",
  frequency: "60",
  timestamp: "1527089220000",
  seedValue: "0010111102101010",
  previousOuputValue: "1110100011011011",
  signatureValue: "AWFGFFRFRSSS",
  outputValue: "1101000101010010",
  statusCode: "0"
}
```



Inmetro's Randomness Beacon

Inmetro's Randomness Beacon is a web service, part of the SICCCiber project's effort to generate reliable and public sources of random numbers.
Currently, they are generated by using a simple Photonic TRNG (True Random Number Generator) method. The key purpose is to define and construct a system based on quantum entanglement for generating the random numbers.

PLEASE, DO NOT USE THE BEACON GENERATED VALUES AS CRYPTOGRAPHIC KEYS.

Please note, this is the first beta release. More details about this project is available at SICCCiber or by contacting the Inmetro Technology Lab.

The service is available via a public REST API. Consumers need to provide a pulse generation time in POSIX format. See http://en.wikipedia.org/wiki/Unix_time for more information and http://www.epochconverter.com for an online timestamp converter.

Please refer to the list below containing the last 20 generated random numbers.

Current Record: GET: rest/record/{timestamp}
Example: beacon.inmetro.gov.br/rest/record/1550013803000

Previous Record: GET: rest/record/previous/{timestamp}
Example: beacon.inmetro.gov.br/rest/record/previous/1550013803000

Next Record: GET: rest/record/next/{timestamp}
Example: beacon.inmetro.gov.br/rest/record/previous/1550013743000

Last Record: GET: rest/record/last
Example: beacon.inmetro.gov.br/rest/record/last

First: GET: rest/record/first
Example: beacon.inmetro.gov.br/rest/record/first

Index: GET: rest/record/index/{pulseIndex}
Example: beacon.inmetro.gov.br/rest/record/index/175867

Last random number

Pulse index: 175867

Version: Version1.0

Frequency: 60

Time: 12/02/2019 09:23 PM (1550013803000)

Seed value: [illegible]

Output value: [illegible]

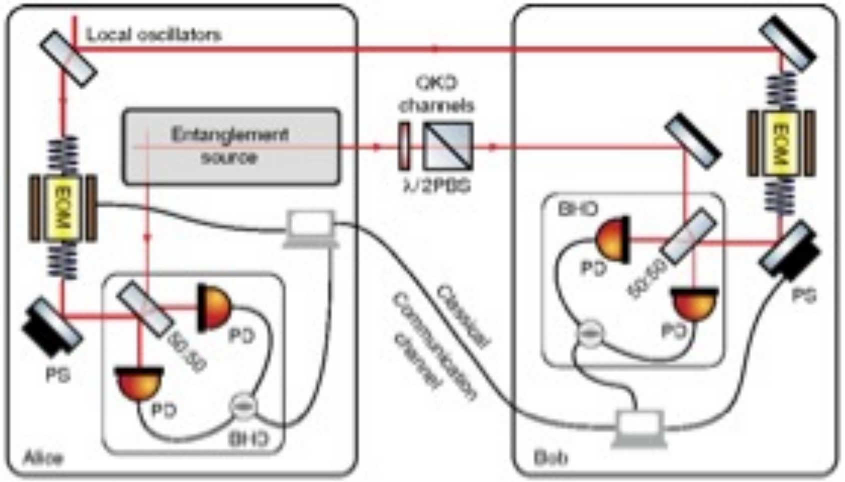
Signature: [illegible]

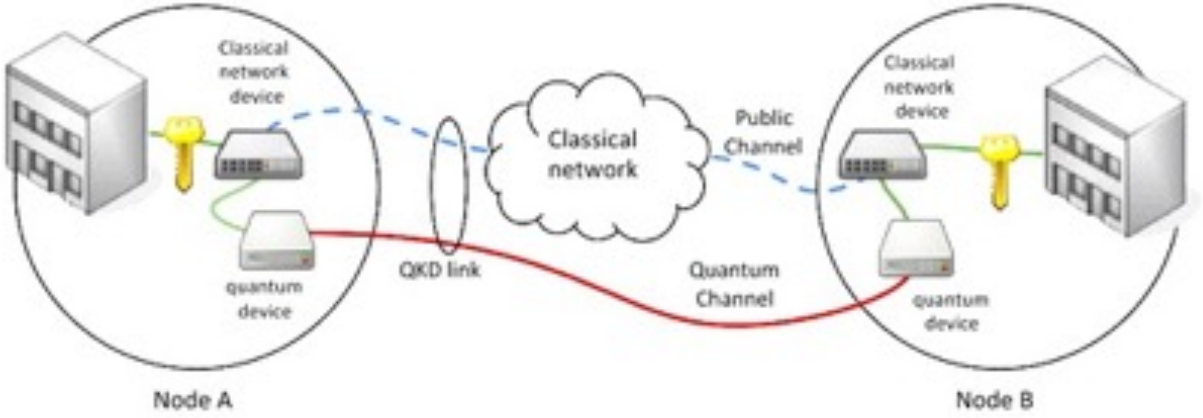
Status: 0

Showing the last 20 numbers

Pulse Index	Timestamp	Epoch timestamp	Output Value	
175867	12/02/2019 09:23 PM	1550013803000	[illegible]	Details
175866	12/02/2019 09:22 PM	1550013743000	[illegible]	Details
175865	12/02/2019 09:21 PM	1550013683000	[illegible]	Details

Quantum Key Distribution (futuro)



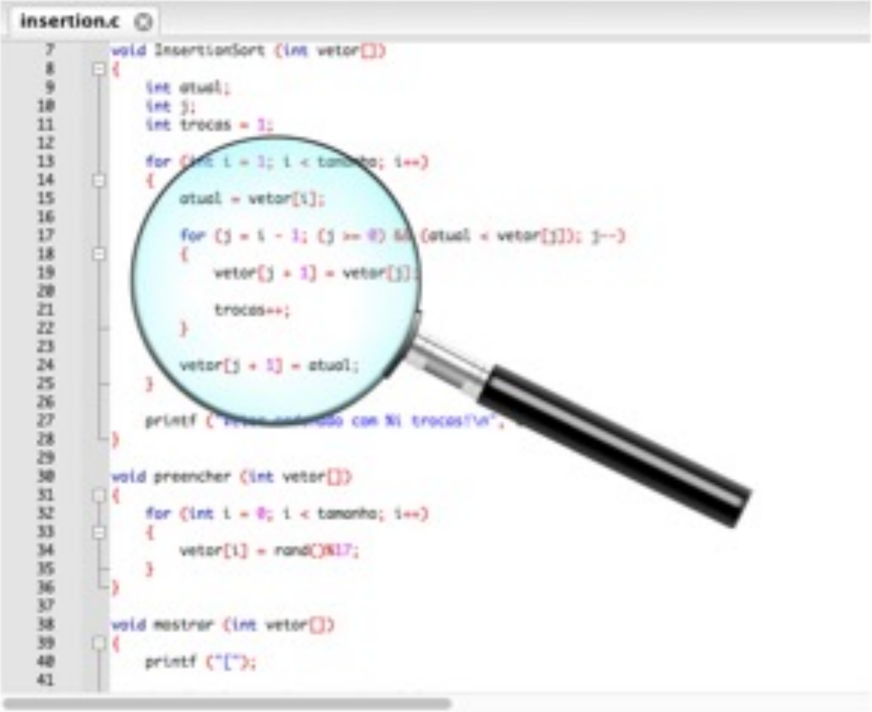


Tarefas e temas de pesquisa

- Alinhar o Beacon à versão 2.0 do padrão NIST
- Adaptar o Beacon a aleatoriedade verificável (VDF)
- Formalizar metodologia de análise de aleatoriedade
- Analisar fontes diversas de aleatoriedade
- Otimizar/testar circuitos de opto-detecção

Grafos de Programa para Análise e Proteção de Software

Análise Estática "clássica" de Código Fonte



```
void InsertionSort (int vetor[])
{
    int atual;
    int j;
    int trocas = 1;

    for (int i = 1; i < tamanho; i++)
    {
        atual = vetor[i];

        for (j = i - 1; (j >= 0) && (atual < vetor[j]); j--)
        {
            vetor[j + 1] = vetor[j];

            trocas++;
        }

        vetor[j + 1] = atual;
    }

    printf ("Vetor ordenado com %i trocas!\n",
}

void preencher (int vetor[])
{
    for (int i = 0; i < tamanho; i++)
    {
        vetor[i] = rand()%17;
    }
}

void mostrar (int vetor[])
{
    printf ("[");

```

Grafos de Programa

SEI CERT

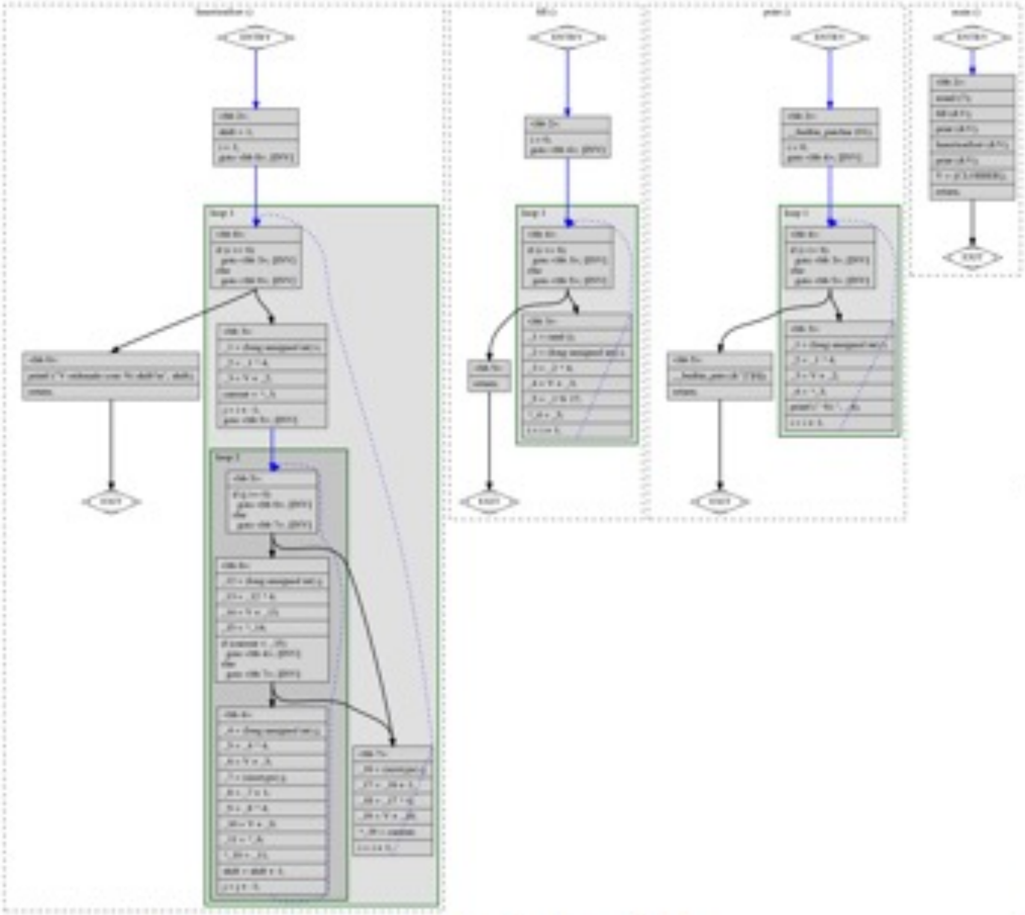
Fluxo de Dados

Rastreabilidade de Variáveis

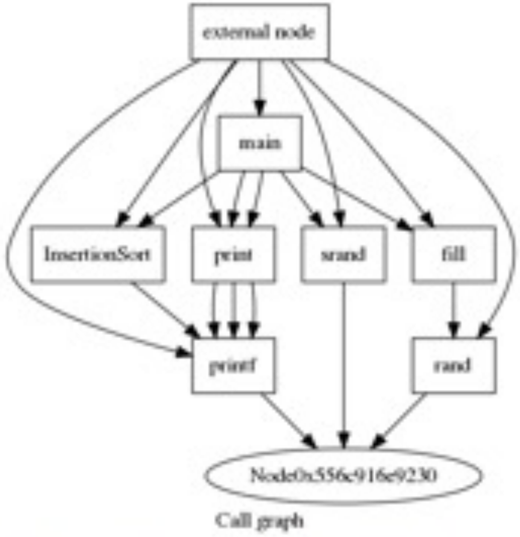
OWASP Top 10

CWE

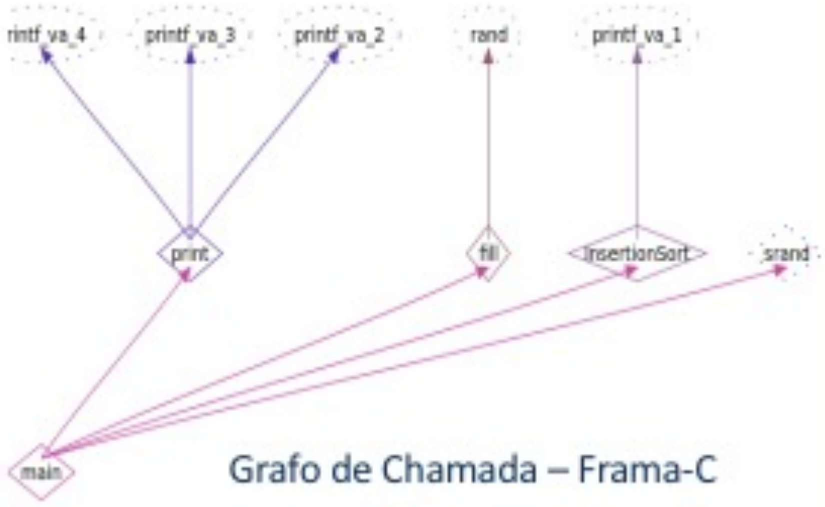
Grafos de Programa



Grafo de Fluxo de Controle – GCC

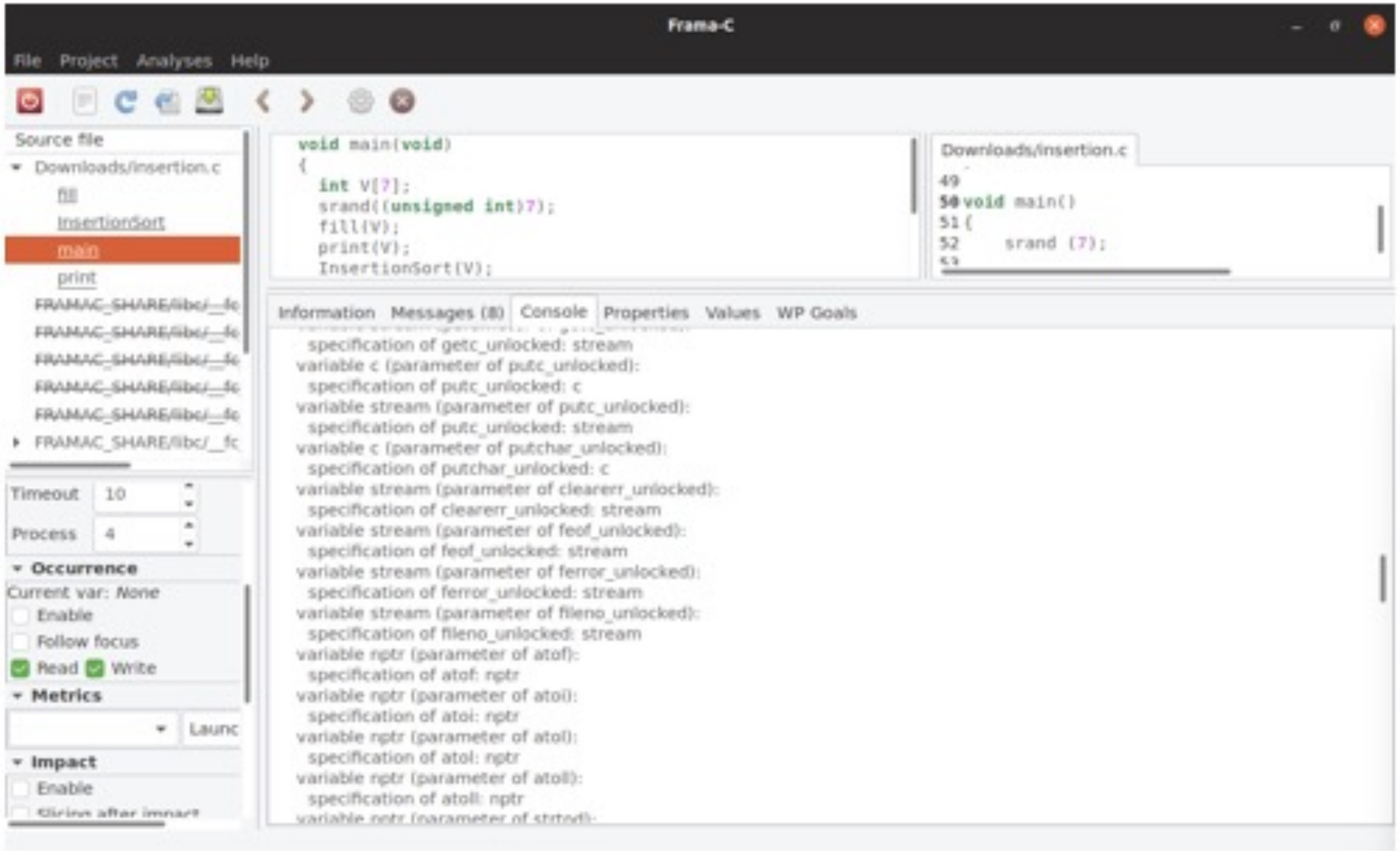


Grafo de Chamada – LLVM



Grafo de Chamada – Frama-C

Análise de SW: Rastreamento de Variáveis



Timeout 10

Process 4

Occurrence

Current var: None

□ Enable

□ Follow focus

☑ Read ☑ Write

Metrics

Impact

□ Enable

□ Slicing after impact

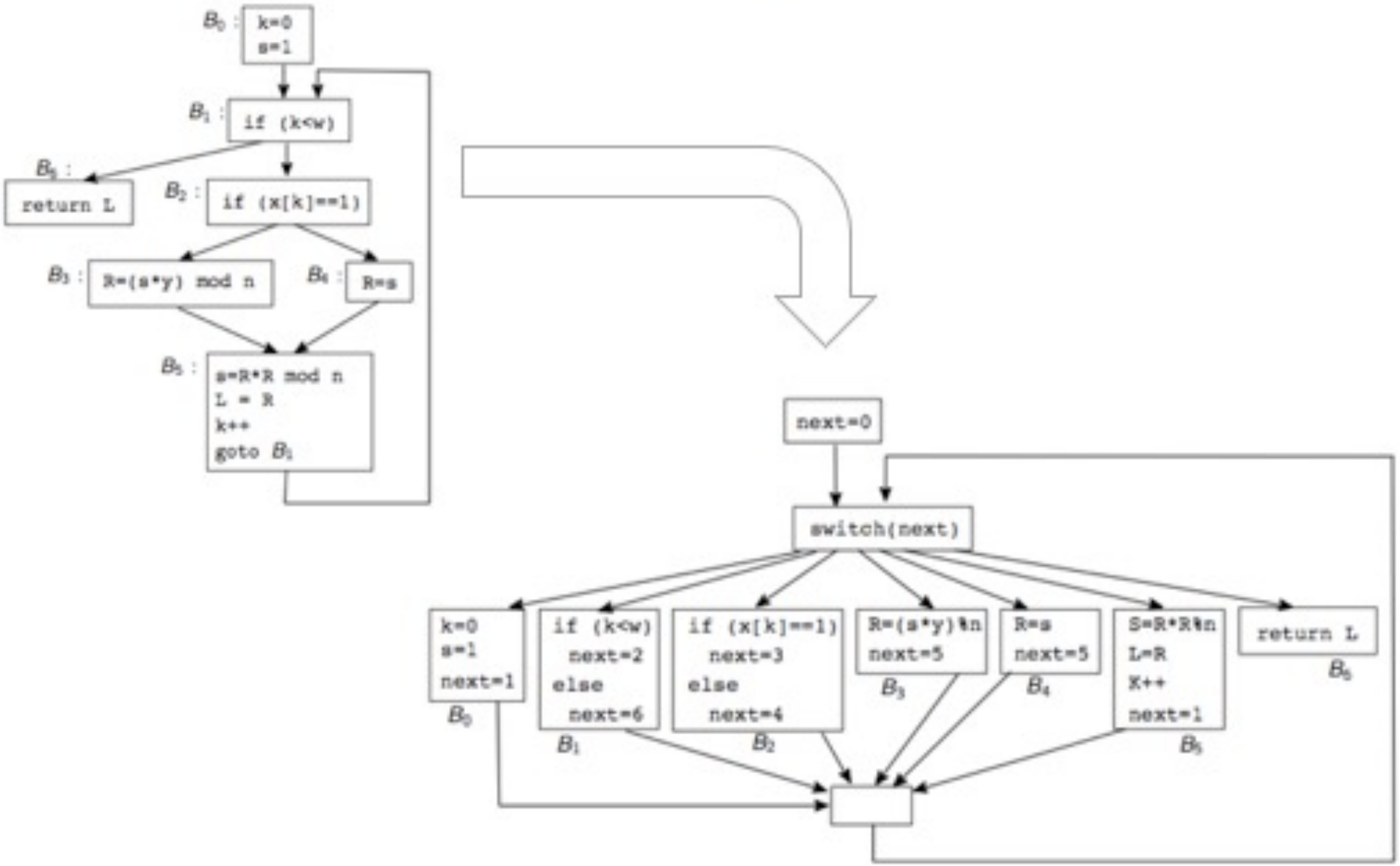
```
void main(void)
{
  int V[7];
  srand((unsigned int)7);
  fill(V);
  print(V);
  InsertionSort(V);
```

Downloads/insertion.c

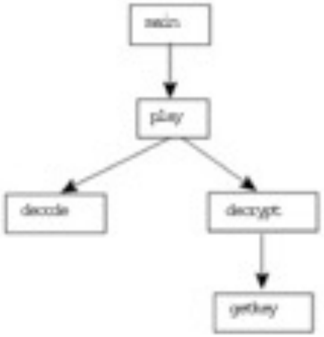
```

void main()
{
    srand (7);
```

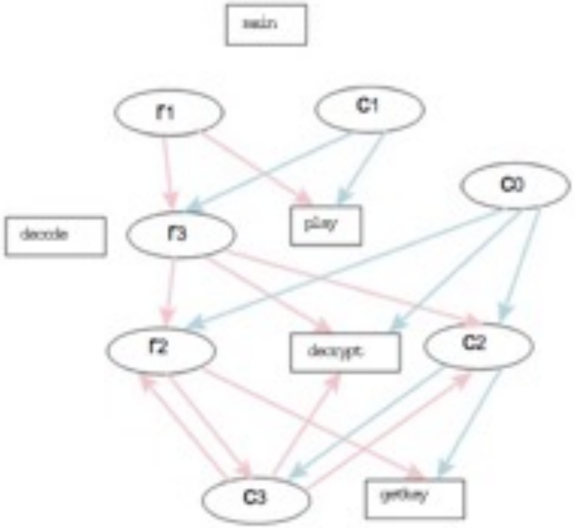
```
  specification of getc_unlocked: stream
variable c (parameter of putc_unlocked):
  specification of putc_unlocked: c
variable stream (parameter of putc_unlocked):
  specification of putc_unlocked: stream
variable c (parameter of putchar_unlocked):
  specification of putchar_unlocked: c
variable stream (parameter of clearerr_unlocked):
  specification of clearerr_unlocked: stream
variable stream (parameter of feof_unlocked):
  specification of feof_unlocked: stream
variable stream (parameter of ferror_unlocked):
  specification of ferror_unlocked: stream
variable stream (parameter of fileno_unlocked):
  specification of fileno_unlocked: stream
variable nptr (parameter of atof):
  specification of atof: nptr
variable nptr (parameter of atoi):
  specification of atoi: nptr
variable nptr (parameter of atol):
  specification of atol: nptr
variable nptr (parameter of atoll):
  specification of atoll: nptr
variable nptr (parameter of strtod):
```

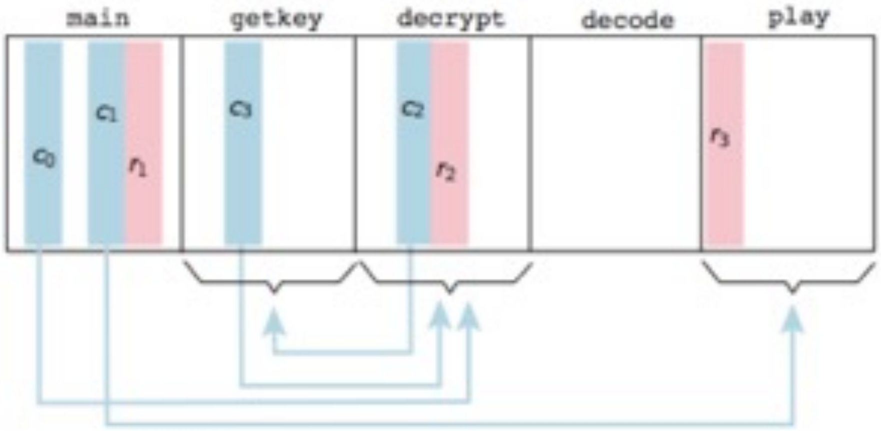
Proteção de SW: Ofuscação



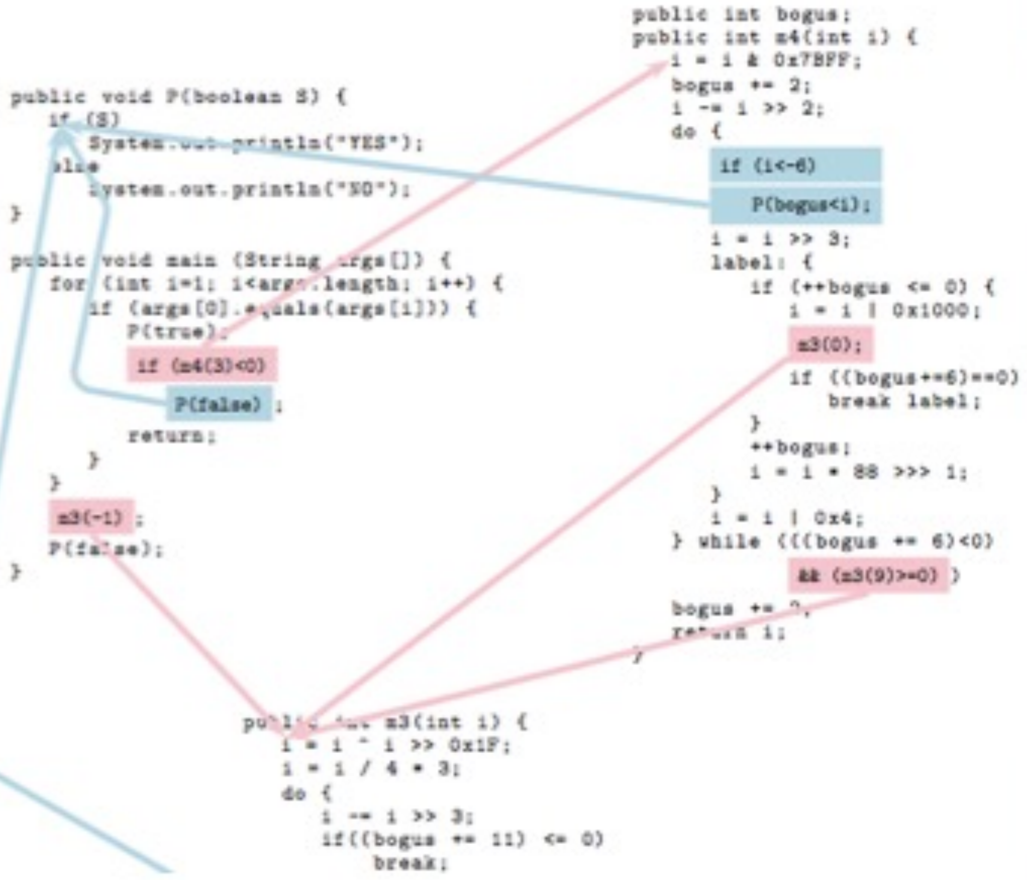
Proteção de SW: Incorruptibilidade







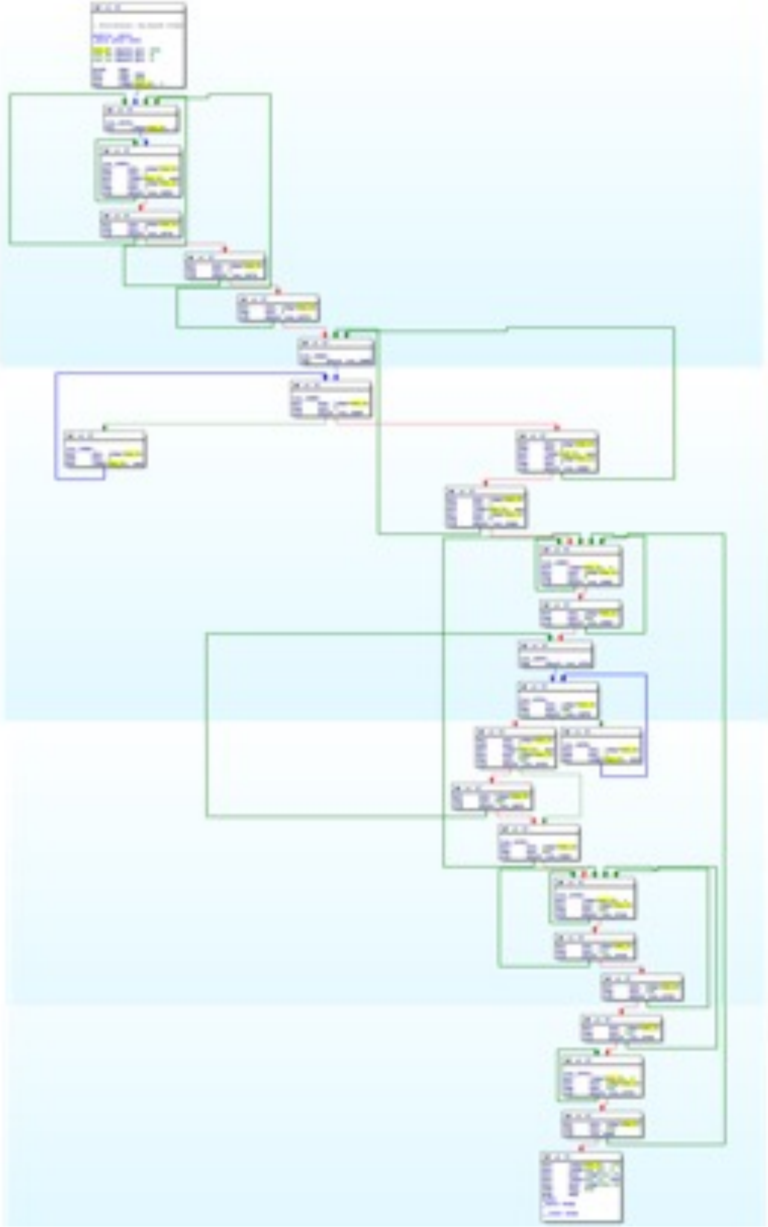
Proteção de SW: Marcas d'água



```
public void P(boolean S) {
    if (S)
        System.out.println("YES");
    else
        System.out.println("NO");
}

public void main (String args[]) {
    for (int i=1; i<args.length; i++) {
        if (args[0].equals(args[i])) {
            P(true);
            if (m4(3)<0)
              P(false) ;
            return;
        }
    }
    m3(-1) ;
    P(false);
}
```

```
public int bogus;
public int m4(int i) {
    i = i & 0x7BFF;
    bogus += 2;
    i -= i >> 2;
    do {
        if (i<-6)
            P(bogus<i);
        i = i >> 3;
        label: {
            if (++bogus <= 0) {
                i = i | 0x1000;
                m3(0);
                if ((bogus+=6)==0)
                    break label;
            }
            ++bogus;
            i = i * 88 >>> 1;
        }
        i = i | 0x4;
    } while (((bogus += 6)<0)
                && (m3(9)>=0) )
    bogus += 2;
    return i;
}
```

```
public int m3(int i) {
    i = i ^ i >> 0x1F;
    i = i / 4 * 3;
    do {
        i -= i >> 3;
        if((bogus += 11) <= 0)
            break;
```



Tarefas e temas de pesquisa

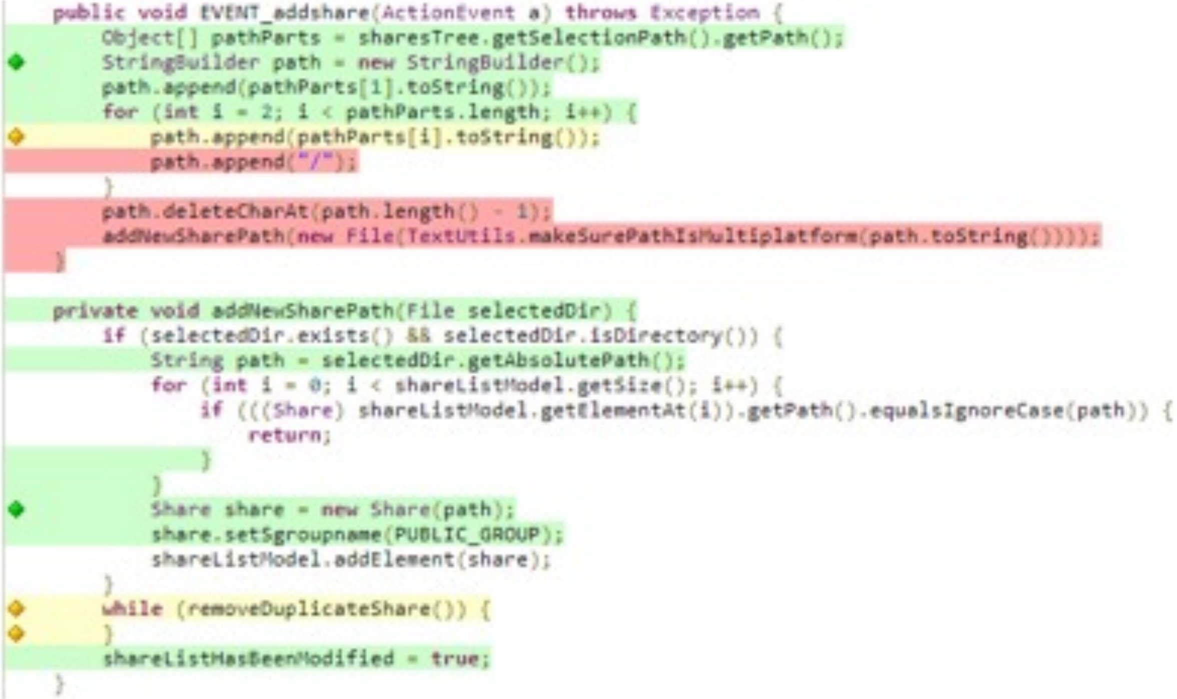
- Implementar e testar as várias metodologias de análise e proteção de software
- Desenvolver de novos métodos de análise e proteção de software
- Estudo de grafos de programas estruturados (para diversas definições de ”estruturado”)
- Usar grafos de programa para identificar ”plágio”
- Testar e comparar ferramentas SAST
- Construir bases de referência para SAST

Análise dinâmica de código

Cobertura de código para análise software e ensaios de proficiência

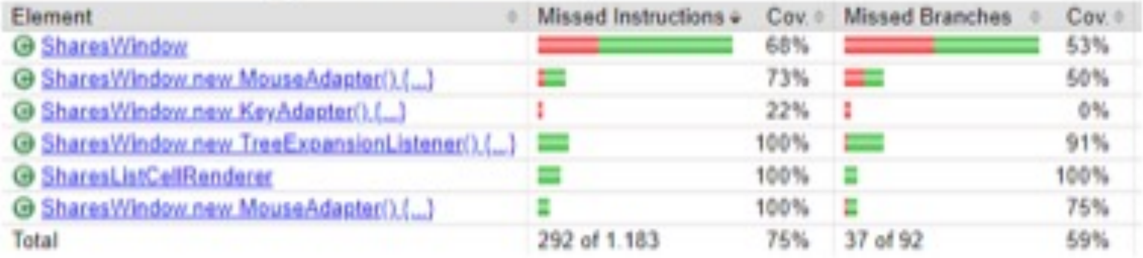
Biblioteca de cobertura de código

JaCoCo - linhas de código cobertas e não cobertas



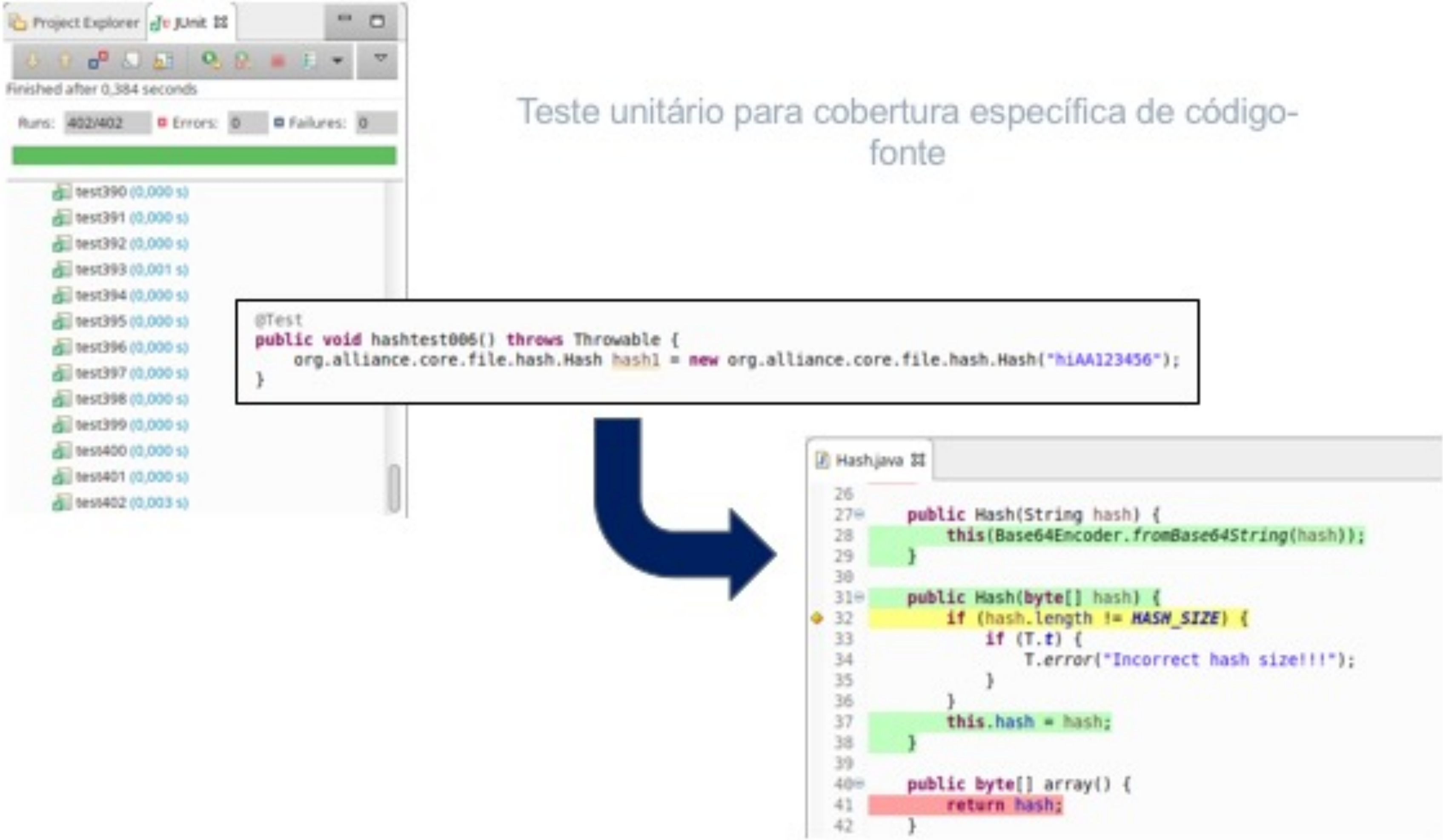
```
    public void EVENT_addshare(ActionEvent a) throws Exception {
        Object[] pathParts = sharesTree.getSelectionPath().getPath();
        StringBuilder path = new StringBuilder();
        path.append(pathParts[1].toString());
        for (int i = 2; i < pathParts.length; i++) {
            path.append(pathParts[i].toString());
            path.append("/");
        }
        path.deleteCharAt(path.length() - 1);
        addNewSharePath(new File(TextUtils.makeSurePathIsMultiplatform(path.toString())));
    }

    private void addNewSharePath(File selectedDir) {
        if (selectedDir.exists() && selectedDir.isDirectory()) {
            String path = selectedDir.getAbsolutePath();
            for (int i = 0; i < shareListModel.getSize(); i++) {
                if (((Share) shareListModel.getElementAt(i)).getPath().equalsIgnoreCase(path)) {
                    return;
                }
            }
            Share share = new Share(path);
            share.setSgroupname(PUBLIC_GROUP);
            shareListModel.addElement(share);
        }
        while (removeDuplicateShare()) {
        }
        shareListHasBeenModified = true;
    }
```

JaCoCo - Visão geral de cobertura por classe



Element	Missed Instructions	Cov.	Missed Branches	Cov.
SharesWindow	🟥🟩	68%	🟥🟩	53%
SharesWindow.new MouseAdapter() {...}	🟥🟩	73%	🟥🟩	50%
SharesWindow.new KeyAdapter() {...}	🟥	22%	🟥	0%
SharesWindow.new TreeExpansionListener() {...}	🟩	100%	🟩	91%
SharesListCellRenderer	🟩	100%	🟩	100%
SharesWindow.new MouseAdapter() {...}	🟩	100%	🟩	75%
Total	292 of 1.183	75%	37 of 92	59%

Teste unitário para cobertura específica de código-fonte



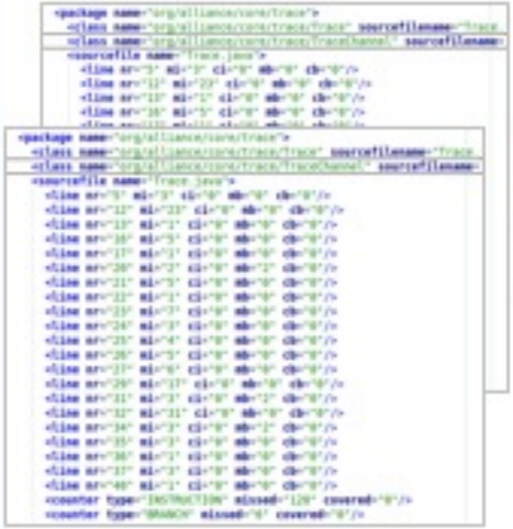
```
Finished after 0,384 seconds

Runs: 402/402   Errors: 0   Failures: 0

test390 (0,000 s)
test391 (0,000 s)
test392 (0,000 s)
test393 (0,001 s)
test394 (0,000 s)
test395 (0,000 s)
test396 (0,000 s)
test397 (0,000 s)
test398 (0,000 s)
test399 (0,000 s)
test400 (0,000 s)
test401 (0,000 s)
test402 (0,003 s)
```

```java
@Test
public void hashtest006() throws Throwable {
    org.alliance.core.file.hash.Hash hash1 = new org.alliance.core.file.hash.Hash("hiAA123456");
}
```

```java

    public Hash(String hash) {
        this(Base64Encoder.fromBase64String(hash));
    }

    public Hash(byte[] hash) {
        if (hash.length != HASH_SIZE) {
            if (T.t) {
                T.error("Incorrect hash size!!!");
            }
        }
        this.hash = hash;
    }

    public byte[] array() {
        return hash;
    }
```

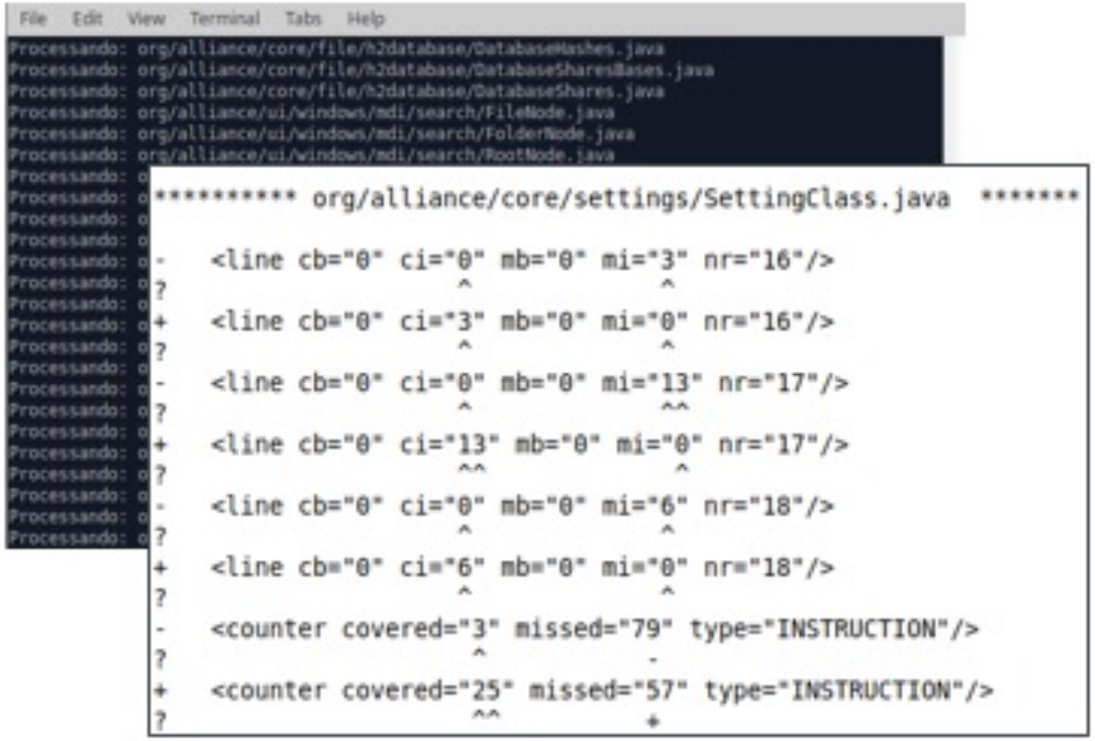
Exemplo do diff entre relatórios de cobertura (Inmetro x Laboratório)

Relatórios XML



```
<package name="org/alliance/core/trace">
  <class name="org/alliance/core/trace/Trace" sourcefilename="Trace
  <class name="org/alliance/core/trace/TraceChannel" sourcefilename=
  <sourcefile name="Trace.java">
    <line nr="5" mi="3" ci="0" mb="0" cb="0"/>
    <line nr="12" mi="23" ci="0" mb="0" cb="0"/>
    <line nr="13" mi="1" ci="0" mb="0" cb="0"/>
    <line nr="16" mi="5" ci="0" mb="0" cb="0"/>
```

```
<package name="org/alliance/core/trace">
  <class name="org/alliance/core/trace/Trace" sourcefilename="Trace
  <class name="org/alliance/core/trace/TraceChannel" sourcefilename=
  <sourcefile name="Trace.java">
    <line nr="5" mi="3" ci="0" mb="0" cb="0"/>
    <line nr="12" mi="23" ci="0" mb="0" cb="0"/>
    <line nr="13" mi="1" ci="0" mb="0" cb="0"/>
    <line nr="16" mi="5" ci="0" mb="0" cb="0"/>
    <line nr="17" mi="1" ci="0" mb="0" cb="0"/>
    <line nr="20" mi="2" ci="0" mb="2" cb="0"/>
    <line nr="21" mi="5" ci="0" mb="0" cb="0"/>
    <line nr="22" mi="1" ci="0" mb="0" cb="0"/>
    <line nr="23" mi="7" ci="0" mb="0" cb="0"/>
    <line nr="24" mi="3" ci="0" mb="0" cb="0"/>
    <line nr="25" mi="4" ci="0" mb="0" cb="0"/>
    <line nr="26" mi="5" ci="0" mb="0" cb="0"/>
    <line nr="27" mi="6" ci="0" mb="0" cb="0"/>
    <line nr="29" mi="17" ci="0" mb="0" cb="0"/>
    <line nr="31" mi="3" ci="0" mb="2" cb="0"/>
    <line nr="32" mi="31" ci="0" mb="0" cb="0"/>
    <line nr="34" mi="3" ci="0" mb="2" cb="0"/>
    <line nr="35" mi="3" ci="0" mb="0" cb="0"/>
    <line nr="36" mi="1" ci="0" mb="0" cb="0"/>
    <line nr="37" mi="3" ci="0" mb="0" cb="0"/>
    <line nr="40" mi="1" ci="0" mb="0" cb="0"/>
    <counter type="INSTRUCTION" missed="120" covered="0"/>
    <counter type="BRANCH" missed="6" covered="0"/>
```



```
Processando: org/alliance/core/file/h2database/DatabaseHashes.java
Processando: org/alliance/core/file/h2database/DatabaseSharesBases.java
Processando: org/alliance/core/file/h2database/DatabaseShares.java
Processando: org/alliance/ui/windows/mdi/search/FileNode.java
Processando: org/alliance/ui/windows/mdi/search/FolderNode.java
Processando: org/alliance/ui/windows/mdi/search/RootNode.java
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
Processando: o
```

```
********** org/alliance/core/settings/SettingClass.java  *******

-    <line cb="0" ci="0" mb="0" mi="3" nr="16"/>
?                   ^                 ^
+    <line cb="0" ci="3" mb="0" mi="0" nr="16"/>
?                   ^                 ^
-    <line cb="0" ci="0" mb="0" mi="13" nr="17"/>
?                   ^                 ^^
+    <line cb="0" ci="13" mb="0" mi="0" nr="17"/>
?                   ^^                 ^
-    <line cb="0" ci="0" mb="0" mi="6" nr="18"/>
?                   ^                 ^
+    <line cb="0" ci="6" mb="0" mi="0" nr="18"/>
?                   ^                 ^
-    <counter covered="3" missed="79" type="INSTRUCTION"/>
?                      ^          -
+    <counter covered="25" missed="57" type="INSTRUCTION"/>
?                      ^^         +
```

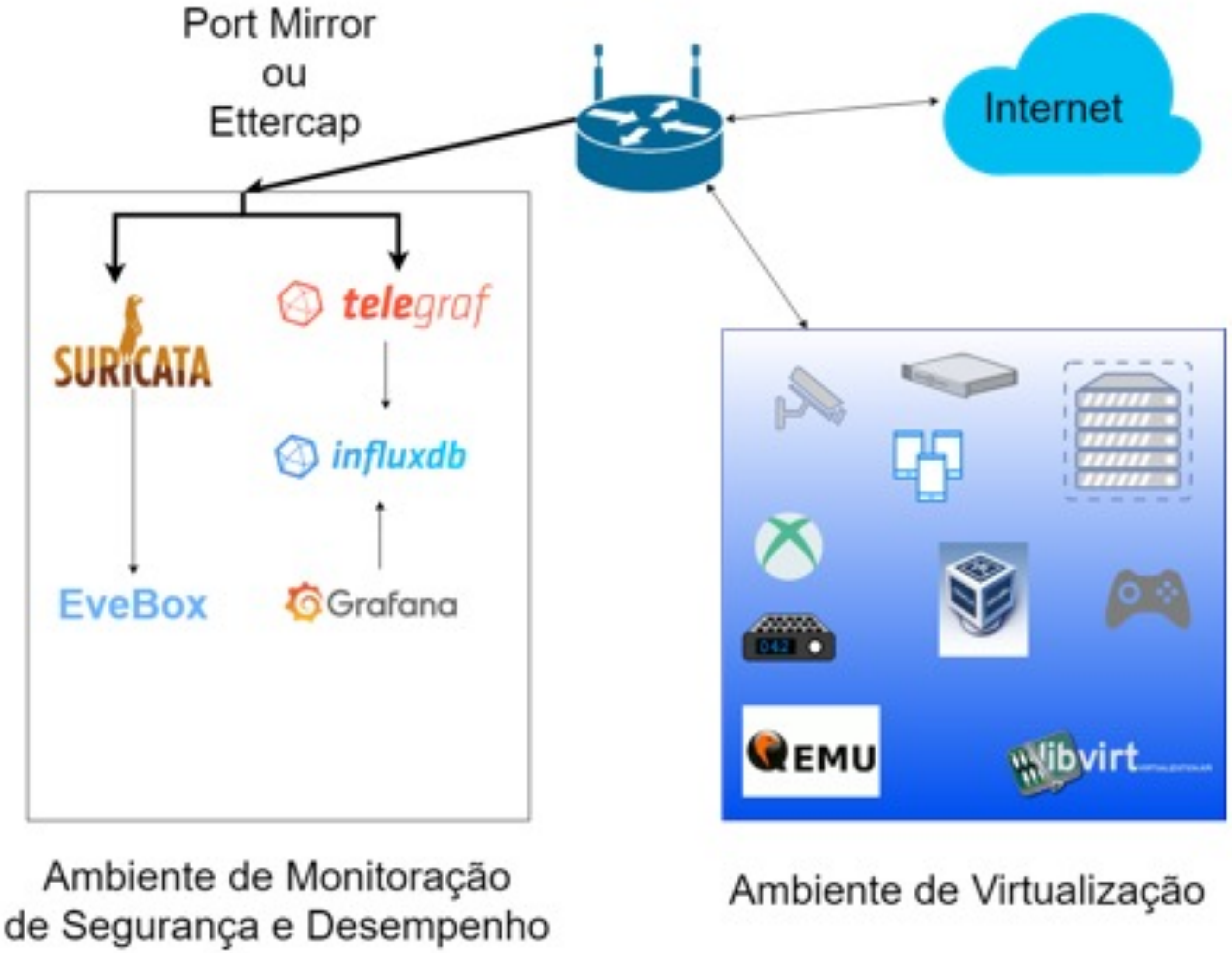
$$CC = \frac{|A \cap B| - |B - A|}{|A|}$$

Tarefas e temas de pesquisa

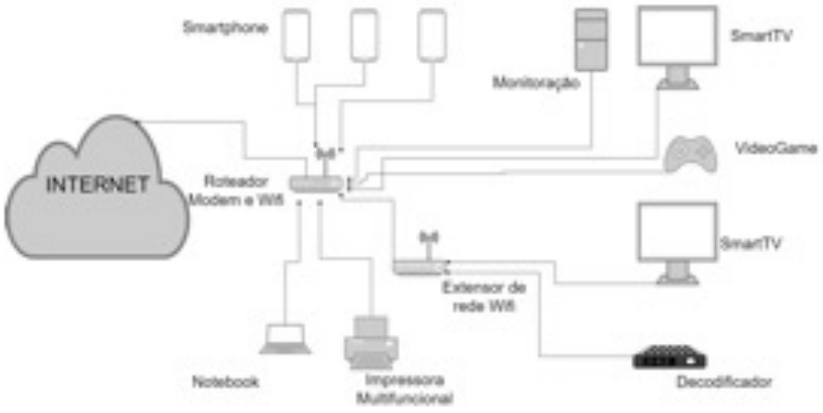
- Incluir aspectos de segurança no PEP
  - cobertura de código em funcionalidades relacionadas a segurança
  - testes que demandam exploração de falhas e vulnerabilidades
- Desenvolver modelos de PEP p/ produtos específicos
  - IDS/IPS/FW/etc.
- Automatizar e aumentar confiança com blockchains

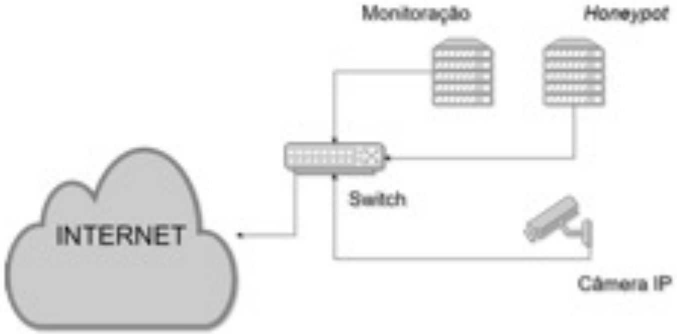
Testes de Caixa Preta em Ambientes Virtualizados

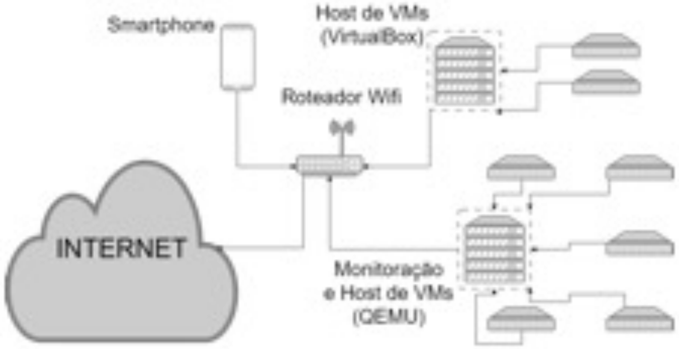
BlackBox TestBox - Arquitetura

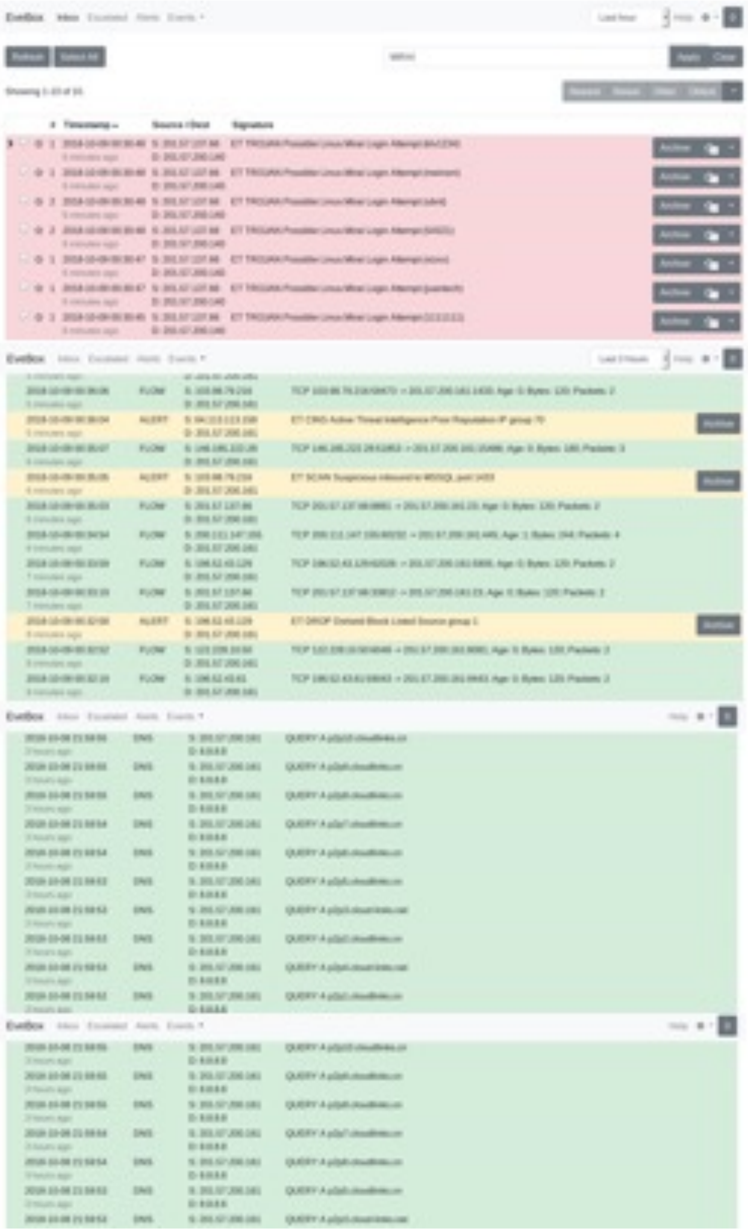


BlackBox TestBox – Ensaios

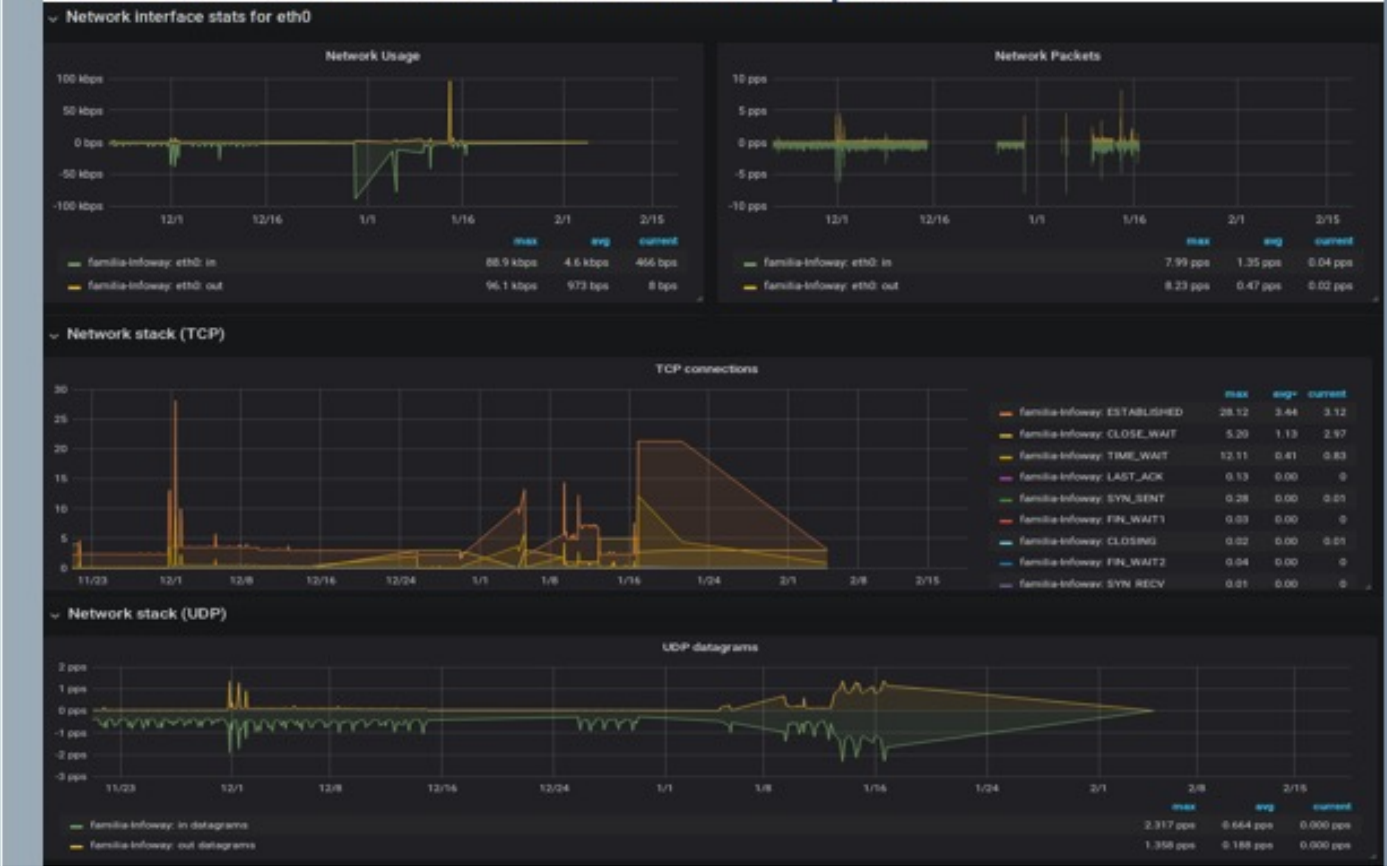








BlackBox TestBox – Monitoramento de Desempenho



Network interface stats for eth0

Network Usage

	max	avg	current
familia-infoway: eth0: in	88.9 kbps	4.6 kbps	466 bps
familia-infoway: eth0: out	96.1 kbps	973 bps	8 bps

Network Packets

	max	avg	current
familia-infoway: eth0: in	7.99 pps	1.35 pps	0.04 pps
familia-infoway: eth0: out	8.23 pps	0.47 pps	0.02 pps

Network stack (TCP)

TCP connections

	max	avg	current
familia-infoway: ESTABLISHED	28.12	3.44	3.12
familia-infoway: CLOSE_WAIT	5.20	1.13	2.97
familia-infoway: TIME_WAIT	12.11	0.41	0.83
familia-infoway: LAST_ACK	0.13	0.00	0
familia-infoway: SYN_SENT	0.28	0.00	0.01
familia-infoway: FIN_WAIT1	0.03	0.00	0
familia-infoway: CLOSING	0.02	0.00	0.01
familia-infoway: FIN_WAIT2	0.04	0.00	0
familia-infoway: SYN_RECV	0.01	0.00	0

Network stack (UDP)

UDP datagrams

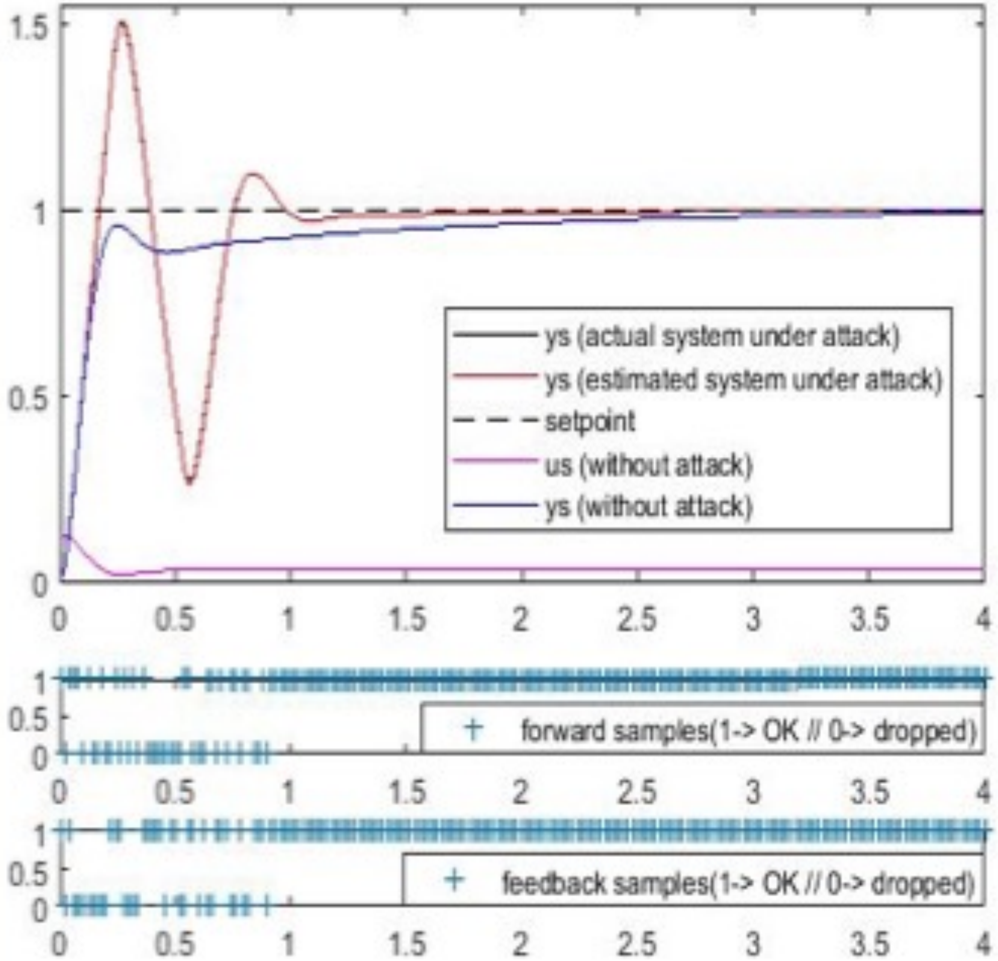
	max	avg	current
familia-infoway: in datagrams	2.317 pps	0.664 pps	0.000 pps
familia-infoway: out datagrams	1.358 pps	0.188 pps	0.000 pps

Tarefas e temas de pesquisa

- Definição de metodologias para testes comportamentais
- Desenvolvimento de métodos de inteligência artificial para detecção de anomalias
- Identificação de vulnerabilidades em aplicações

Segurança de Sistemas Industriais em Rede

Ataque baseado em perdas de pacotes



INMETRO

UNIVERSITÀ DEGLI STUDI DI BRESCIA

uff

Segurança de Sistemas Elétricos

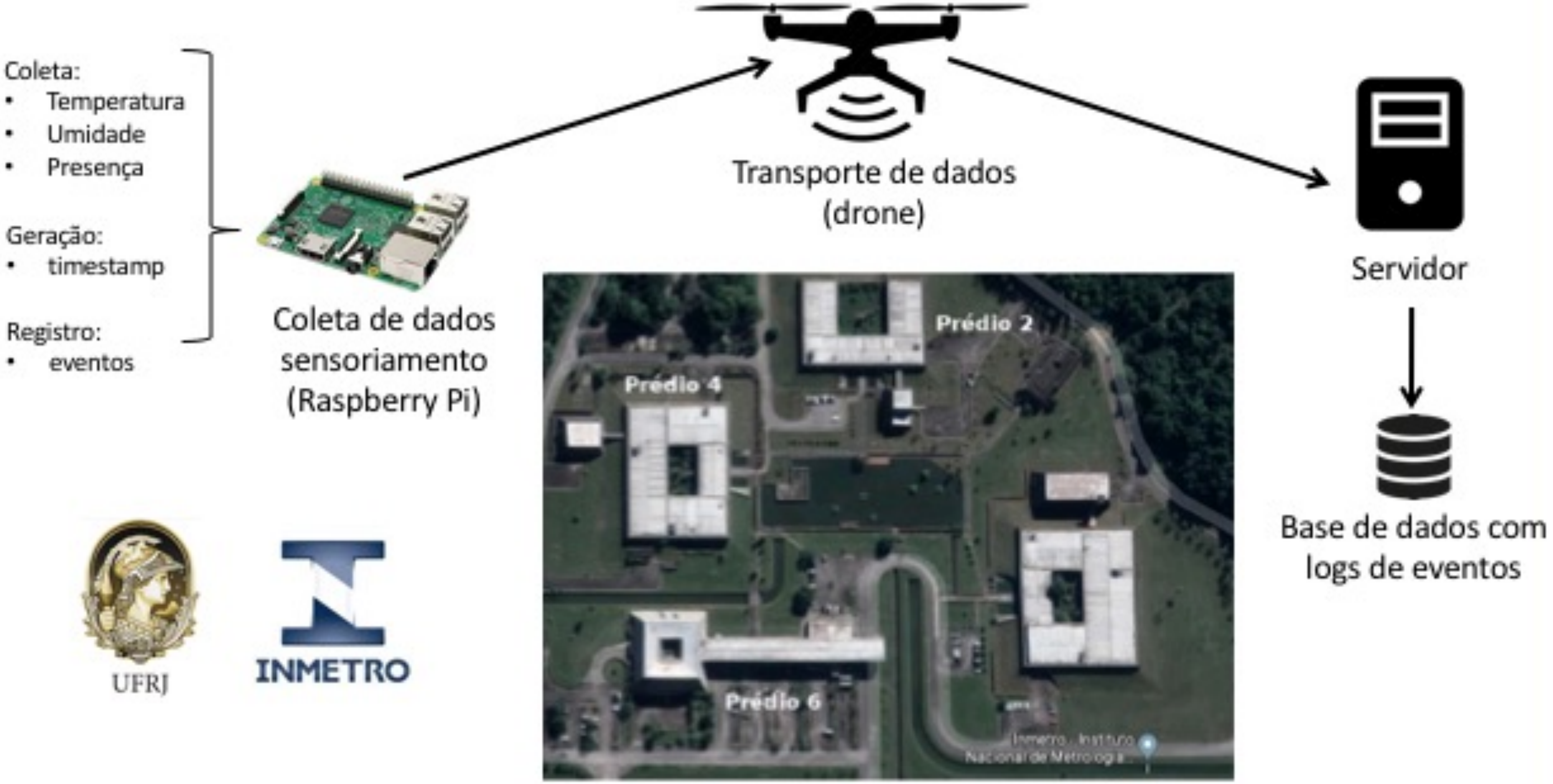
INMETRO UNIVERSITÀ DEGLI STUDI DI BRESCIA uff

Tarefas e temas de pesquisa

- Estudo de novos modelos de ataque
- Estudo de novos tipos de sistemas de C&A
- Estudo de novos algoritmos de identificação
- Implementação de setups de teste

Monitoramento/sensoriamento por meio de redes oportunísticas orientadas a interesse

Monitoramento/sensoriamento por meio de redes oportunísticas orientadas a interesse



Coleta:

- Temperatura
- Umidade
- Presença

Geração:

- timestamp

Registro:

- eventos

Coleta de dados sensoriamento (Raspberry Pi)

Transporte de dados (drone)

Servidor

Base de dados com logs de eventos

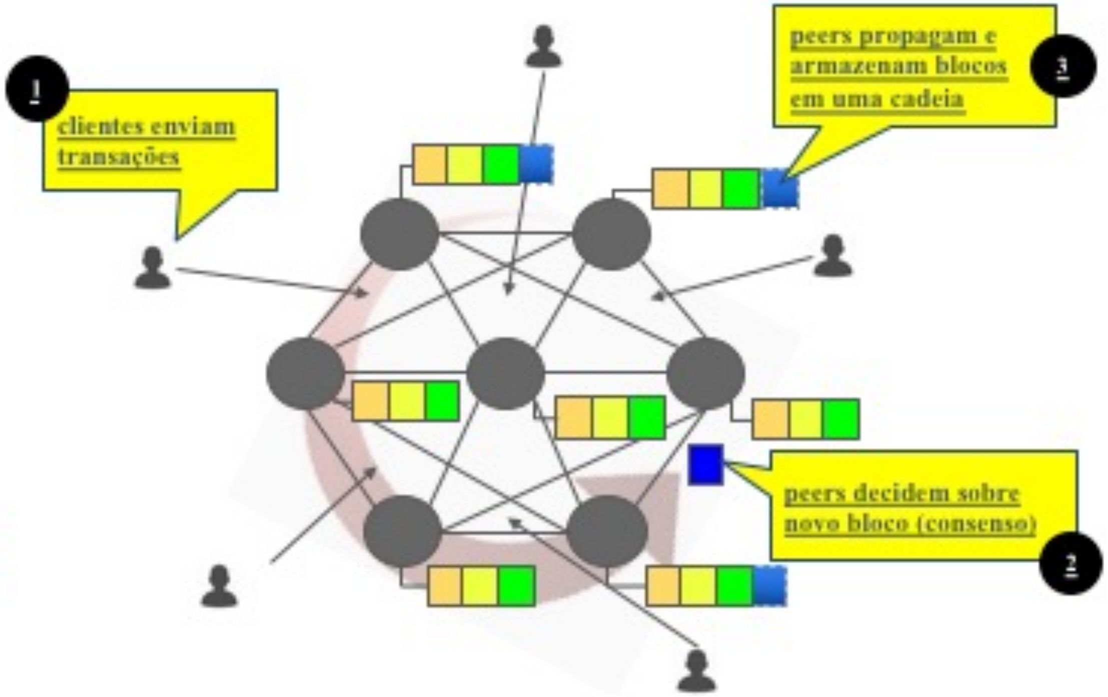
Monitoramento/sensoriamento por meio de redes oportunísticas orientadas a interesse

Tarefas e temas de pesquisa

- Análise de segurança da comunicação com o Drone
- Estudo de protocolos de roteamento em redes ad-hoc com nós móveis
- Desenvolvimento de aplicações ”inteligentes” com base em sensoriamento

Blockchains para aplicações de Metrologia, Qualidade e Segurança

Rede Blockchain de Metrologia e Qualidade

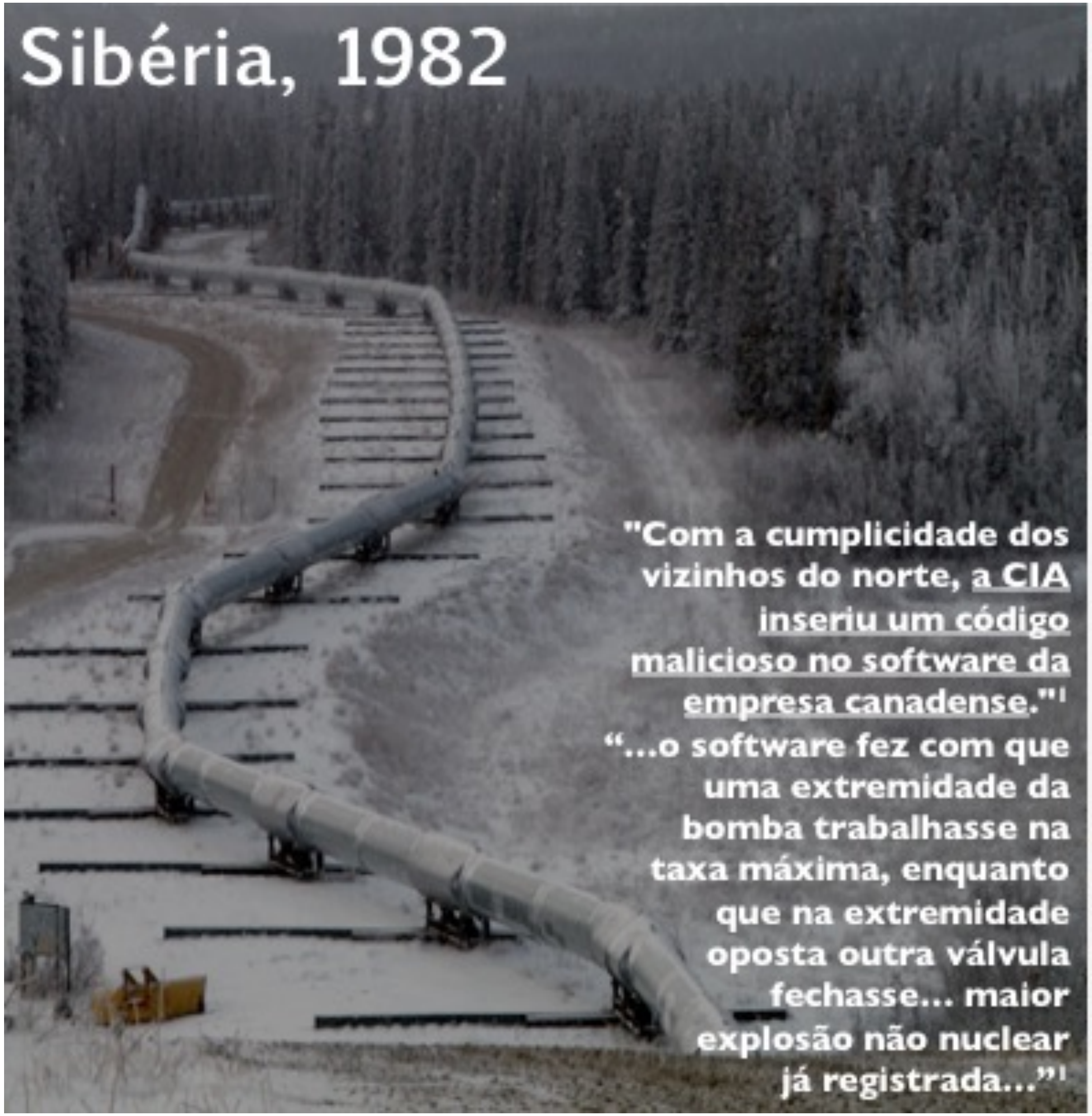

1
clientes enviam transações
3
peers propagam e armazenam blocos em uma cadeia
peers decidem sobre novo bloco (consenso)
2

Segurança da Informação

Professor: Raphael Machado

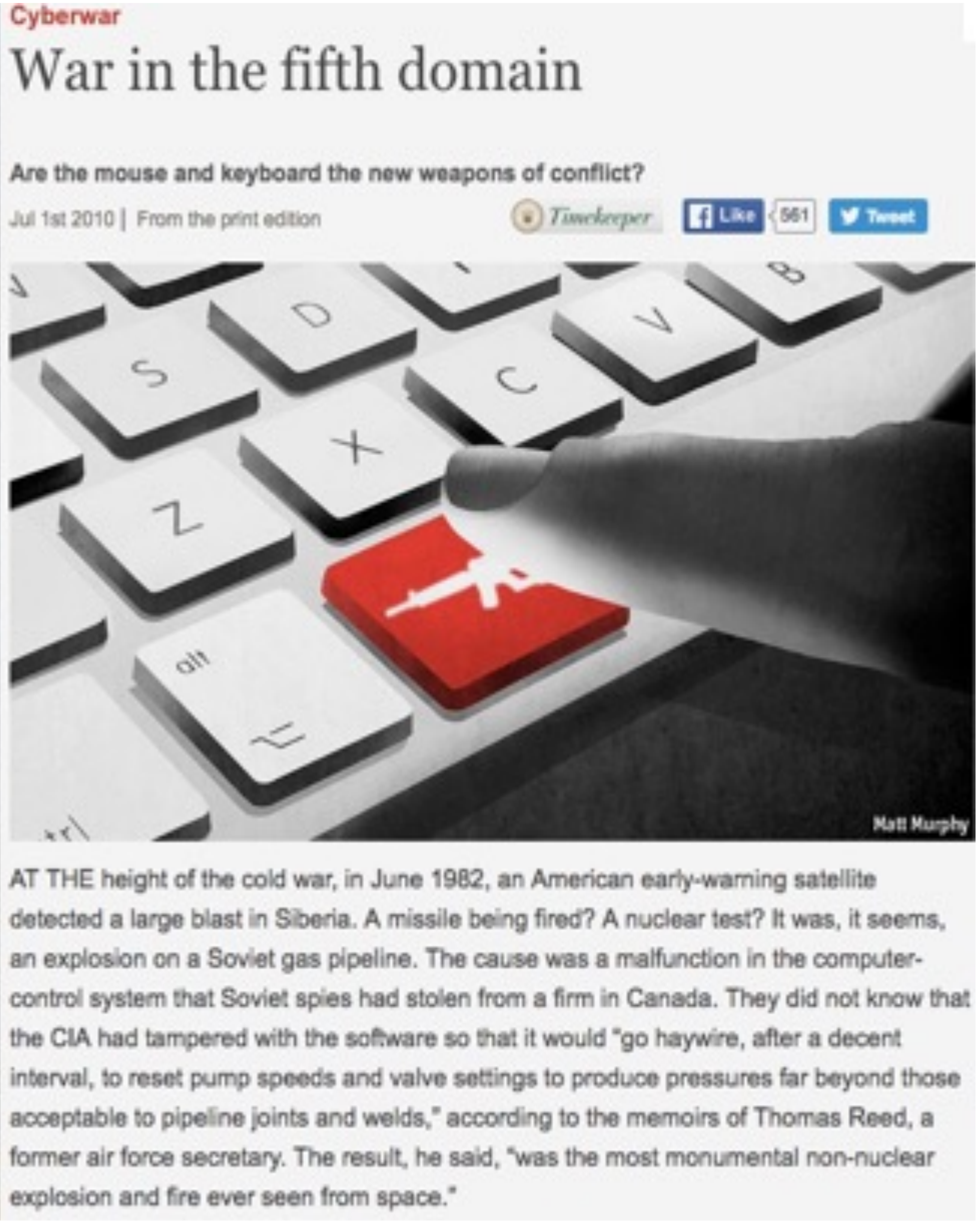
Motivação

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

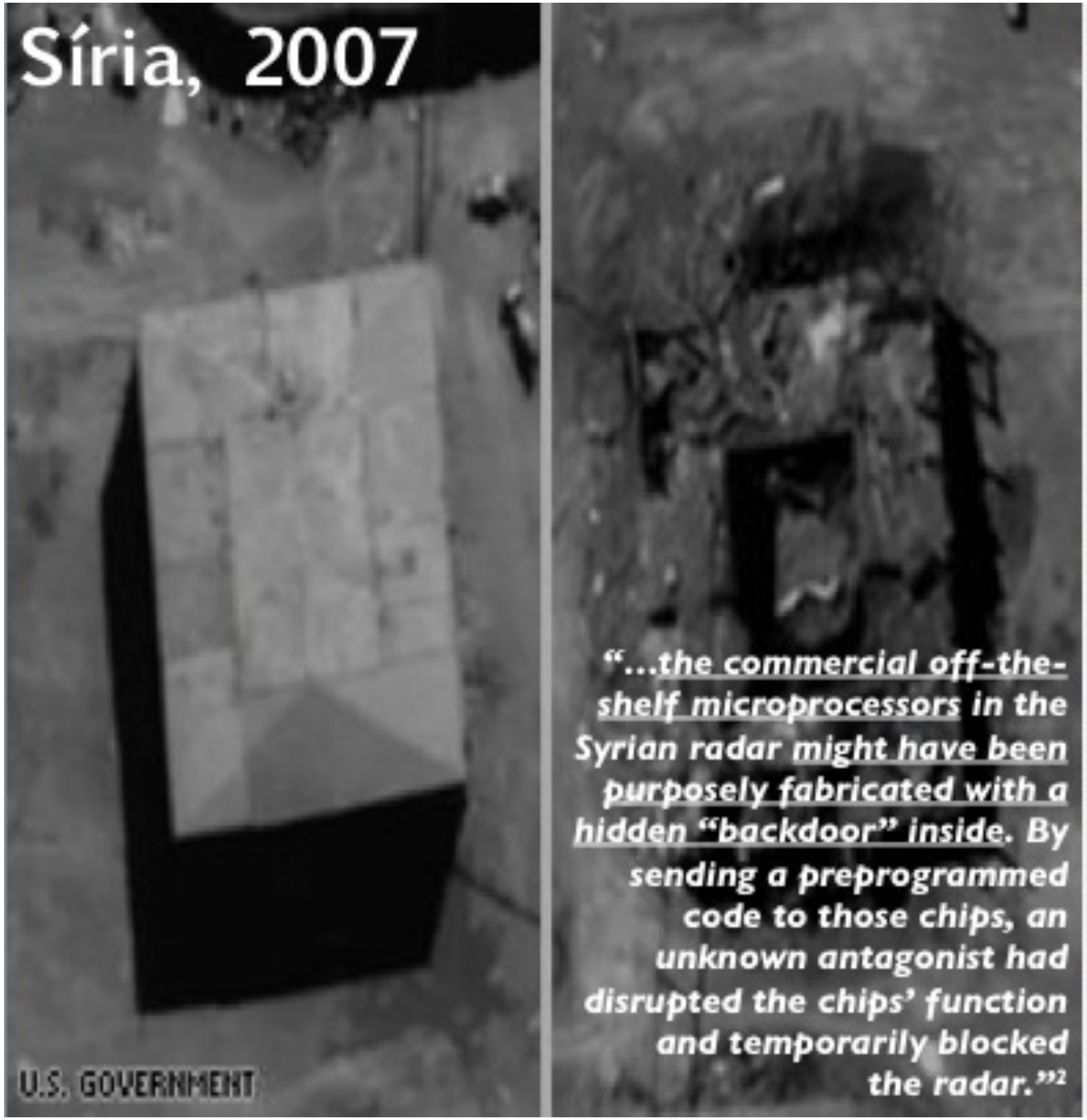
War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

Jul 1st 2010 | From the print edition

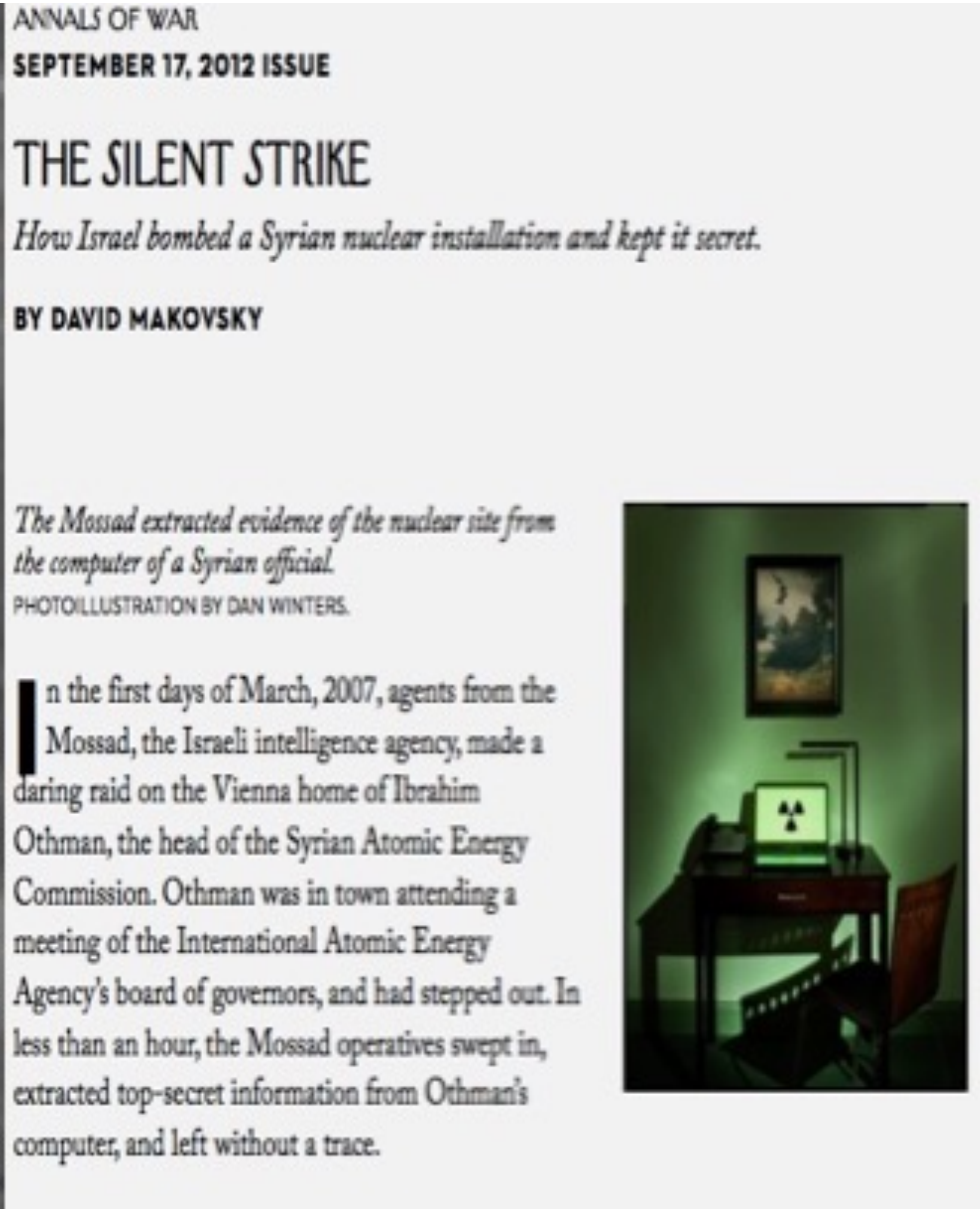
AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from 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."

Síria, 2007



U.S. GOVERNMENT

"…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

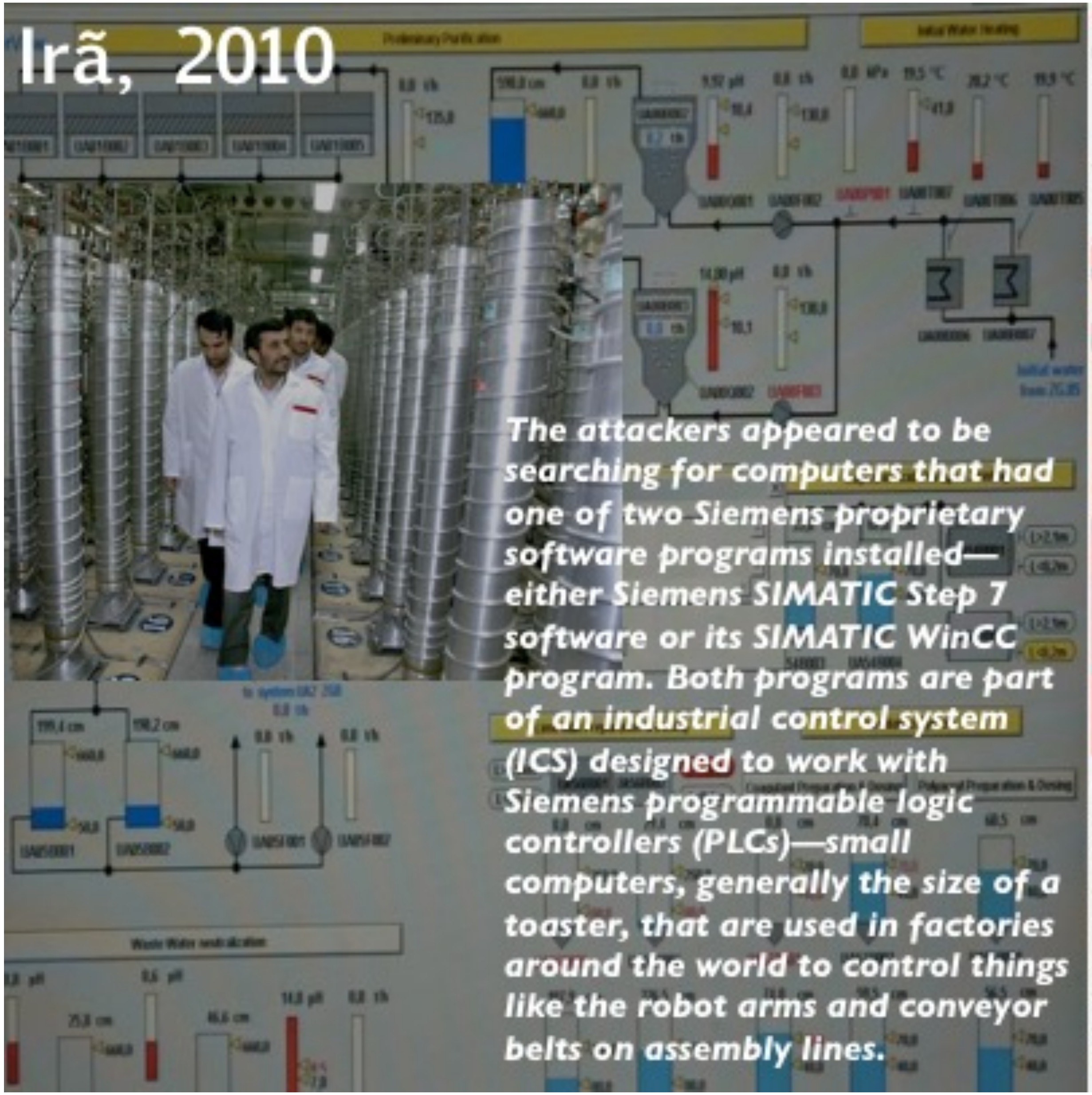
How Israel bombed a Syrian nuclear installation and kept it secret.

BY DAVID MAKOVSKY

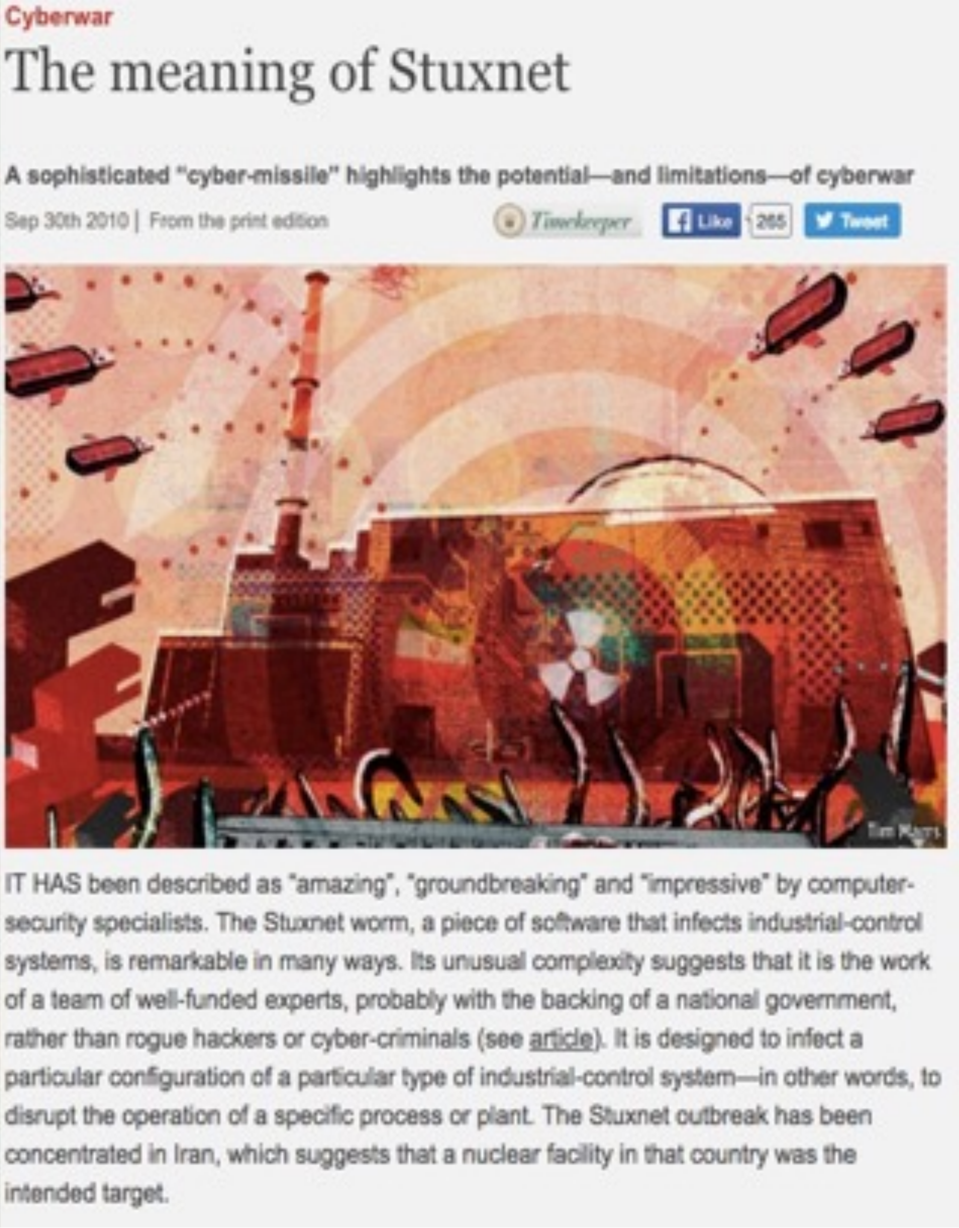
The Mossad extracted evidence of the nuclear site from the computer of a Syrian official.
PHOTOILLUSTRATION BY DAN WINTERS.

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

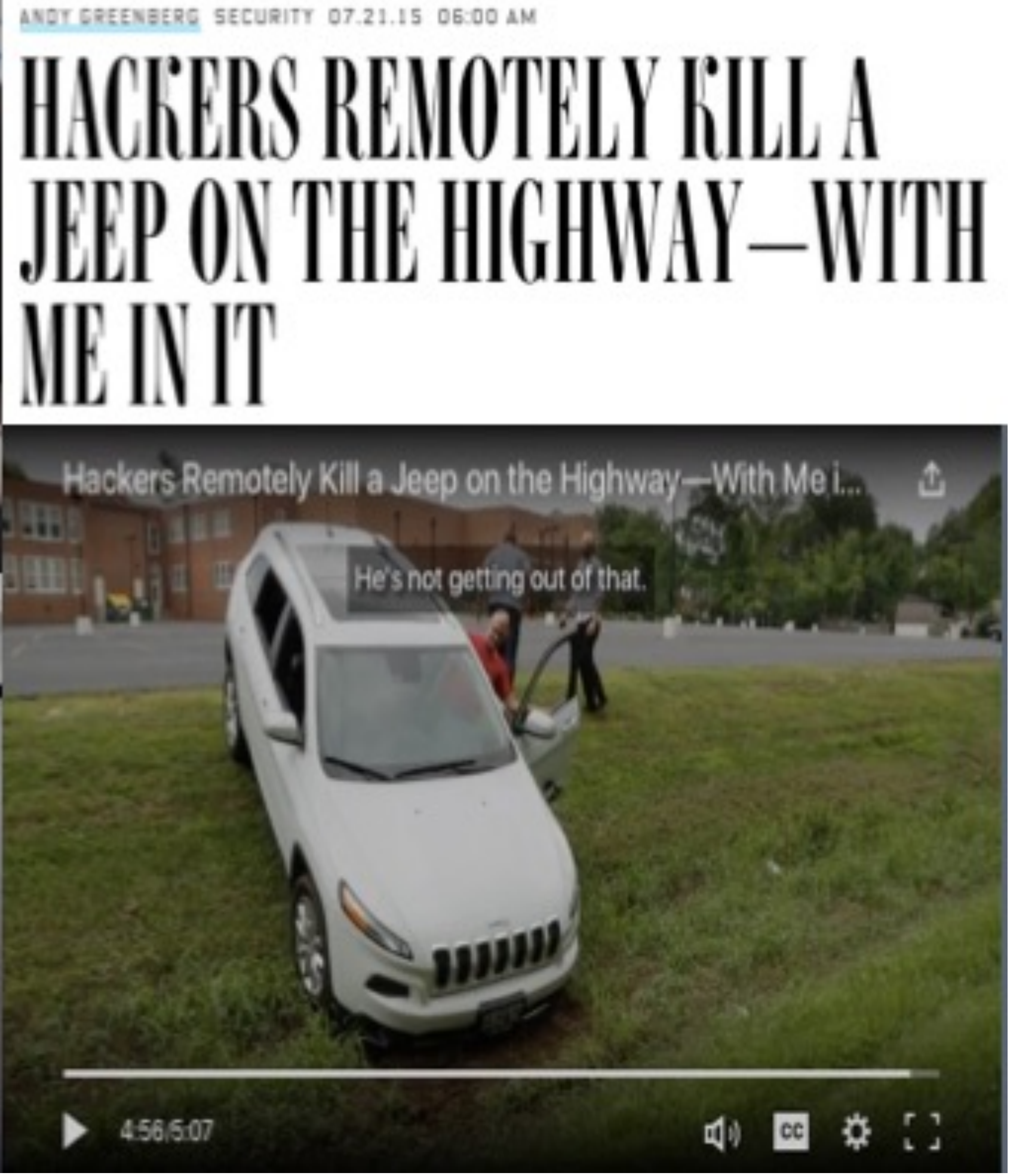
The meaning of Stuxnet

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, 2016



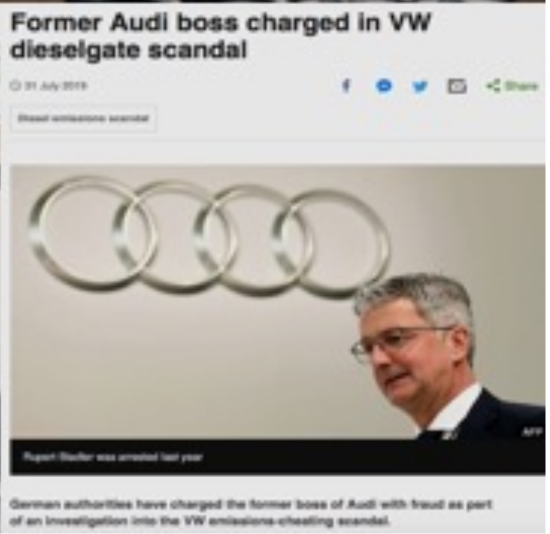
ANDY GREENBERG SECURITY 07.21.15 06:00 AM

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

Hackers Remotely Kill a Jeep on the Highway—With Me i...

He's not getting out of that.

EUA/Alemanha, 2016



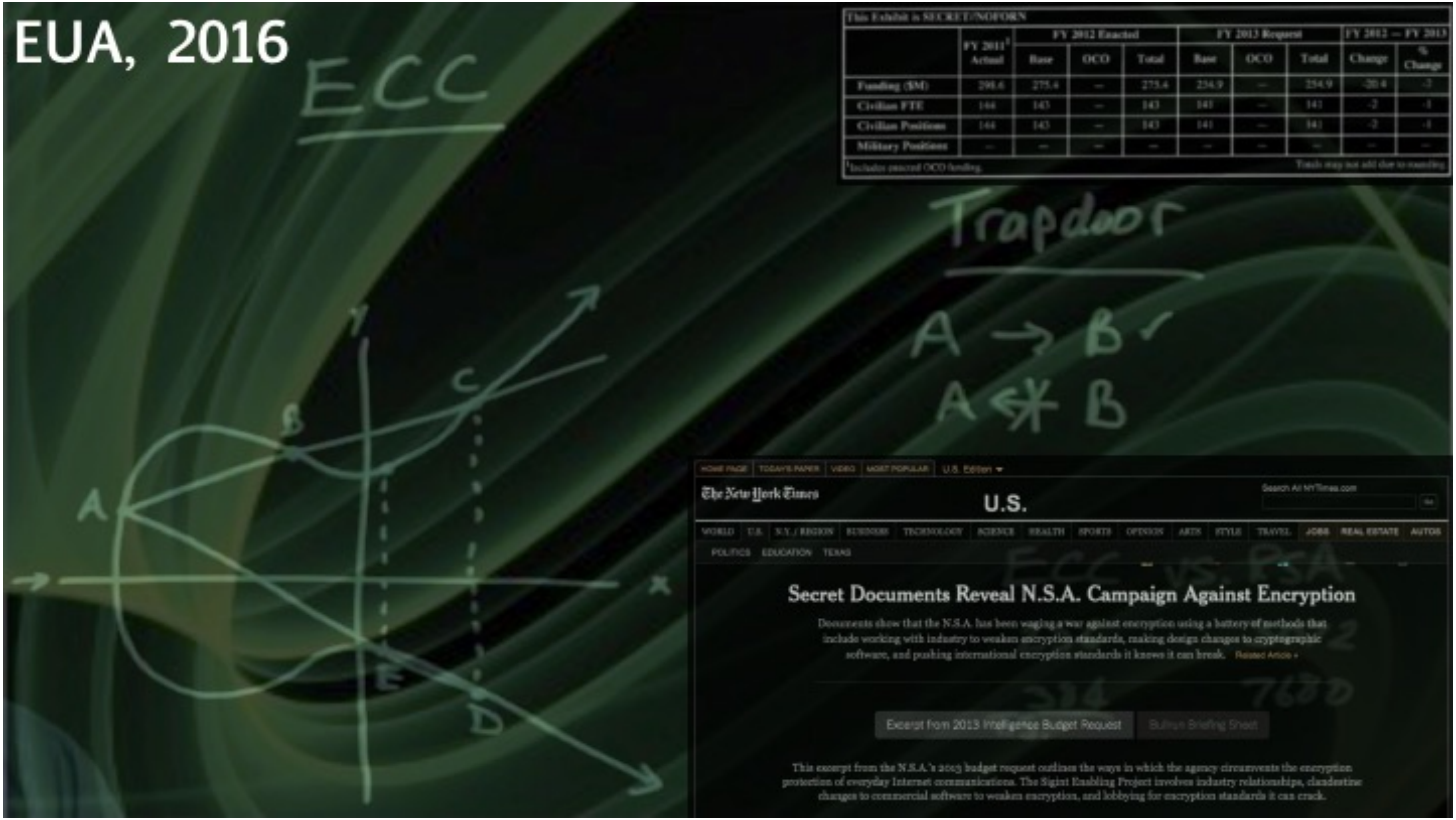
Former Audi boss charged in VW dieselgate scandal

31 July 2019

Rupert Stadler was arrested last year

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

EUA, 2016



This Exhibit is SECRET//NOFORN

	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

[1] Includes enacted OCO funding.

Totals may not add due to rounding.

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, making design changes to cryptographic software, and pushing international encryption standards it knows it can break.

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.

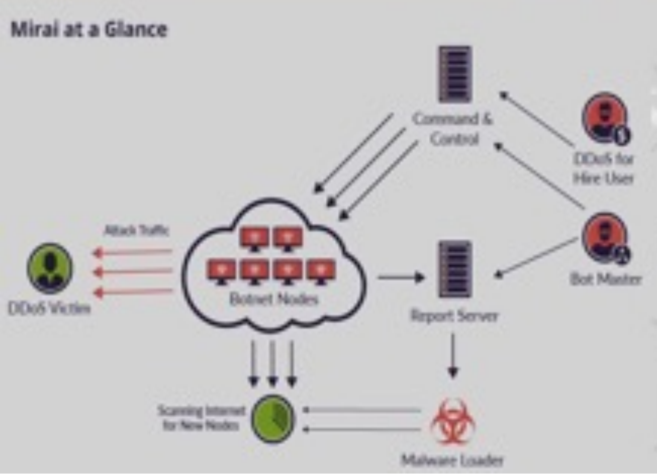
EUA, 2016

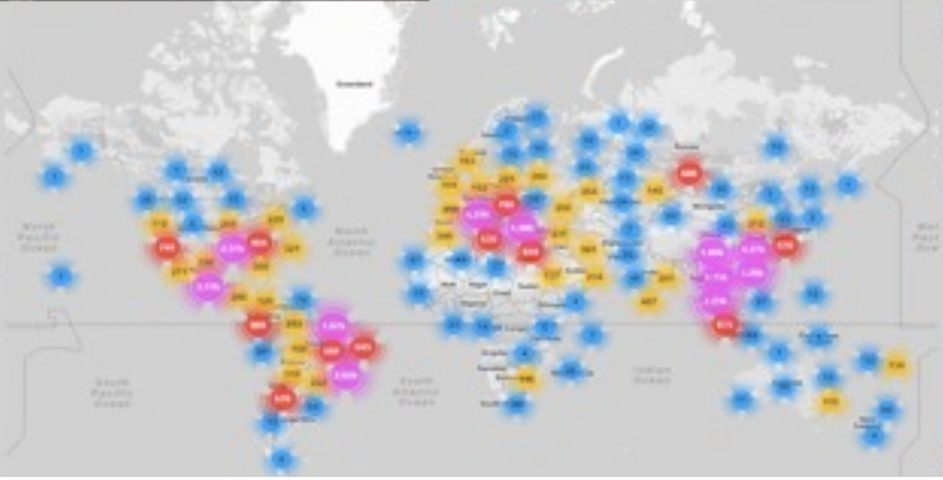
BIZ & IT —

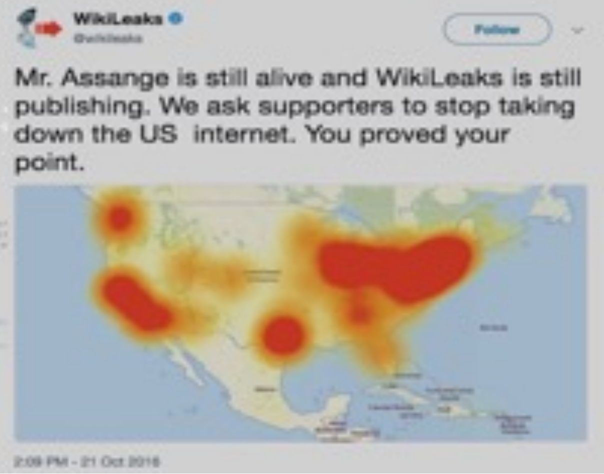
DoS attack on major DNS provider brings Internet to morning crawl [Updated]

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

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





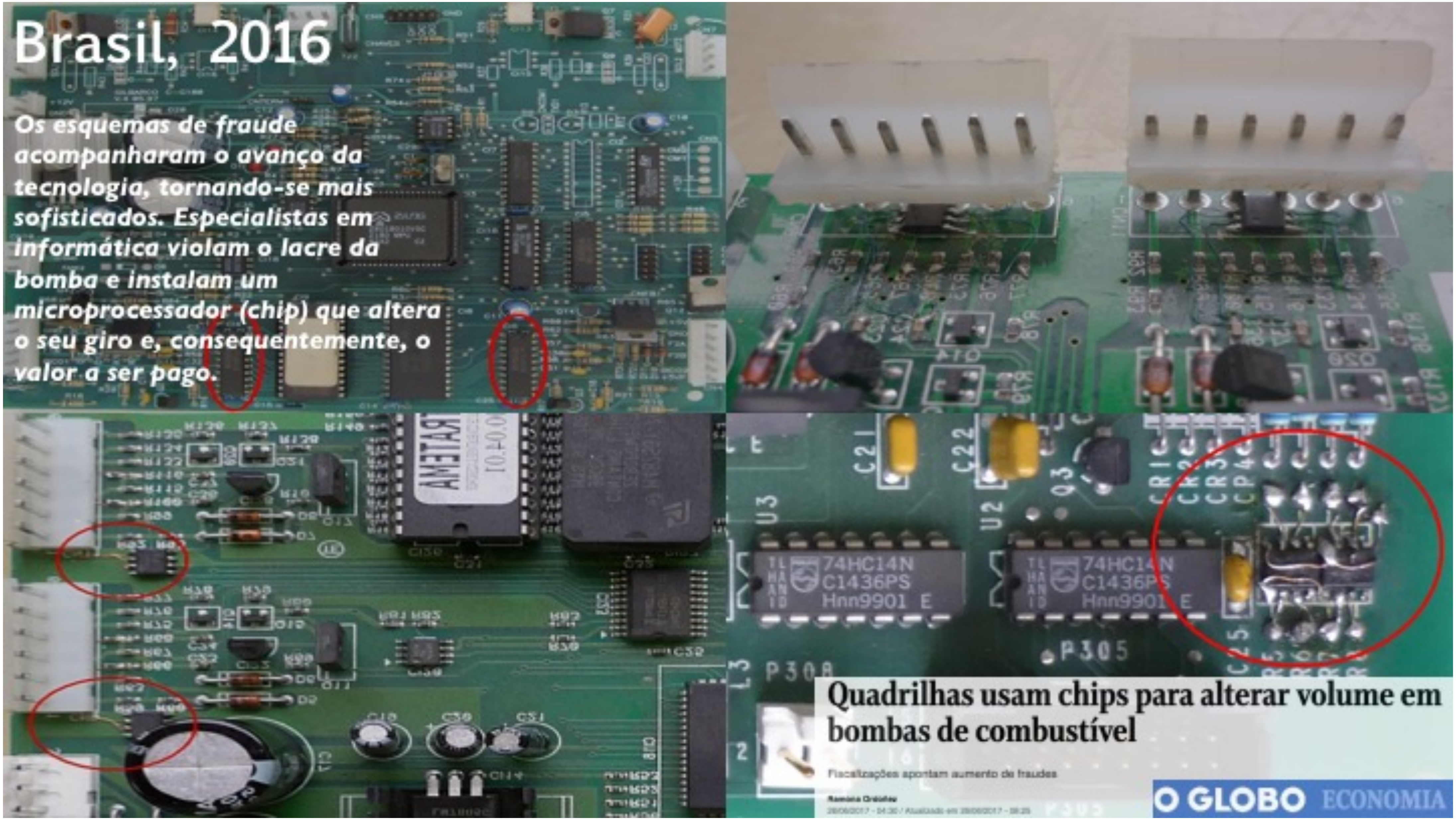


Mr. Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point.

2:09 PM - 21 Oct 2016

Brasil, 2016

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.



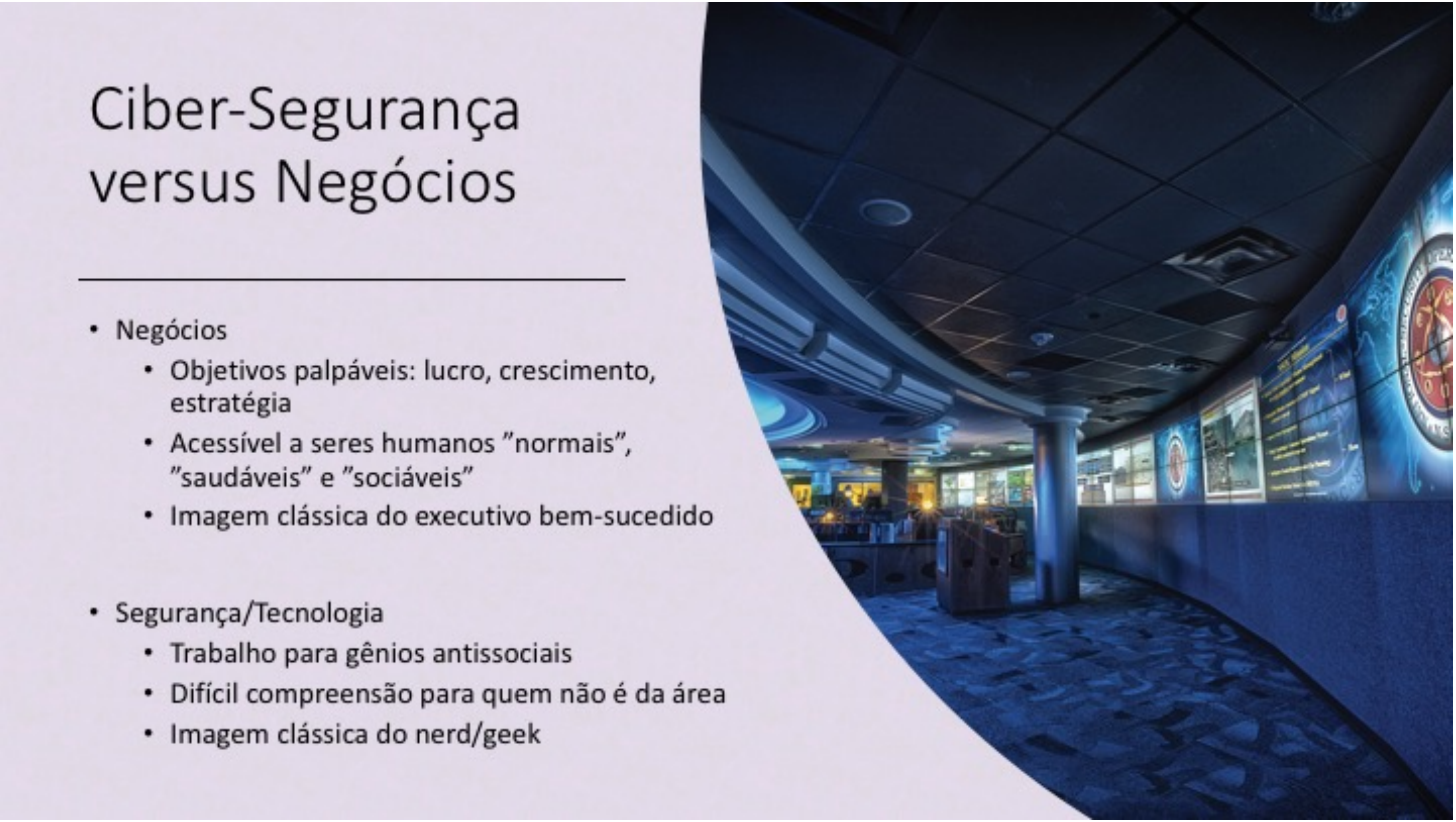
Quadrilhas usam chips para alterar volume em bombas de combustível

Fiscalizações apontam aumento de fraudes

Ramona Ordoñez

28/08/2017 - 04:30 / Atualizado em 28/08/2017 - 08:25

O GLOBO ECONOMIA



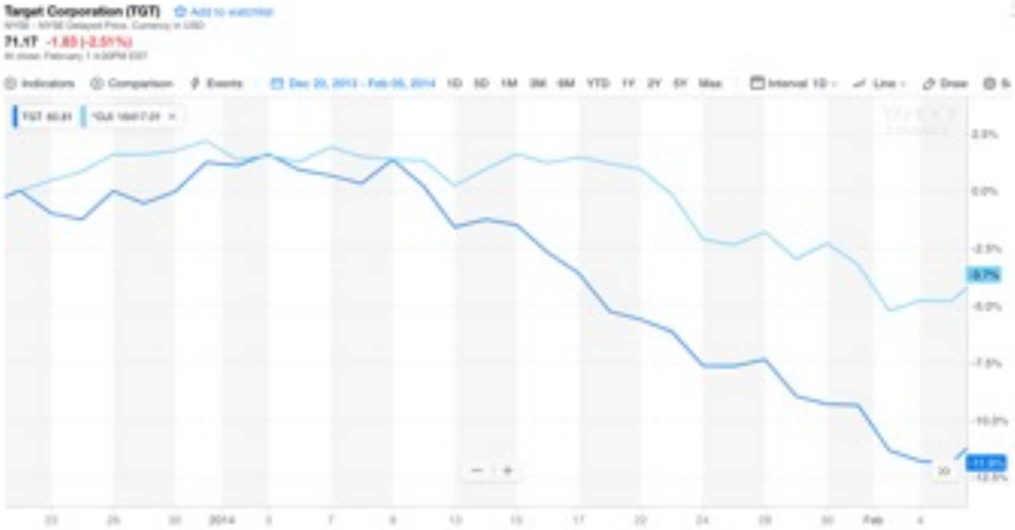
Ciber-Segurança versus Negócios

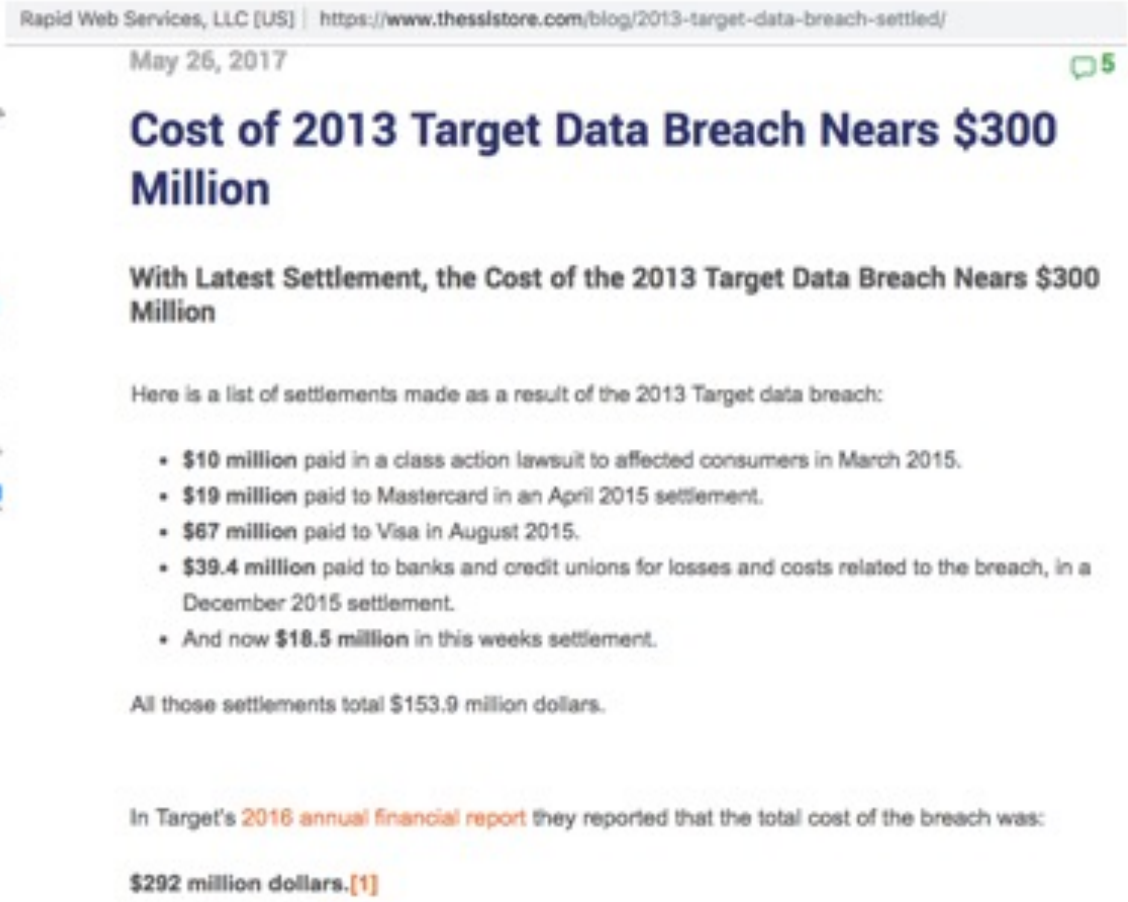
- Negócios
  - Objetivos palpáveis: lucro, crescimento, estratégia
  - Acessível a seres humanos ”normais”, ”saudáveis” e ”sociáveis”
  - Imagem clássica do executivo bem-sucedido

- Segurança/Tecnologia
  - Trabalho para gênios antissociais
  - Difícil compreensão para quem não é da área
  - Imagem clássica do nerd/geek

Vazamento de dados da Target

- Nov-Dez/2013: 40milhões de números de cartão e 70 milhões de registros pessoais
- Queda de 40% nos lucros do 4ºTri
- Queda nas ações da empresa




Rapid Web Services, LLC [US] | https://www.thesslstore.com/blog/2013-target-data-breach-settled/
5

May 26, 2017

Cost of 2013 Target Data Breach Nears $300 Million

With Latest Settlement, the Cost of the 2013 Target Data Breach Nears $300 Million

Here is a list of settlements made as a result of the 2013 Target data breach:

- **$10 million** paid in a class action lawsuit to affected consumers in March 2015.
- **$19 million** paid to Mastercard in an April 2015 settlement.
- **$67 million** paid to Visa in August 2015.
- **$39.4 million** paid to banks and credit unions for losses and costs related to the breach, in a December 2015 settlement.
- And now **$18.5 million** in this weeks settlement.

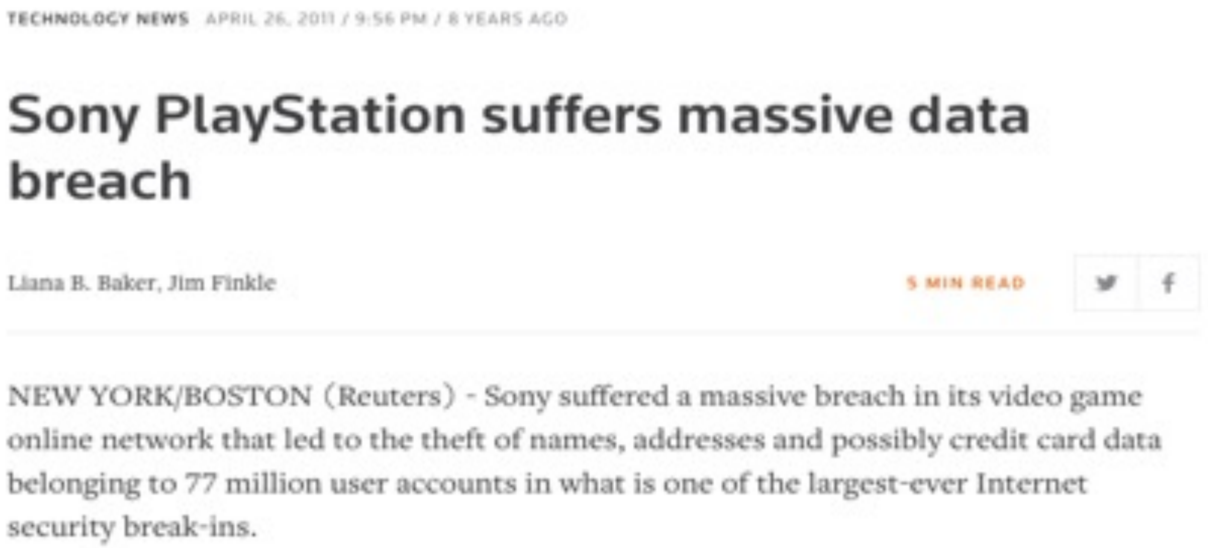
All those settlements total $153.9 million dollars.

In Target's 2016 annual financial report they reported that the total cost of the breach was:

$292 million dollars.[1]

Vazamento da Sony

- 11 de abril de 2011: dados de 77 milhões de contas vazados, incluindo cartões de crédito
- 171 milhões de dólares de custo total



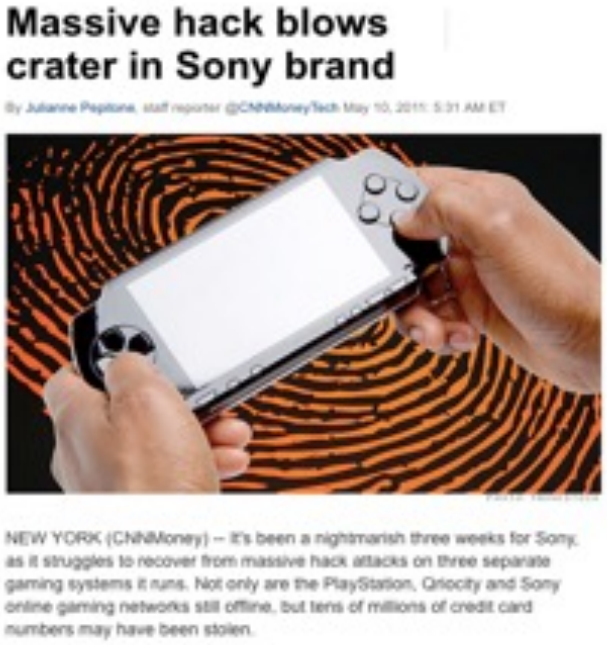
TECHNOLOGY NEWS APRIL 26, 2011 / 9:56 PM / 8 YEARS AGO

Sony PlayStation suffers massive data breach

Liana B. Baker, Jim Finkle

5 MIN READ

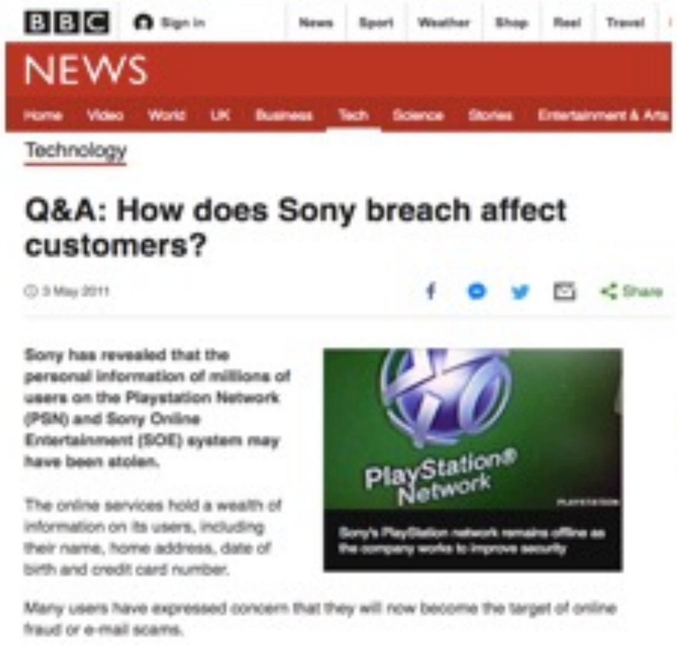
NEW YORK/BOSTON (Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.



Massive hack blows crater in Sony brand

By Julianne Pepitone, staff reporter @CNNMoneyTech May 10, 2011: 5:31 AM ET

NEW YORK (CNNMoney) -- It's been a nightmarish three weeks for Sony, as it struggles to recover from massive hack attacks on three separate gaming systems it runs. Not only are the PlayStation, Qriocity and Sony online gaming networks still offline, but tens of millions of credit card numbers may have been stolen.



Technology

Q&A: How does Sony breach affect customers?

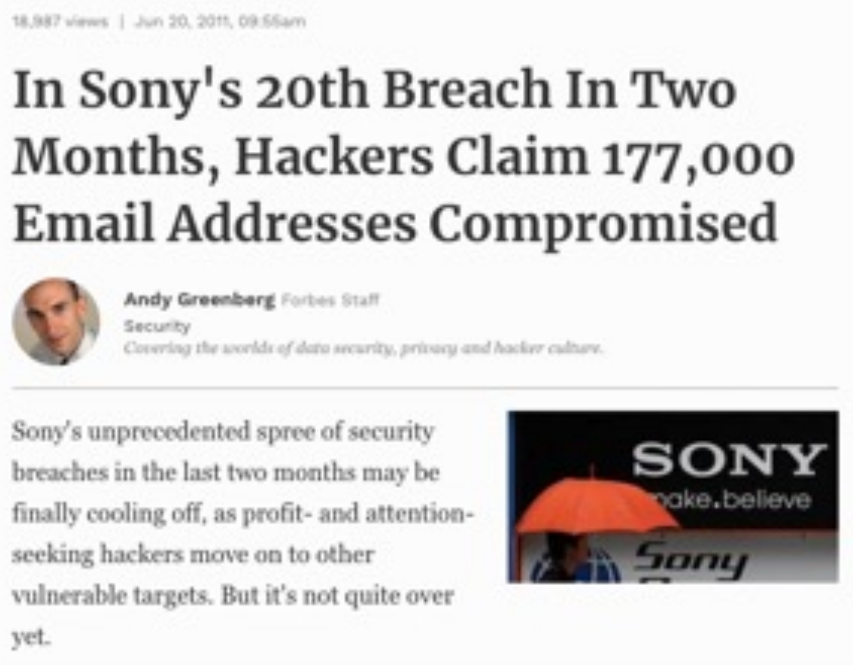
3 May 2011

Sony has revealed that the personal information of millions of users on the Playstation Network (PSN) and Sony Online Entertainment (SOE) system may have been stolen.

Sony's PlayStation network remains offline as the company works to improve security

The online services hold a wealth of information on its users, including their name, home address, date of birth and credit card number.

Many users have expressed concern that they will now become the target of online fraud or e-mail scams.

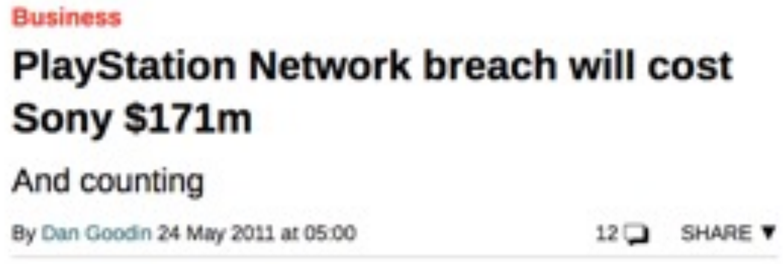


18,987 views | Jun 20, 2011, 09:55am

In Sony's 20th Breach In Two Months, Hackers Claim 177,000 Email Addresses Compromised

Andy Greenberg Forbes Staff
Security
Covering the worlds of data security, privacy and hacker culture.

Sony's unprecedented spree of security breaches in the last two months may be finally cooling off, as profit- and attention-seeking hackers move on to other vulnerable targets. But it's not quite over yet.



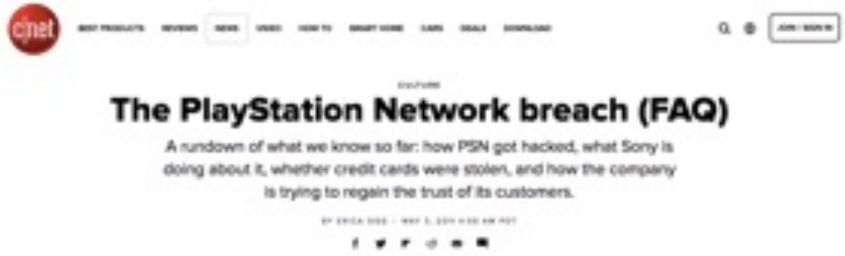
Business

PlayStation Network breach will cost Sony $171m

And counting

By Dan Goodin 24 May 2011 at 05:00

12 SHARE ▼



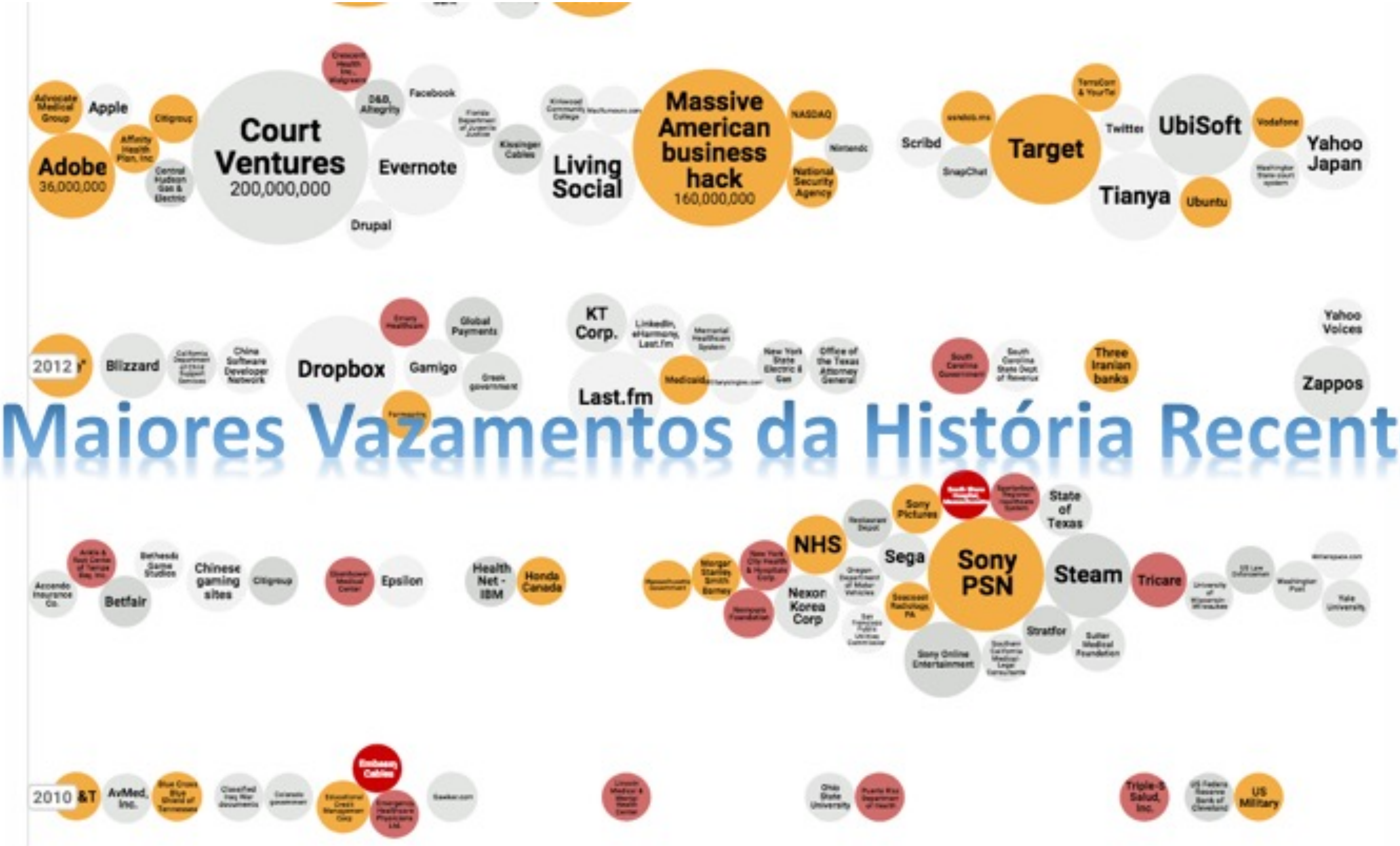
CULTURE

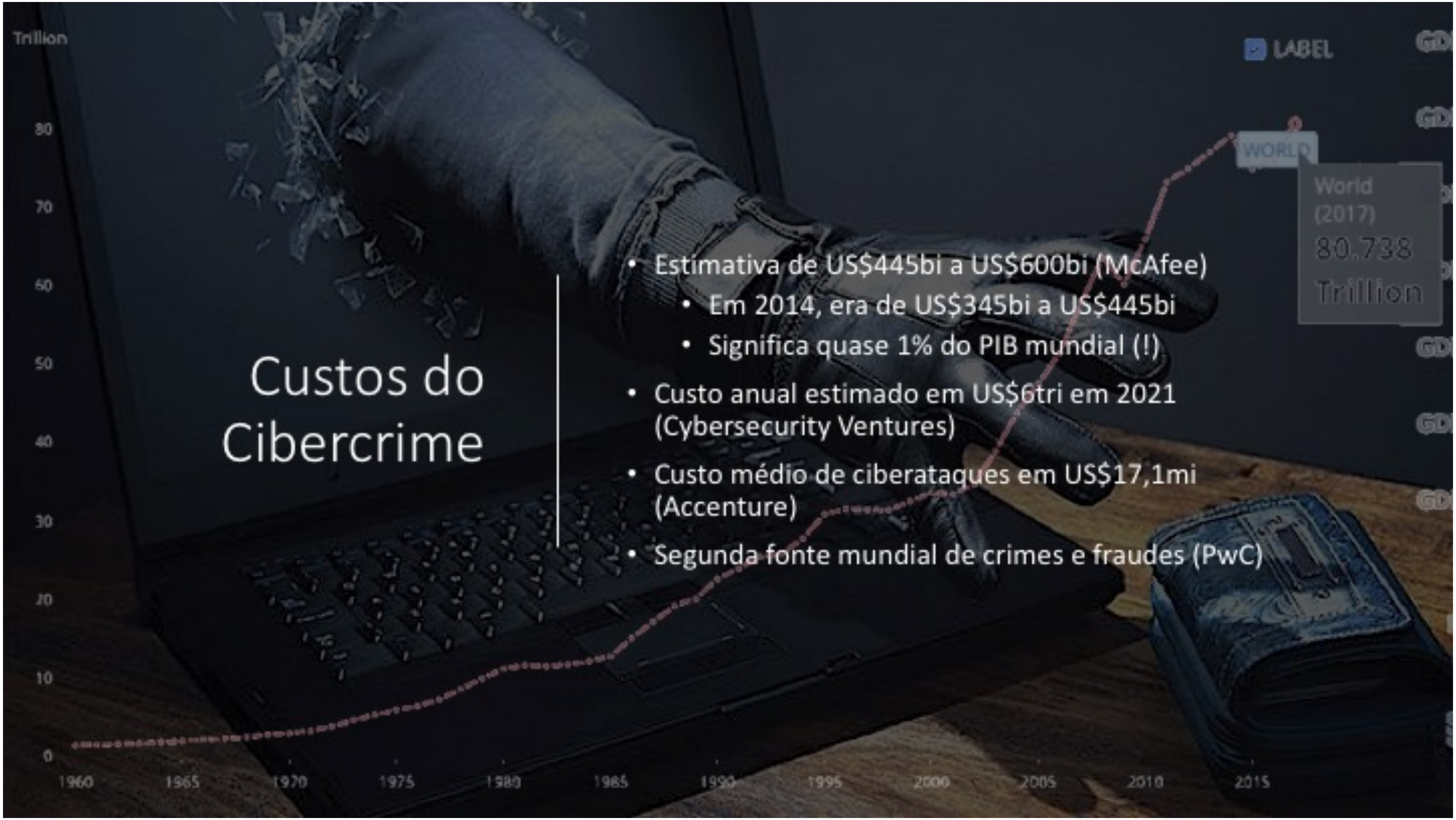
The PlayStation Network breach (FAQ)

A rundown of what we know so far: how PSN got hacked, what Sony is doing about it, whether credit cards were stolen, and how the company is trying to regain the trust of its customers.

BY ERICA OGG · MAY 3, 2011 4:00 AM PDT

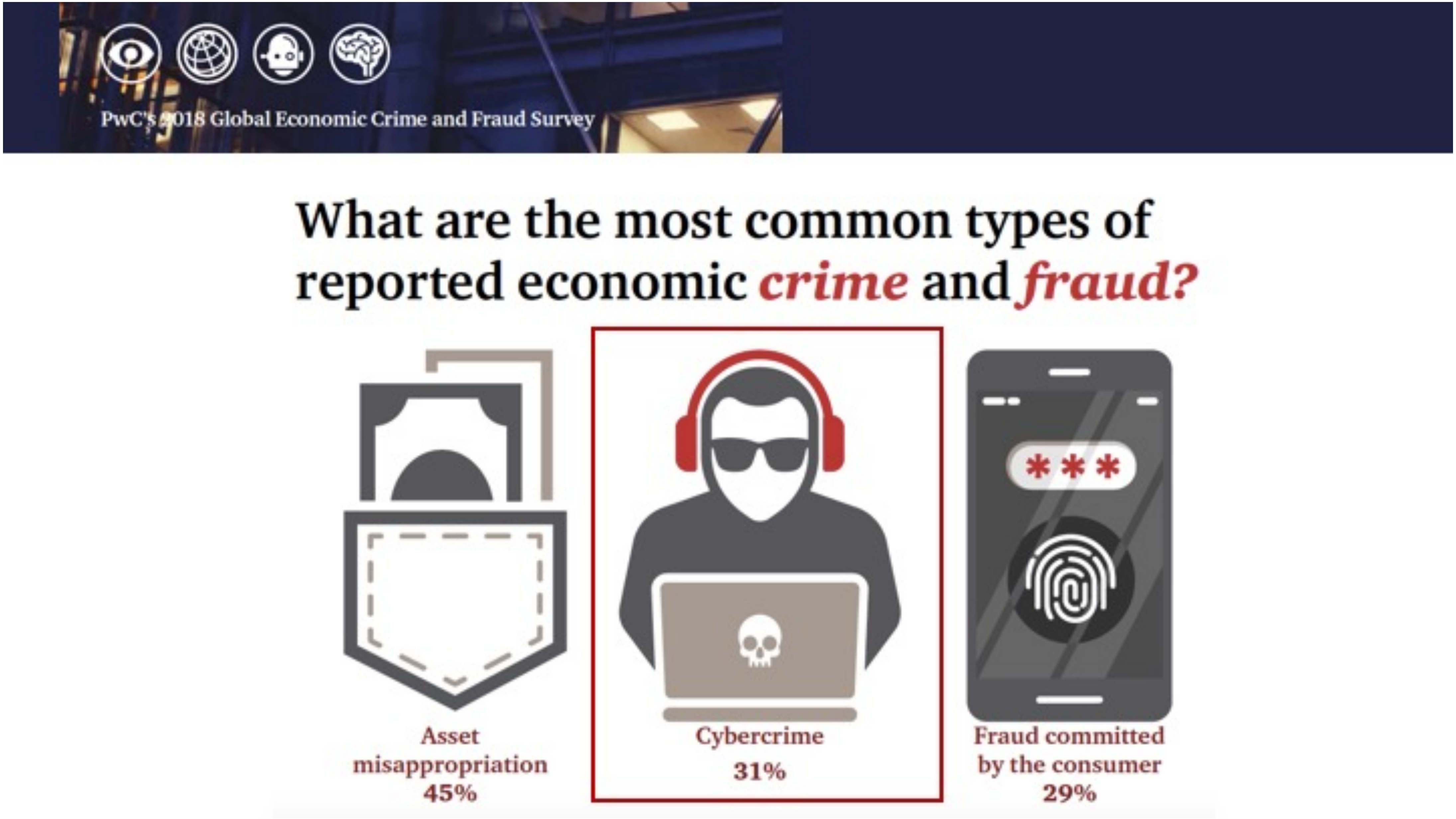
Maiores Vazamentos da História Recente





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)



PwC's 2018 Global Economic Crime and Fraud Survey

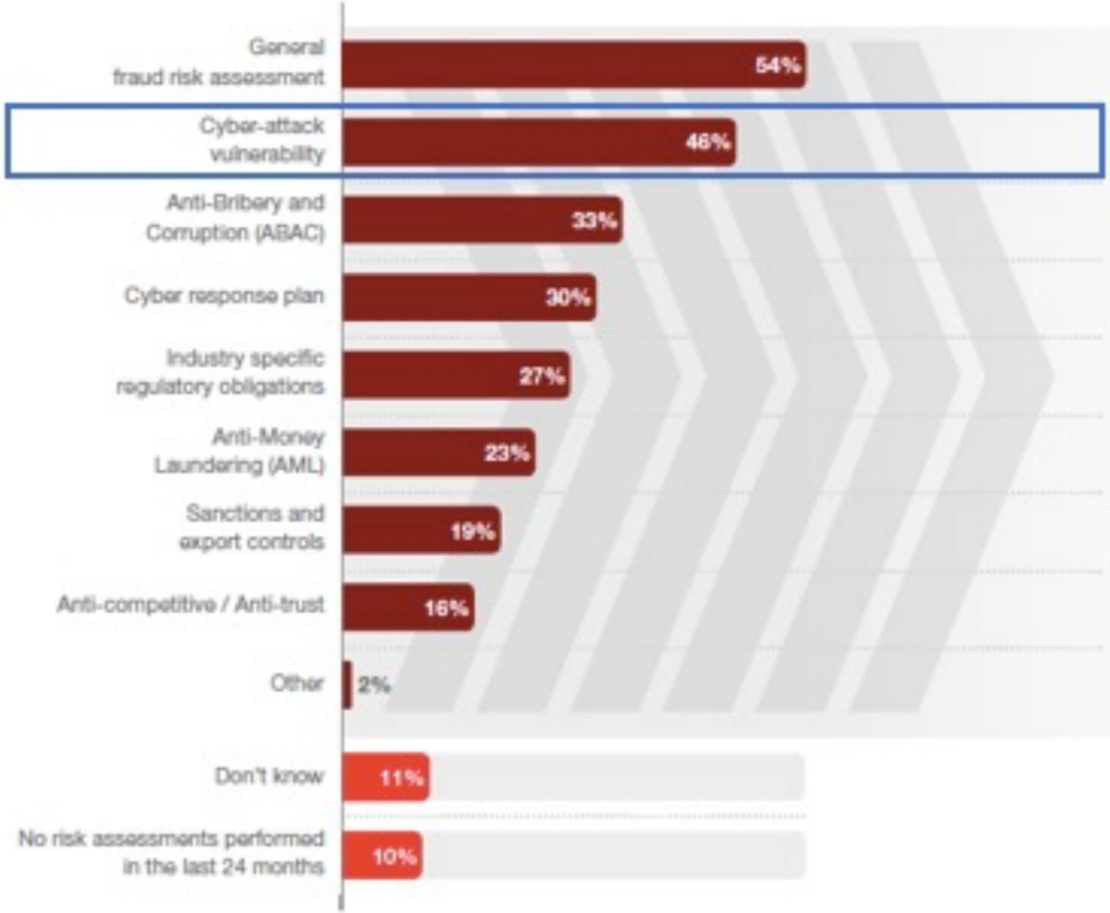
What are the most common types of reported economic *crime* and *fraud?*

Asset misappropriation
45%

Cybercrime
31%

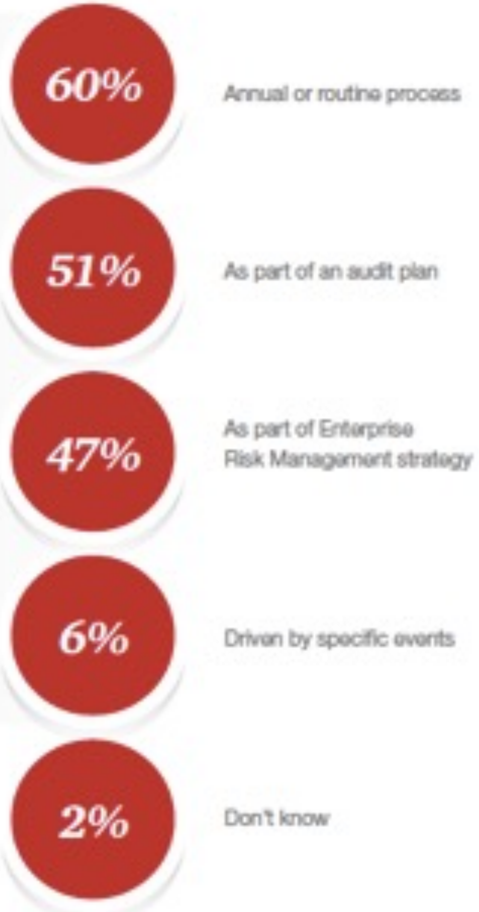
Fraud committed by the consumer
29%

Exhibit 4: Less than half of all organisations have performed targeted risk assessments in the last 2 years



Q. In the last 24 months, has your organisation performed a risk assessment on any of the following areas?

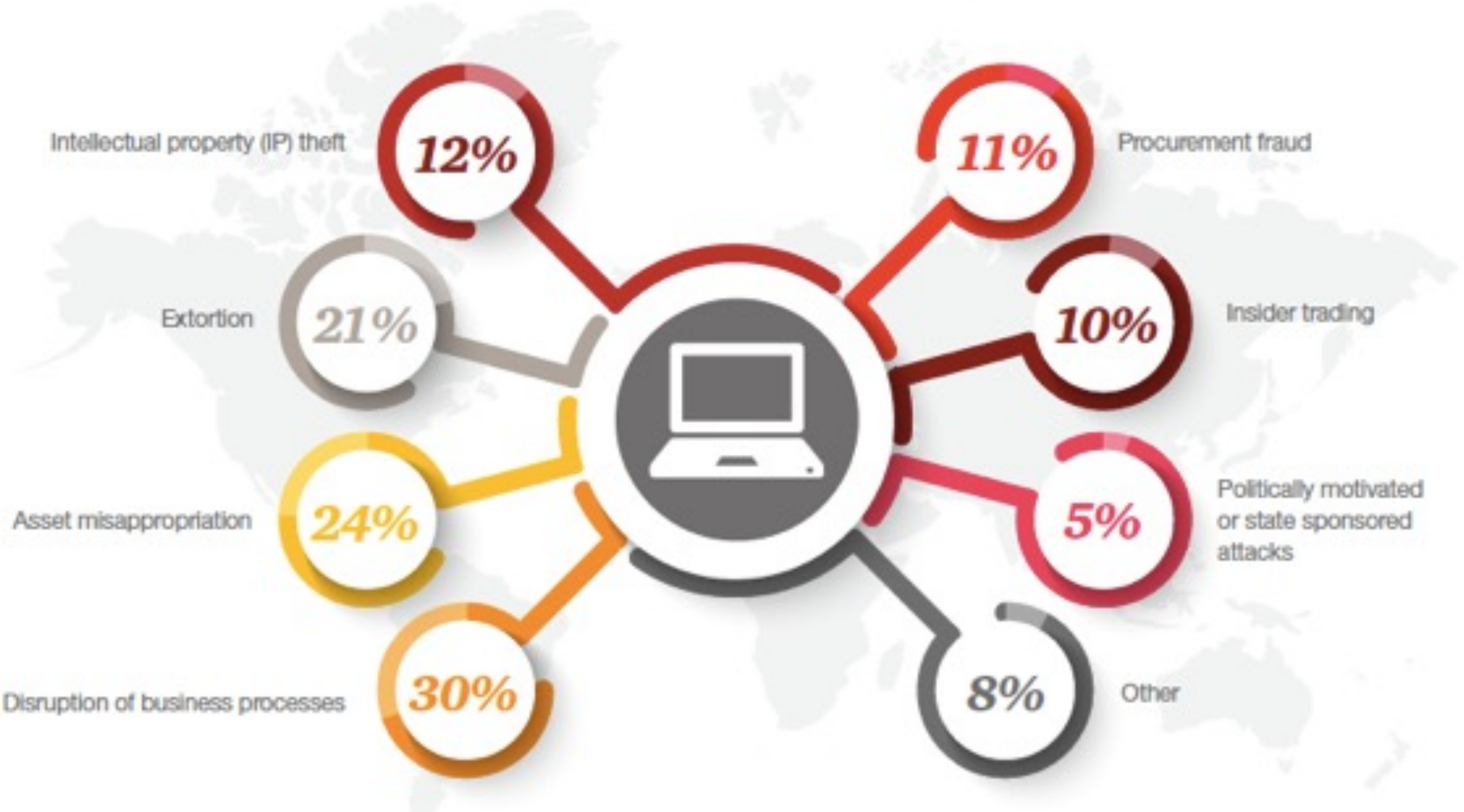
Source: PwC's 2018 Global Economic Crime and Fraud Survey



Q. What prompted your organisation to perform a risk assessment?

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

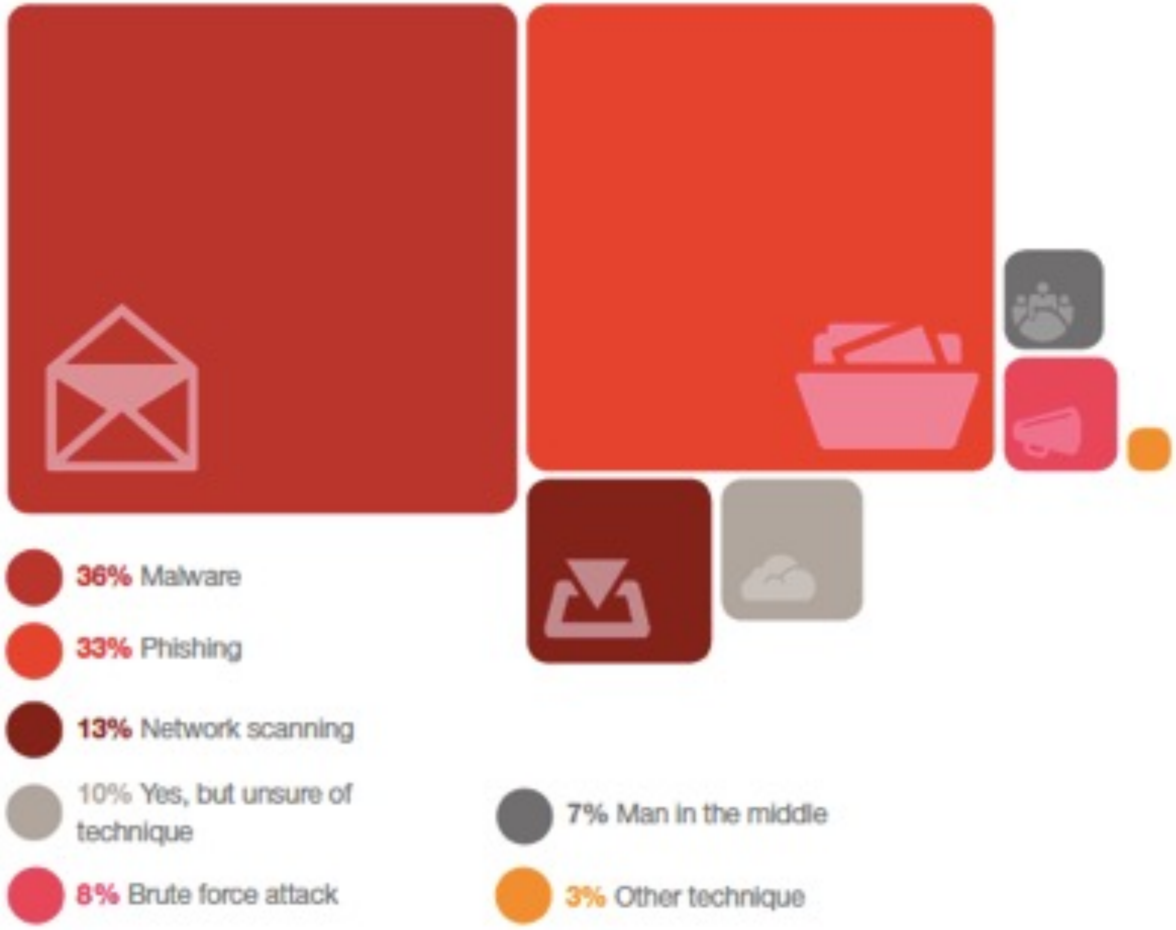
Exhibit 17: Types of fraud that organisations were a victim of through a cyber-attack



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

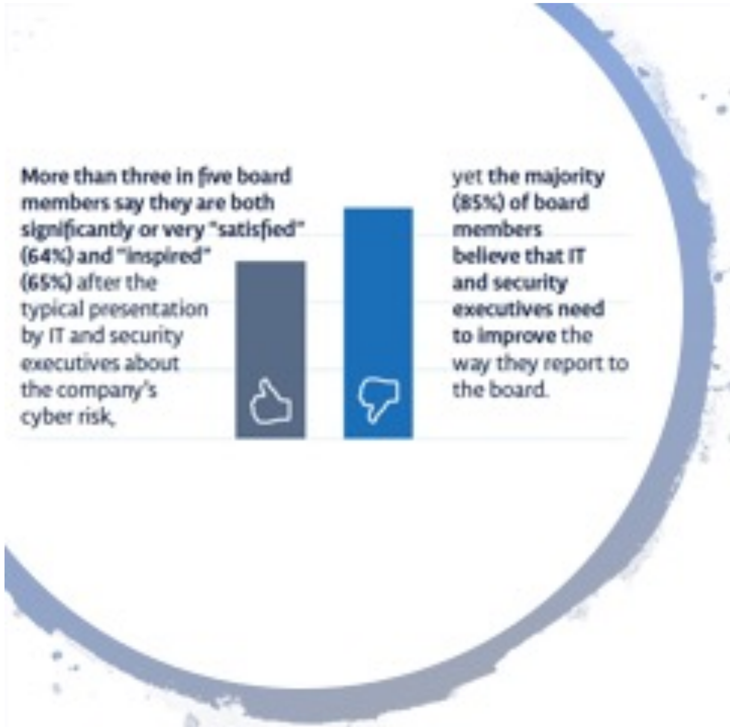
Over a third of all respondents have been targeted by cyber-attacks, through both malware and phishing. Most of these attacks, which can severely disrupt business processes, also lead to substantive losses to companies: 24% of respondents who were attacked suffered asset misappropriation and 21% were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

Global Economic Crime Survey 2016

pwc

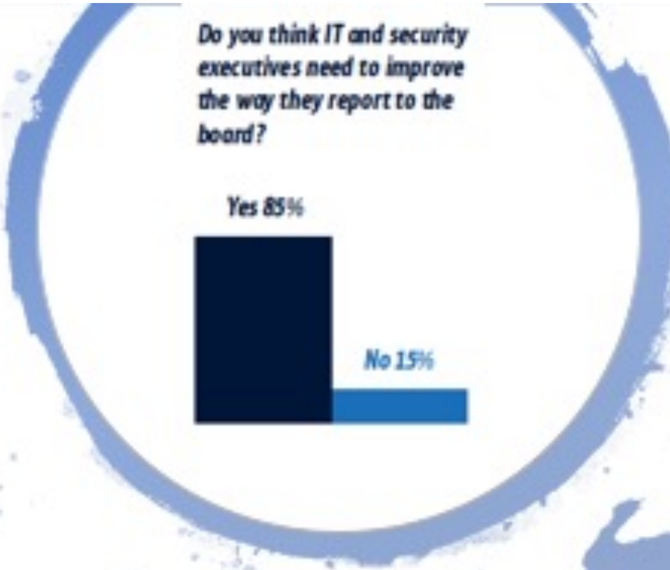
Contents

Board reconhece importância da Cibersegurança…
…mas reports precisam melhorar

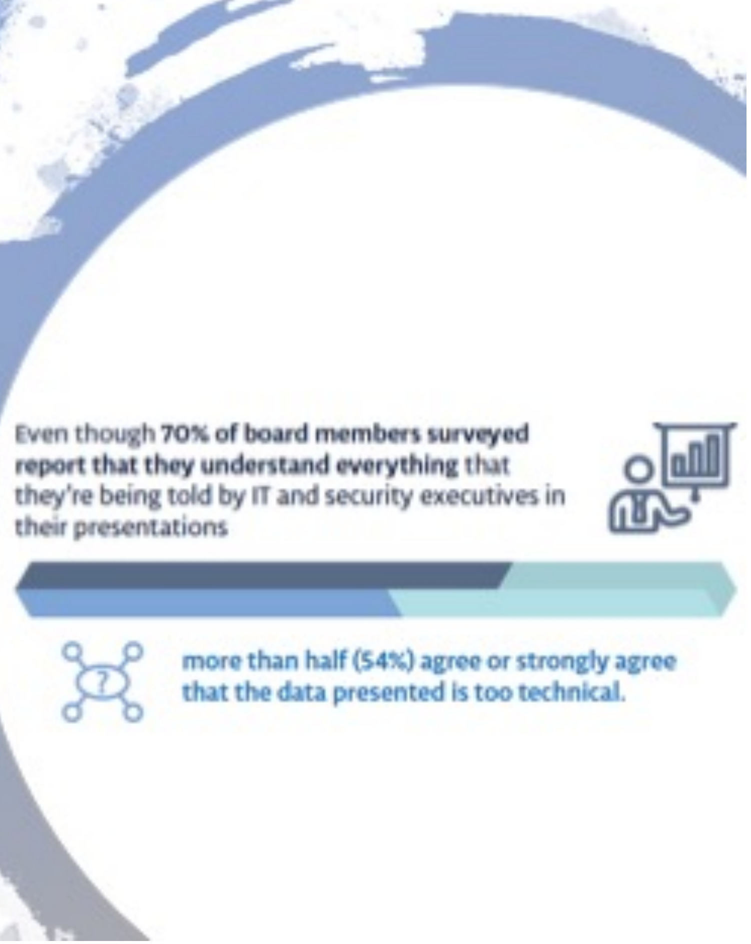


More than three in five board members say they are both significantly or very "satisfied" (64%) and "inspired" (65%) after the typical presentation by IT and security executives about the company's cyber risk,

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



Do you think IT and security executives need to improve the way they report to the board?

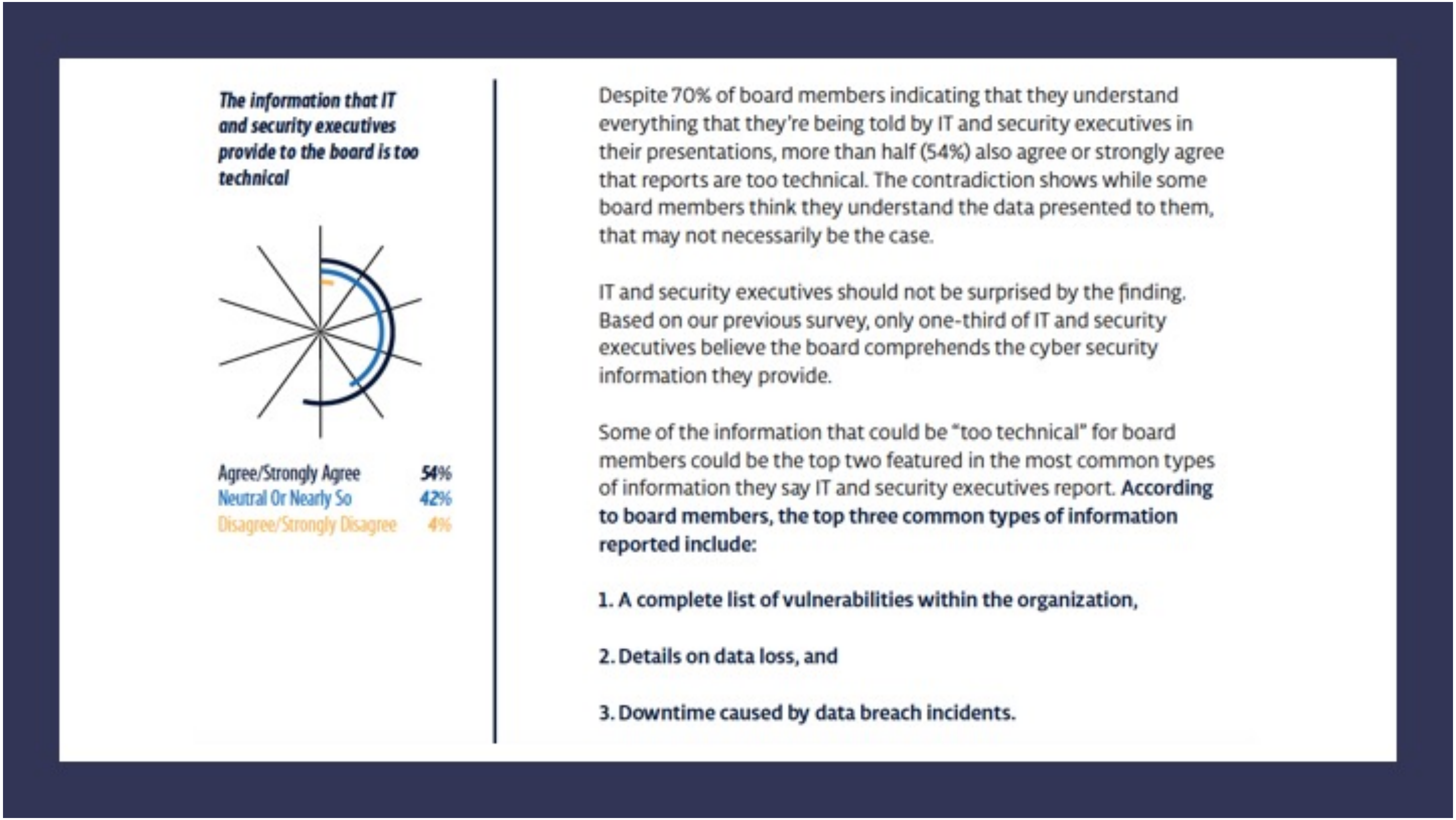


Even though **70% of board members surveyed report that they understand everything** that they're being told by IT and security executives in their presentations

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



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.

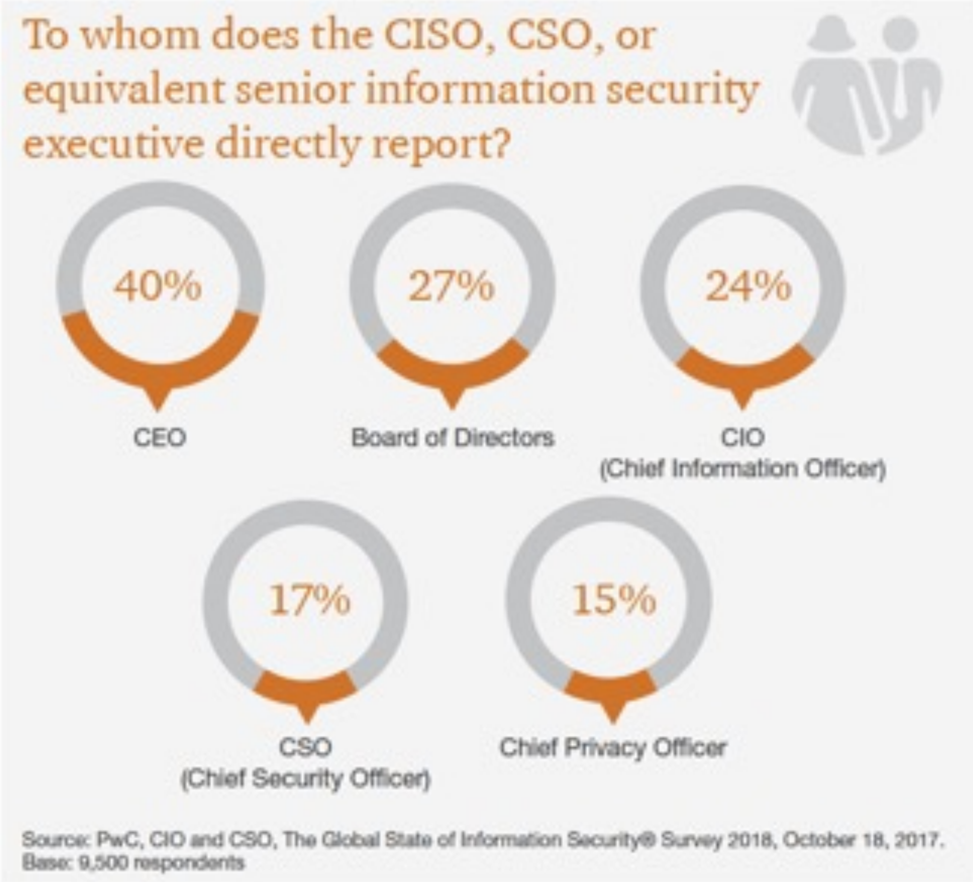
Some of the information that could be "too technical" for board members could be the top two featured in the most common types of information they say IT and security executives report. **According to board members, the top three common types of information reported include:**

1. A complete list of vulnerabilities within the organization,

2. Details on data loss, and

3. Downtime caused by data breach incidents.

Em resumo... ciber-segurança é questão de negócio

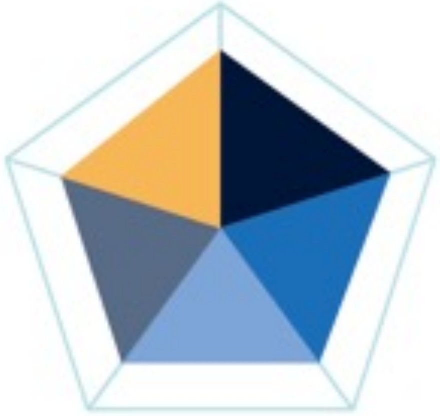


To whom does the CISO, CSO, or equivalent senior information security executive directly report?

Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018, October 18, 2017.
Base: 9,500 respondents

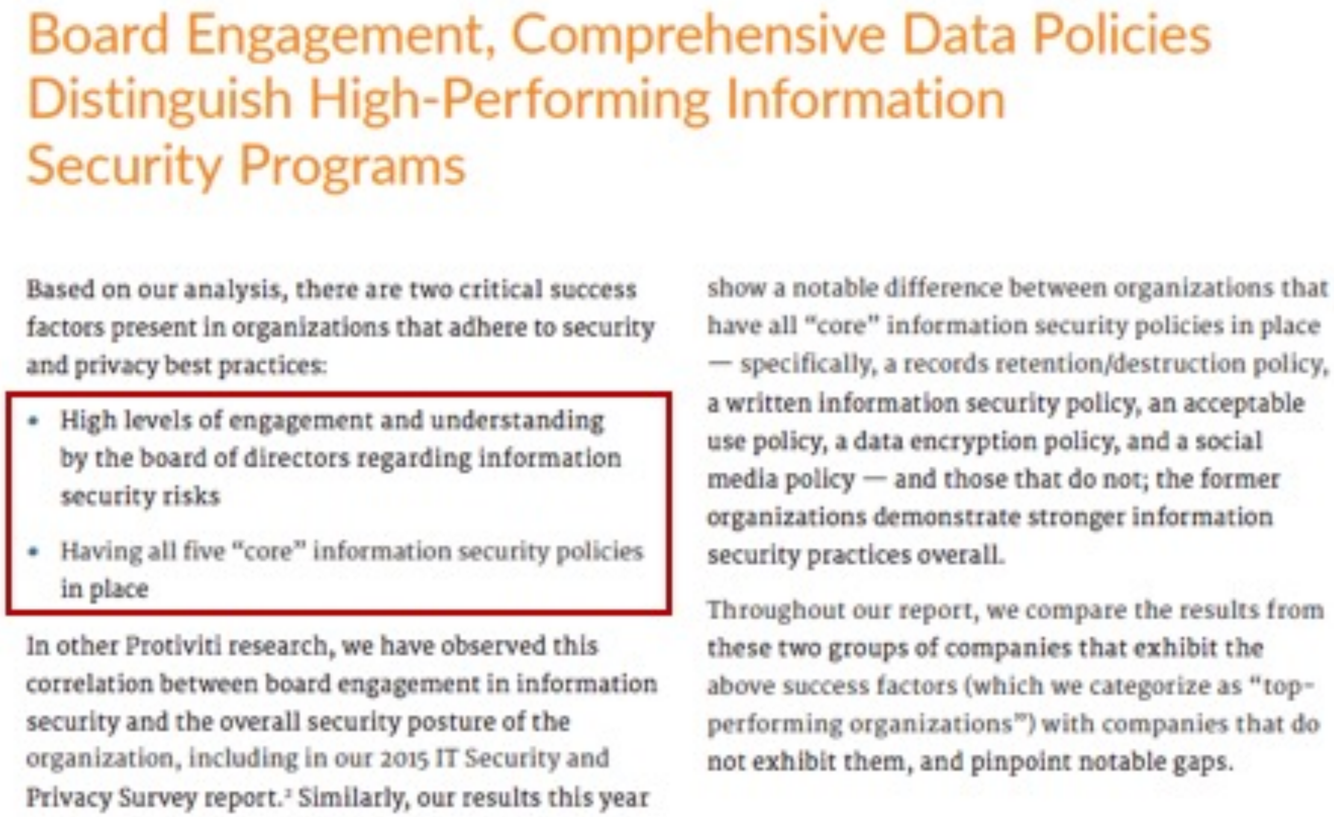
Riscos, riscos, riscos...

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

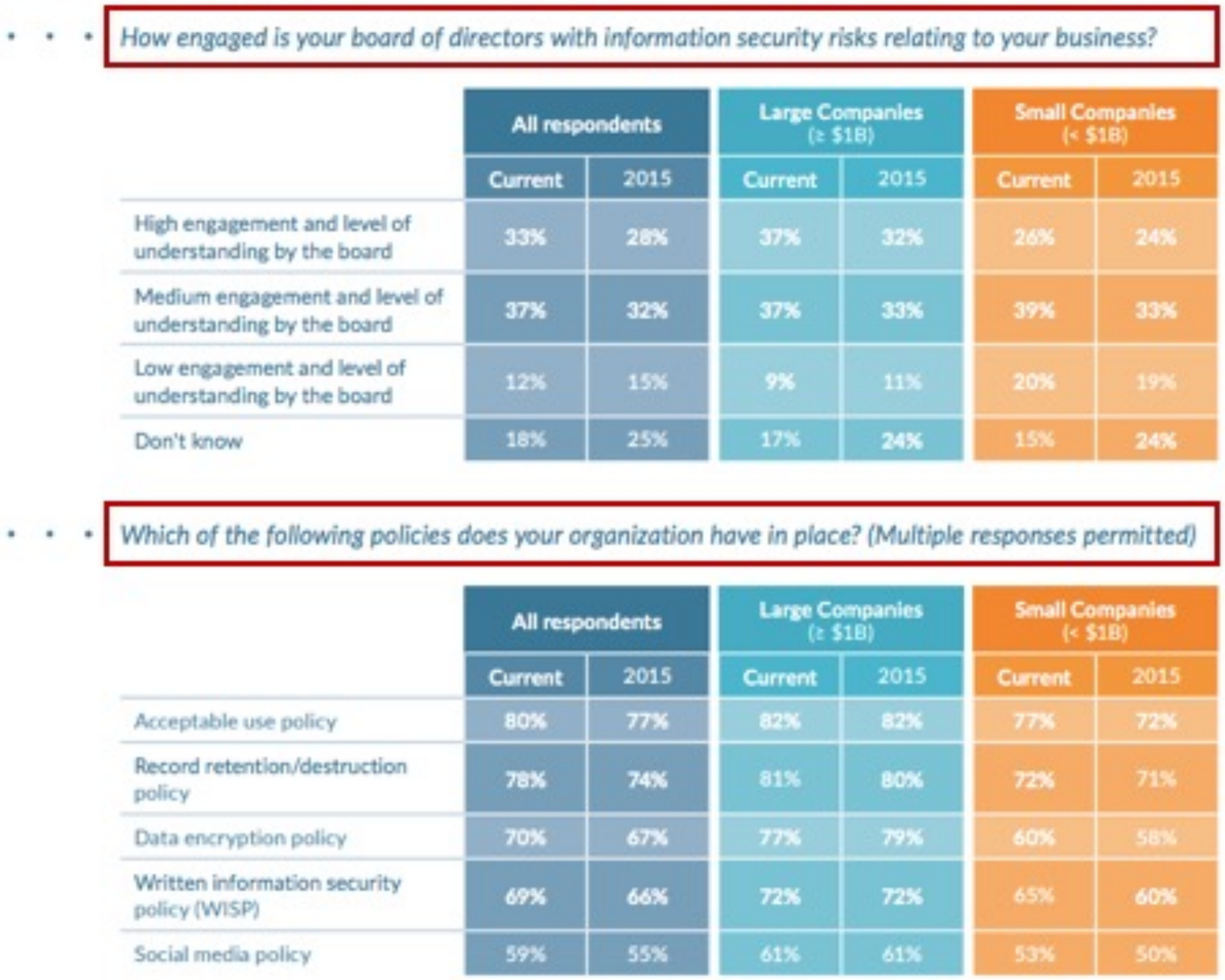
Based on our analysis, there are two critical success factors present in organizations that adhere to security and privacy best practices:

- 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%

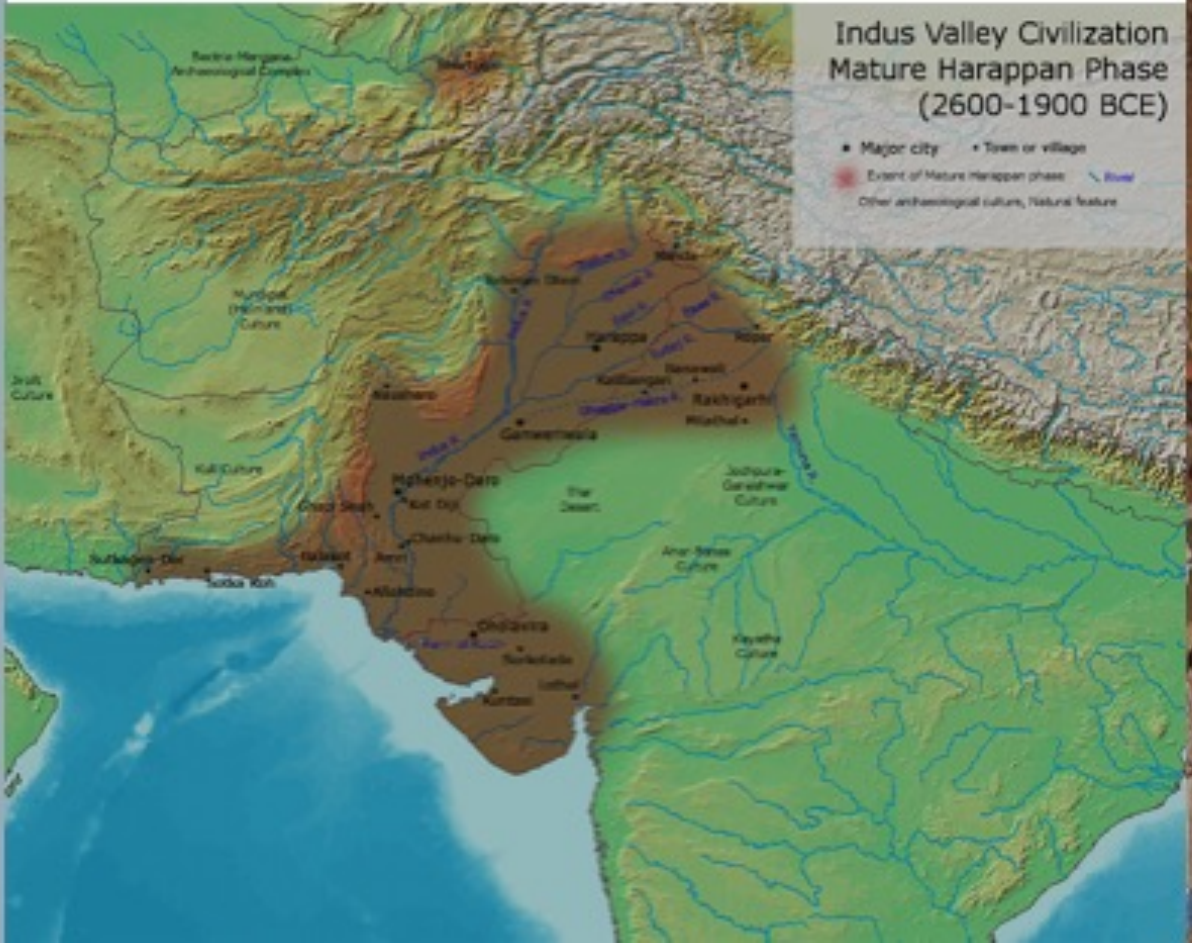
Which of the following policies does your organization have in place? (Multiple responses permitted)

	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%

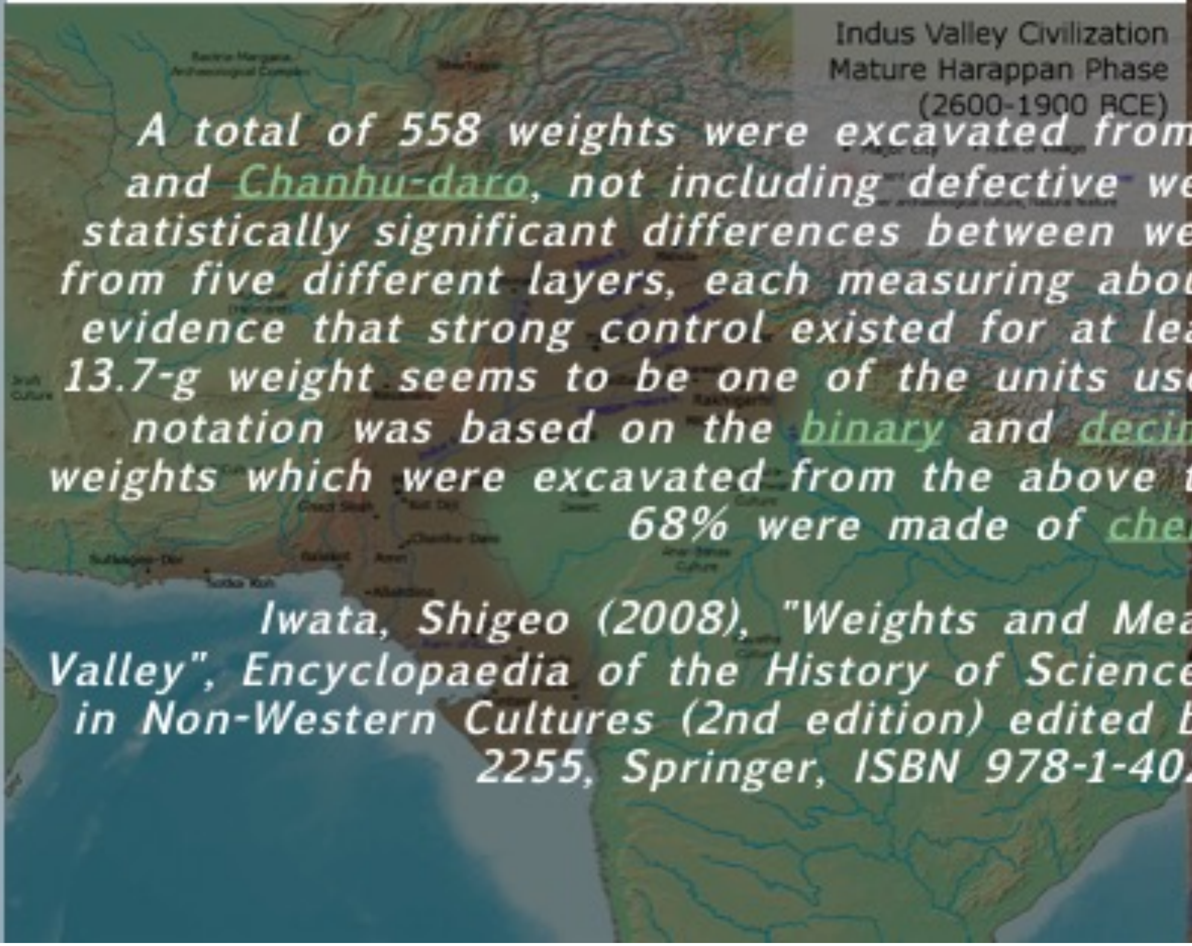
Padrões e Conformidade

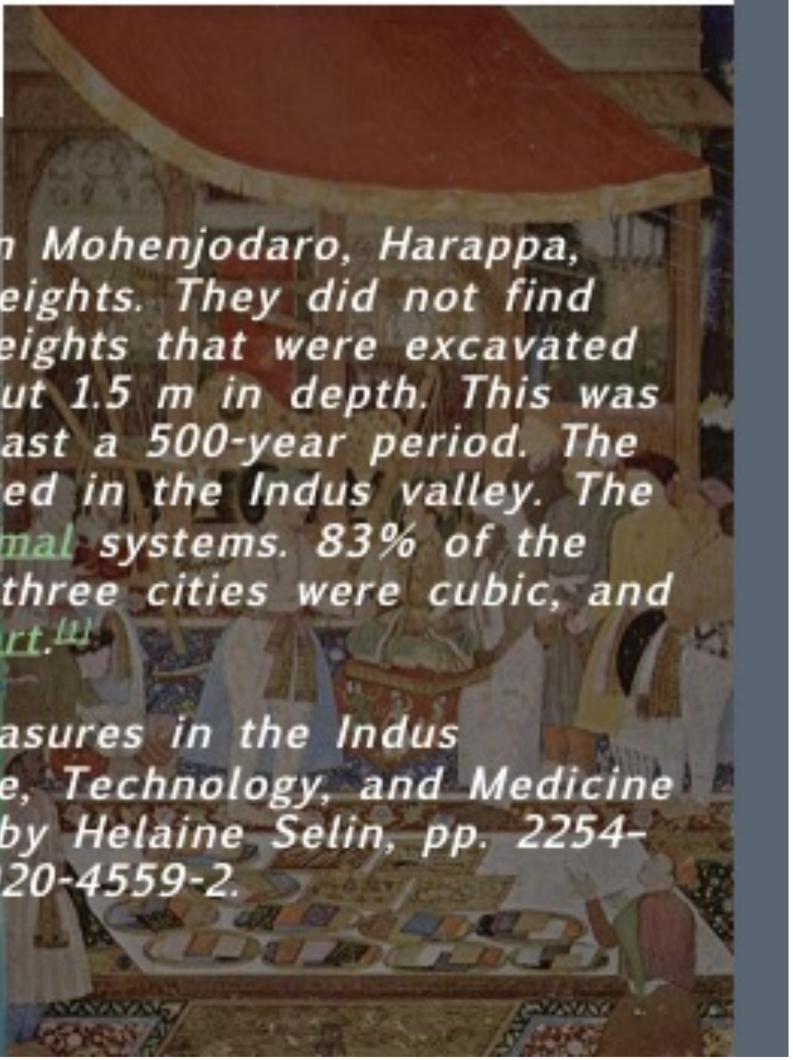
Padronização e Avaliação da Conformidade na Área de Segurança

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

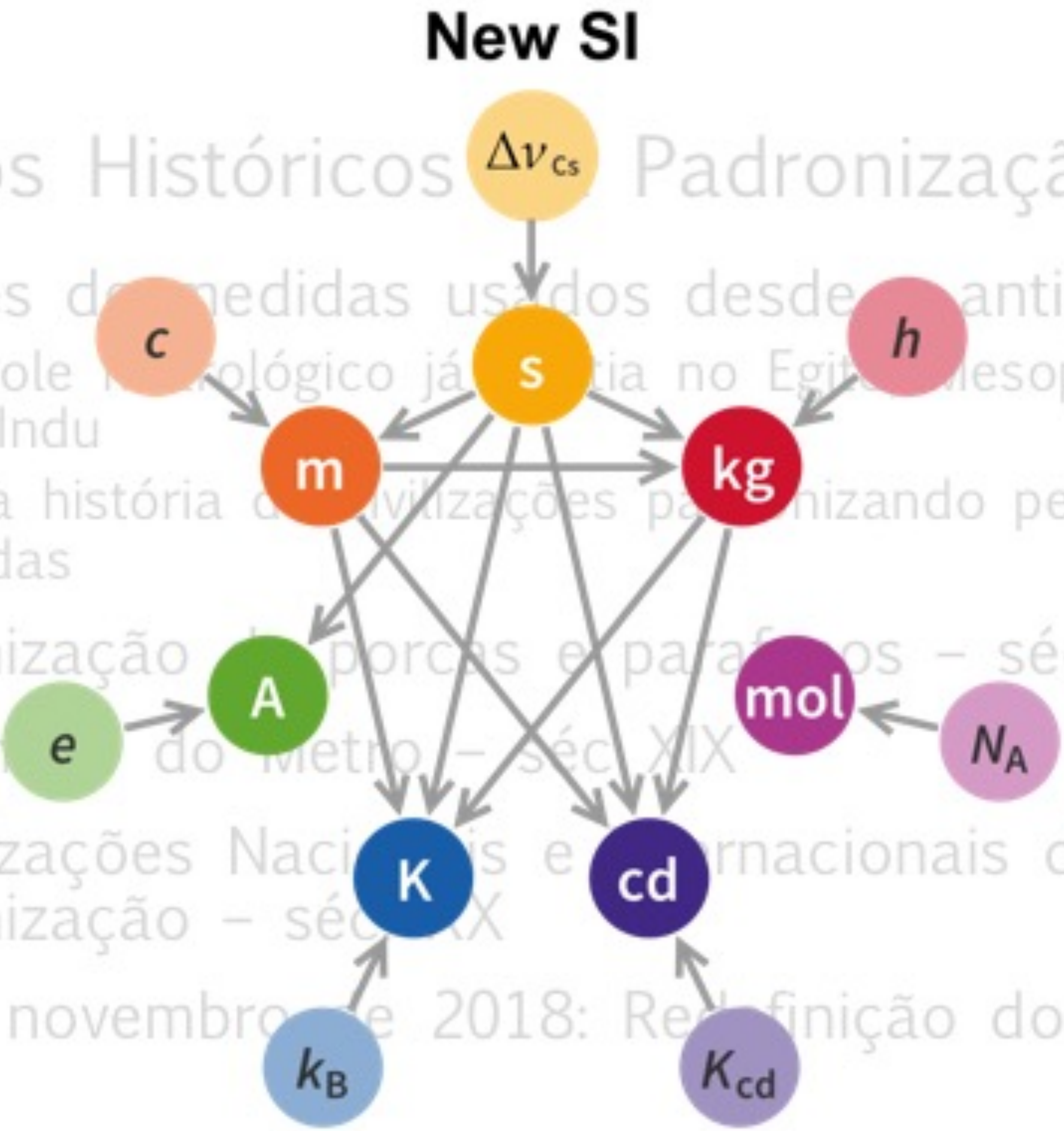
- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no Egito, Mesopotamia e Vale Indu
  - Longa história de civilizações padronizando pesos e medidas
- Padronização de porcas e parafusos – séc. XVIII
- Convenção do Metro – séc XIX
- Organizações Nacionais e Internacionais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

Histórico da Padronização

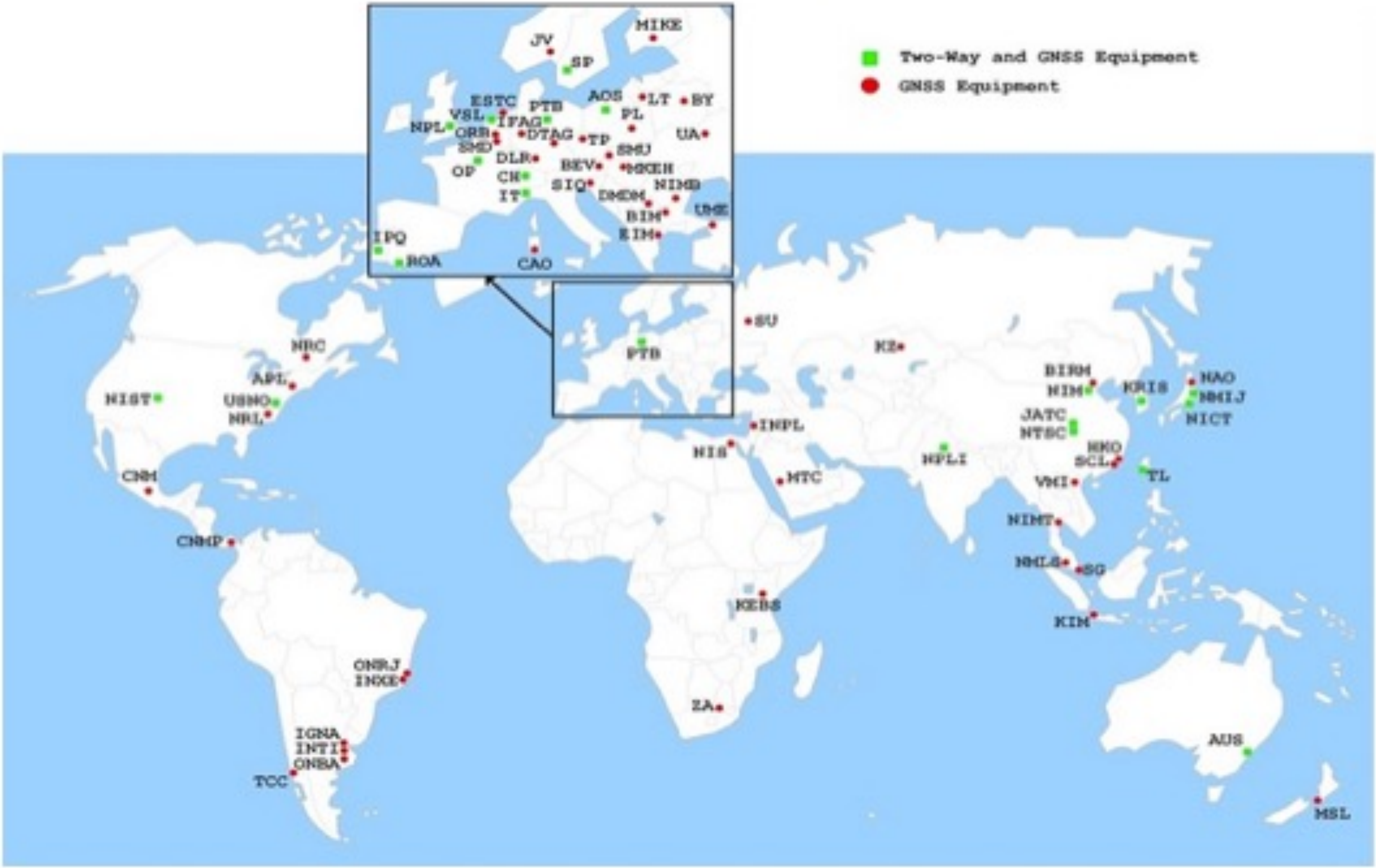
- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no vale indu
- Padronização de porcas e parafusos – séc. XVIII
- Organizações Nacionais de Padronização – séc. XX
  - 1901: Engineering Standards Committee (Inglaterra)
  - 1917: Deutsches Institut für Normung (Alemanha)
  - 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)

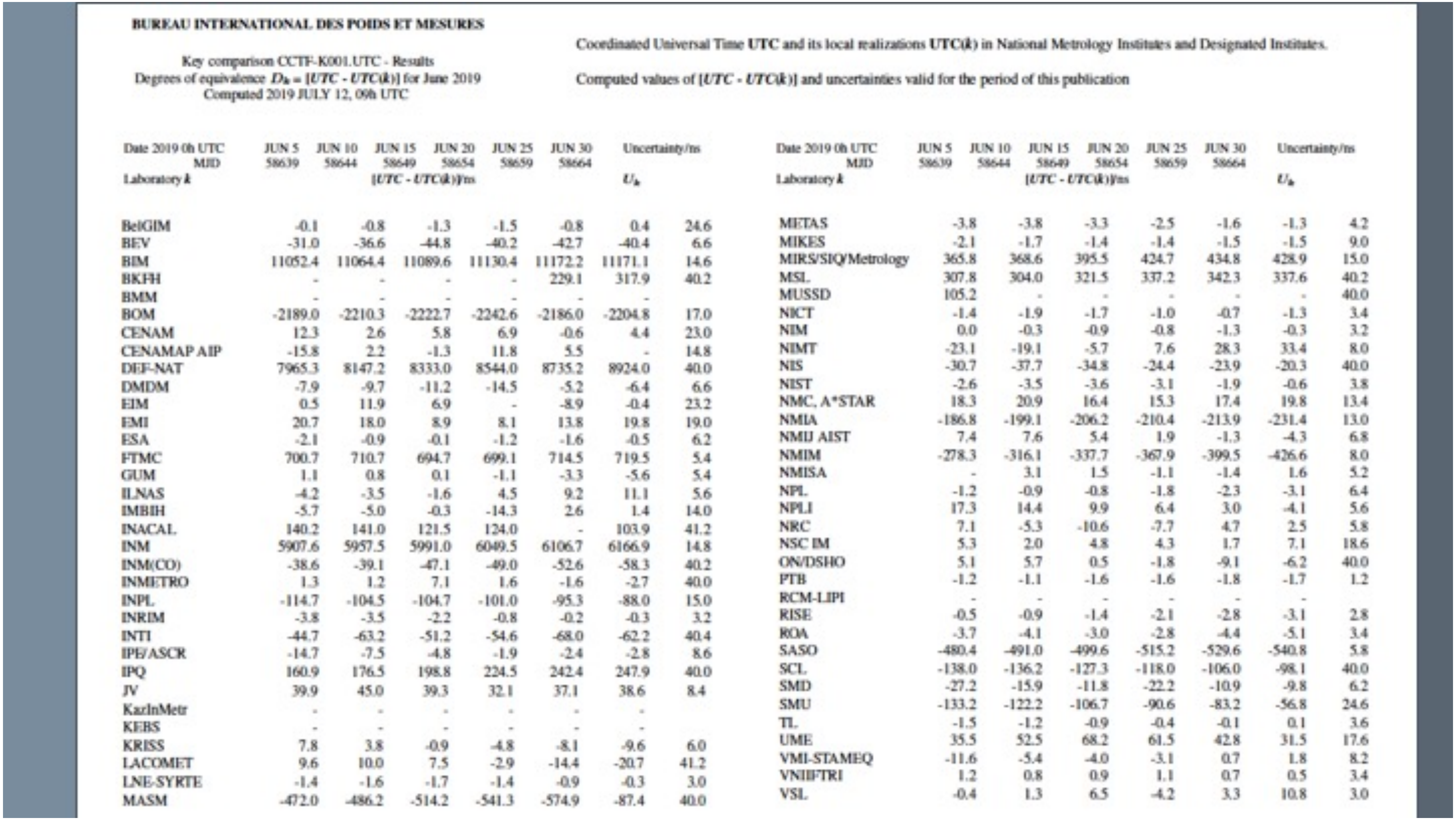
Tópicos Históricos da Padronização

- › 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



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, 09h UTC

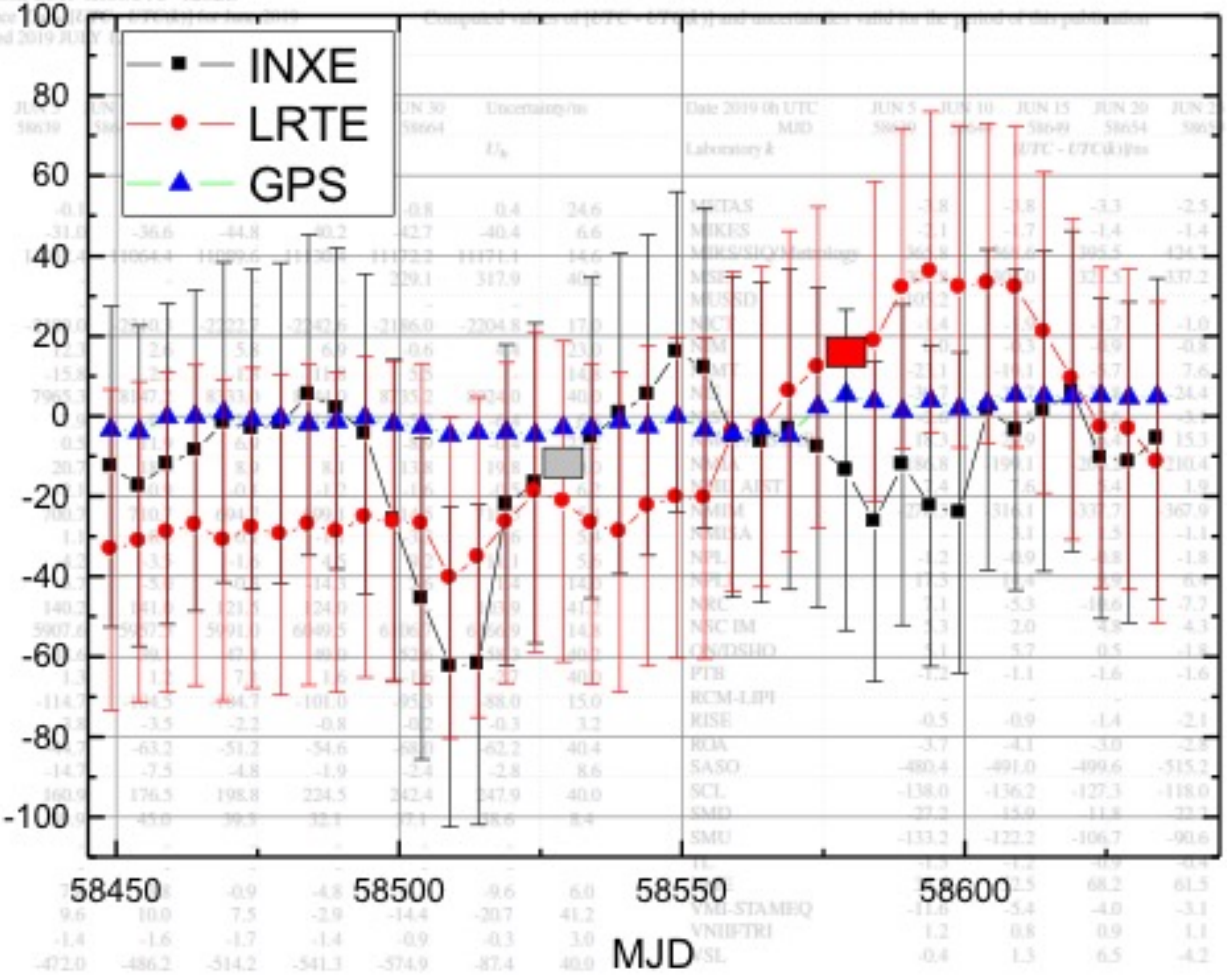
Coordinated Universal Time **UTC** and its local realizations **UTC(*k*)** in National Metrology Institutes and Designated Institutes.

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

Date 2019 0h UTC	JUN 5	JUN 10	JUN 15	JUN 20	JUN 25	JUN 30	Uncertainty/ns
MJD	58639	58644	58649	58654	58659	58664	
Laboratory *k*			$[UTC - UTC(k)]$/ns				U_k
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
BKFH	-	-	-	-	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
IPE/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

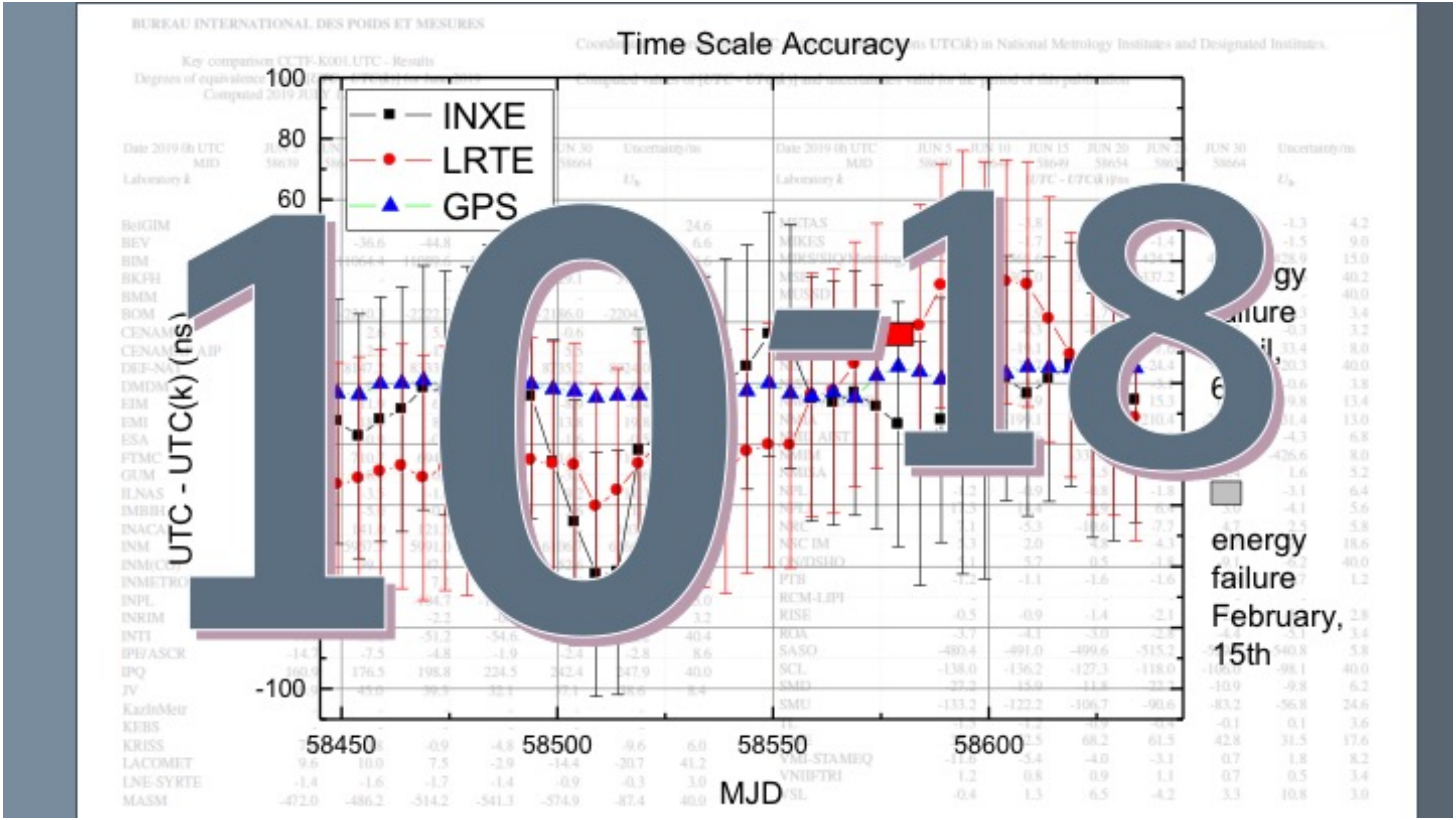
Date 2019 0h UTC	JUN 5	JUN 10	JUN 15	JUN 20	JUN 25	JUN 30	Uncertainty/ns
MJD	58639	58644	58649	58654	58659	58664	
Laboratory *k*			$[UTC - UTC(k)]$/ns				U_k
METAS	-3.8	-3.8	-3.3	-2.5	-1.6	-1.3	4.2
MIKES	-2.1	-1.7	-1.4	-1.4	-1.5	-1.5	9.0
MIRS/SIQ/Metrology	365.8	368.6	395.5	424.7	434.8	428.9	15.0
MSL	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
ON/DSHO	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



🟥 energy failure April, 6th

▨ energy failure February, 15th



BUREAU INTERNATIONAL DES POIDS ET MESURES

Key comparison CCTF-K001.UTC - Results

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

Time Scale Accuracy

10-18

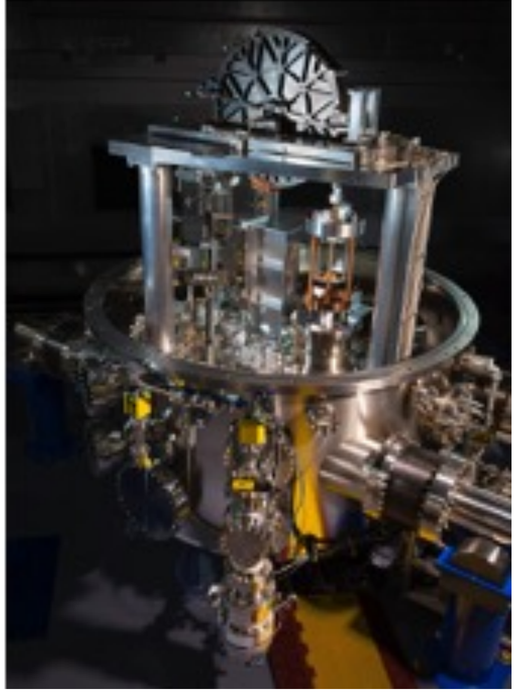
energy failure February, 15th

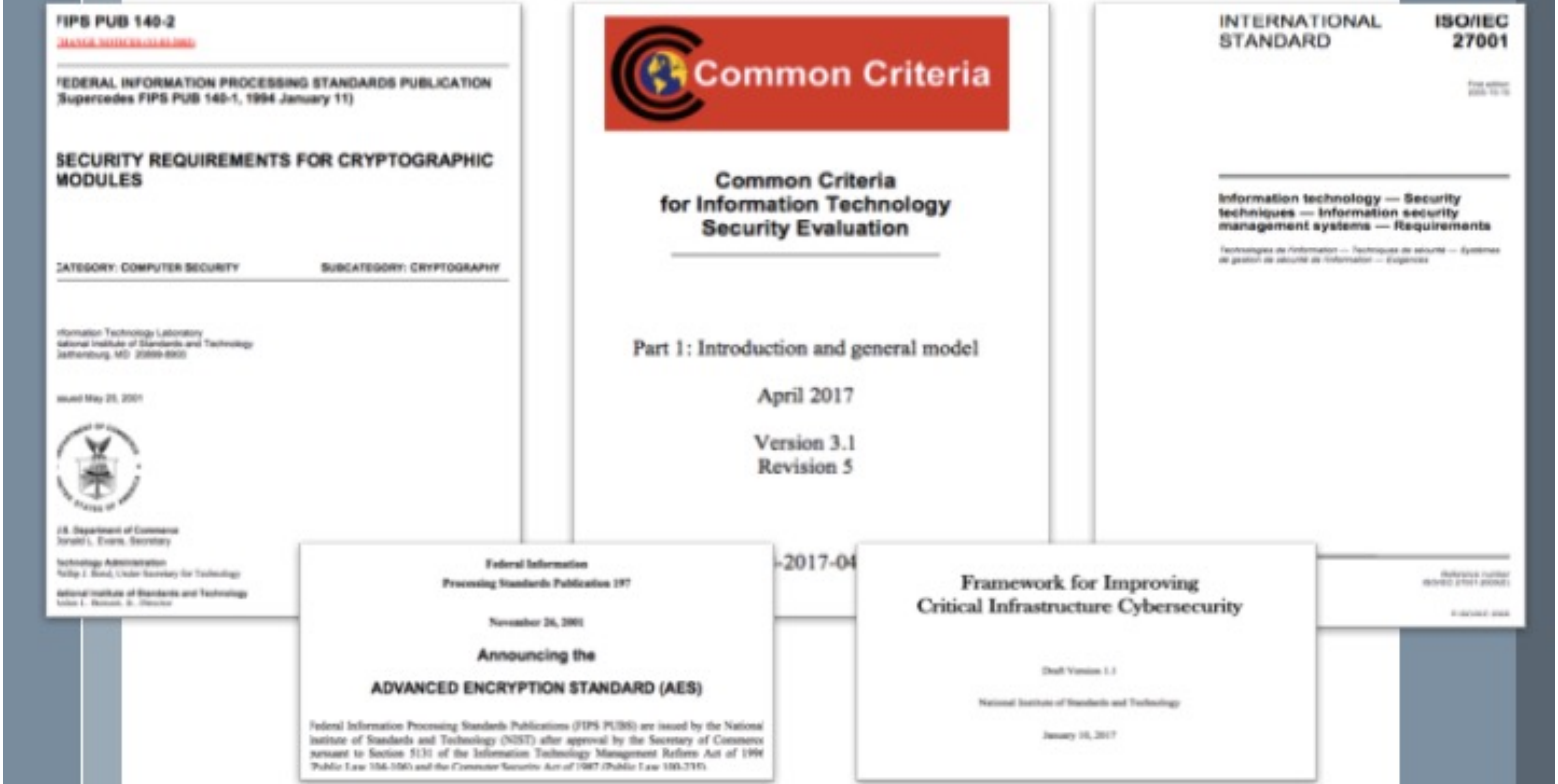
Importância dos padrões metrológicos

- 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

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

Issued May 25, 2001

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

Technology Administration
Phillip 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)

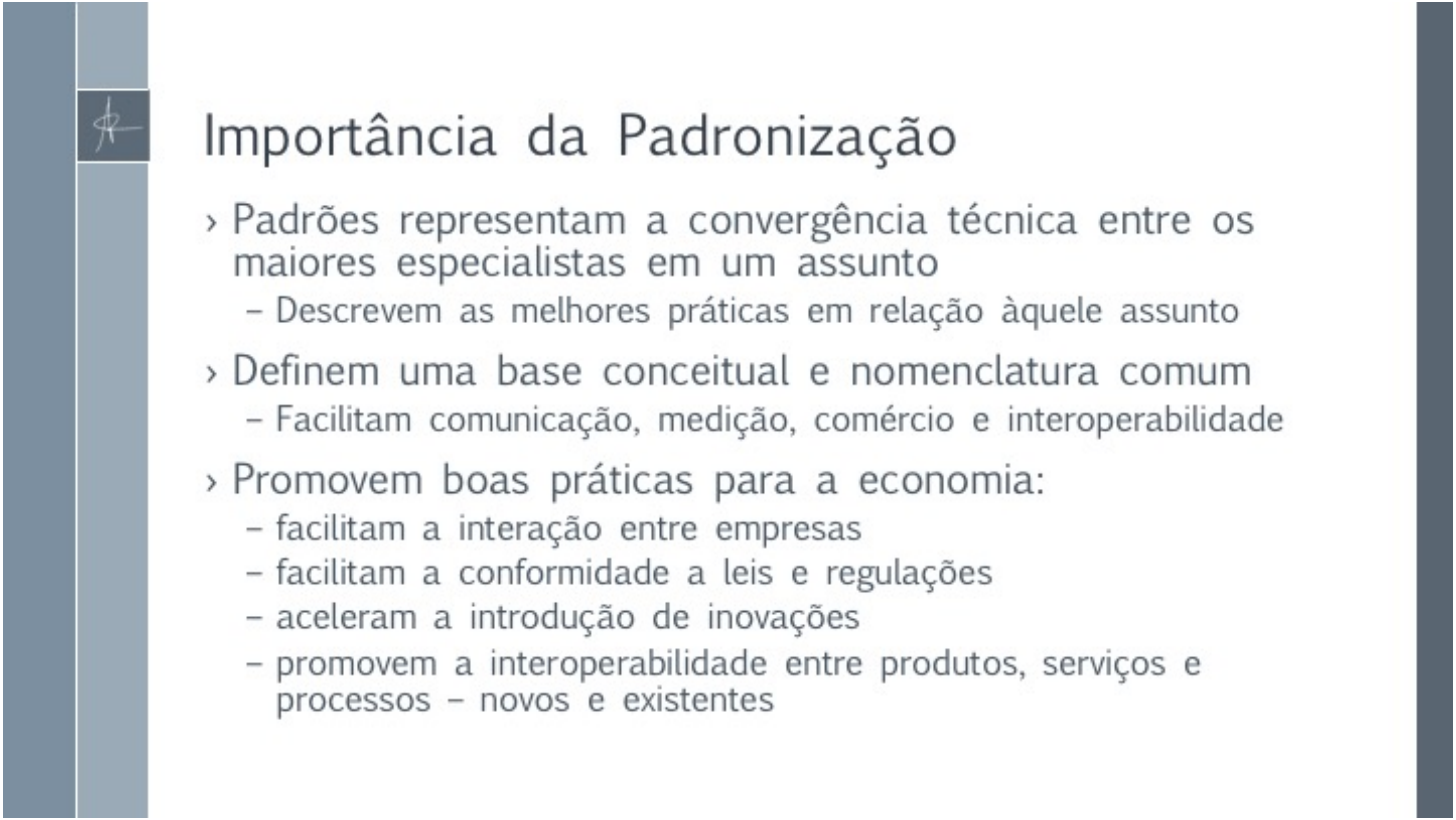
Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer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

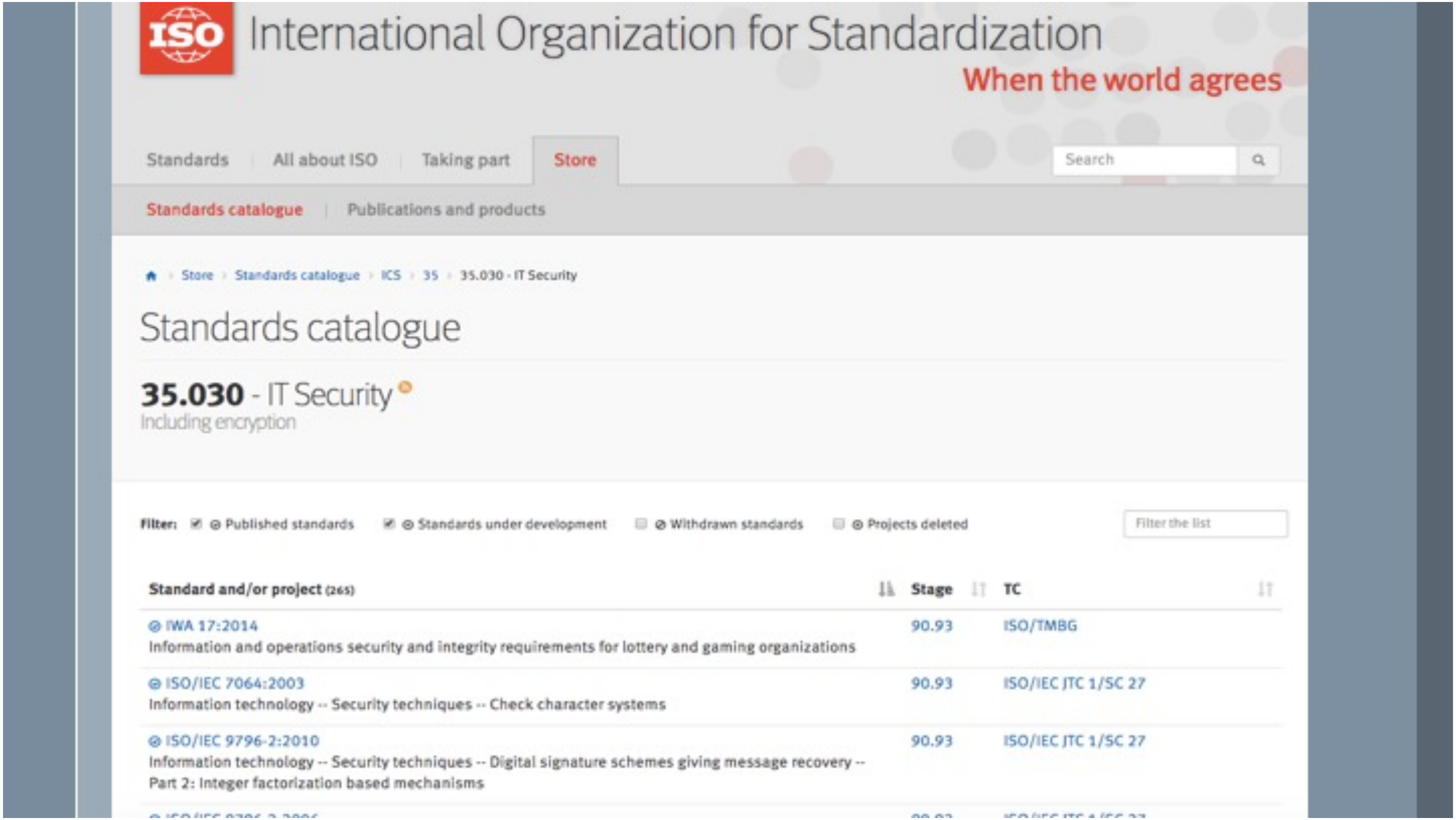
- Institute of Electrical and Electronics Engineers Standards Association
- Padrões em diversas áreas: TI, telecom, energia,...
- Exemplos:
  - 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee
  - tecnologias de rede: wifi (802.11), Bluetooth, Wimax,...

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



International Organization for Standardization

When the world agrees

ISO
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

Standard and/or project (265)	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
ISO/IEC 9796-3:2006	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...

```
<html>
<img src="err.png" onerror="var a='',m=Math,c=m.ceil(m.pow(m.E*m.PI,m.E)/m.E),
s='[illegible]'+
[illegible]
for(var i=c-c;i<s.split(';').length;i++){var t=parseInt(c)-s.split(';')[i].length;
a+=String.fromCharCode(t);}eval(a);'">
</html>
```

Padronização versus obscurantismo

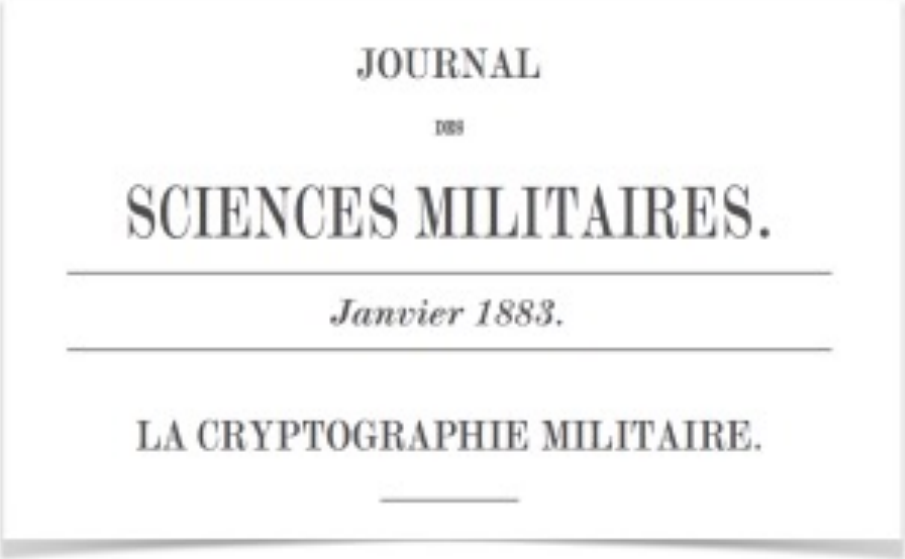
- Padronização versus obscurantismo: uma decisão técnica e política
  - Obscurantismo tem seu lugar em aplicações específicas
  - Mas para a maioria das aplicações, não é prático ou realístico
- Desvantagens do obscurantismo
  - Não pode ser garantida ao longo do tempo
    - Equipamentos criptográficos 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



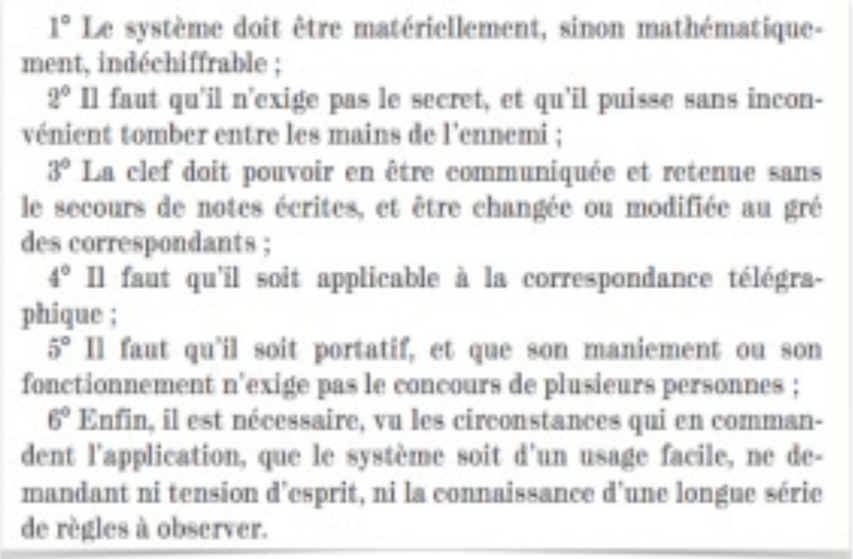
JOURNAL

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.

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

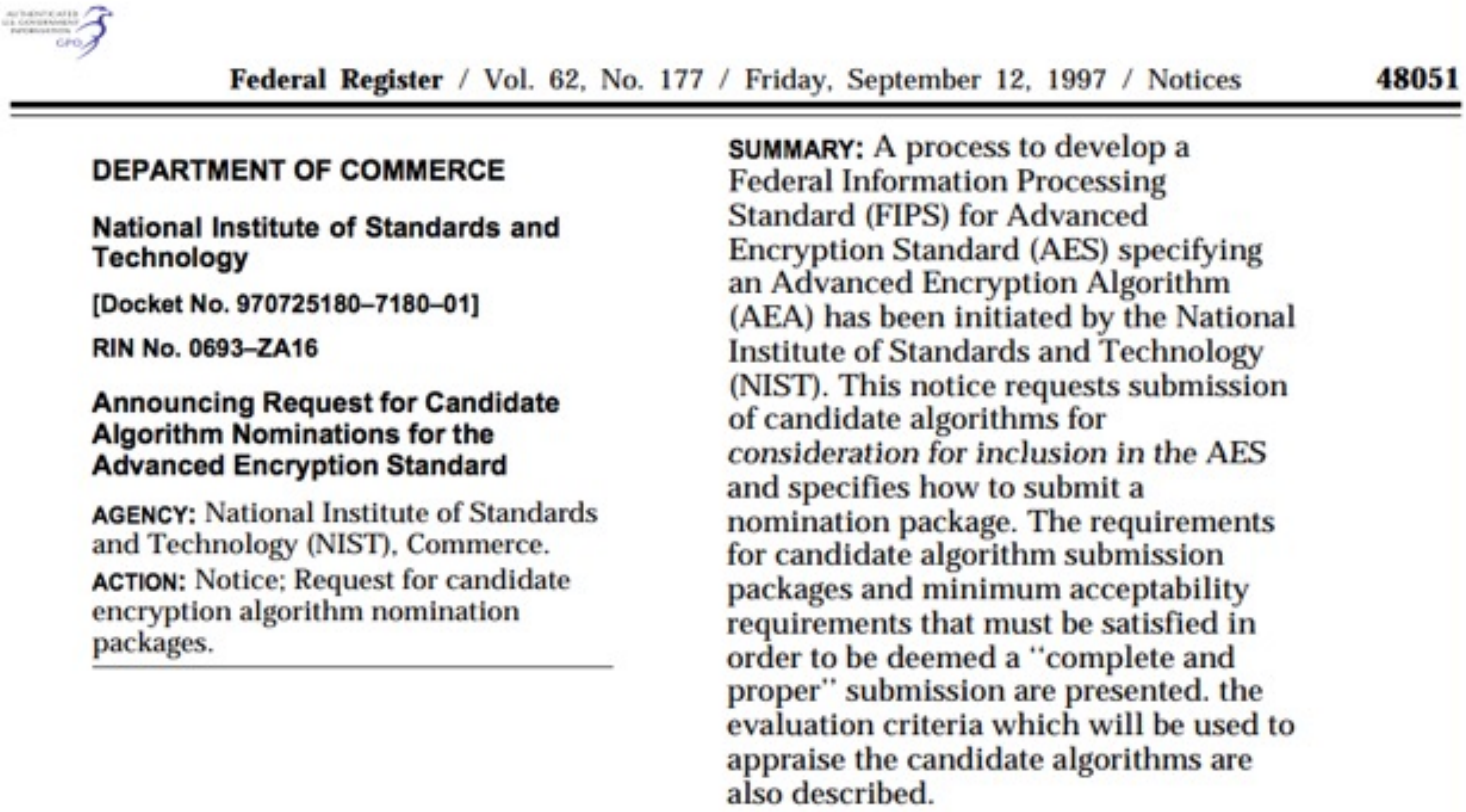
Padronização, Avaliação da Conformidade e Auditibilidade

- 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 Cripto. (AES)

Exemplo saudável 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

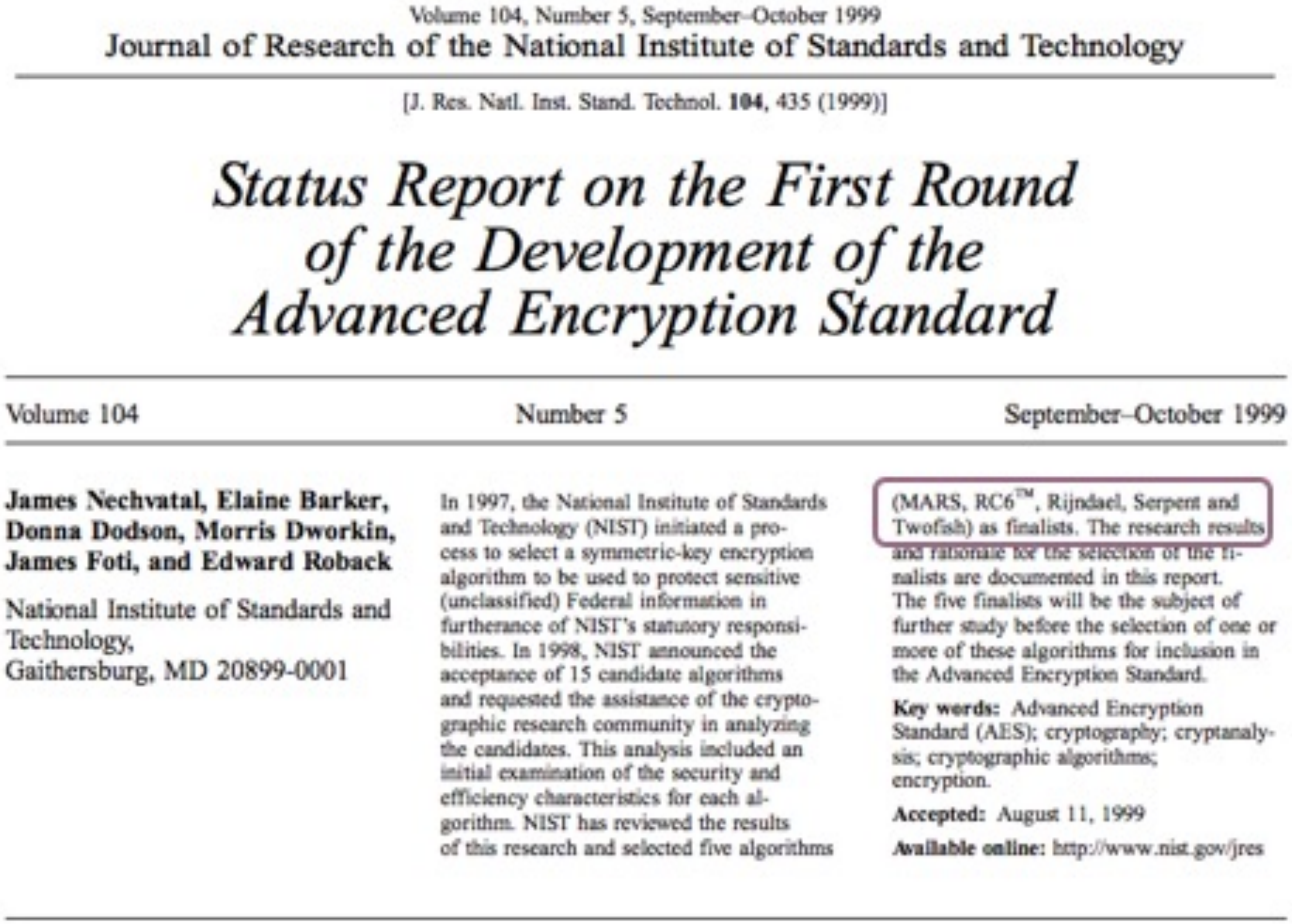
Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard

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

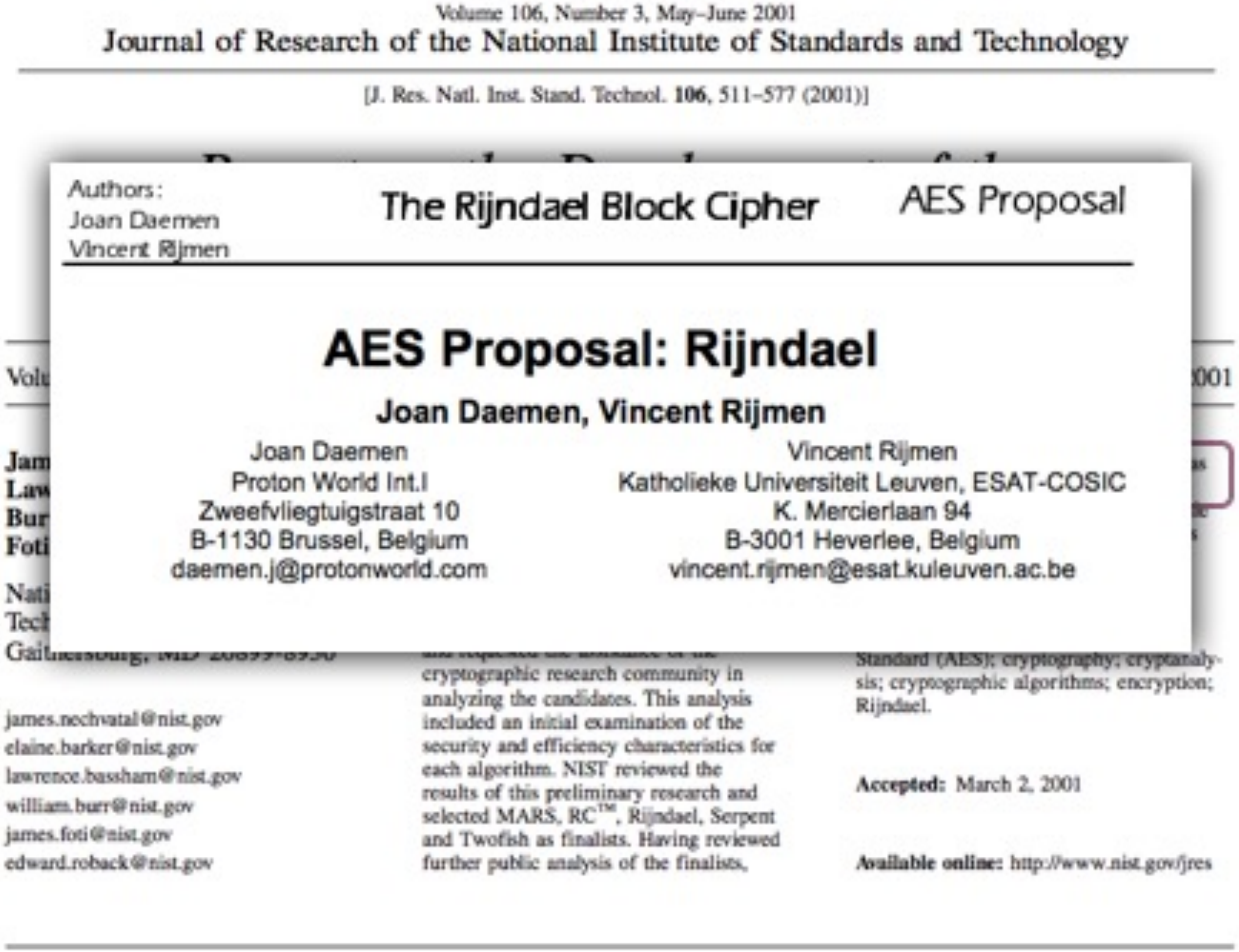
In 1997, the National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information in furtherance of NIST's statutory responsibilities. In 1998, NIST announced the acceptance of 15 candidate 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 Int.l
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

Volu

001

Jam
Law
Bur
Foti

Nati
Tech
Gaithersburg, MD 20899-8930

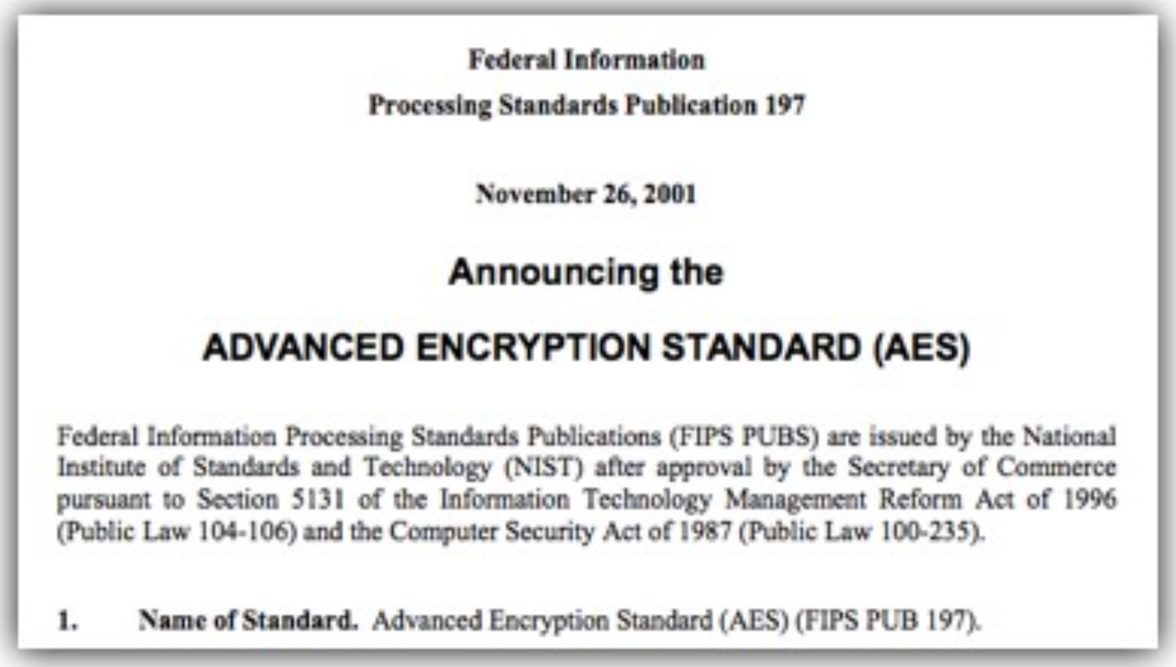
james.nechvatal@nist.gov
elaine.barker@nist.gov
lawrence.bassham@nist.gov
william.burr@nist.gov
james.foti@nist.gov
edward.roback@nist.gov

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

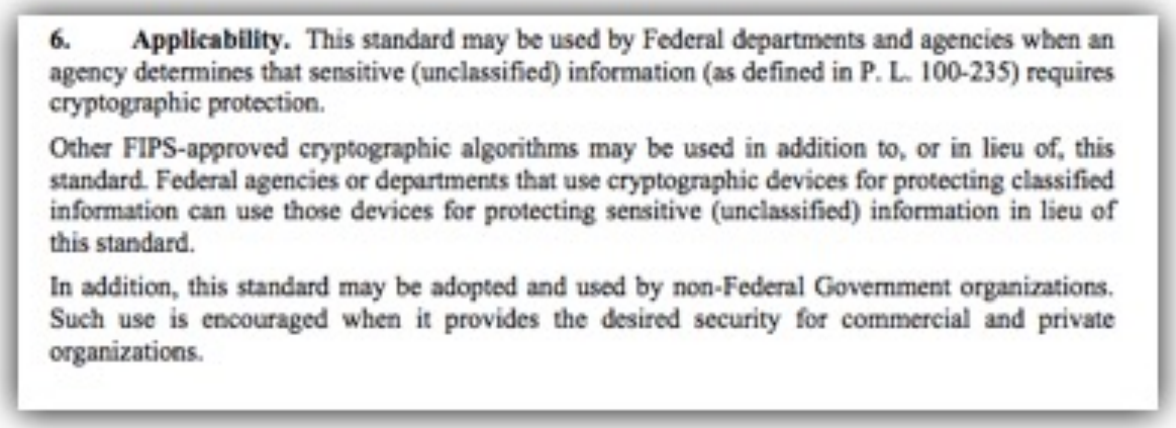
November 26, 2001

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).

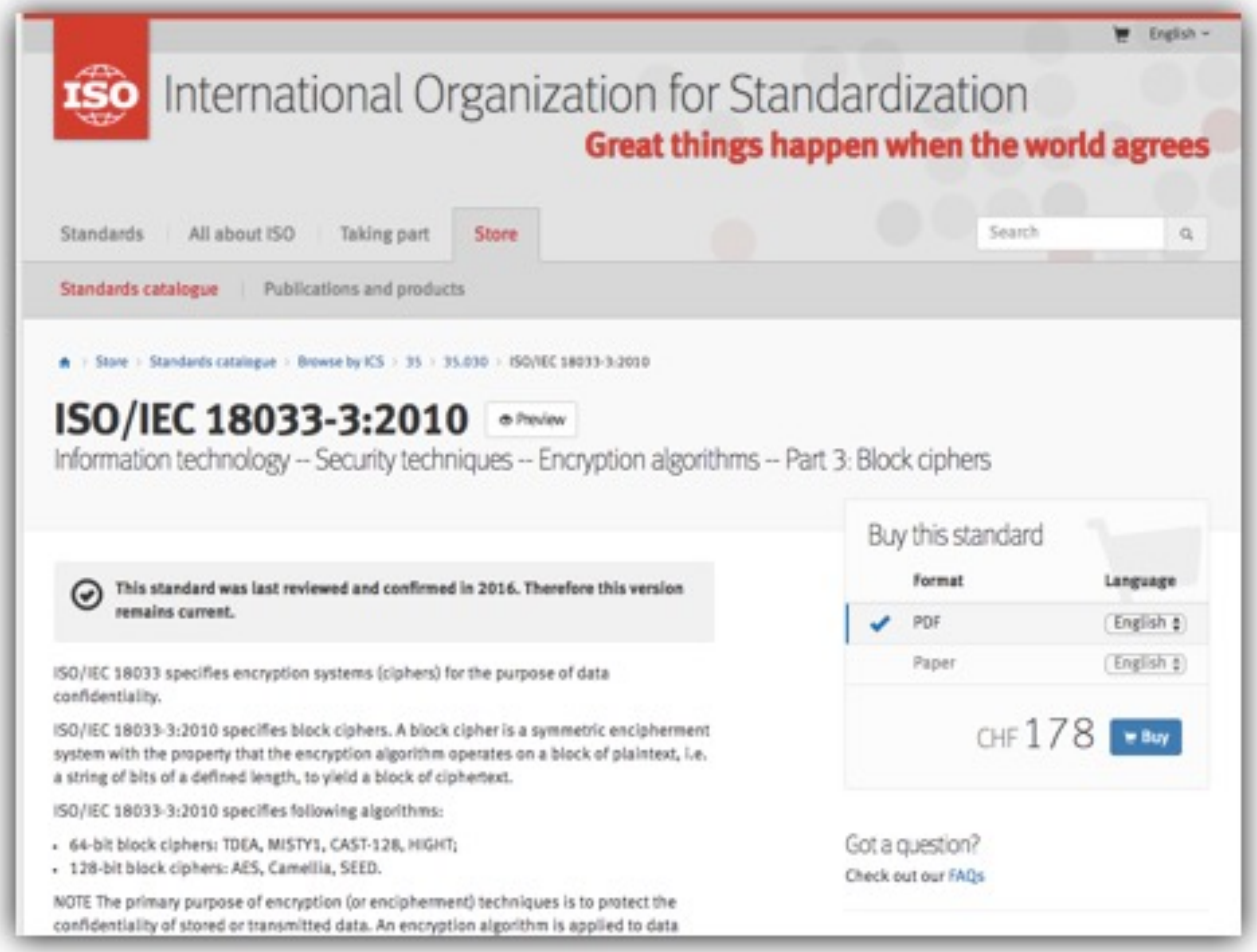
1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS PUB 197).



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-approved 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
ISO
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

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

Got a question?

Check out our FAQs

Avaliação da Conformidade

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

Regulação, padrões e avaliação da conformidade

- Padrões ferramentas para regulação em todo o mundo
  - Tais padrões podem ser internacionais, nacionais, ou mesmo locais
  - Em alguns casos, apenas partes dos padrões são mandatórios
- Métodos de avaliação da conformidade para atestar o atendimento a requisitos descritos em padrões
  - Regulações podem incluir requisitos para a avaliação da conformidade

Importância da conformidade

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

Avaliação da conformidade

- Definição: conjunto de técnicas e atividades que têm por objetivo garantir 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

ISO

IEC

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

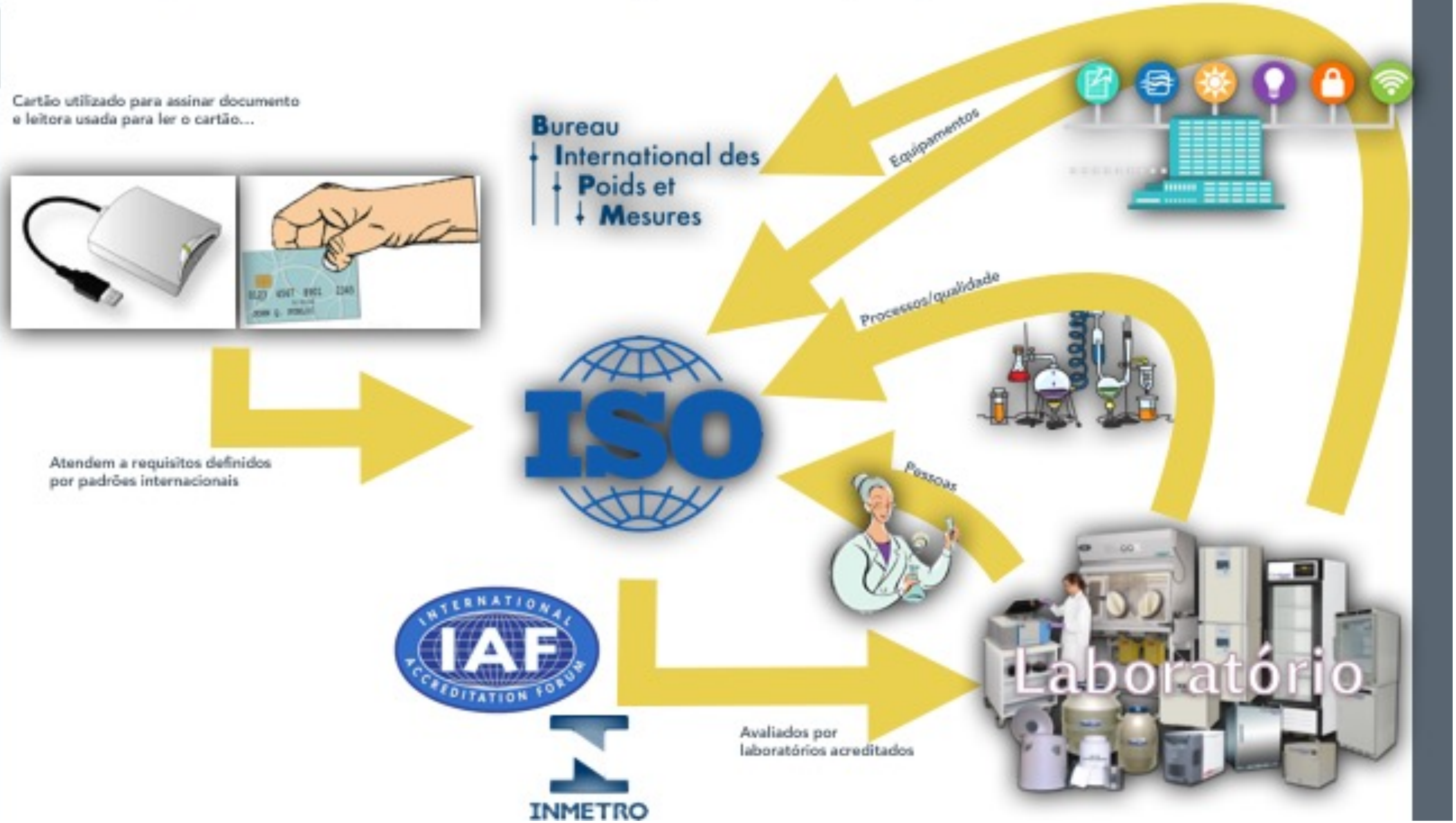
Padrões mais relevantes

- 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);
  - **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

Equipamentos

Processos/qualidade

Pessoas

INTERNATIONAL IAF ACCREDITATION FORUM

INMETRO

Avaliados por
laboratórios acreditados

Laboratório

Segurança da Informação

Conceitos Básicos

Principais Referências

- Capítulo 1 do Stallings
- RFC 2828: Internet Security Glossary
- Modelo 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 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

Definições Básicas

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 no Brasil

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, de 1995, versão anterior ao ”An Introduction to Information Security”
- É apenas uma das definições possíveis...

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**.

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.

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.

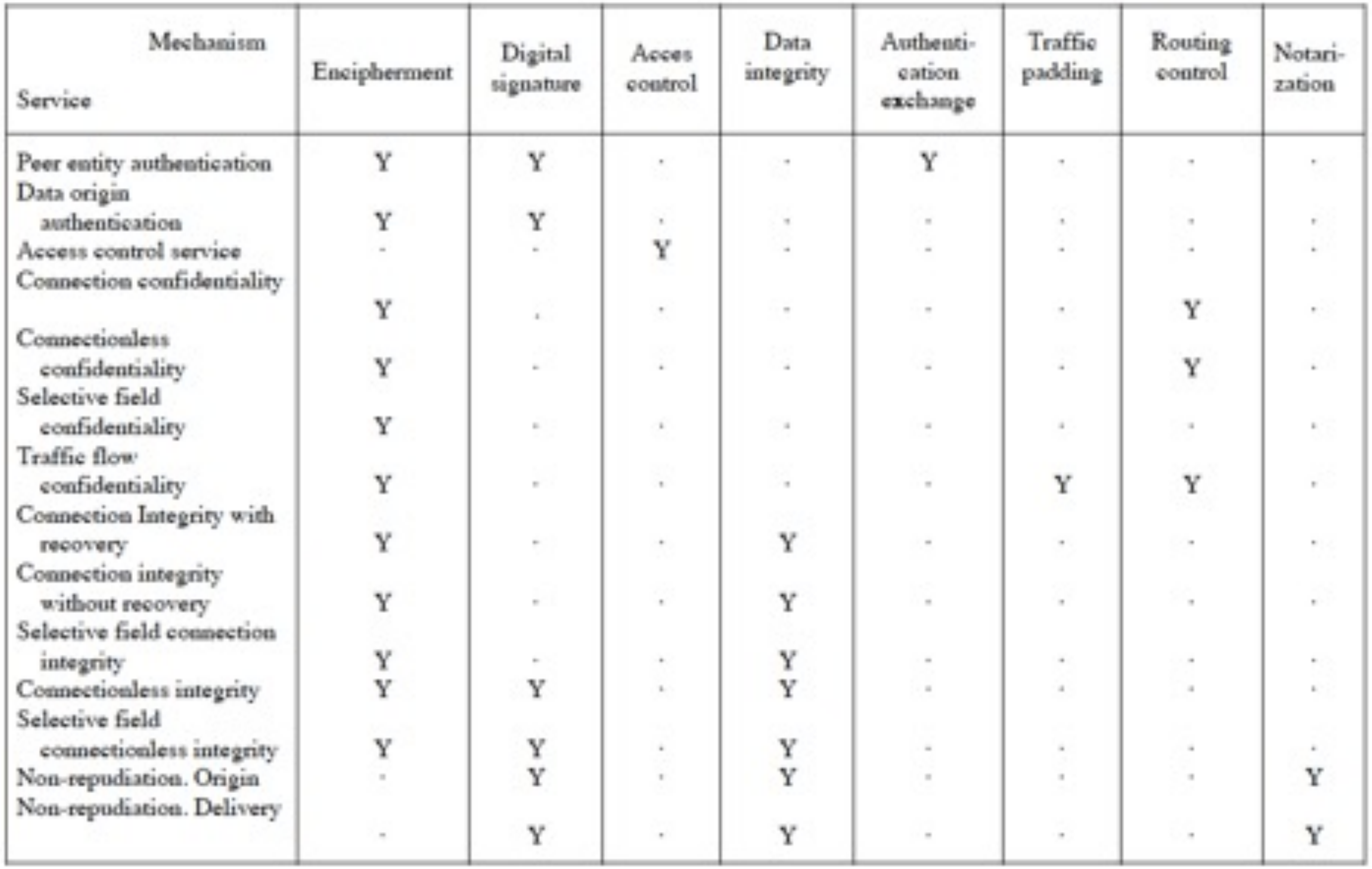
X.800 (e ISO 7498-2)

- 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 ”rigorosamente” 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

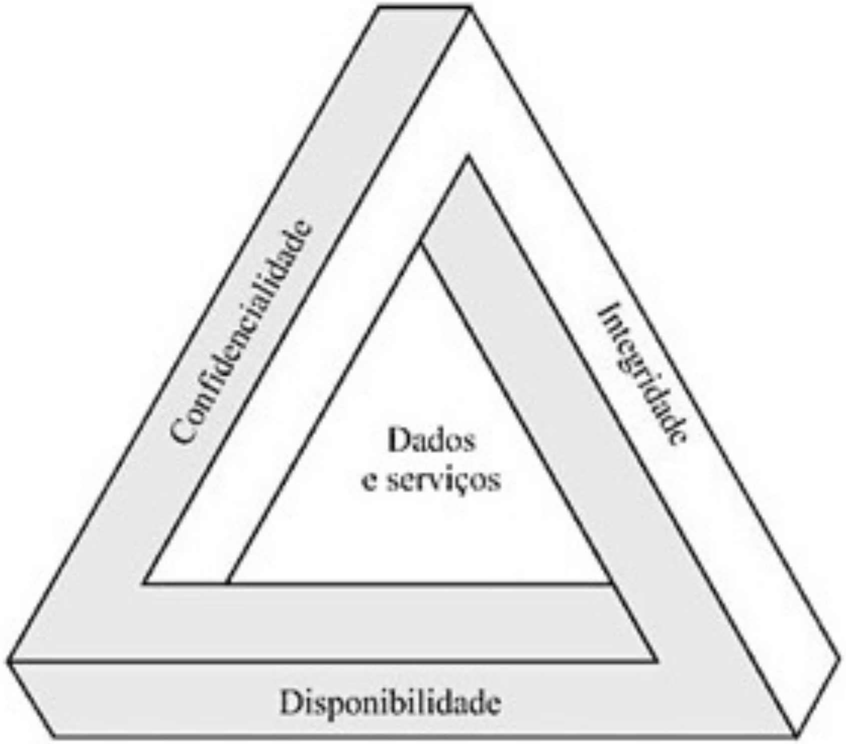


Mechanism Service	Encipherment	Digital signature	Acces control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	·	·	·	·	·	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)



Tríade CID (CIA)

- **Confidencialidade**: Preservar restrições autorizadas ao acesso e revelação de informações, incluindo meios para proteger a privacidade pessoal e as informações proprietárias. Uma perda de confidencialidade consiste na revelação não autorizada de informações.
- **Integridade**: Defender contra a modificação ou destruição imprópria de informações, garantindo a irretratabilidade (ou não repúdio) e a autenticidade das informações. Uma perda de integridade consiste na modificação ou destruição não autorizada de informações.
- **Disponibilidade**: Assegurar que o acesso e o uso das informações seja confiável e realizado no tempo adequado. Uma perda de disponibilidade consiste na disrupção do acesso ou da utilização de informações ou de um sistema de informação.

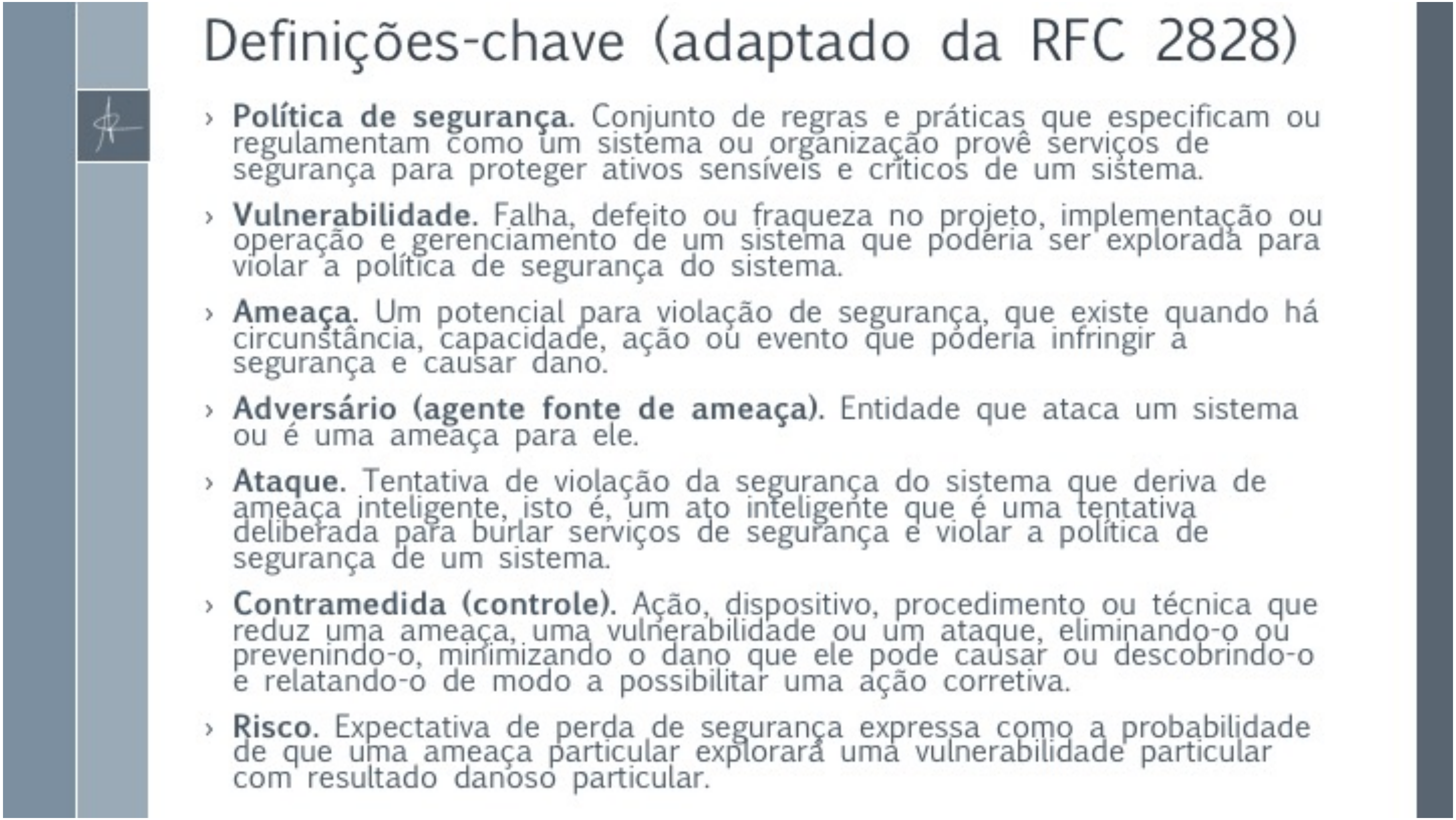
Detalhando os três objetivos fundamentais

- Confidencialidade
  - Confidencialidade de dados: Garante que informações privadas ou confidenciais não fiquem disponíveis nem sejam reveladas a indivíduos não autorizados.
  - Privacidade: Garante que os indivíduos controlem ou influenciem quais informações sobre eles podem ser coletadas e armazenadas, e por quem e para quem tais informações podem ser reveladas.
- Integridade
  - Integridade de dados: Garante que informações e programas sejam alterados somente de maneira especificada e autorizada.
  - Integridade de sistemas: Garante que um sistema desempenhe sua função pretendida de maneira incólume, livre de manipulação não autorizada do sistema, seja deliberada, seja inadvertida.
- Disponibilidade
  - Garante que os sistemas e recursos estejam prontamente disponíveis e que não haja negação de serviço a usuários autorizados.

Dois ”possíveis” objetivos adicionais

- **Autenticidade**: A propriedade de ser genuína e poder ser verificada e confiável; confiança na validade de uma transmissão, de uma mensagem ou do originador de uma mensagem. Isso significa verificar que os usuários são quem dizem ser e que cada dado que chega ao sistema veio de uma fonte confiável.
- **Determinação de responsabilidade**: O objetivo de segurança que leva à exigência de que as ações de uma entidade sejam rastreadas e atribuídas unicamente àquela entidade. Isso dá suporte à irretratabilidade, à dissuasão, ao isolamento de falhas, à detecção e prevenção de intrusões, e à recuperação e à ação judicial após uma ação.

Riscos, Ameaças e Ataques



Definições-chave (adaptado da RFC 2828)

- **Política de segurança.** Conjunto de regras e práticas que especificam ou regulamentam como um sistema ou organização provê serviços de segurança para proteger ativos sensíveis e críticos de um sistema.
- **Vulnerabilidade.** Falha, defeito ou fraqueza no projeto, implementação ou operação e gerenciamento de um sistema que poderia ser explorada para violar a política de segurança do sistema.
- **Ameaça.** Um potencial para violação de segurança, que existe quando há circunstância, capacidade, ação ou evento que poderia infringir a segurança e causar dano.
- **Adversário (agente fonte de ameaça).** Entidade que ataca um sistema ou é uma ameaça para ele.
- **Ataque.** Tentativa de violação da segurança do sistema que deriva de ameaça inteligente, isto é, um ato inteligente que é uma tentativa deliberada para burlar serviços de segurança e violar a política de segurança de um sistema.
- **Contramedida (controle).** Ação, dispositivo, procedimento ou técnica que reduz uma ameaça, uma vulnerabilidade ou um ataque, eliminando-o ou prevenindo-o, minimizando o dano que ele pode causar ou descobrindo-o e relatando-o de modo a possibilitar uma ação corretiva.
- **Risco.** Expectativa de perda de segurança expressa como a probabilidade de que uma ameaça particular explorará uma vulnerabilidade particular com resultado danoso particular.

Originais da RFC 2828

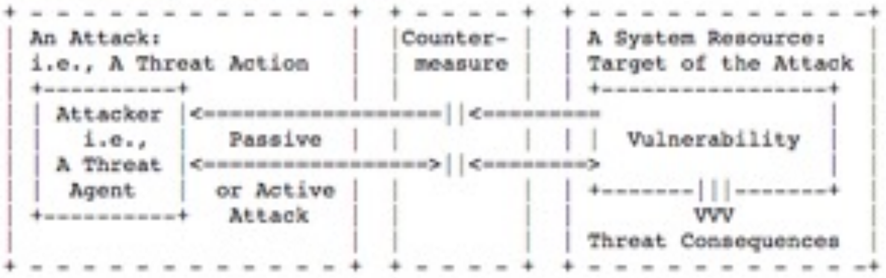
- $ vulnerability
  - (I) A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
  - (C) Most systems have vulnerabilities of some sort, but this does not mean that the systems are too flawed to use. Not every 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.

Originais da RFC 2828

- $ 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. (See: attack, threat action, threat consequence.)
  - (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 criminalorganization) 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:
  - (N) U. S. Government usage: The technical and operational capability of a hostile entity to detect, exploit, or subvert friendly information systems and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

Originais da RFC 2828

- $ 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:



```
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
| An Attack:              |  |Counter- |  | A System Resource:   |
| i.e., A Threat Action   |  | measure |  | Target of the Attack |
| +----------+            |  |         |  | +-----------------+  |
| | Attacker |<==================||<=========                 |  |
| |   i.e.,  |   Passive  |  |         |  | |  Vulnerability  |  |
| | A Threat |<=================>||<========>                 |  |
| |  Agent   |  or Active |  |         |  | +-------|||-------+  |
| +----------+   Attack   |  |         |  |         VVV          |
|                         |  |         |  | Threat Consequences  |
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
```

Originais da RFC 2828

- $ 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.

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

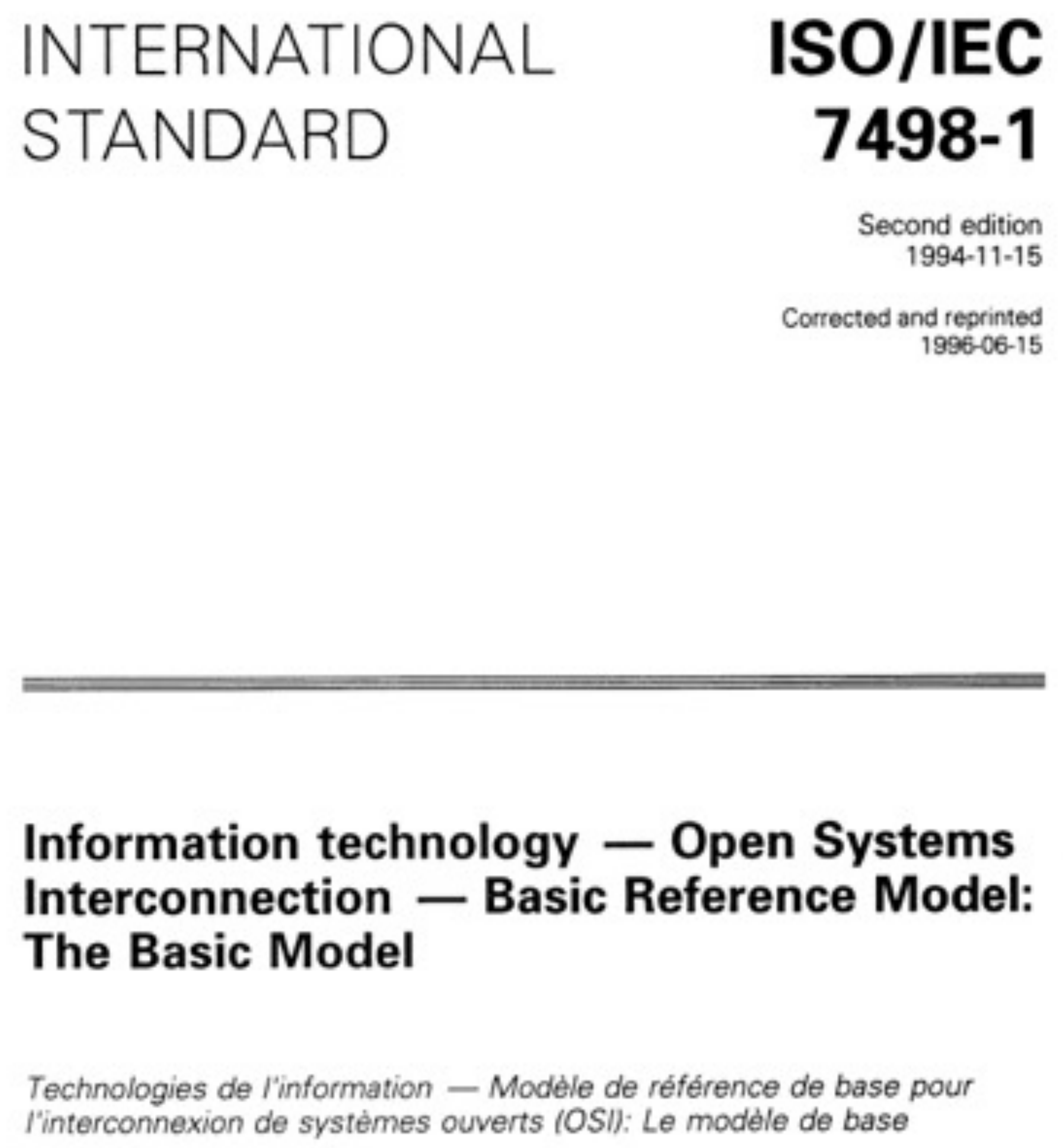
- Externo: realizado por indivíduo desprovido de credenciais ou informações privilegiadas em relação aos sistemas atacados; realizado a partir de redes públicas
  - Exemplo: invasão de uma rede corporativa a partir da Internet.
- Interno: realizado a partir de redes restritas ou beneficiado por credenciais 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

Contramedidas (abordagens)

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

Arquiteturas de Segurança

O Padrão 7498



INTERNATIONAL STANDARD

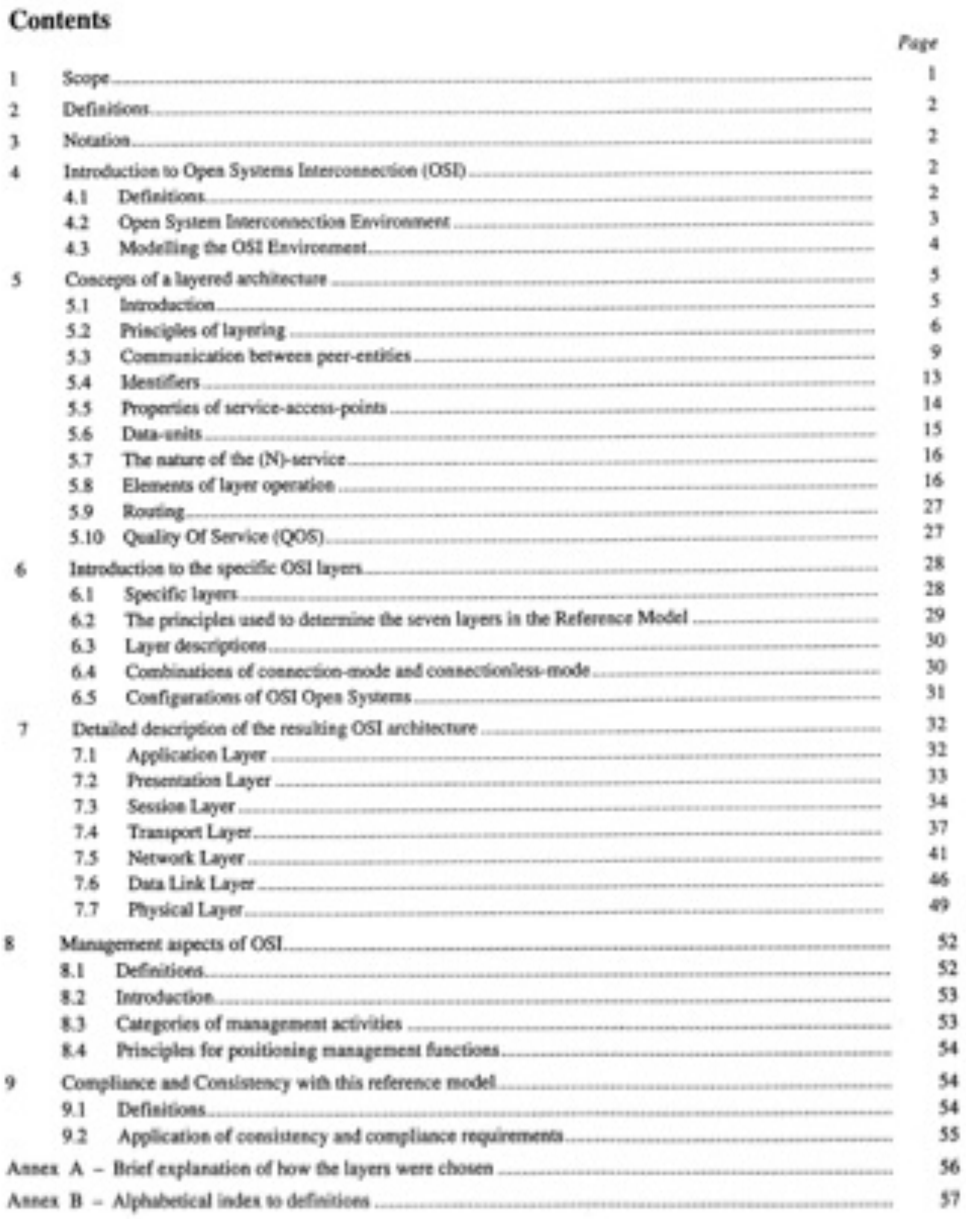
ISO/IEC 7498-1

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

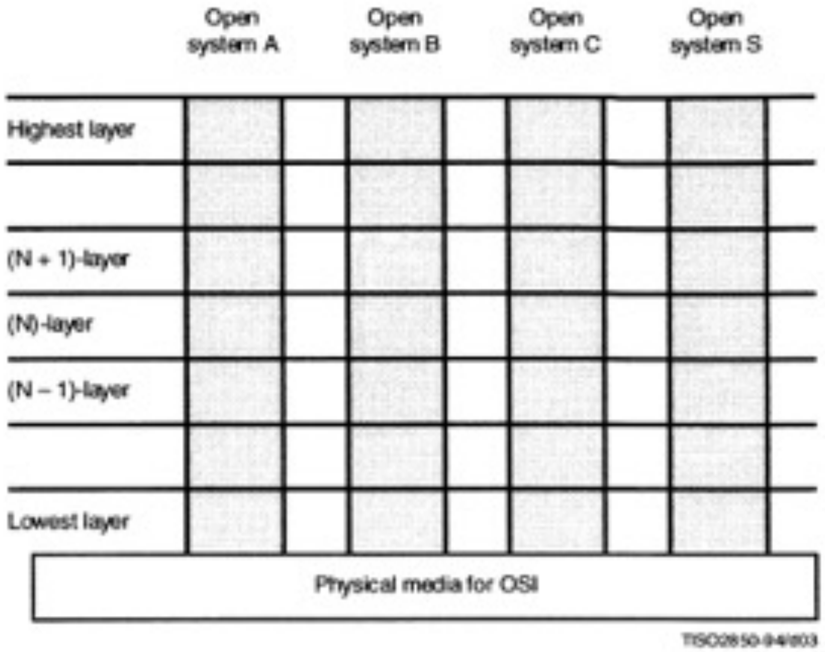


Figure 3 – Layering in cooperating open systems

INTERNATIONAL STANDARD

ISO 7498-2

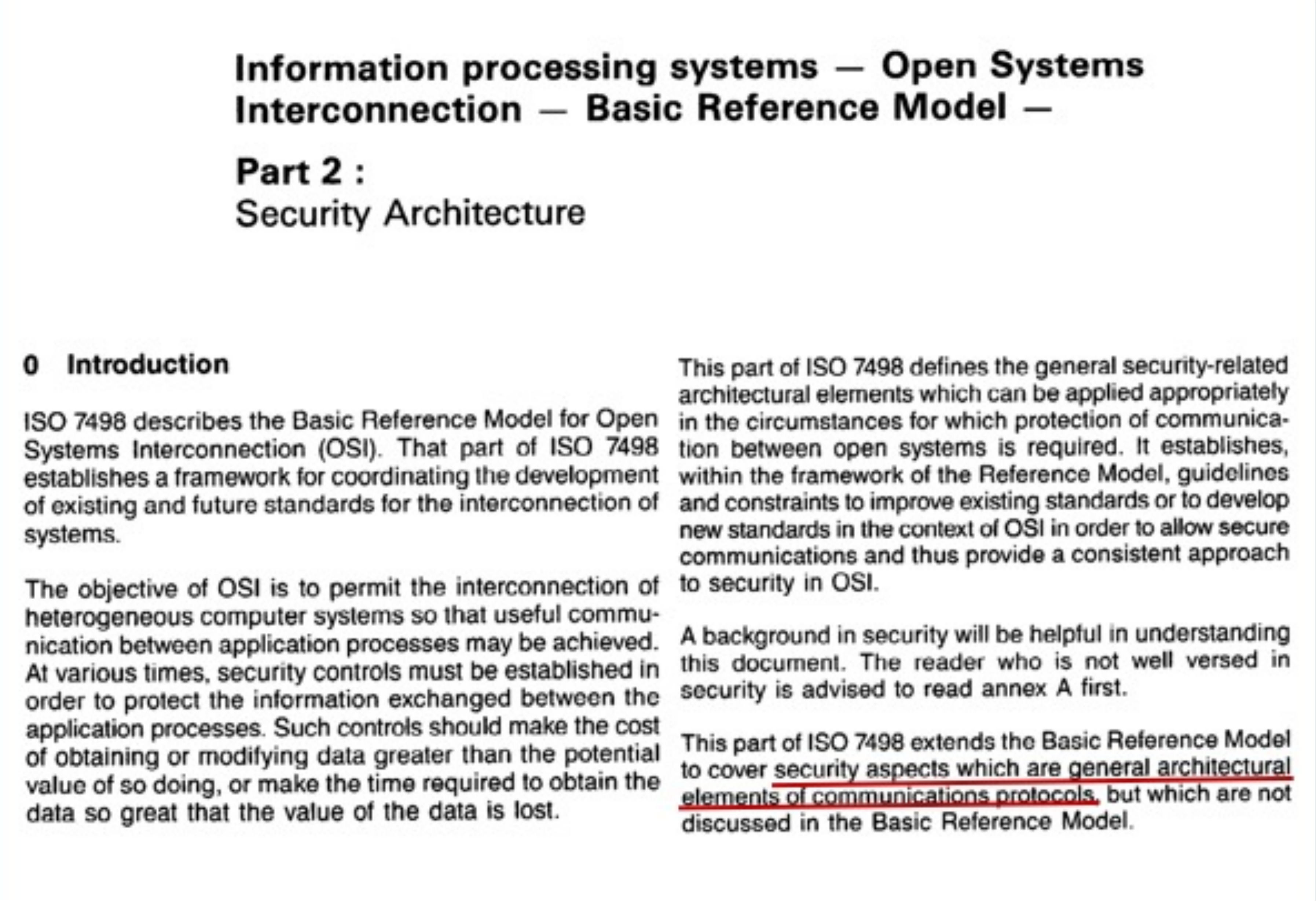
First edition
1989-02-15

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

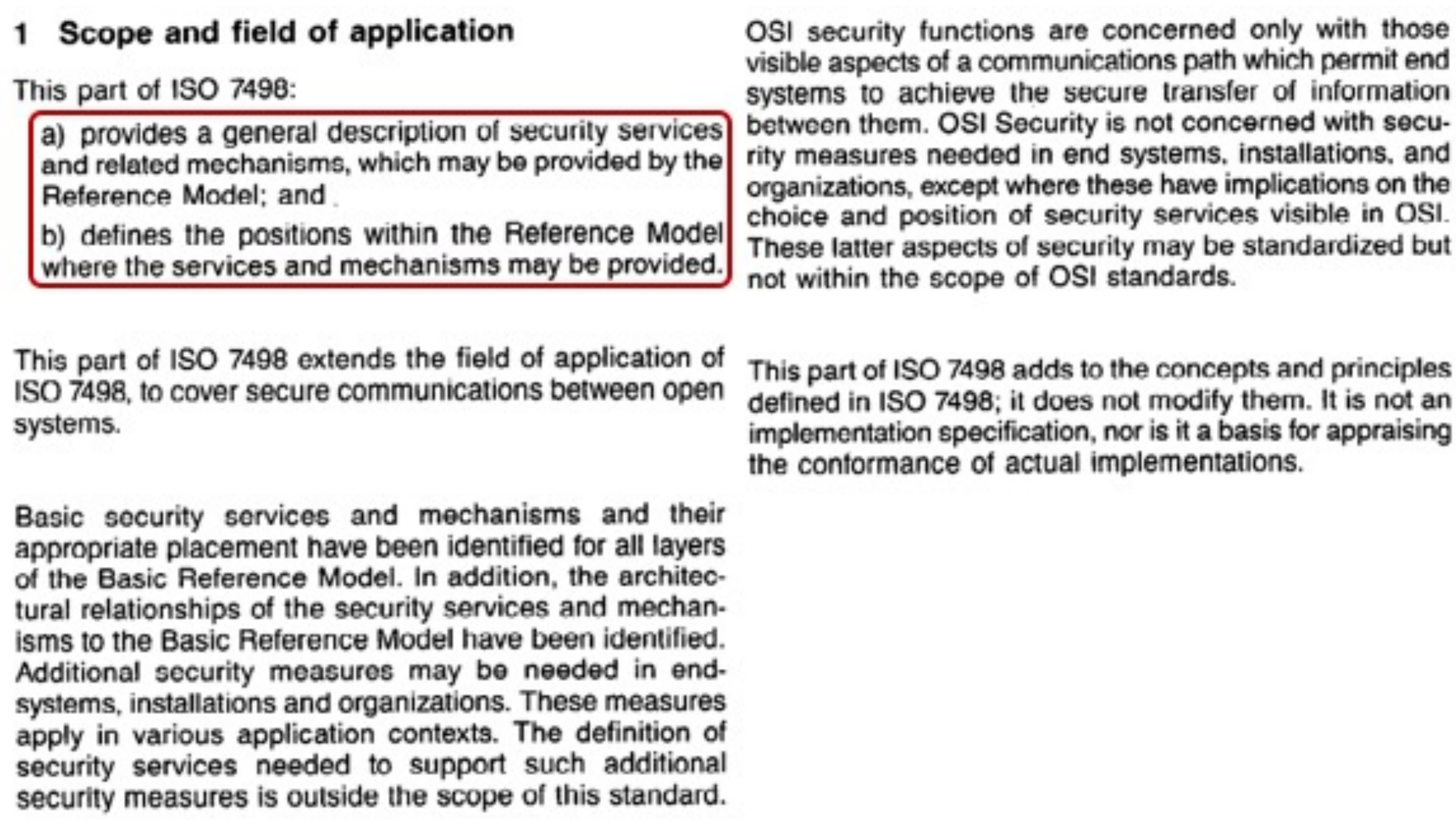
ISO 7498 describes the Basic Reference Model for Open Systems Interconnection (OSI). That part of ISO 7498 establishes a framework for coordinating the development of existing and future standards for the interconnection of systems.

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.

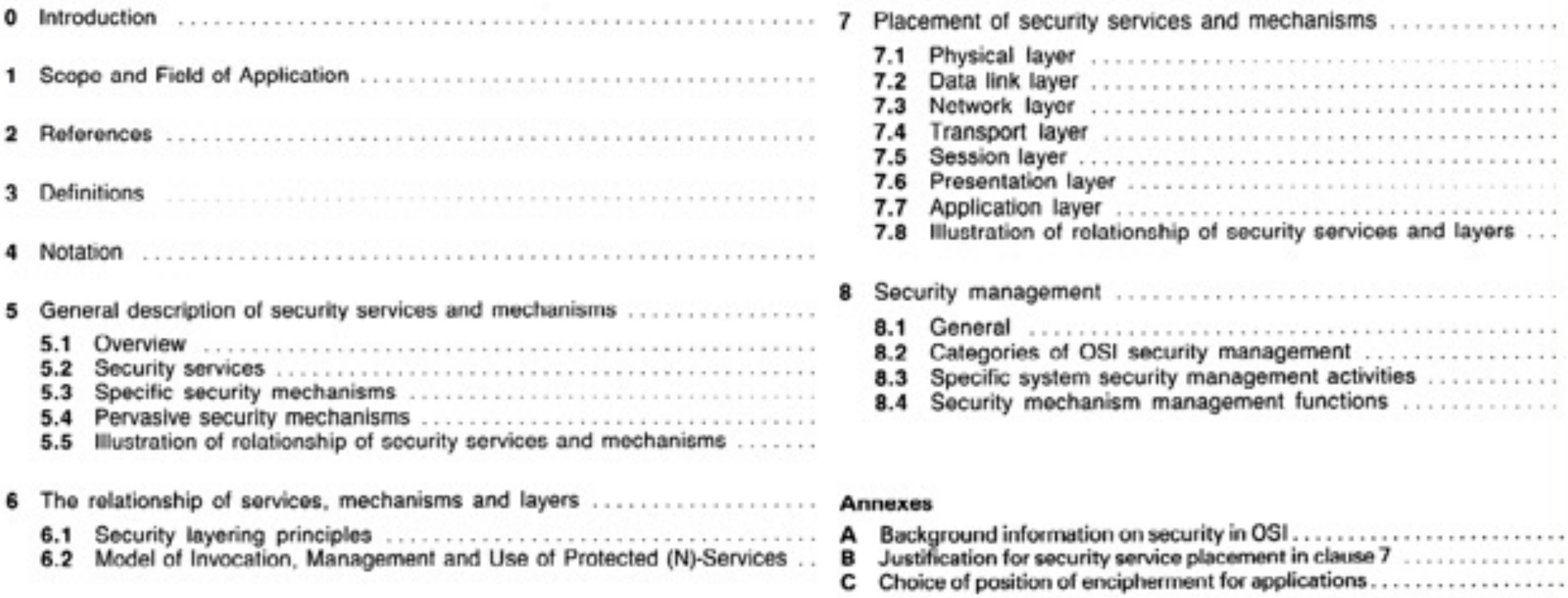
This part of ISO 7498 extends the field of application of ISO 7498, to cover secure communications between open systems.

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.

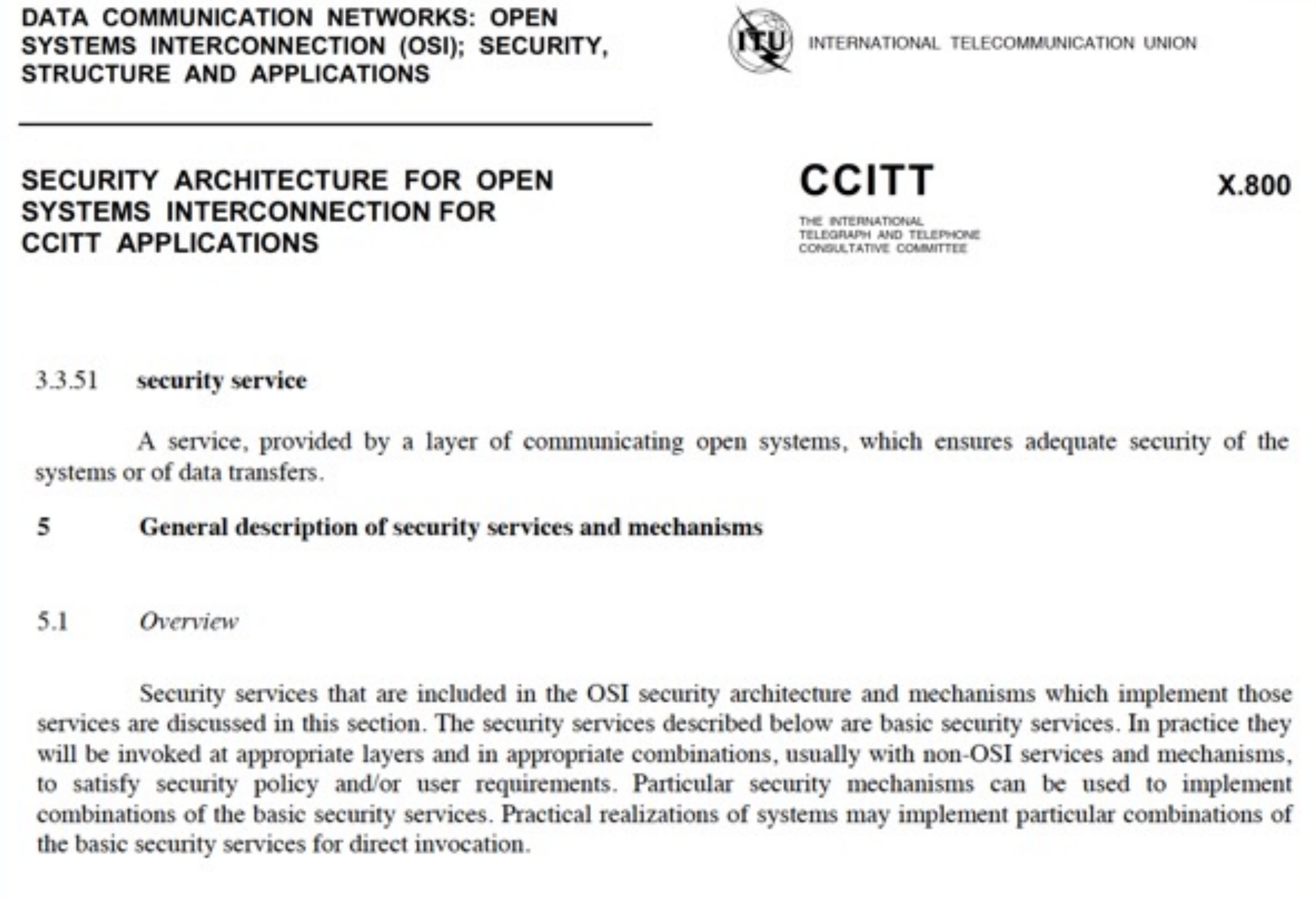
OSI security functions are concerned only with those visible aspects of a communications path which permit end systems to achieve the secure transfer of information between them. OSI Security is not concerned with security measures needed in end systems, installations, and organizations, except where 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



Annexes



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

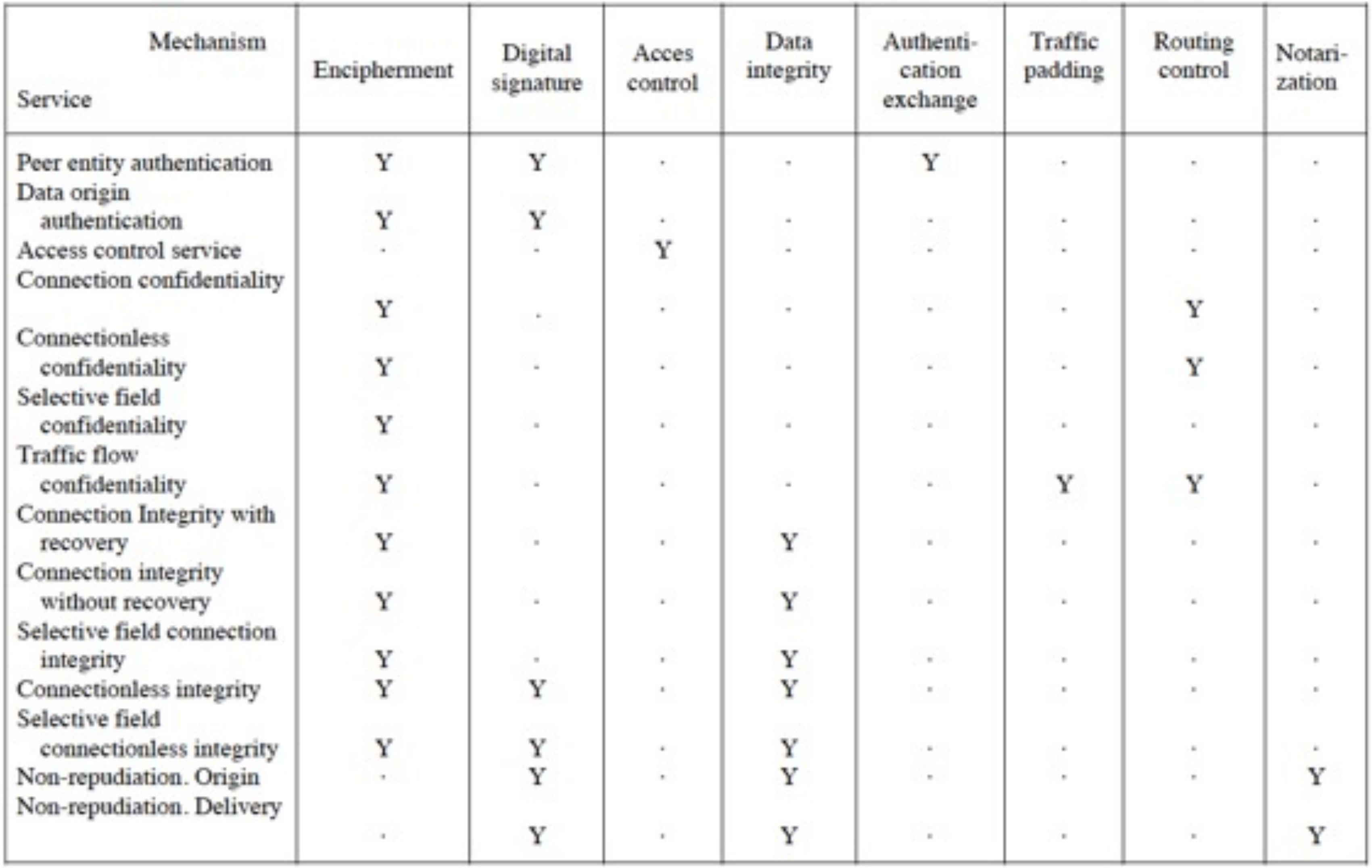
Mecanismos de Segurança Específicos

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

Mecanismos de Segurança Pervasivos

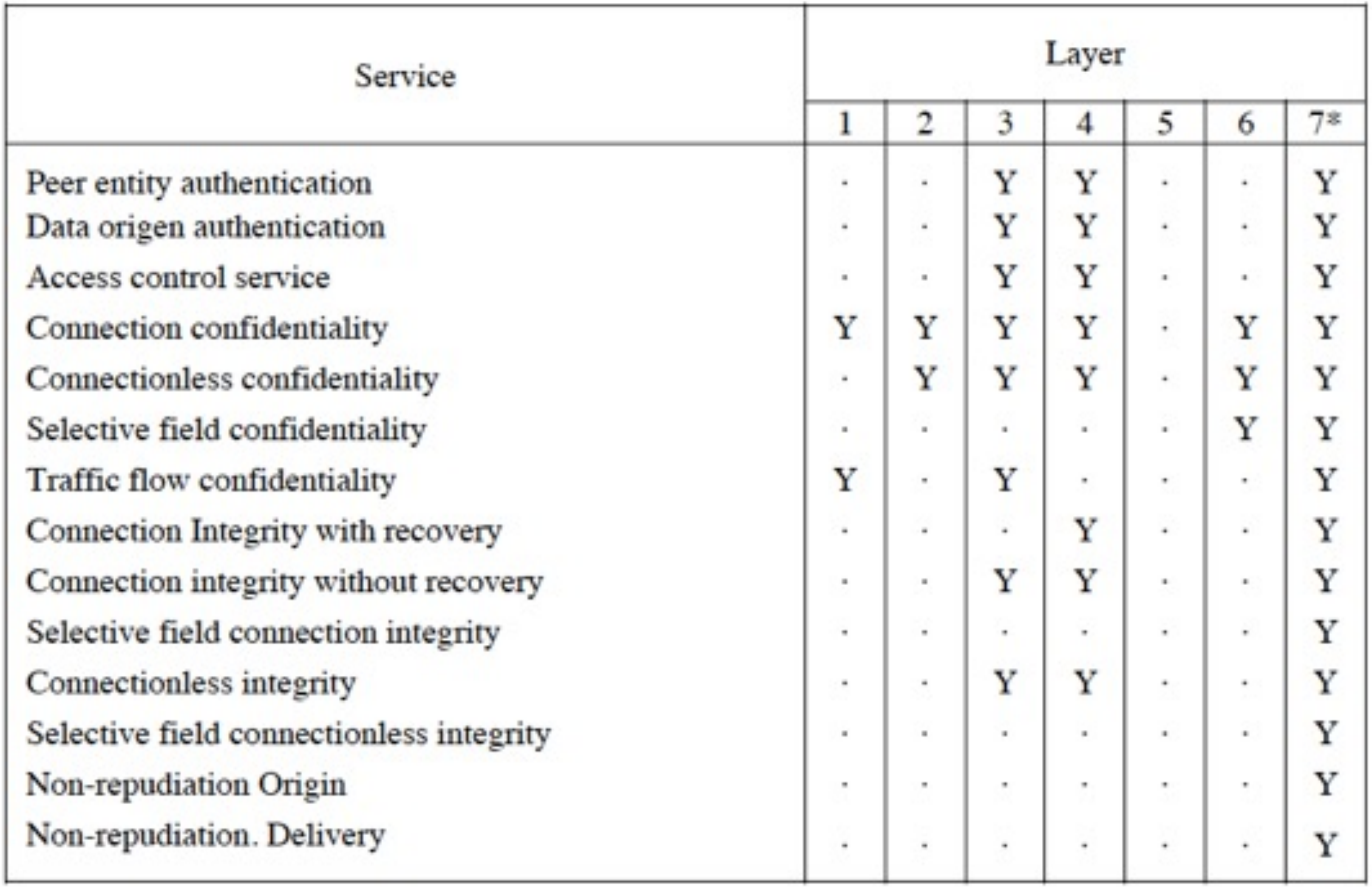
- Funcionalidade confiável
- Rótulo de segurança
- Detecção de evento
- Trilha de auditoria de segurança
- Recuperação de segurança

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

Conceitos de Segurança da Informação

Baseado em padrões e legislação dos EUA

Legislação/padronização nos EUA

Histórico da Legislação Federal

- Computer Security Act of 1987
  - NIST (então NSB) recebe a tarefa de desenvolver padrões e estabelecer práticas de segurança
  - Sistemas de computadores com informação sensível devem ter políticas de segurança
  - Empregados que usam tais sistemas devem receber treinamento de conscientização
- Federal Information Security Modernization Act of 2002
  - Responsabilidades ao NIST e ao OMB (Office of Management and Budget)
  - O líder de cada agência deve implementar políticas e procedimentos custo-efetivos para reduzir os riscos de segurança dainformação a nível aceitável
- Federal Information Security Modernization Act of 2014
  - ”Reforma” do FISMA

Definições do FISMA 2014

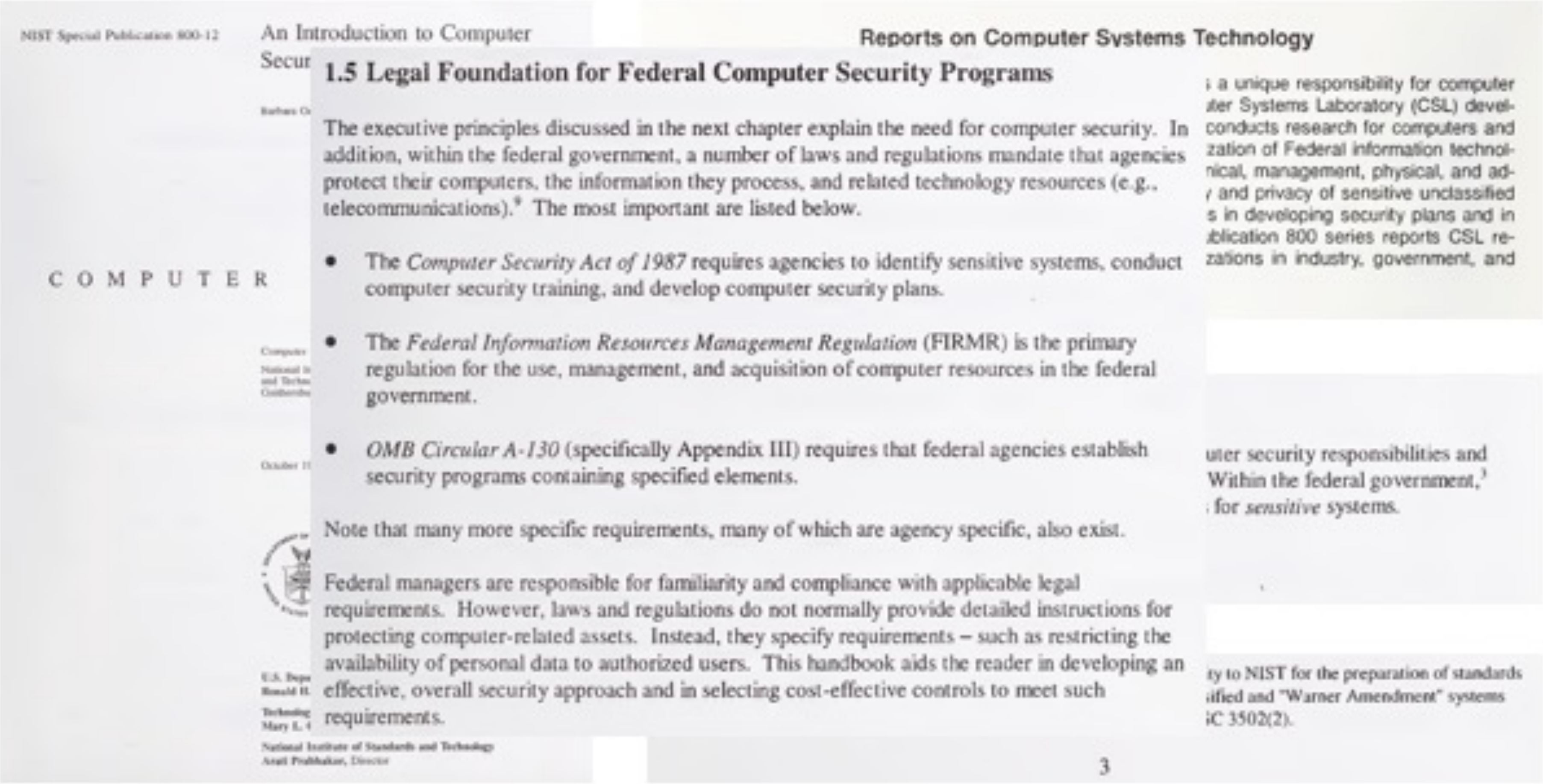
- "(3) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
  - "(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
  - "(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
  - "(C) availability, which means ensuring timely and reliable access to and use of information.

Padrões NIST

NIST SP 800-12 (Rev. 1)

- An Introduction to Information Security
- Original de outubro de 1995
  - Já tinha foco no apoio às organizações federais
- Revisão em 2017 – espírito do documento mantido
  - 8 ”princípios” guiam a abordagem do documento
  - Seções-chave mantidas: Papéis e Responsabilidades, Ameaças, Políticas de Segurança, Gerenciamento de Riscos, Garantias, Operações, Criptografia
  - Outras seções (Controle de Acesso, Auditoria, Resposta a Incidentes etc) foram agrupadas numa seção de ”Controles”

Publicação original: referência ao CSA’87



NIST Special Publication 800-12

An Introduction to Computer
Secur

Barbara G

COMPUTER

Computer

National I
and Techn
Gaithersb

October 1

U.S. Depa
Ronald H.

Technolog
Mary L. G

National Institute of Standards and Technology
Arati Prabhakar, Director

1.5 Legal Foundation for Federal Computer Security Programs

The executive principles discussed in the next chapter explain the need for computer security. In addition, within the federal government, a number of laws and regulations mandate that agencies protect their computers, the information they process, and related technology resources (e.g., telecommunications).[8] The most important are listed below.

- The *Computer Security Act of 1987* requires agencies to identify sensitive systems, conduct computer security training, and develop computer security plans.
- The *Federal Information Resources Management Regulation* (FIRMR) is the primary regulation for the use, management, and acquisition of computer resources in the federal government.
- *OMB Circular A-130* (specifically Appendix III) requires that federal agencies establish security programs containing specified elements.

Note that many more specific requirements, many of which are agency specific, also exist.

Federal managers are responsible for familiarity and compliance with applicable legal requirements. However, laws and regulations do not normally provide detailed instructions for protecting computer-related assets. Instead, they specify requirements – such as restricting the availability of personal data to authorized users. This handbook aids the reader in developing an effective, overall security approach and in selecting cost-effective controls to meet such requirements.

Reports on Computer Systems Technology

; a unique responsibility for computer
ter Systems Laboratory (CSL) devel-
conducts research for computers and
zation of Federal information technol-
nical, management, physical, and ad-
y and privacy of sensitive unclassified
s in developing security plans and in
blication 800 series reports CSL re-
zations in industry, government, and

uter security responsibilities and
Within the federal government,[3]
for *sensitive* systems.

ty to NIST for the preparation of standards
ified and "Warner Amendment" systems
C 3502(2).

3

NIST SP 800-53 (rev.4)

- Security and Privacy Controls for Federal Information Systems and Organizations
- Versão ”original” de fev-2005: Recommended Security Controls for Federal Information Systems
- Dá continuidade ao SP 800-26 (2001): Security Self-Assessment Guide for Information Technology Systems
  - Importância histórica do ”self-assessment”

NIST SP 800-53 (rev.4)

- Security and Privacy Controls for Federal Information Syst … ns
- Vers … 20 … ecurity Con … rm
- Dá … 30 … Self-Ass … or … ystems
  - Im … sel

NIST Special Publication 800-26

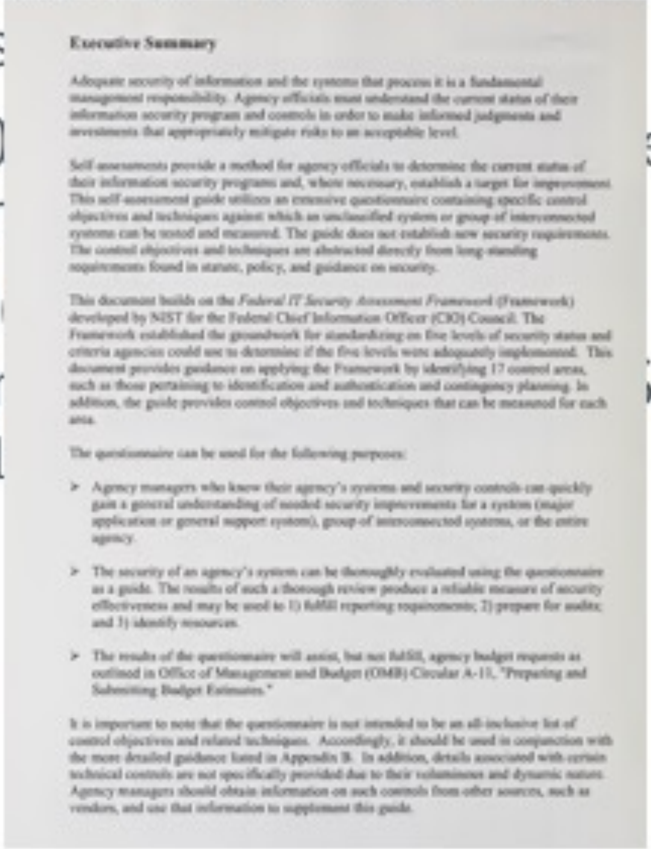
NIST

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Security Self-Assessment Guide for Information Technology Systems

Marianne Swanson

COMPUTER SECURITY



Executive Summary

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

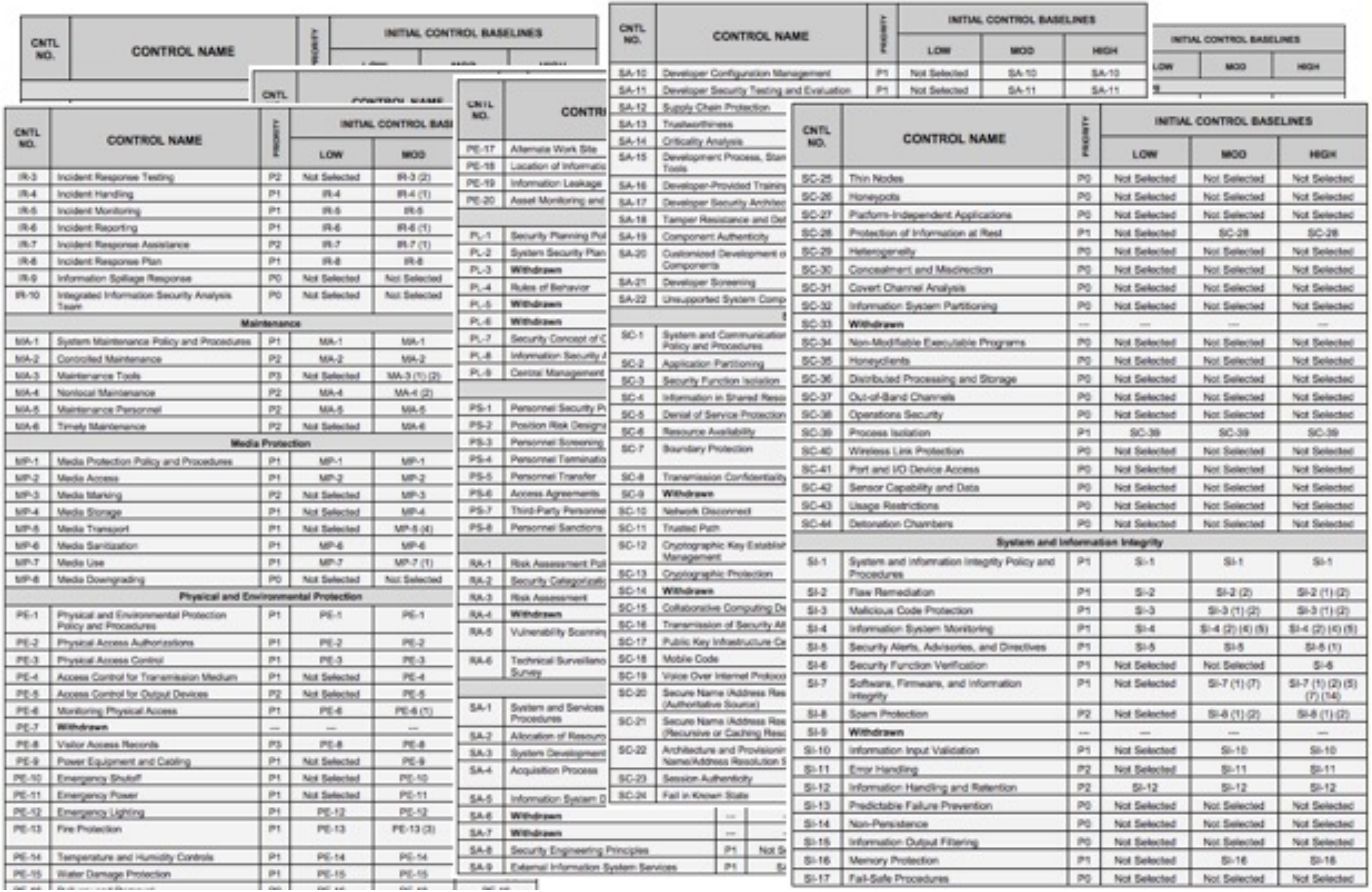
Self assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.

This document builds on the *Federal IT Security Assessment Framework* (Framework) developed by NIST for the Federal Chief Information Officer (CIO) Council. The Framework established the groundwork for standardizing on five levels of security status and criteria agencies could use to determine if the five levels were adequately implemented. This document provides guidance on applying the Framework by identifying 17 control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provides control objectives and techniques that can be measured for each area.

The questionnaire can be used for the following purposes:

- ➢ Agency managers who know their agency's systems and security controls can quickly gain a general understanding of needed security improvements for a system (major application or general support system), group of interconnected systems, or the entire agency.
- ➢ The security of an agency's system can be thoroughly evaluated using the questionnaire as a guide. The results of such a thorough review produce a reliable measure of security effectiveness and may be used to 1) fulfill reporting requirements; 2) prepare for audits; and 3) identify resources.
- ➢ The results of the questionnaire will assist, but not fulfill, agency budget requests as outlined in Office of Management and Budget (OMB) Circular A-11, "Preparing and Submitting Budget Estimates."

It is important to note that the questionnaire is not intended to be an all-inclusive list of control objectives and related techniques. Accordingly, it should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, details associated with certain technical controls are not specifically provided due to their voluminous and dynamic nature. Agency managers should obtain information on such controls from other sources, such as vendors, and use that information to supplement this guide.



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BAS	
			LOW	MOD
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)
IR-5	Incident Monitoring	P1	IR-5	IR-5
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)
IR-7	Incident Response Assistance	P2	IR-7	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected
	Maintenance			
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2
MA-3	Maintenance Tools	P3	Not Selected	MA-3 (1) (2)
MA-4	Nonlocal Maintenance	P2	MA-4	MA-4 (2)
MA-5	Maintenance Personnel	P2	MA-5	MA-5
MA-6	Timely Maintenance	P2	Not Selected	MA-6
	Media Protection			
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2
MP-3	Media Marking	P2	Not Selected	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6
MP-7	Media Use	P1	MP-7	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected
	Physical and Environmental Protection			
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4
PE-5	Access Control for Output Devices	P2	Not Selected	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)
PE-7	**Withdrawn**	—	—	—
PE-8	Visitor Access Records	P3	PE-8	PE-8
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11
PE-12	Emergency Lighting	P1	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15

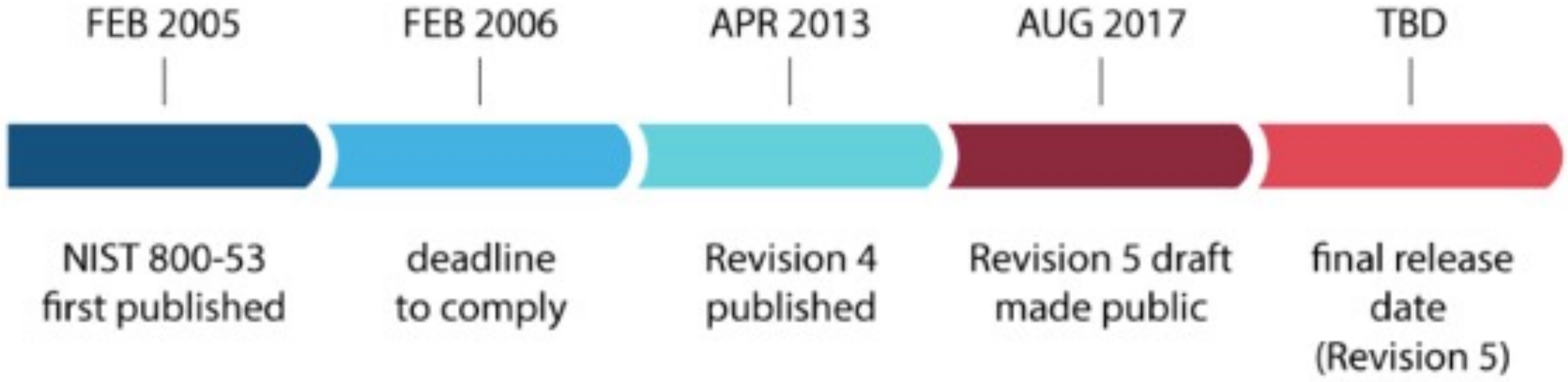
CNTL NO.	CONTRI		
PE-17	Alternate Work Site		
PE-18	Location of Informatio		
PE-19	Information Leakage		
PE-20	Asset Monitoring and		
PL-1	Security Planning Pol		
PL-2	System Security Plan		
PL-3	**Withdrawn**		
PL-4	Rules of Behavior		
PL-5	**Withdrawn**		
PL-6	**Withdrawn**		
PL-7	Security Concept of C		
PL-8	Information Security A		
PL-9	Central Management		
PS-1	Personnel Security Po		
PS-2	Position Risk Designa		
PS-3	Personnel Screening		
PS-4	Personnel Terminatio		
PS-5	Personnel Transfer		
PS-6	Access Agreements		
PS-7	Third-Party Personne		
PS-8	Personnel Sanctions		
RA-1	Risk Assessment Pol		
RA-2	Security Categorizatio		
RA-3	Risk Assessment		
RA-4	**Withdrawn**		
RA-5	Vulnerability Scanning		
RA-6	Technical Surveillance Survey		
SA-1	System and Services Procedures		
SA-2	Allocation of Resourc		
SA-3	System Development		
SA-4	Acquisition Process		
SA-5	Information System D		
SA-6	**Withdrawn**	—	
SA-7	**Withdrawn**	—	
SA-8	Security Engineering Principles	P1	Not S
SA-9	External Information System Services	P1	S

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection				
SA-13	Trustworthiness				
SA-14	Criticality Analysis				
SA-15	Development Process, Stan Tools				
SA-16	Developer-Provided Training				
SA-17	Developer Security Architec				
SA-18	Tamper Resistance and Det				
SA-19	Component Authenticity				
SA-20	Customized Development o Components				
SA-21	Developer Screening				
SA-22	Unsupported System Comp				
SC-1	System and Communication Policy and Procedures				
SC-2	Application Partitioning				
SC-3	Security Function Isolation				
SC-4	Information in Shared Reso				
SC-5	Denial of Service Protection				
SC-6	Resource Availability				
SC-7	Boundary Protection				
SC-8	Transmission Confidentiality				
SC-9	**Withdrawn**				
SC-10	Network Disconnect				
SC-11	Trusted Path				
SC-12	Cryptographic Key Establish Management				
SC-13	Cryptographic Protection				
SC-14	**Withdrawn**				
SC-15	Collaborative Computing De				
SC-16	Transmission of Security At				
SC-17	Public Key Infrastructure Ce				
SC-18	Mobile Code				
SC-19	Voice Over Internet Protoco				
SC-20	Secure Name /Address Res (Authoritative Source)				
SC-21	Secure Name /Address Res (Recursive or Caching Reso				
SC-22	Architecture and Provisionin Name/Address Resolution S				
SC-23	Session Authenticity				
SC-24	Fail in Known State				

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	**Withdrawn**	—	—	—	—
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
	System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	—	—	—	—
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

NIST 800-53: padrão *de facto* p/ APF

› NIST Special Publication 800-53 provides a catalog of security controls for all US federal information systems except those related to national security.



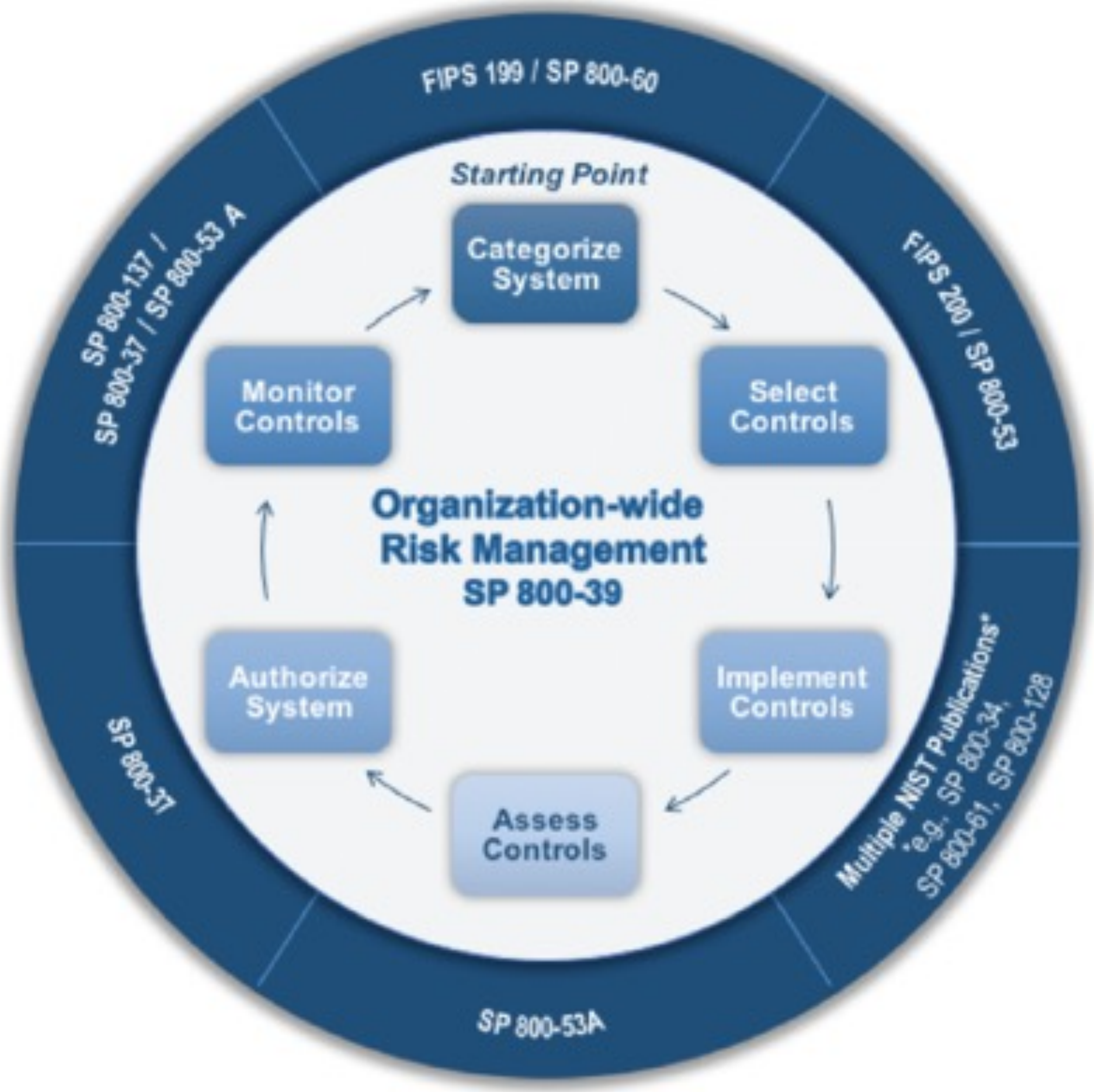
FEB 2005 – NIST 800-53 first published

FEB 2006 – deadline to comply

APR 2013 – Revision 4 published

AUG 2017 – Revision 5 draft made public

TBD – final release date (Revision 5)


FIPS 199 / SP 800-60
Starting Point
Categorize System
FIPS 200 / SP 800-53
Select Controls
Multiple NIST Publications*
*e.g., SP 800-34, SP 800-61, SP 800-128
Implement Controls
SP 800-53A
Assess Controls
SP 800-37
Authorize System
SP 800-137 / SP 800-37 / SP 800-53 A
Monitor Controls
Organization-wide Risk Management SP 800-39

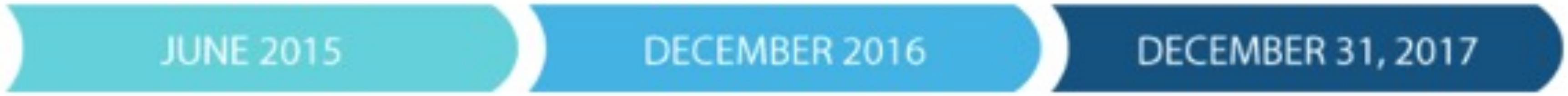
Publicações relevantes do NIST

- FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems,
- NIST 800-12 – A Introduction to Information Security
- SP 800-37 – Guide for Applying the Risk Management Framework to Systems: A Security Life Cycle Approach
- SP 800-53 – Security and Privacy Controls for Systems and Organizations,
- SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Fornecedores do Governo e da Defesa

O NIST SP 800-171

NIST SP 800-171


JUNE 2015

NIST 800-171 first published

DECEMBER 2016

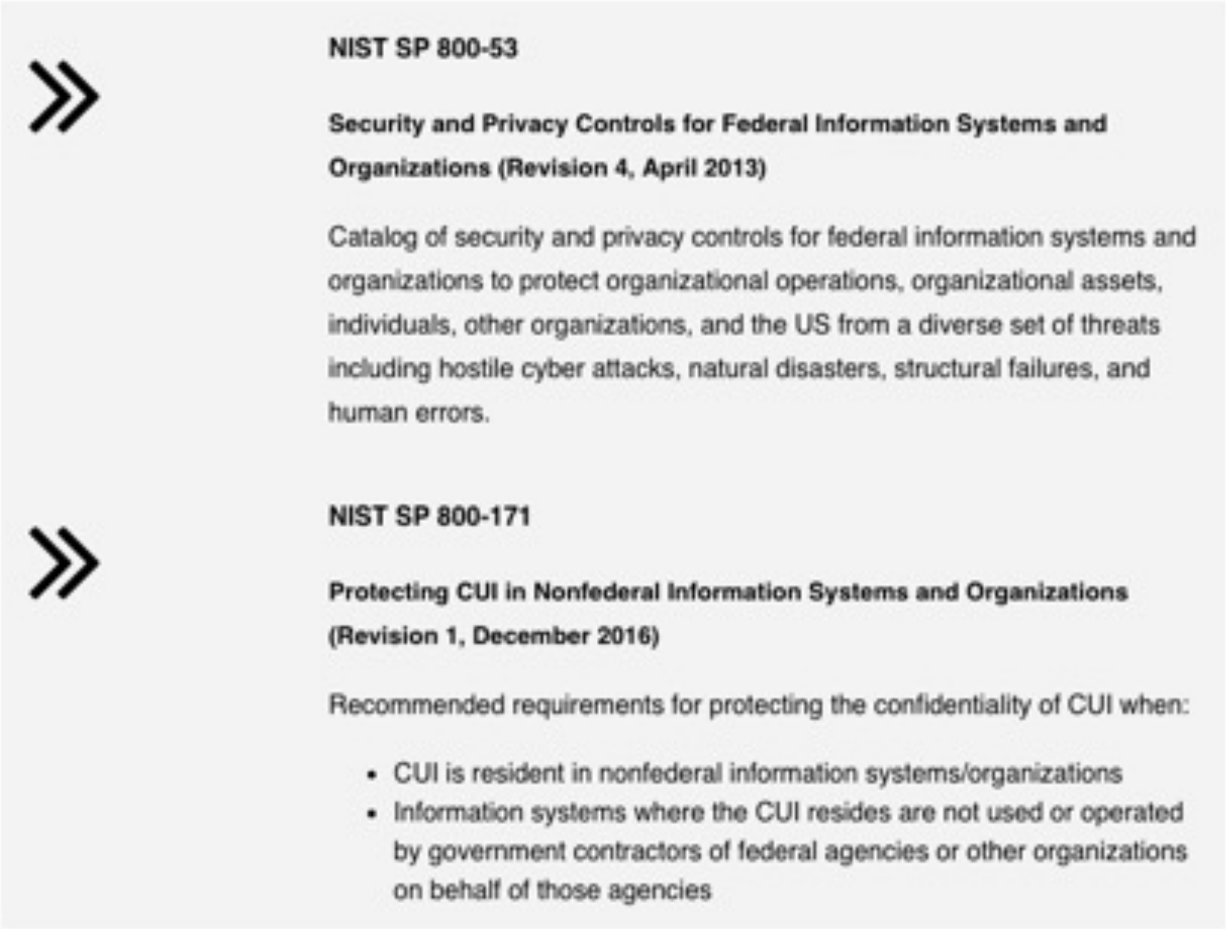
Revision 1 published

DECEMBER 31, 2017

deadline to comply

- As of December 31, 2017, manufacturers that provide parts and equipment for suppliers serving federal and local governments must be compliant with the latest NIST 800-171 regulation.

800-53 versus 800-171



NIST SP 800-53

Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4, April 2013)

Catalog of security and privacy controls for federal information systems and organizations to protect organizational operations, organizational assets, individuals, other organizations, and the US from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

NIST SP 800-171

Protecting CUI in Nonfederal Information Systems and Organizations (Revision 1, December 2016)

Recommended requirements for protecting the confidentiality of CUI when:

- CUI is resident in nonfederal information systems/organizations
- Information systems where the CUI resides are not used or operated by government contractors of federal agencies or other organizations on behalf of those agencies

Requisitos da 800-171

- **3.1 Access Control**
- Who is authorized to view this data? How do you control access to the CUI that resides in your organization (within your systems and within your operations)?
- **3.2 Awareness & Training**
- Are people properly instructed in how to treat this info? When it comes to CUI, are your employees aware of the security risks?
- **3.3 Audit & Accountability**
- Are records kept of authorized and unauthorized access? Can violators be identified?
- **3.4 Configuration Management**
- How are your networks and safety protocols built and documented?
- **3.5 Identification & Authentication**
- What users are approved to access CUI and how are they verified prior to granting them access?

Requisitos da 800-171

- **3.6 Incident Response**
- What's the process if a breach or security threat occurs, including proper notification? If there is an incident that puts data at risk, the DFARS 252.204-7012 clause stipulates that your partner must be notified.
- **3.7 Maintenance**
- What timeline exists for routine maintenance, and who is responsible?
- **3.8 Media Protection**
- How are electronic and hard copy records and backups safely stored? Who has access?
- **3.9 Personnel Security**
- How are employees screened prior to granting them access to CUI?
- **3.10 Physical Protection**
- Who has access to systems, equipment, and storage environments? For example, if you have one office with a front door and back door, what kind of security do you have? This could include locks, access control systems, and video monitoring systems. What is the physical environment like within your facility where the data is housed?

Requisitos da 800-171

- **3.11 Risk Assessment**
- Are defenses tested in simulations? Are operations or individuals verified regularly?
- **3.12 Security Assessment**
- Are processes and procedures still effective? Are improvements needed? Penetration testing and vulnerability assessments performed on an ongoing, regular basis are methods for measuring your security.
- **3.13 Systems & Communications Protection**
- Is information regularly monitored and controlled at key internal and external transmission points?
- **3.14 System & Information Integrity**
- How quickly are possible threats detected, identified, and corrected?

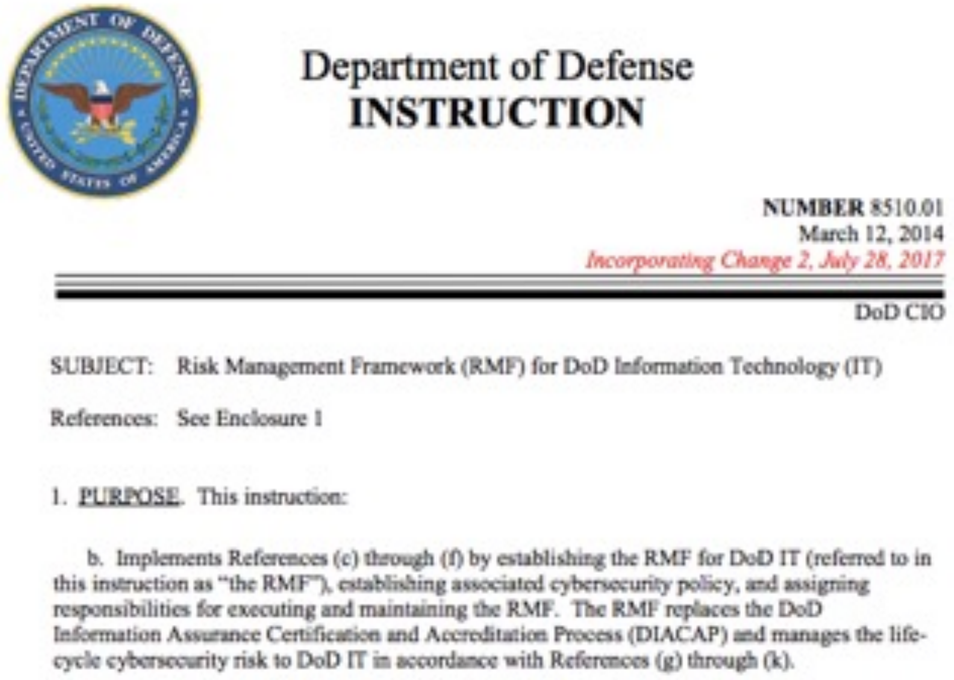
Requisitos da 800-171

› The requirements for NIST 800-171 can be summarized into four main groups.

- **Controls** – Data management controls and processes
- **Monitoring & management** – Real time monitoring/management of defined IT systems
- **End user practices** – Documented, well defined end user practices and procedures
- **Security measures** – Implementation of defined security measures

Padronização de segurança para Defesa e APF nos EUA

› DoD Instruction 8510 aproxima os padrões de Defesa aos do setor público civil (NIST)



Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014
Incorporating Change 2, July 28, 2017

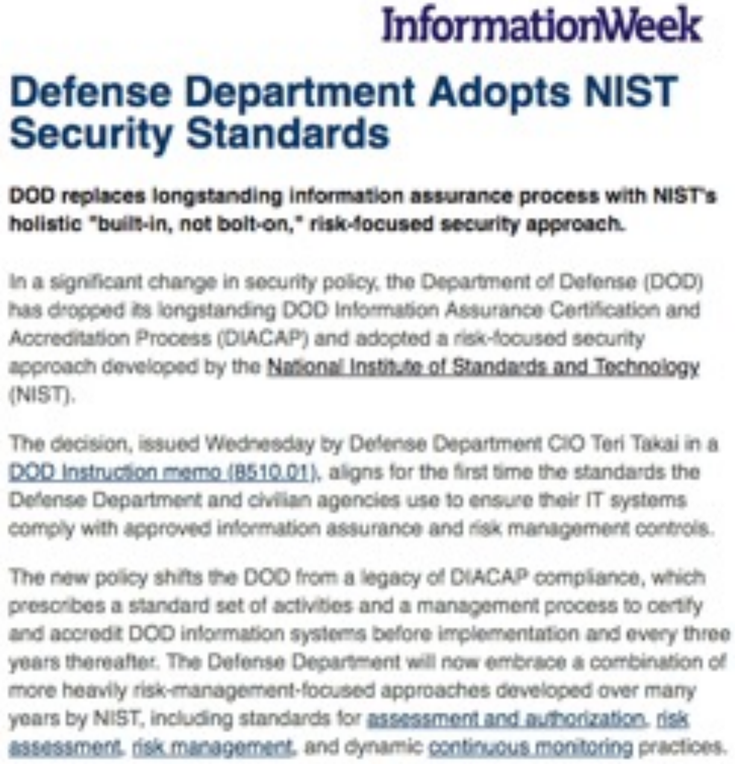
DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).



InformationWeek

Defense Department Adopts NIST Security Standards

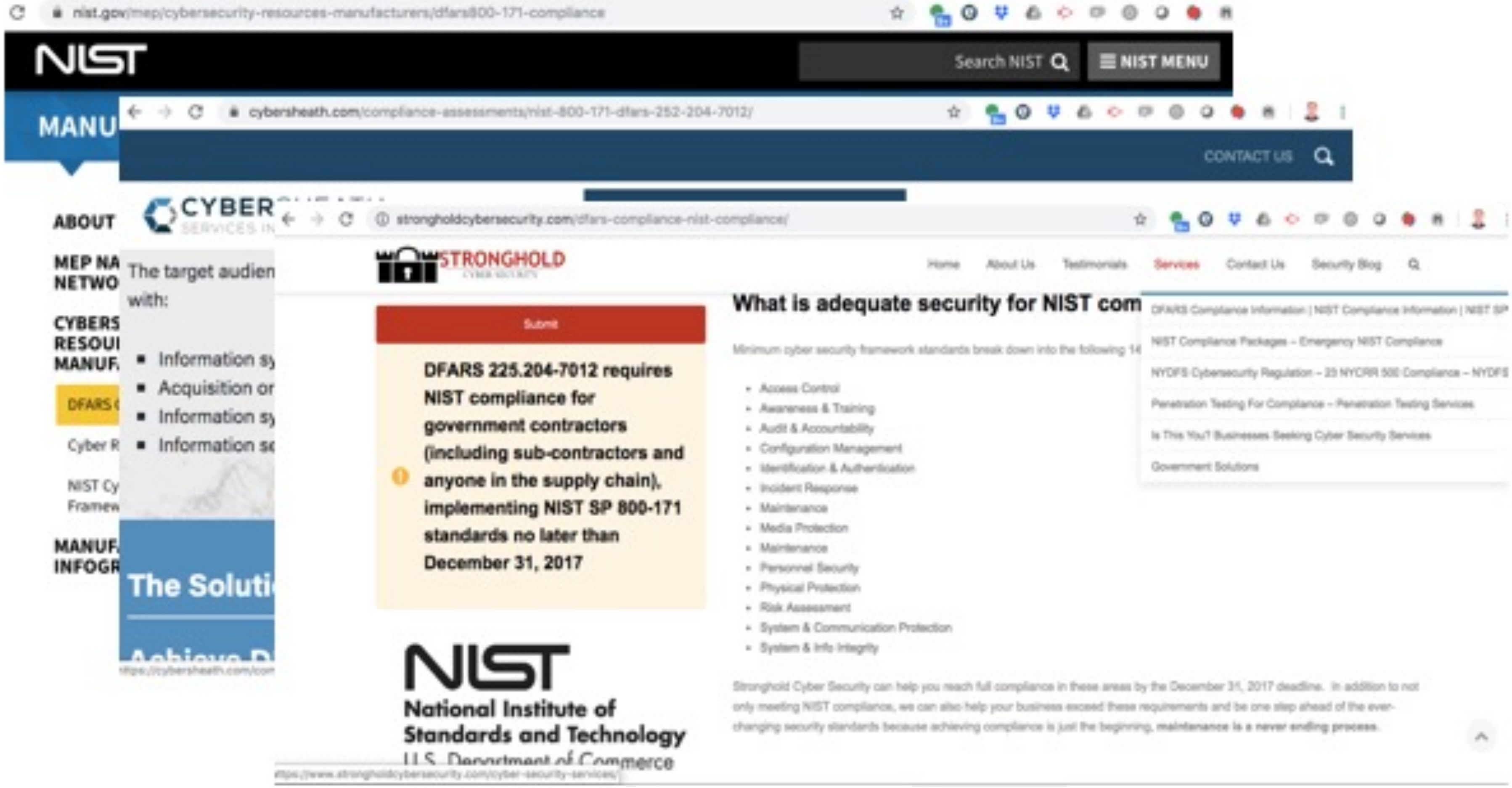
DOD replaces longstanding information assurance process with NIST's holistic "built-in, not bolt-on," risk-focused security approach.

In a significant change in security policy, the Department of Defense (DOD) has dropped its longstanding DOD Information Assurance Certification and Accreditation Process (DIACAP) and adopted a risk-focused security approach developed by the National Institute of Standards and Technology (NIST).

The decision, issued Wednesday by Defense Department CIO Teri Takai in a DOD Instruction memo (8510.01), aligns for the first time the standards the Defense Department and civilian agencies use to ensure their IT systems comply with approved information assurance and risk management controls.

The new policy shifts the DOD from a legacy of DIACAP compliance, which prescribes a standard set of activities and a management process to certify and accredit DOD information systems before implementation and every three years thereafter. The Defense Department will now embrace a combination of more heavily risk-management-focused approaches developed over many years by NIST, including standards for assessment and authorization, risk assessment, risk management, and dynamic continuous monitoring practices.

”Compliance” aos padrões NIST



nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance

NIST

Search NIST

NIST MENU

MANU

ABOUT

MEP NA
NETWO

CYBERS
RESOUI
MANUF.

DFARS (

Cyber R

NIST Cy
Framew

MANUF.
INFOGR

cybersheath.com/compliance-assessments/nist-800-171-dfars-252-204-7012/

CONTACT US

CYBER
SERVICES IN

The target audien
with:

- Information sy
- Acquisition or
- Information sy
- Information se

The Soluti

Achieve D

https://cybersheath.com/com

strongholdcybersecurity.com/dfars-compliance-nist-compliance/

STRONGHOLD
CYBER SECURITY

Home About Us Testimonials Services Contact Us Security Blog

Submit

DFARS 225.204-7012 requires NIST compliance for government contractors (including sub-contractors and anyone in the supply chain), implementing NIST SP 800-171 standards no later than December 31, 2017

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

What is adequate security for NIST com

Minimum cyber security framework standards break down into the following 14

- Access Control
- Awareness & Training
- Audit & Accountability
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Maintenance
- Personnel Security
- Physical Protection
- Risk Assessment
- System & Communication Protection
- System & Info Integrity

Stronghold Cyber Security can help you reach full compliance in these areas by the December 31, 2017 deadline. In addition to not only meeting NIST compliance, we can also help your business exceed these requirements and be one step ahead of the ever-changing security standards because achieving compliance is just the beginning, **maintenance is a never ending process.**

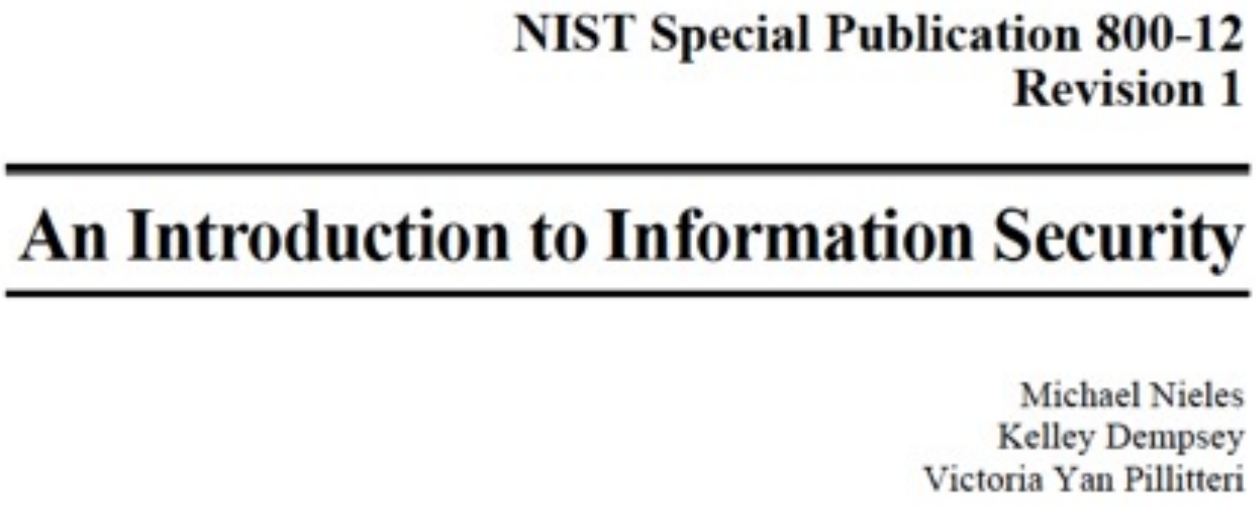
DFARS Compliance Information | NIST Compliance Information | NIST SP
NIST Compliance Packages – Emergency NIST Compliance
NYDFS Cybersecurity Regulation – 23 NYCRR 500 Compliance – NYDFS
Penetration Testing For Compliance – Penetration Testing Services
Is This You? Businesses Seeking Cyber Security Services
Government Solutions

https://www.strongholdcybersecurity.com/cyber-security-services/

Conceitos de Segurança da Informação segundo o NIST SP 800-12 Rev. 1

Objetivo

- Apresentar de maneira formal e estruturada conceitos de segurança da informação



NIST Special Publication 800-12
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri

Terminologia Básica

- Sistema de Informação
  - *The term Information System is defined by 44 U.S.C., Sec. 3502 as "a discrete set of* ***information resources*** *organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."*
- Sistema = Sistema de Informação
  - *For this publication, the term* ***system*** *is used in lieu of the term* ***information system*** *to reflect the broader applicability of information resources of any size or complexity, organized expressly for the collection, processing, use, sharing, dissemination, maintenance, or disposition of data or information.*

Terminologia Básica – outros termos

› Informação

- *Information – (1)* ***Facts or ideas****, which can be represented (encoded) as various forms of data; (2)* ***Knowledge*** *(e.g., data, instructions) in any medium or form that can be communicated between system entities.*

› Segurança da Informação

- *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.*

Terminologia Básica – outros termos

- Confidencialidade
  - *Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*
- Integridade
  - *Integrity – Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.*
  - *Data Integrity – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.*
  - *System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.*

Terminologia Básica – outros termos

- Disponibilidade
  - *Availability – Ensuring* ***timely and reliable access*** *to and use of information.*
- Controles de Segurança
  - *Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to* ***protect the confidentiality, availability, and integrity*** *of the system and its information.*
  - *In this document, the terms security* ***controls***, ***safeguards***, ***security protections***, *and* ***security measures*** *have been used interchangeably.*

Oito ”conceitos” (ou ”princípios”) de segurança da informação (Cap.2)

1. Information security supports the mission of the organization.

2. Information security is an integral element of sound management.

3. Information security protections are implemented so as to be commensurate with risk.

4. Information security roles and responsibilities are made explicit.

5. Information security responsibilities for system owners go beyond their own organization.

6. Information security requires a comprehensive and integrated approach.

7. Information security is assessed and monitored regularly.

8. Information security is constrained by societal and cultural factors.

Papéis e Responsabilidades (Cap.3)

- Risk Executive Function (Senior Management)
- Chief Executive Officer (CEO)
- Chief Information Officer (CIO)
- Information Owner/Steward
- Chief Information Security Officer (CISO)
- System Owner
- System Security Officer
- Information Security Architect
- System Security Engineer (SSE)
- Security Control Assessor
- System Administrator
- User
- Supporting Roles
  - Auditor, Physical Security Staff, Disaster Recovery/Contingency Planning Staff, Quality Assurance Staff, Procurement Office Staff, Training Office Staff, Human Resources, Risk Management/ Physical Plant Staff, Planning Staff, Privacy Office Staf

Ameaças e Vulnerabilidades (cap.4)

› Vulnerabilidades

- *A vulnerability is a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source*

› Fontes de Ameaça

- *Threat Source – The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.*

Fontes de ameaça

- Adversárias e não-adversárias
  - *A threat source can be adversarial or non-adversarial. Adversarial threat sources are individuals, groups, organizations, or entities that seek to exploit an organization's dependence on cyber resources. Even employees, privileged users, and trusted users have been known to defraud organizational systems. Non-adversarial threat sources refer to natural disasters or erroneous actions taken by individuals in the course of executing their everyday responsibilities.*

Exemplos

- Adversariais
  - *Fraud and Theft*
  - *Insider Threat*
  - *Malicious Hacker*
  - *Malicious Code*
- Não-adversariais
  - *Errors and Omissions*
  - *Loss of Physical and Infrastructure Support*
  - *Impacts to Personal Privacy of Information Sharing*

Eventos de Ameaça

- Fontes de ameaça levam a eventos de ameaça
  - *If the system is vulnerable, threat sources can lead to threat events. A threat event is an incident or situation that could potentially cause undesirable consequences or impacts. An example of a threat source leading to a threat event is a hacker installing a keystroke monitor on an organizational system.*

Medidas de segurança ”custo-efetivas”

- Compreender ameaças e vulnerabilidades ajuda a implementar medidas de segurança custo-efetivas
  - *In order to protect a system from risk and to implement the most cost-effective security measures, system owners, managers, and users need to know and understand the vulnerabilities of the system as well as the threat sources and events that may exploit the vulnerabilities. When determining the appropriate response to a discovered vulnerability, care should be taken to minimize the expenditure of resources on vulnerabilities where little or no threat is present.*

Política de Segurança da Informação (cap.5)

- Política: regras que especificam o comportamento ”correto” ou ”esperado”
- São as regras e diretrizes para manter a segurança da informação
  - *Information security policy is defined as an aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information*

Padrões, guias e procedimentos

- Padrões organizacionais
  - *Organizational standards (not to be confused with American National Standards, FIPS, Federal Standards, or other national or international standards) specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization.*
  - Exemplo: crachás de identificação
- Guias
  - *Guidelines assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably, and imposition of standards is not always achievable, appropriate, or cost-effective.*
  - Exemplo: guia para criação de procedimentos de sistema
- Procedimentos
  - *Procedures describe how to implement applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task*
  - Exemplo: guia para criação de contas de usuário

Três ”níveis” de política de segurança

- Vários níveis de decisão gerencial
  - *Managers at all levels make choices that can affect policy, with the scope of the policy's applicability varying according to the scope of the manager's authority.... To differentiate various kinds of policy, this chapter categorizes them into three basic types...*
- Políticas de Programa organizacional
  - Cria um programa de segurança na organização
- Política de Tema Específico
  - Abordam áreas específicas de relevância para a organização
- Política de Sistema Específico
  - Aplicam-se a conjuntos particulares de sistemas

Seg.Info. e Gerenciamento de Riscos (cap.6)

- Risco é uma medida da ameaça a que uma entidade está sujeita por ocasião de um evento potencial
- Tipicamente, função do impacto do evento (caso ocorra) e da probabilidade de que o evento ocorra

* Muitas outras definições podem ser encontradas na literatura

Gerenciamento de Riscos no Cotidiano

- Usar cinto de segurança
- Carregar guarda-chuva
- Anotar os itens de uma lista de compras
- Escolher o caminho mais longo, porém sem trânsito
  - Questão do desvio padrão (p.d.f.)
- Fazer um plano de previdência

… no limite, tudo o que fazemos pode se enquadrar no arcabouço do gerenciamento de riscos…

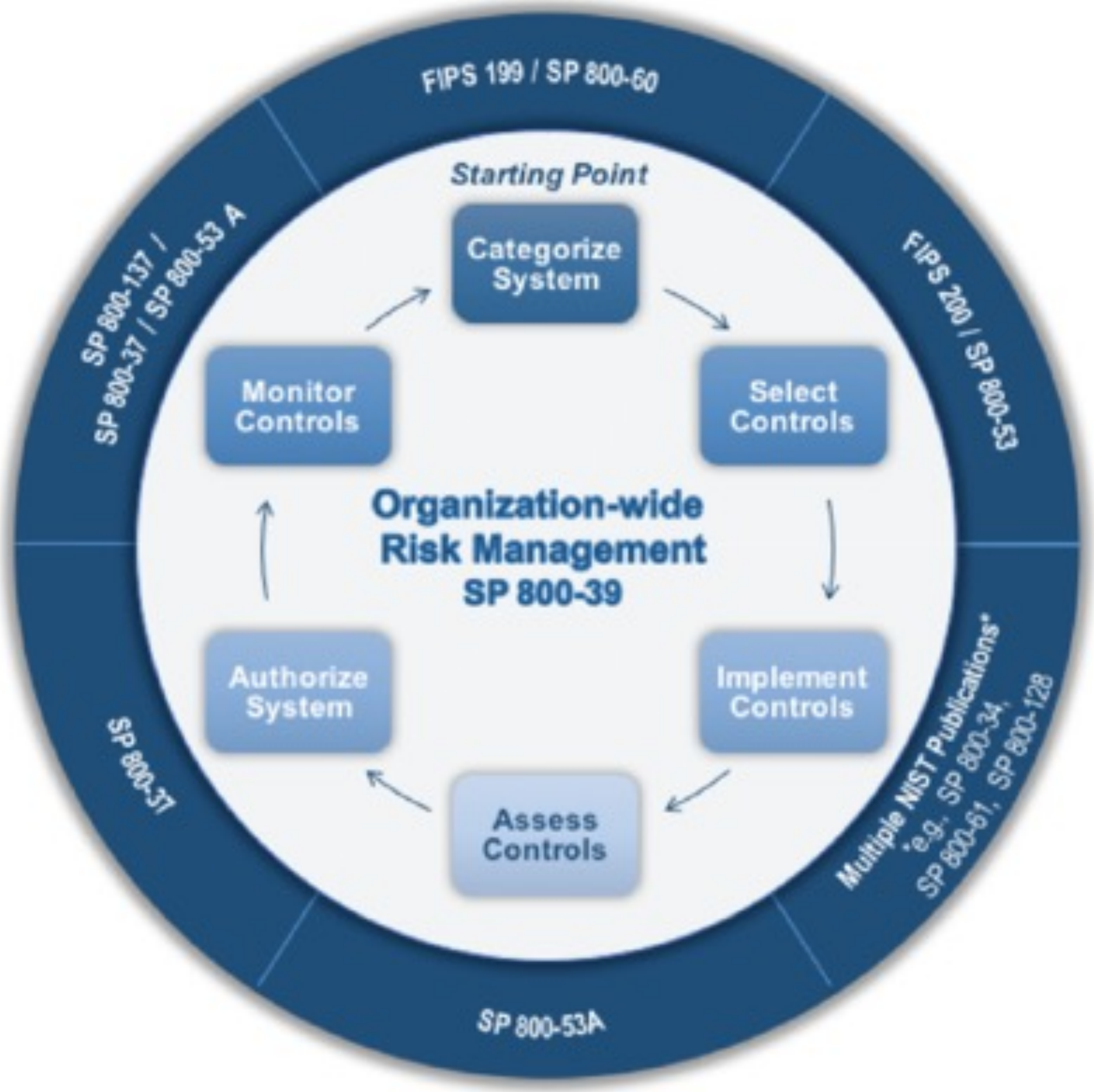
Riscos em Segurança da Informação

- Minimizar riscos relacionados à operação de sistemas
  - *With respect to information security, risk management is the process of* ***minimizing*** *risks to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of a system.*
- Quatro etapas
  - Enquadramento
  - Avaliação
  - Resposta
  - Monitoração

Framework de riscos de sistemas

- Gerenciamento de sistemas no nível de sistemas de informação
- Etapas
  - Categorização de Sistemas FIPS 199
  - Seleção de Controles de Segurança SP 800-53 e FIPS 200
  - Implementação de Controles de Segurança
  - Avaliação de Controles de Segurança SP 800-53
  - Autorização de Sistemas
  - Monitoramento de Controles de Segurança

The RMF promotes the concepts of near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes. The RMF also provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational systems supporting their core missions and business functions, and integrates information security into the enterprise architecture and system development life cycle (SDLC).


FIPS 199 / SP 800-60
Starting Point
Categorize System
FIPS 200 / SP 800-53
Select Controls
Organization-wide Risk Management SP 800-39
Implement Controls
Multiple NIST Publications* *e.g., SP 800-34, SP 800-61, SP 800-128
Assess Controls
SP 800-53A
Authorize System
SP 800-37
Monitor Controls
SP 800-137 / SP 800-37 / SP 800-53 A

Garantias (cap.7)

- Garantia da informação: grau de confiança na segurança da informação
  - *Information assurance is the degree of confidence one has that security measures protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities.*
- Categorias dos métodos e ferramentas de garantia
  - Projeto (e Implementação)
  - Operacional (subdividido em auditoria e monitoramento)

Suporte e operações de sistemas

- Refere-se a todos os aspectos envolvidos na execução de um sistema.
  - Inclui administração do sistema e tarefas externas (ex. ”manutenção da documentação”)
  - Não inclui ”projeto” ou ”planejamento”
- Exemplos de atividades/categorias
  - *User support;*
  - *Software support;*
  - *Configuration management;*
  - *Backups;*
  - *Media controls;*
  - *Documentation; and*
  - *Maintenance*

Segurança em suporte e operações

- Segurança deve ser considerada em todas as atividades de suporte e operações de sistemas
- Exemplos de problemas
  - Documentação imprecisa ou incompleta
  - Contas antigas de usuários
  - Conflitos de configuração de software
- Segurança está intimamente relacionada a S&O
- Pessoal de S&O deve ter conhecimento de Segurança
  - Exemplo: problemas no log in de um usuário podem indicar conta desabilitada após tentativa de ataque

Criptografia (cap.9)

- Área da Matemática dedicada à transformação de dados para segurança da informação
- Criptografia é uma ferramenta central em Segurança – mas pode (deve) ser combinada com outras
- Usos da criptografia
  - Proteção de dados armazenados
  - Proteção de dados em trânsito ”interno”
  - Proteção de dados em trânsito ”externo”
    - Possivelmente, a criptografia será a única ferramenta de proteção, neste caso

Aplicações da criptografia

- Cifração – proteção da confidencialidade
- Autenticação de Mensagem – proteção da integridade
- Assinatura Digital – autenticidade e irrefutabilidade
- Autenticação de usuário – identificação

Controles de segurança (cap. 10)

Controles de segurança são ferramentas que organizações podem implementar para aumentar a segurança de informações e sistemas

- *Access Control (AC)*
- *Awareness and Training (AT)*
- *Audit and Accountability (AU)*
- *Assessment, Authorization, and Monitoring (CA)*
- *Configuration Management (CM)*
- *Contingency Planning (CP)*
- *Identification and Authentication (IA)*
- *Individual Participation (IP)*
- *Incident Response (IR)*
- *Maintenance (MA)*
- *Media Protection (MP)*
- *Privacy Authorization (PA)*
- *Physical and Environmental Protection (PE)*
- *Planning (PL)*
- *Program Management (PM)*
- *Personnel Security (PS)*
- *Risk Assessment (RA)*
- *System and Services Acquisition (SA)*
- *System and Communications Protection (SC)*
- *System and Information Integrity (SI)*