Segurança da Informação

Professor: Raphael Machado

Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

1.0: Organização e Proposta do Curso

Sobre o Professor

- Atua na área de segurança desde 2003 (e com TIC desde o milênio passado=)
- Experiência de Pesquisa, Ensino, Governo, Defesa e Mercado
- Calouro aqui na UFF =)

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"
  - Informativo: transmissão de informações (ex.: histórico de ransomware)
  - Formativo: apresentação de conceitos (ex.: criptografia)

Organização do curso

- Total de 30 dias letivos
  - 20 aulas
  - 4 dias de prova
  - 6 dias livres para atividades, pesquisa, exercícios etc
- Estilo de aula
  - Aulas ”tradicionais” de 2 horas
  - Palestras (1 hora) seguida de aula curta relacionada (+1hora)
  - Aulas em laboratório (implementação / projeto / pesquisa)

Exemplos de palestras

- Beacon: Raphael (Luis Brandão?)
- Blockchain: Wilson (Alyson Lisboa?)
- Ataques Furtivos a NCS: Alan
- Proteção de Software: Lucila
- Propagação de Vírus: Sadoc (?)
- Criptografia na era "quântica" Franklin
- Estratégia Nacional de SI - Alan
- Avaliação da Conformidade - Kuster
- SHCDCiber – Raphael
- ICP-Brasil - Ruy
- ComDCiber - Cel Eiras
- Privacidade - Fabio
- GRC Davidson
- SIEM Victor Santos
- Auditoria de Labs Walderson
- Smart Cities. Rodolfo
- Pentest Magina
- Black Box - Teles
- Inovação e Propriedade intelectual: Leo
- **Mais algum que gostariam de sugerir???**

Avaliação

› Ajustada de acordo com o perfil da turma

› Provas

› Trabalho (Projeto) - opcional

Notas e Critério de Aprovação

- $M = 0.5 * P1 + 0.5 * P2 + 0.2 * T$
- T: Trabalho sobre problema prático de segurança
  - Temas apresentados nas primeiras aulas
- Prova de Substituição: substitui a menor nota entre P1 e P2 (inclusive, caso o aluno tenha faltado)
- Prova Final: substitui a média M

Material Didático - livros

Recursos

- Site
- WhatsApp
- Livros
- Estudos, reportagens, white papers
- Artigos científicos
- Normas
- Manuais
- Vídeos, Webinars, Podcasts
- ...passados a cada aula (ou após)

Survey – perfil da turma

- Qual o curso/formação?
- Qual o percentual concluído do curso?
- Qual a área desejada de atuação?
- Já está fazendo projeto final? Em qual tema?
- Pretende fazer mestrado/doutorado?
- Está interessado em bolsa de pesquisa?
- Deseja atuar na área de segurança?

Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

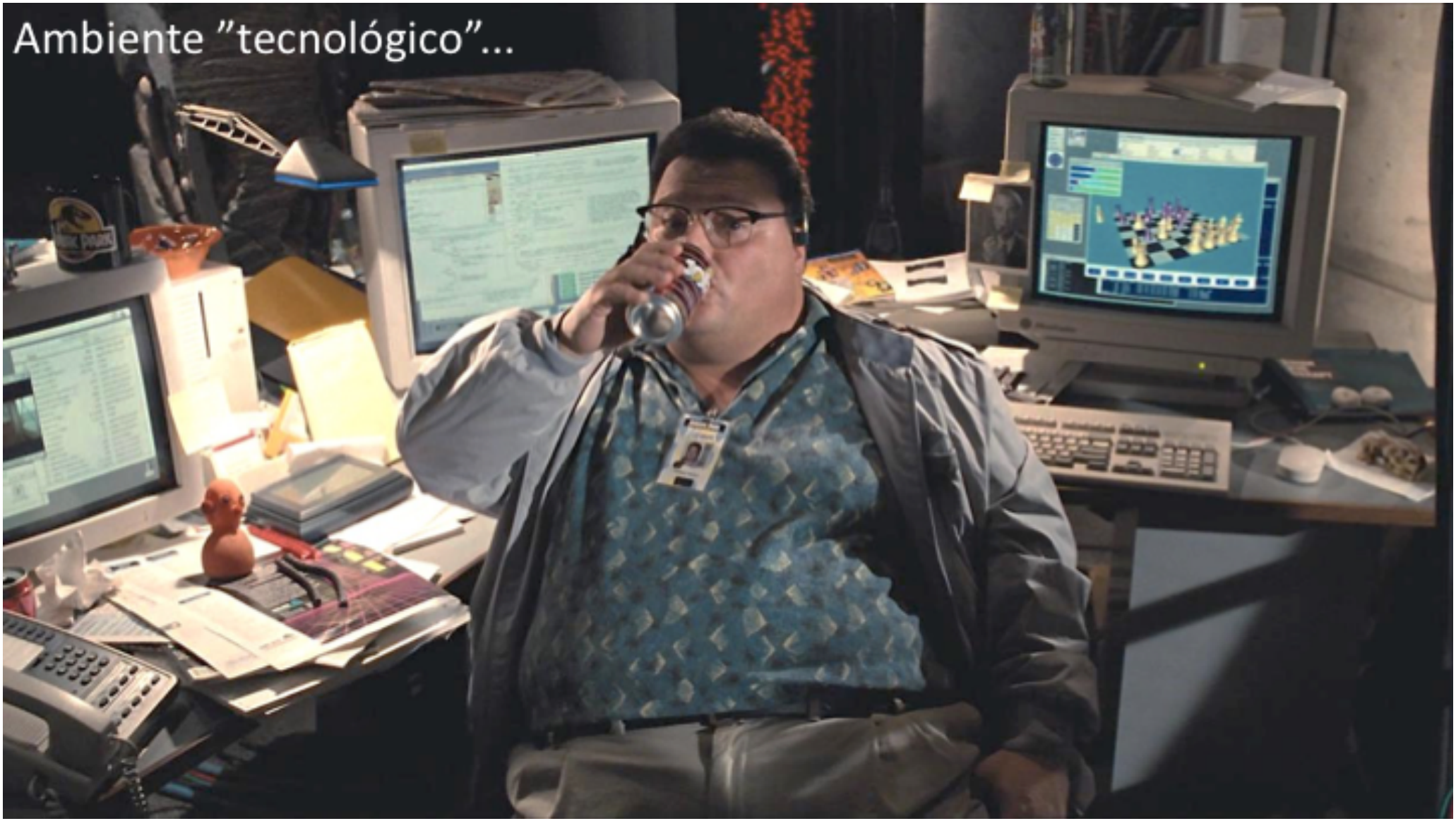
1.1: Segurança e Negócios

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


Imagem ”clássica” de um ambiente de negócios...


Ambiente ”tecnológico”...

Pergunta ”motivacional”

- Você já teve ”vazados” dados pessoais?
  - Número do cartão de crédito
  - Informações médicas
  - Casos de propaganda direcionada

Falácia dos dois "tipos" de organização

Existem dois "tipos" de organização:
as que sofreram um vazamento de informações
e as que ainda vão sofrer...

Falácia costuma ser estendida
a todo tipo de ciberataque


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

May 26, 2017

5

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.

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.

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.

BBC Sign in | News | Sport | Weather | Shop | Reel | Travel

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

Q&A: How does Sony breach affect customers?

3 May 2011 | Share

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.

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.

Business

PlayStation Network breach will cost Sony $171m

And counting

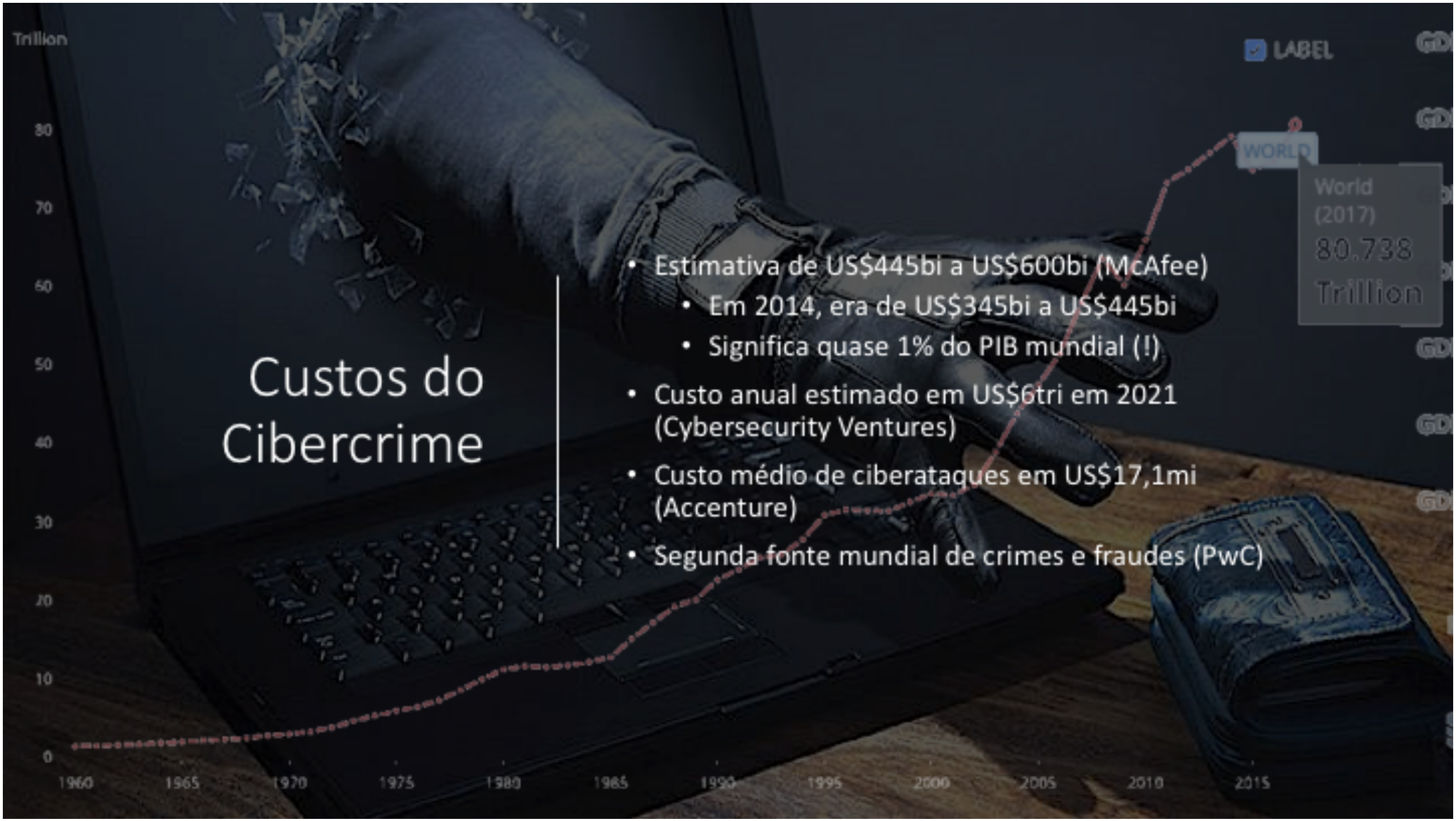
By Dan Goodin 24 May 2011 at 05:00 | 12 | SHARE

cnet

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.


Apple
Adobe
36,000,000
Citigroup
Court Ventures
200,000,000
Facebook
D&B, Allegrity
Evernote
Drupal
Kissinger Cables
Living Social
Massive American business hack
160,000,000
NASDAQ
National Security Agency
Scribd
SnapChat
Target
Twitter
UbiSoft
Vodafone
Yahoo Japan
Tianya
Ubuntu
2012
Blizzard
China Software Developer Network
Dropbox
Gamigo
Global Payments
KT Corp.
Last.fm
Medicaid
Office of the Texas Attorney General
Three Iranian banks
Yahoo Voices
Zappos
Maiores Vazamentos da História Recente
Betfair
Chinese gaming sites
Citigroup
Epsilon
Health Net - IBM
Honda Canada
NHS
Nexon Korea Corp
Sega
Sony PSN
Sony Pictures
State of Texas
Steam
Tricare
Stratfor
2010
&T
AvMed, Inc.
Triple-S Salud, Inc.
US Military



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?*

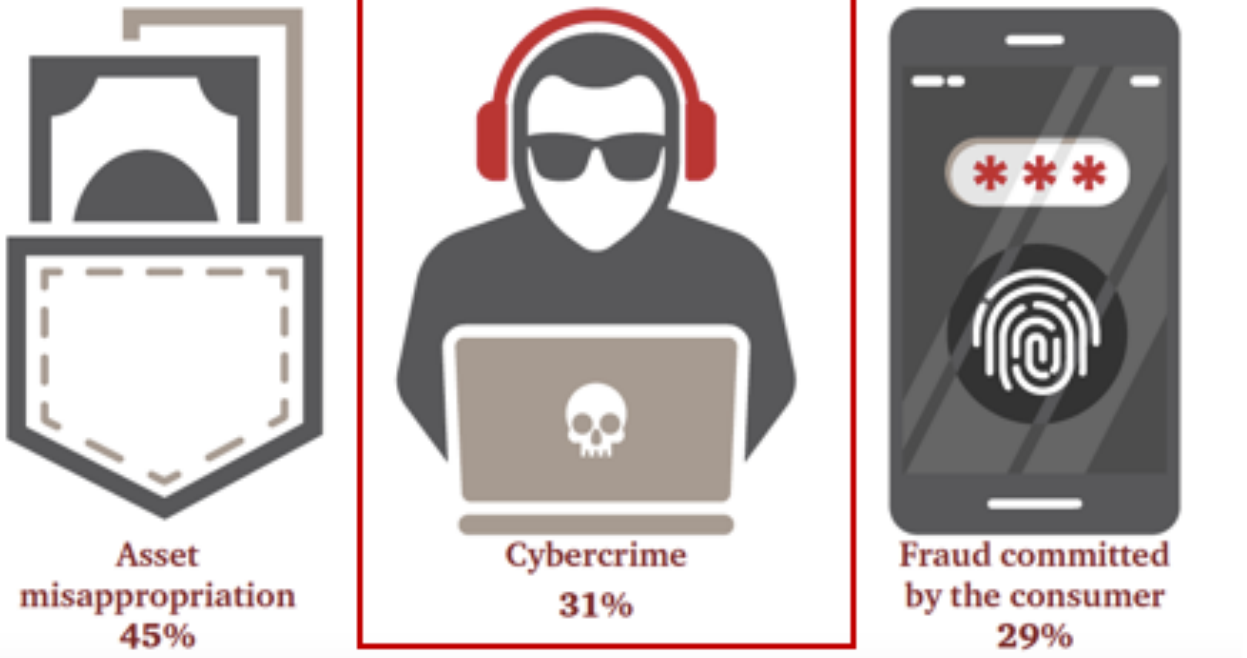
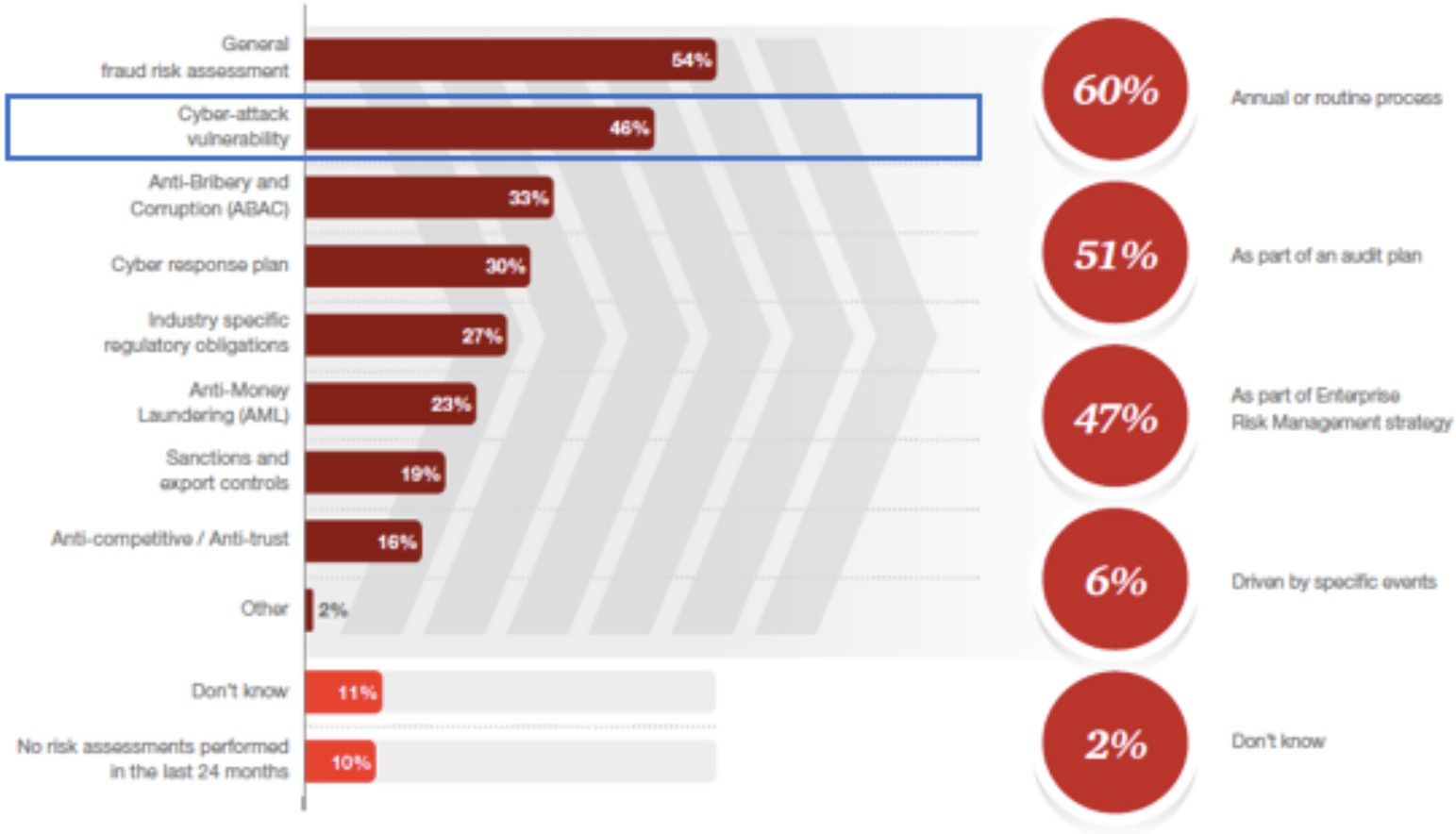


Exhibit 4: Less than half of all organisations have performed targeted risk assessments in the last 2 years



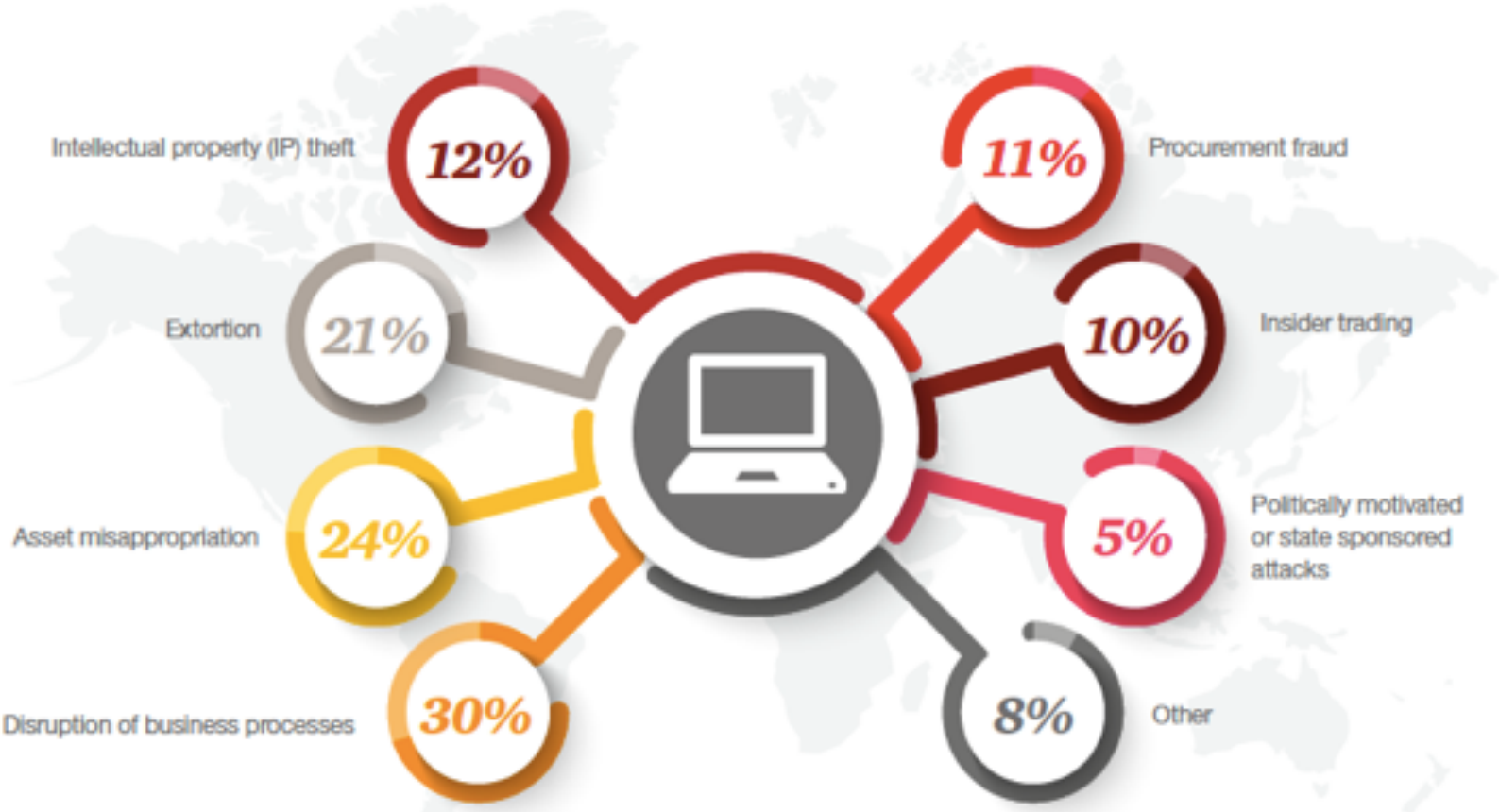
Q. In the last 24 months, has your organisation performed a risk assessment on any of the following areas?

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

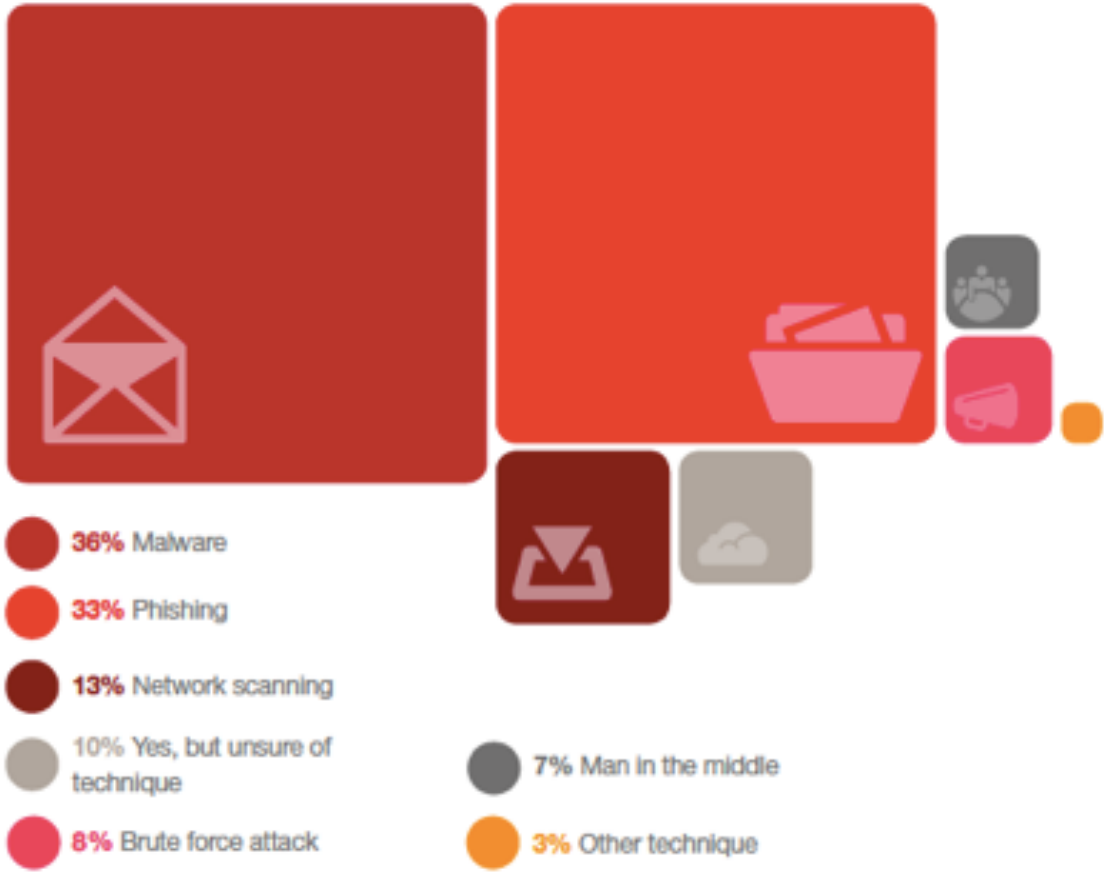
Exhibit 17: Types of fraud that organisations were a victim of through a cyber-attack



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.

pwc

Contents

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

How Boards of Directors Really Feel About Cyber Security Reports

Based on an Osterman Research survey

OSTERMAN RESEARCH

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

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

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

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

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

1. A complete list of vulnerabilities within the organization,

2. Details on data loss, and

3. Downtime caused by data breach incidents.

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

Riscos, riscos, riscos...

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

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

Ciber-segurança significa "negócios"

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

Based on our analysis, there are two critical success 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?*

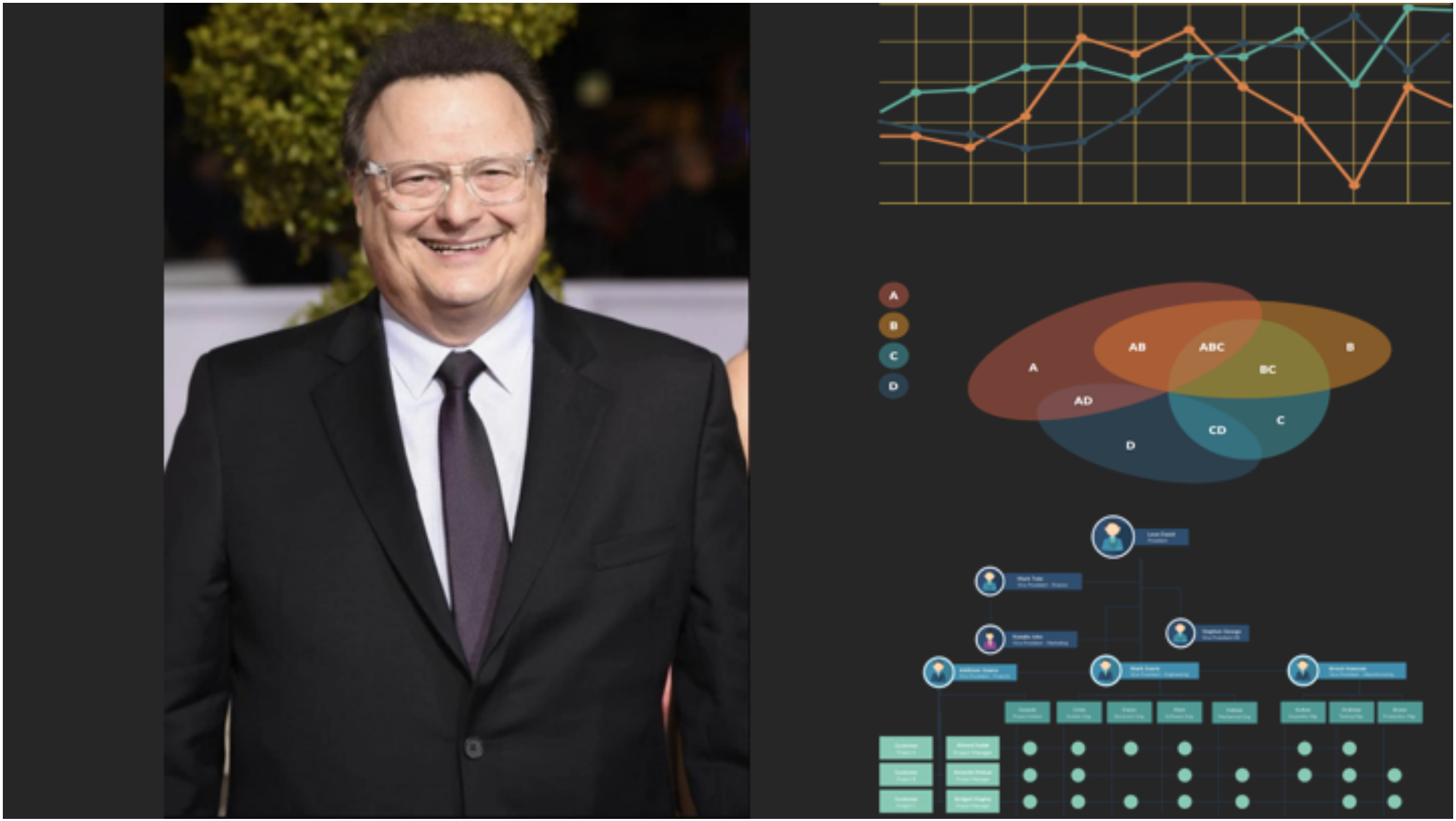
	All respondents		Large Companies (≥ $1B)		Small Companies (< $1B)	
	Current	2015	Current	2015	Current	2015
High engagement and level of understanding by the board	33%	28%	37%	32%	26%	24%
Medium engagement and level of understanding by the board	37%	32%	37%	33%	39%	33%
Low engagement and level of understanding 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%

Objetivo, então, é...


COMMUNICATION
PROTECTION
FIREWALL
MEASURES
RULES
DOS
SECURE
SERVICES
WEB
INTERNET
INFORMATION
LAYER
BROWSER
COMPUTER
SECURITY
TOKEN
ANTIVIRUS
FRAUD
DATA
MALICIOUS
TRANSFER
DDOS
INTRUSION
ATTACKS
CRYPTOGRAPHY
CONTROL
ENCRYPTION
PROTOCOL
NETWORK
VPN
ACCESS


A
B
C
D
AB
ABC
B
A
BC
AD
C
CD
D

Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

1.2: Segurança e Sociedade

Impacto da (falta de) segurança na Sociedade

- Vazamento de informações sensíveis
- Perdas Financeiras
- Indisponibilidade e falhas de serviços relevantes
- Segurança/Defesa Nacional
- Exemplos de Ataques (e ataques e ataques e...)

Vazamentos de Informações: Impactos a Privacidade e Confidencialidade...

BUSINESS NEWS

Yahoo says all three billion accounts hacked in 2013 data theft

Jonathan Stempel, Jim Finkle

5 MIN READ

(Reuters) - Yahoo on Tuesday said that all 3 billion
2013 data theft, tripling its earlier estimate of the siz
in a disclosure that attorneys said sharply increased
owner, Verizon Communications Inc (VZ.N).

44,073 views | Sep 7, 2017, 10:42pm

Equifax Data Breach Impacts 143 Million Americans

Lee Mathews Contributor
Security
Observing, wondering, and writing about tech. Generally in that order.

34,958 views | May 31, 2015, 07:57pm

Heartland Payment Systems Suffers Data Breach

Dave Lewis Contributor
ches and enterprise security.

Data Breach Nears $300

f the 2013 Target Data Breach Nears $300

The New York Ti

Marriott Data Breach Is Tr to Chinese Hackers as U.S. Readies Crackdown on Beij

From the first revelation that the Marriott's computer systems had been breached, there was widespread suspicion that the hacking was part of a broad spy campaign to amass Americans' personal data. Scott Olson/Getty Images

By David E. Sanger, Nicole Perlroth, Glenn Thrush and Alan Rappeport

Dec. 11, 2018

NEWS

Adult Friend Finder confirms data breach 3.5 million records exposed

Hacker claiming responsibility has posted 3,528,458 records online

61,495 views | May 21, 2014, 12:30pm

eBay Suffers Massive Security Breach, All Users Must Change Their Passwords

Gordon Kelly Senior Contributor
I write about technology's biggest companies

TWEET THIS

- all eBay users to urgently change their passwords
- hackers gained access to information including eBay customers' names, their encrypted passwords, email, registered addresses, phone numbers and date of birth

TECHNOLOGY NEWS

Sony PlayStation suffers massive data breach

Liana B. Baker, Jim Finkle

5 MIN READ

Ransomware: impactos a financeiros...

Ataques DDoS: Impactos à disponibilidade...

ZDNet

MUST READ: Microsoft: You're being less toxic online but bullying, harassment still rife

New world record DDoS attack hits 1.7Tbps days after landmark GitHub outage

Memcached denial-of-service attacks are getting bigger by the day, according to new analysis.

By Liam Tung | March 6, 2018

Hacker News users report the following

- Twitter
- Etsy
- Github
- Soundcloud
- Spotify
- Heroku
- Pagerduty
- Shopify
- Intercom

PCW

NEWS REVIEWS HOW-TO VIDEO DEALS BUSINESS LAPTOPS SMARTPHONES HARDWARE SECURITY SOFTWARE GADGETS

Ads by Google DDoS Attack DDoS Spotify A Security Guard

Home / Internet

UPDATED

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more

The sound of silence.

By Brad Chacos

Senior Editor, PCWorld | OCT 21, 2016 3:34 PM PT

WikiLeaks

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

How a cyber attack transformed Estonia

By Damien McGuinness
BBC News, Tallinn, Estonia

27 April 2017 Share

ake news - exactly 10 years ago Estonia e under attack from this modern form of

It is an event that still shapes the country today.

Head bowed, one fist clenched and wearing a World War Two Red Army uniform, the Bronze Soldier stands solemnly in a quiet corner of a cemetery on the edge of the Estonian capital Tallinn.

Flowers have been laid recently at his feet. It is a peaceful and dignified scene. But in April 2007 a row over this statue sparked the first known cyber-attack on an entire country.

The attack showed how easily a hostile state can exploit potential tensions within another society. But it has also helped make Estonia a cyber security hotshot today.

From outrage to outage

Unveiled by the Soviet authorities in 1947, the Bronze Soldier was originally called "Monument to the Liberators of Tallinn". For Russian speakers in Estonia he represents the USSR's victory over Nazism.

But for ethnic Estonians, Red Army soldiers were not liberators. They are seen as occupiers, and the Bronze Solider is a painful symbol of half a century of Soviet oppression.

In 2007 the Estonian government decided to move the Bronze Soldier from the centre of Tallinn to a military cemetery on the outskirts of the city.

The decision sparked outrage in Russian-language media and Russian speakers took to the streets. Protests were exacerbated by false Russian news reports claiming that the statue, and nearby Soviet war graves, were being destroyed.

Explosão na Sibéria (1982)

Cyberwar

War in the fifth d

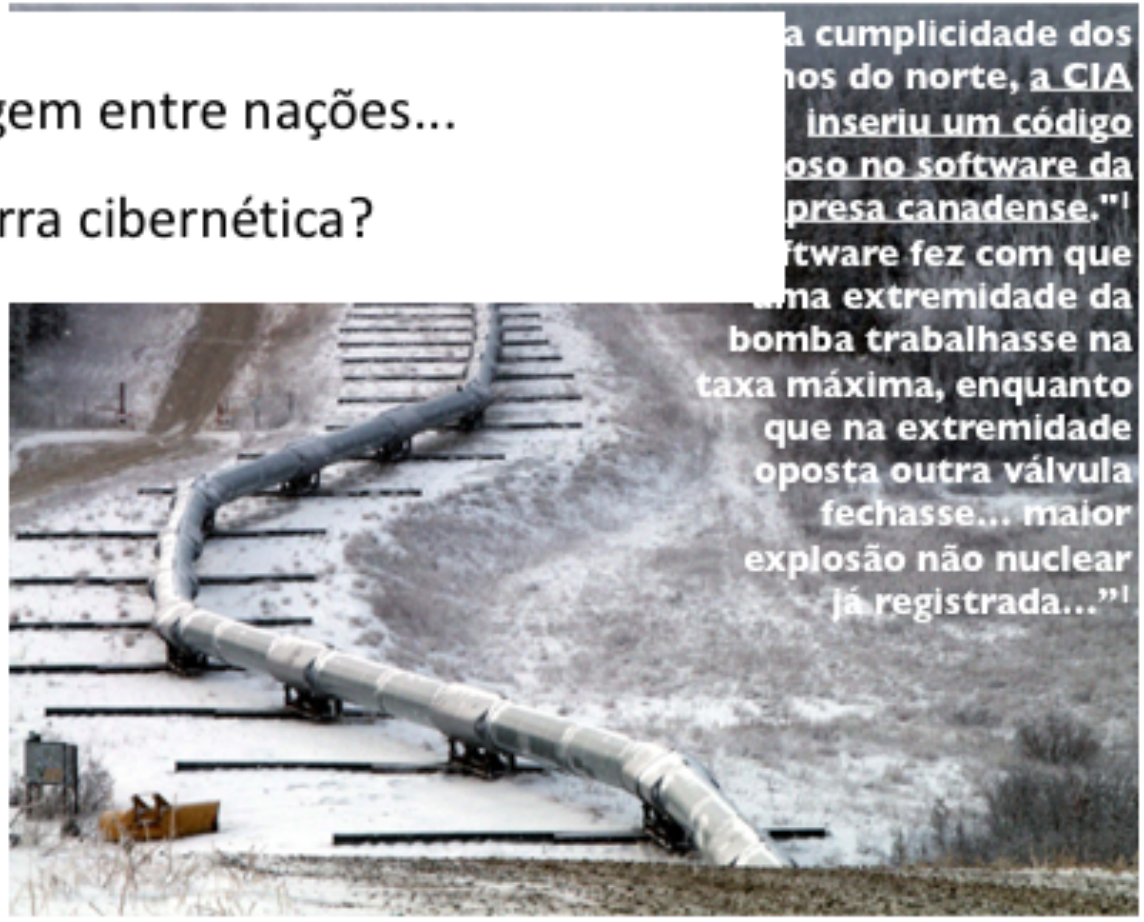
Are the mouse and keyboard the new

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."

Sabotagem entre nações...

Guerra cibernética?



Ataque a Fábrica na Síria (Orchand 2007)

ANNALS OF WAR
SEPTEMBER 17, 2012 ISSUE

THE SILENT STRIKE

How Israel bombed a Syrian nu

BY DAVID MAKOVSKY

Guerra cibernética?

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.

"...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]

Sabotagem ao Programa Nuclear Iraniano (2010)

Cyberwar

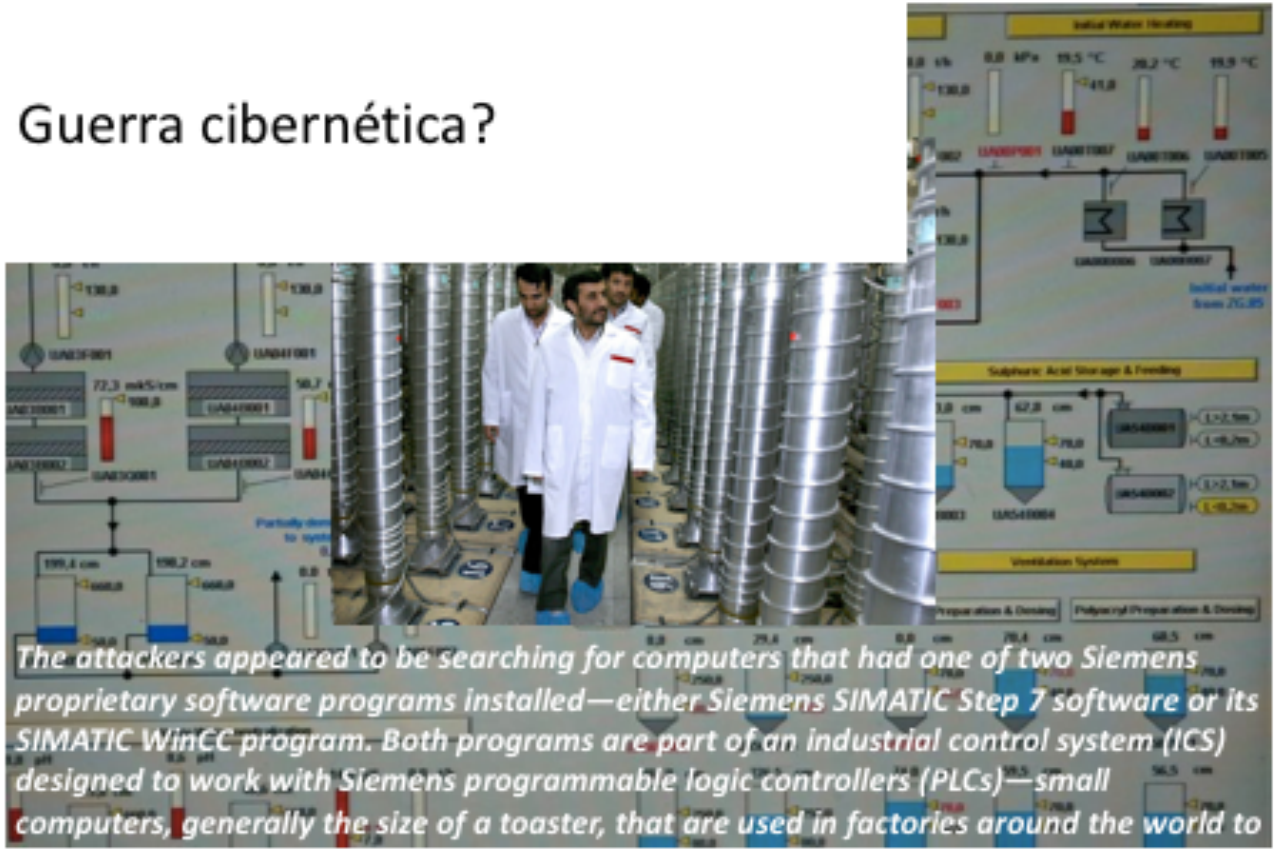
The meaning of Stuxnet

A sophisticated "cyber-missile" highlights t

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.

Guerra cibernética?



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

Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

1.3: Segurança e Tecnologia

Aspectos Técnicos de Segurança da Informação

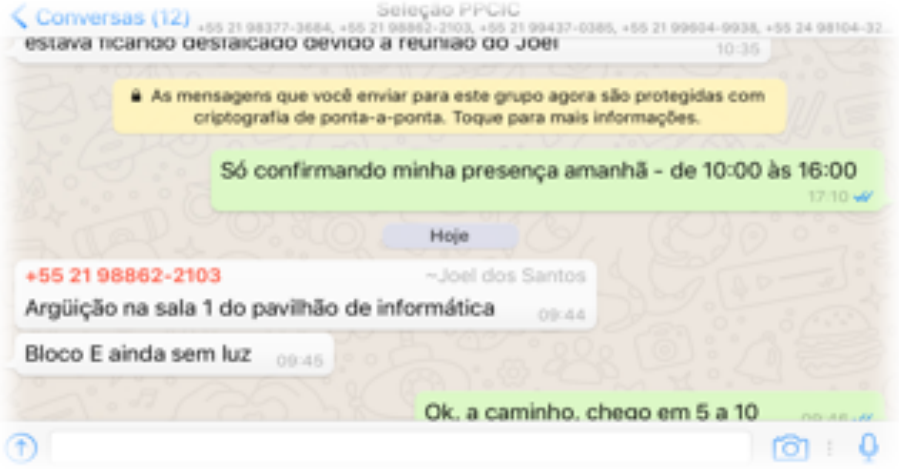
- Ferramentas e métodos para segurança
  - Criptografia
  - Arquiteturas e Protocolos
  - Autenticação
  - Controle de Acesso
  - IDS/IPS/FW/WAF/SIEM/Antivírus
  - Desenvolvimento Seguro e Segurança by Design
  - ...

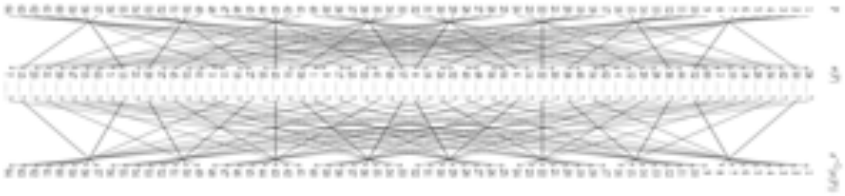
...basicamente, a parte ”didática” que vamos estudar nos livros

Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

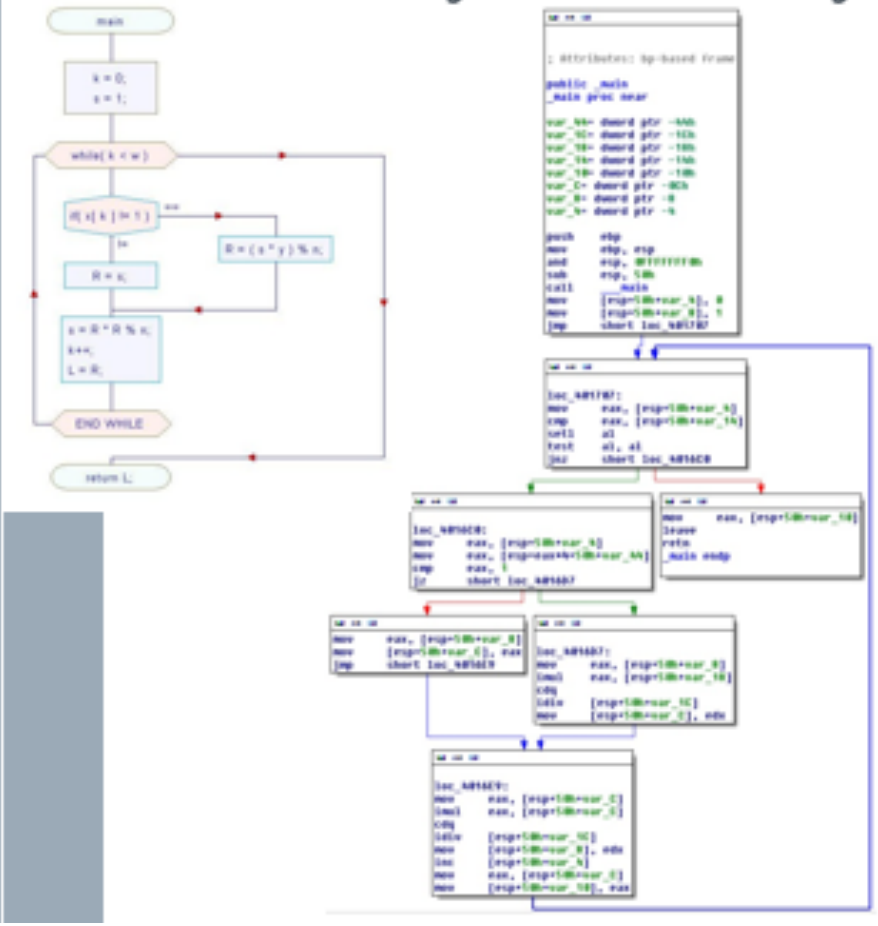
1.4: Segurança e Ciência

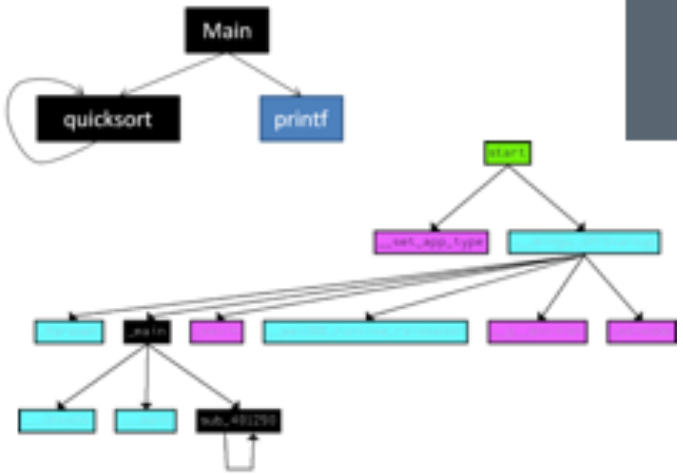
Criptografia, protocolos e arquiteturas de segurança

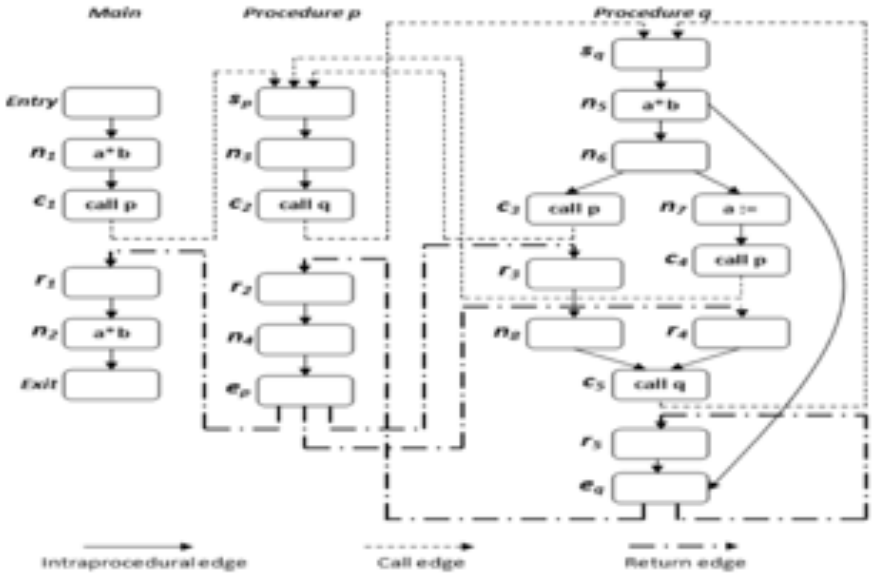




Análise de software, verificação/validação/testes



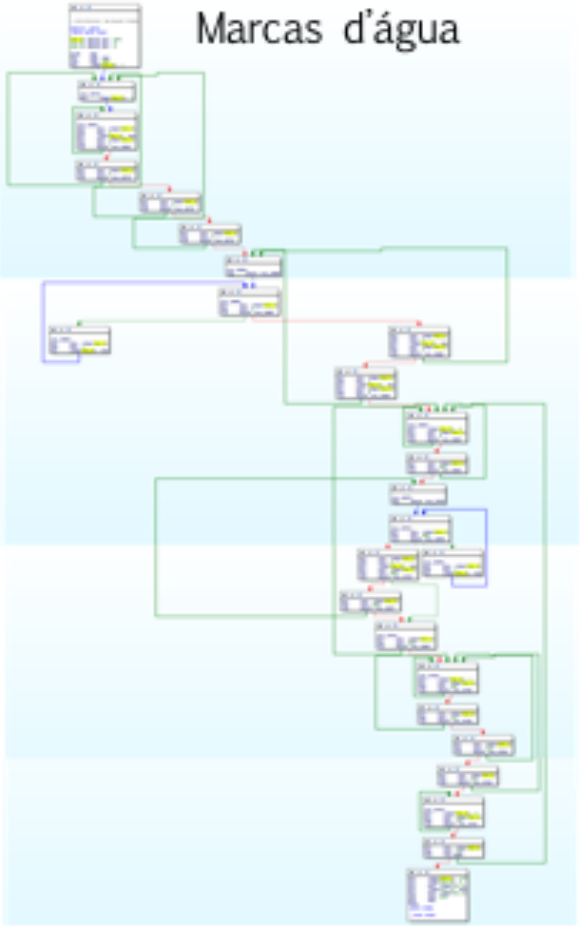




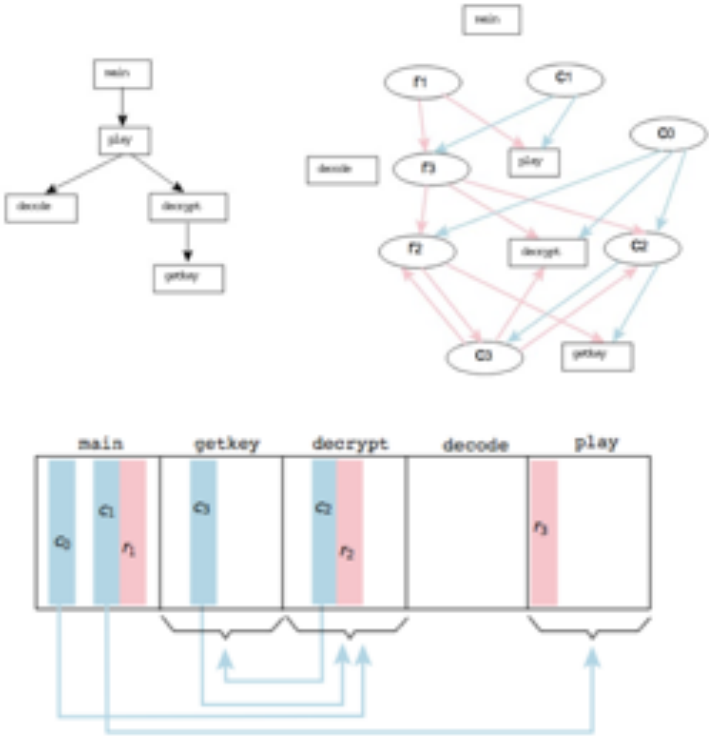
Proteção de software

Ofuscação

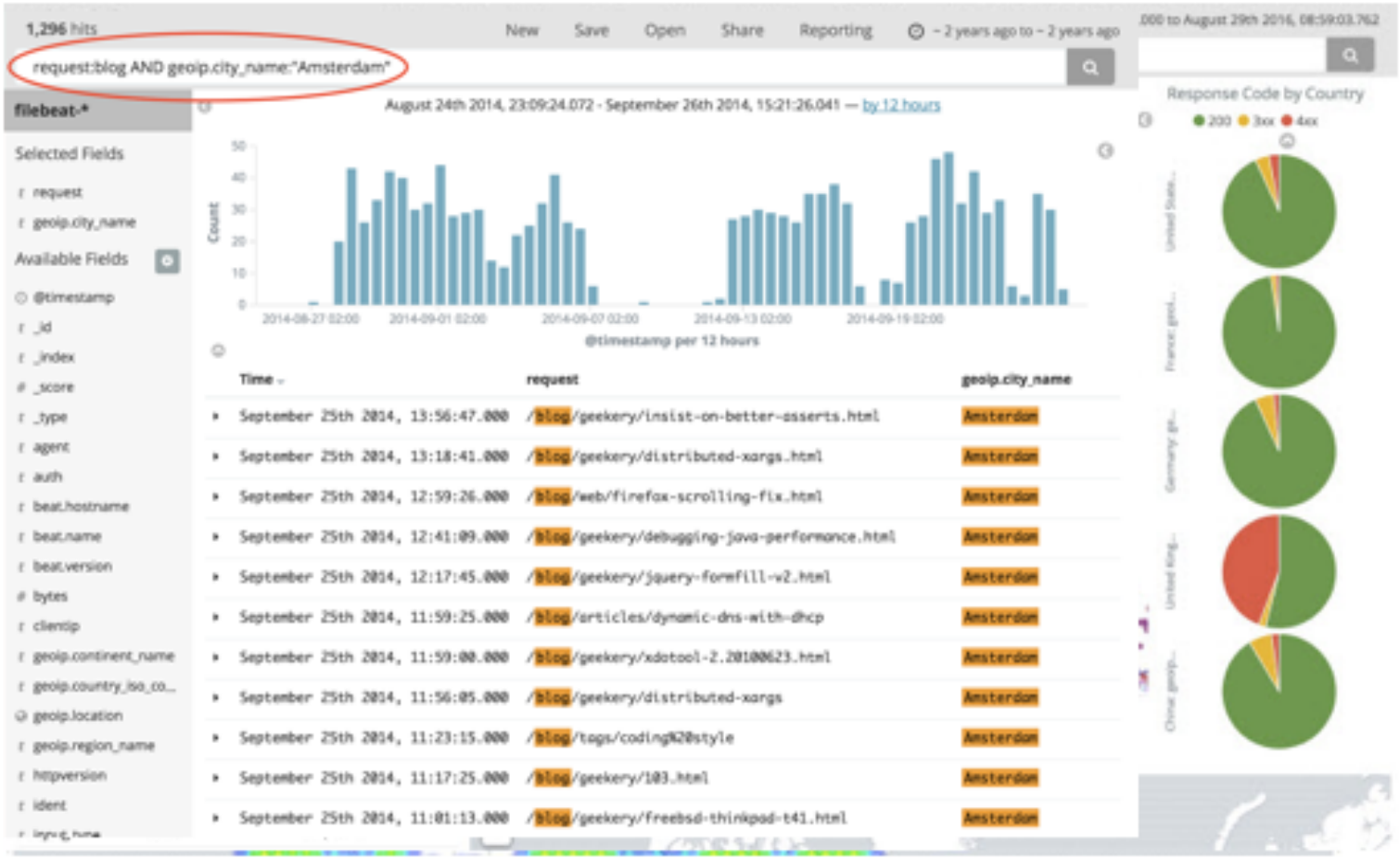
Marcas d'água



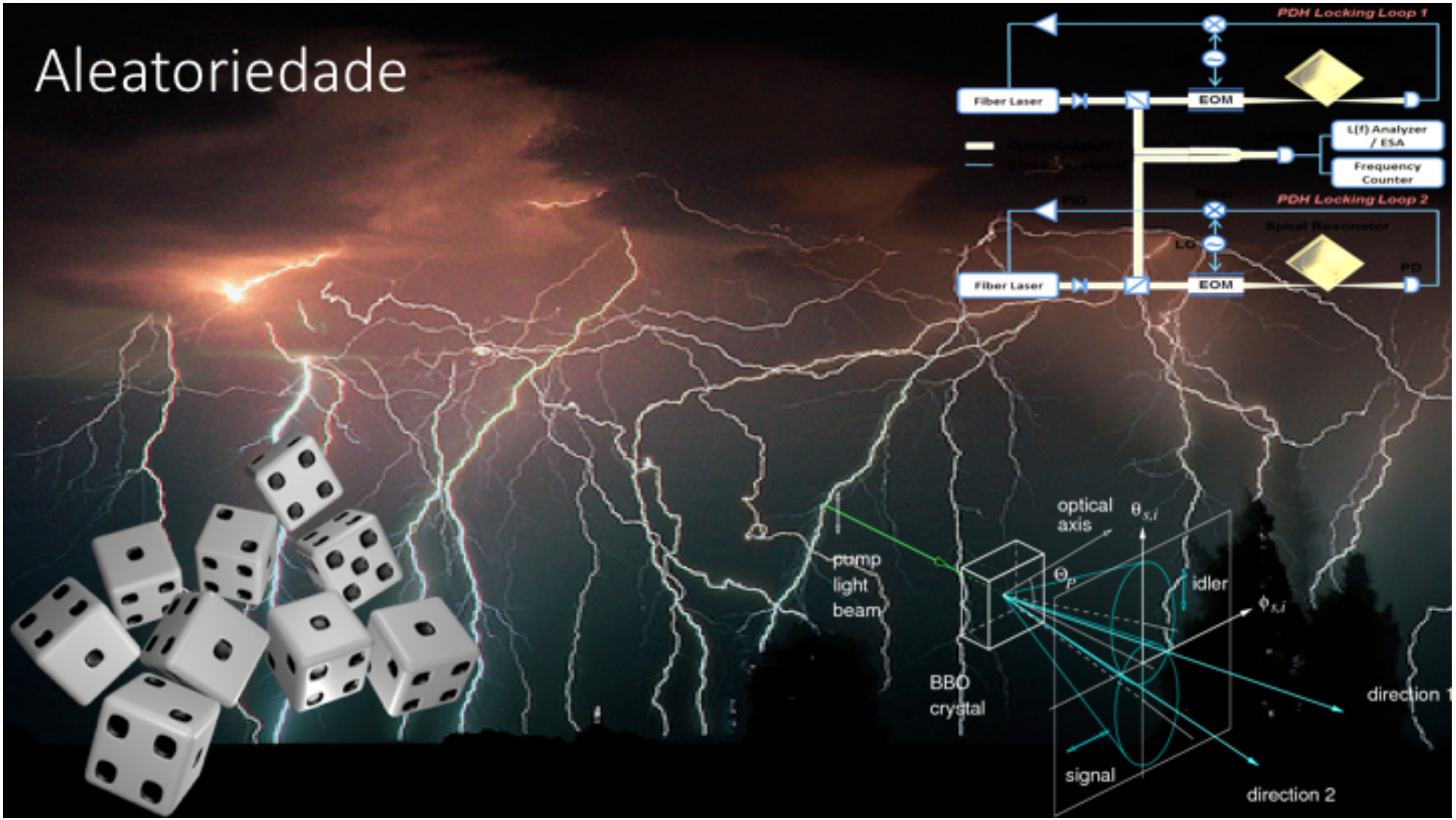
Incorruptibilidade



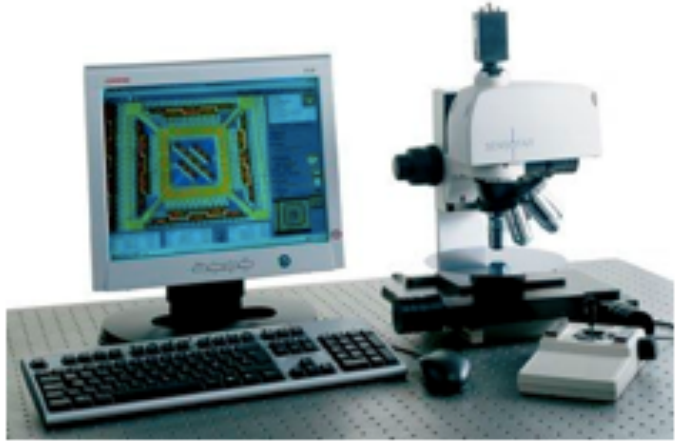
Testes de Segurança Black-Box/comportamental

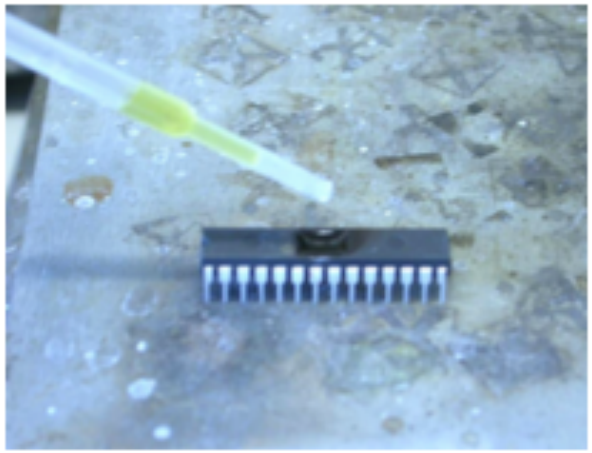


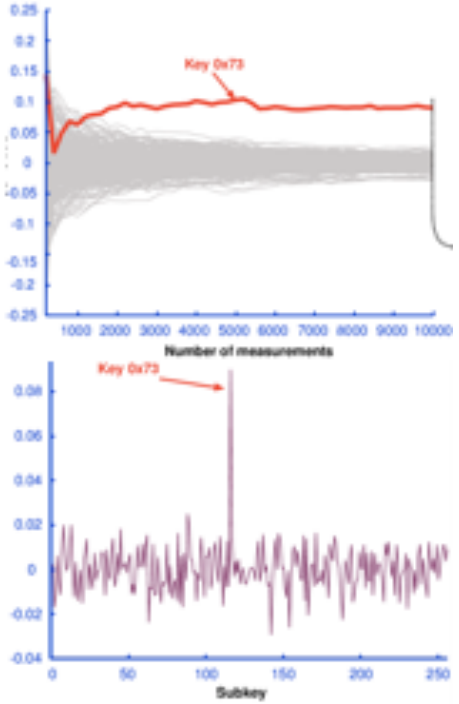
Aleatoriedade

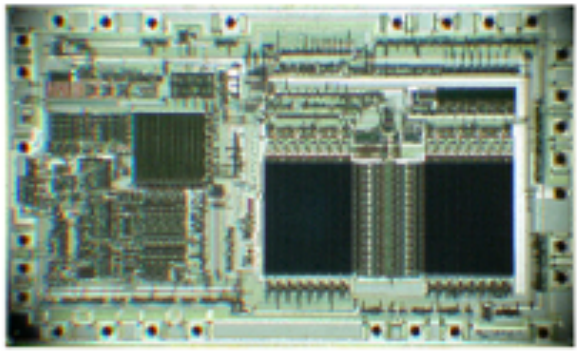


Segurança da Hardware

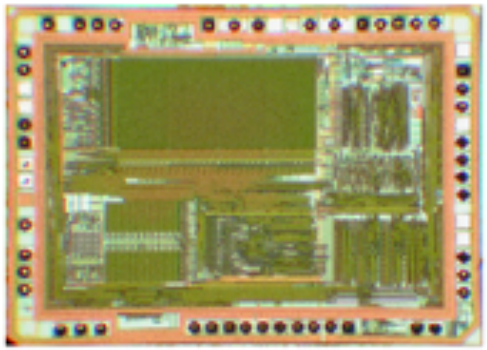




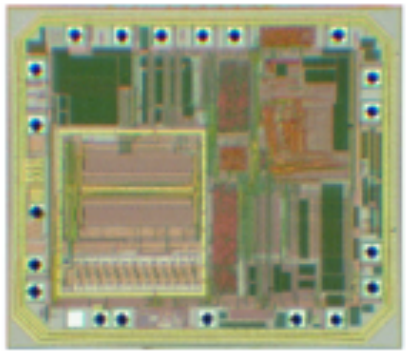




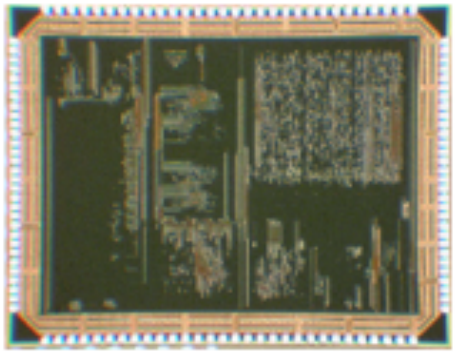
MC68HC705P6A, 1 µm



PIC16F77, 0.5 µm



MSP430F1121A, 0.35 µm



XAP Springbank, 0.18 µm

Gestão de Riscos

Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

1.5: Visão Geral do Conteúdo do Curso

Motivação e Conceitos Básicos

- Por que estudar segurança
- Perdas com ataques de segurança
- Exemplos de ataques de segurança
- Padrões, conformidade e segurança
- Vulnerabilidade, ameaça, risco etc.
- Objetivos de segurança
- Serviços e mecanismos de segurança

Exemplos de Ataques (e Atacantes)

- Estados-nação
- Criminosos
- Ativistas
- Atacantes "acima de qualquer suspeita"...

Conceitos Básicos

- Segurança em Redes
- Segurança de Aplicações
- Os sete "domínios" da segurança (livro)
- Segurança Corporativa
- Segurança como questão de Estado

Criptografia

- Histórico e Conceitos Básicos
- Primitivas e Algoritmos Criptográficos
- Protocolos Criptográficos e Arquitetura de Segurança
- Aleatoriedade e Números Aleatórios

Autenticação de Usuário

- Meios de autenticação
- Autenticação baseada em senha
- Autenticação baseada em token
- Autenticação biométrica
- Autenticação de usuário remoto

Controle de Acesso

- Princípios de controle de acesso
- Sujeitos, objetos e direitos de acesso
- Controle de acesso discricionário
- Controle de acesso mandatório
- Controle de acesso baseado em papéis

Padrões e Conformidade

- Padronização Internacional
- Avaliação da Conformidade
- Sistemas de Gestão de Segurança da Informação
- Gerenciamento de Riscos
- Segurança de Software
- Validação de Módulos Criptográficos

Ameaças

- Vulnerabilidades de software
- Software Malicioso (cap.6 Stallings, cap.21Crypto)
- Ataques DDoS (cap.7 Stallings)
- Ataques a aplicações web

Ferramentas de Defesa

- Segurança de Redes, Endpoint e Usuários
- Firewall +Cap.22-crypto
- IDS +cap21-crypto
- SIEM

Proteção de Software

- Análise de Software e Engenharia Reversa
- Ofuscação de Código
- Incorruptibilidade de Software
- Marcas d'água

Tópicos Selecionados

- Testes de Penetração
- Análise de Malware
- Segurança de sistemas industriais
- Computação Forense
- Ataques Side-Channel
- Blockchain
- ...

Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

1.6: Projeto SICCCiber