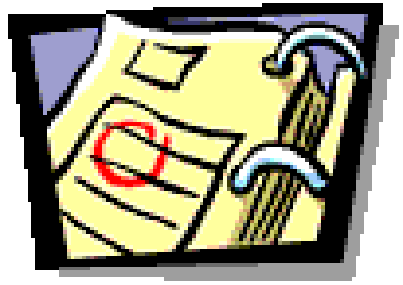
Desafios da Segurança na Internet das coisas

GILBERTO SUDRÉ
TECNOLOGIA

gilberto@sudre.com.br

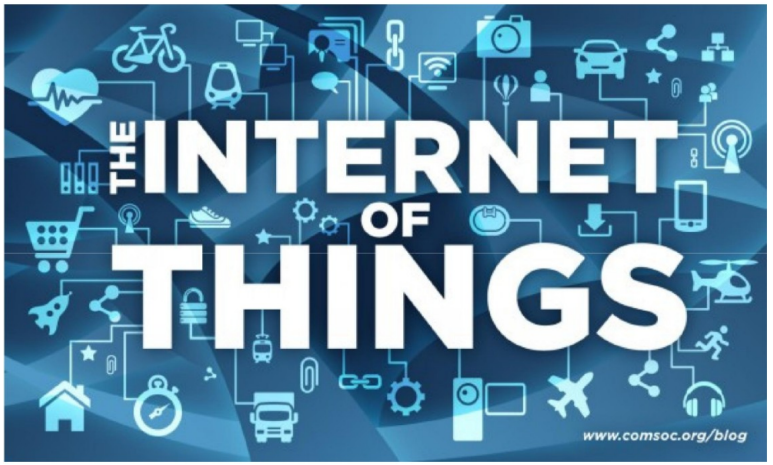
http://gilberto.sudre.com.br

Agenda

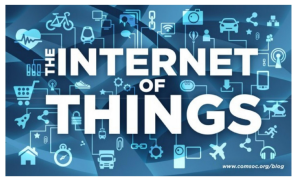


- A Internet das Coisas
- Principais desafios
- Riscos
- Vulnerabilidades
- Ataques
- Defesas
- Mais informações

A Internet das Coisas



A Internet das Coisas

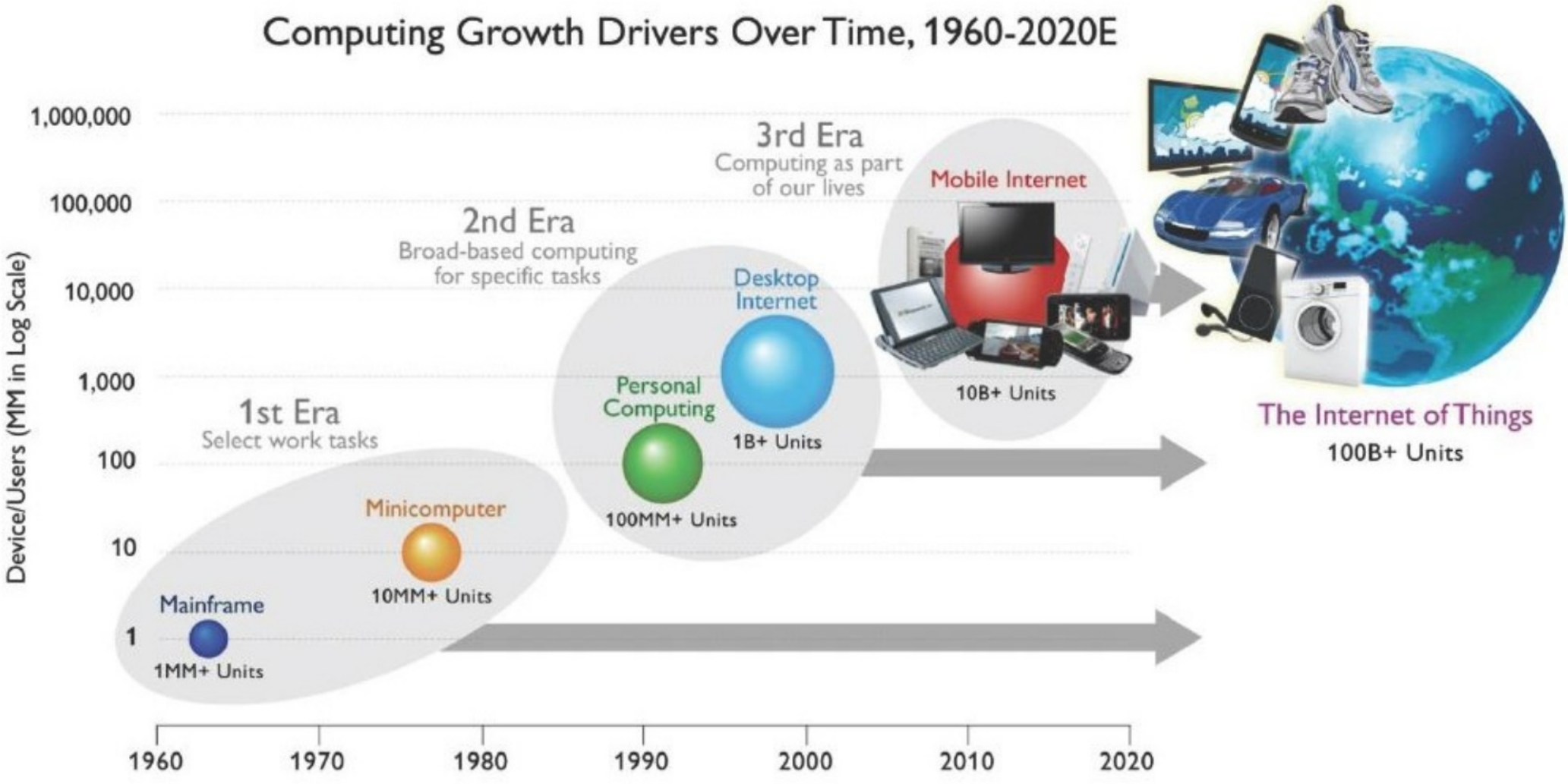


- **Gartner**
  - “A “Internet das coisas” (IoT) é definida como a rede de objetos físicos que contém tecnologia embutida para se comunicar e sentir ou interagir com o ambiente externo ou com estados internos. ”

- **Fórum Brasileiro de IoT**
  - “IoT = Nova infraestrutura que integra a Internet convencional com os objetos permitindo a comunicação entre o mundo virtual e o mundo real”

A Internet das Coisas

Evolução



Source: Adapted from Morgan Stanley, Nov 2009

A Internet das Coisas

Números

Google

9 Bilhões de *IoT devices* em 2018

McKinsey&Company

3,7 Tri USD de valor em 2016

25 Bilhões de *devices* conectados em 2020

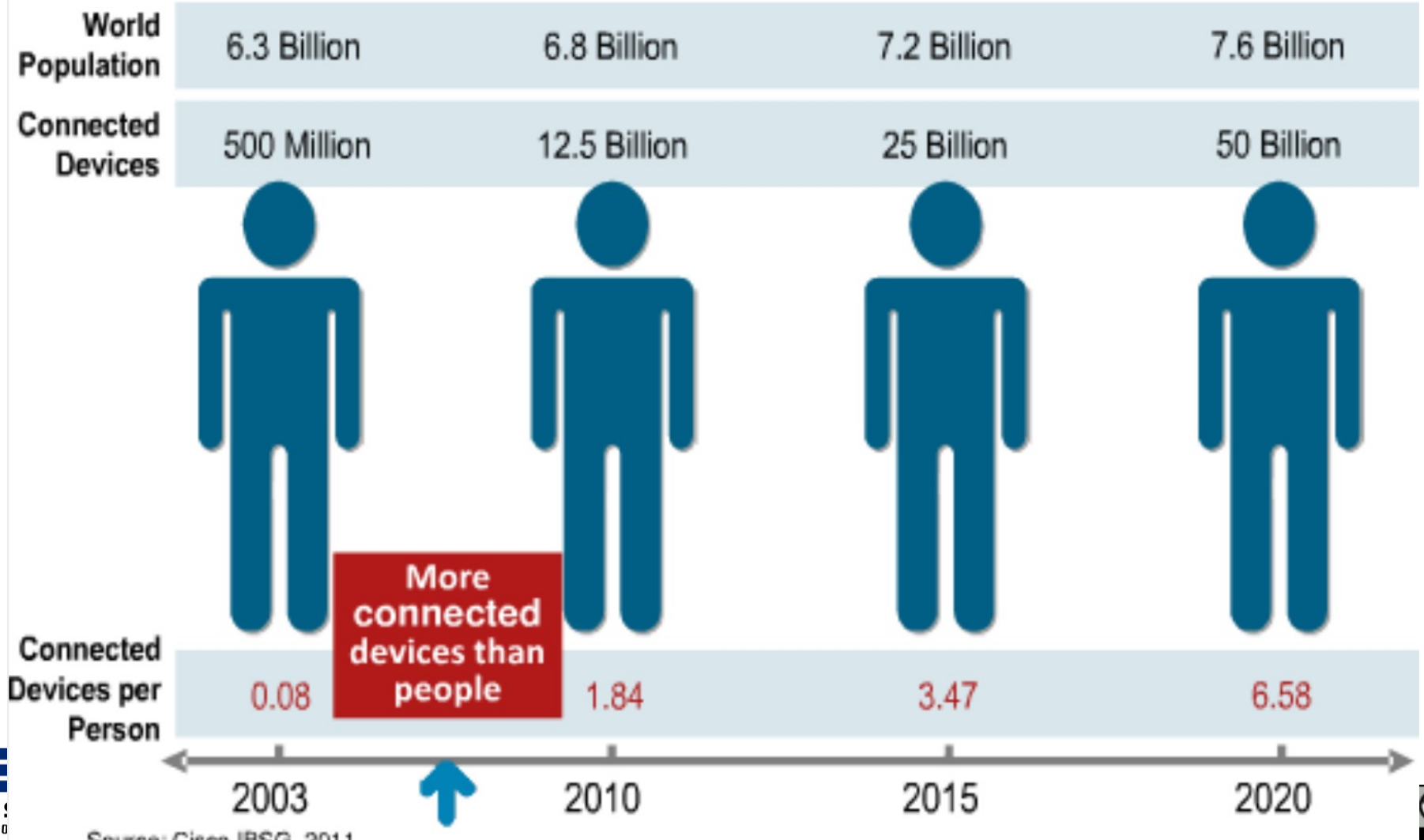
50 Bilhões *smart objects* em 2020

QUALCOMM

CISCO

A Internet das Coisas

Já é uma realidade



Source: Cisco IBSG, 2011

A Internet das Coisas

Onde está a IoT?

Principais Pilares da IoT

- Miniaturização e Nanotecnologia

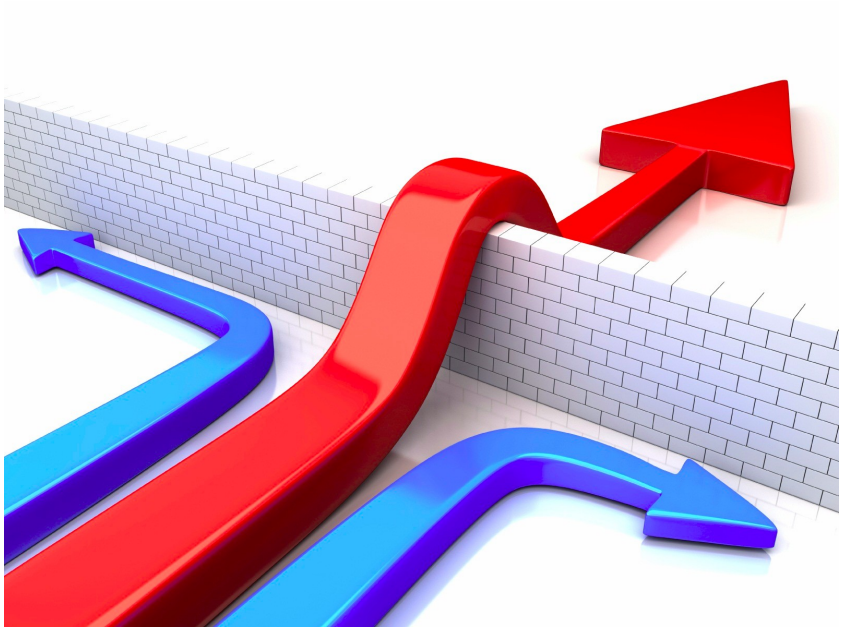
- Objetos: Sensores e Atuadores
  - Roupas, pulseiras, carros, caixas eletrônicos, máquinas industriais, equipamentos médicos, etc.

- Conectividade: tecnologias sem fio

Características das "Coisas"

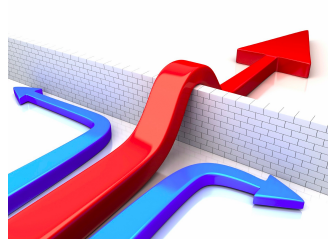
- Existem no mundo real e virtual
- Se comportam de maneira autônoma
- Conectividade (sem fio)
- Interatividade
- Dinamicidade: qualquer momento, lugar ou maneira

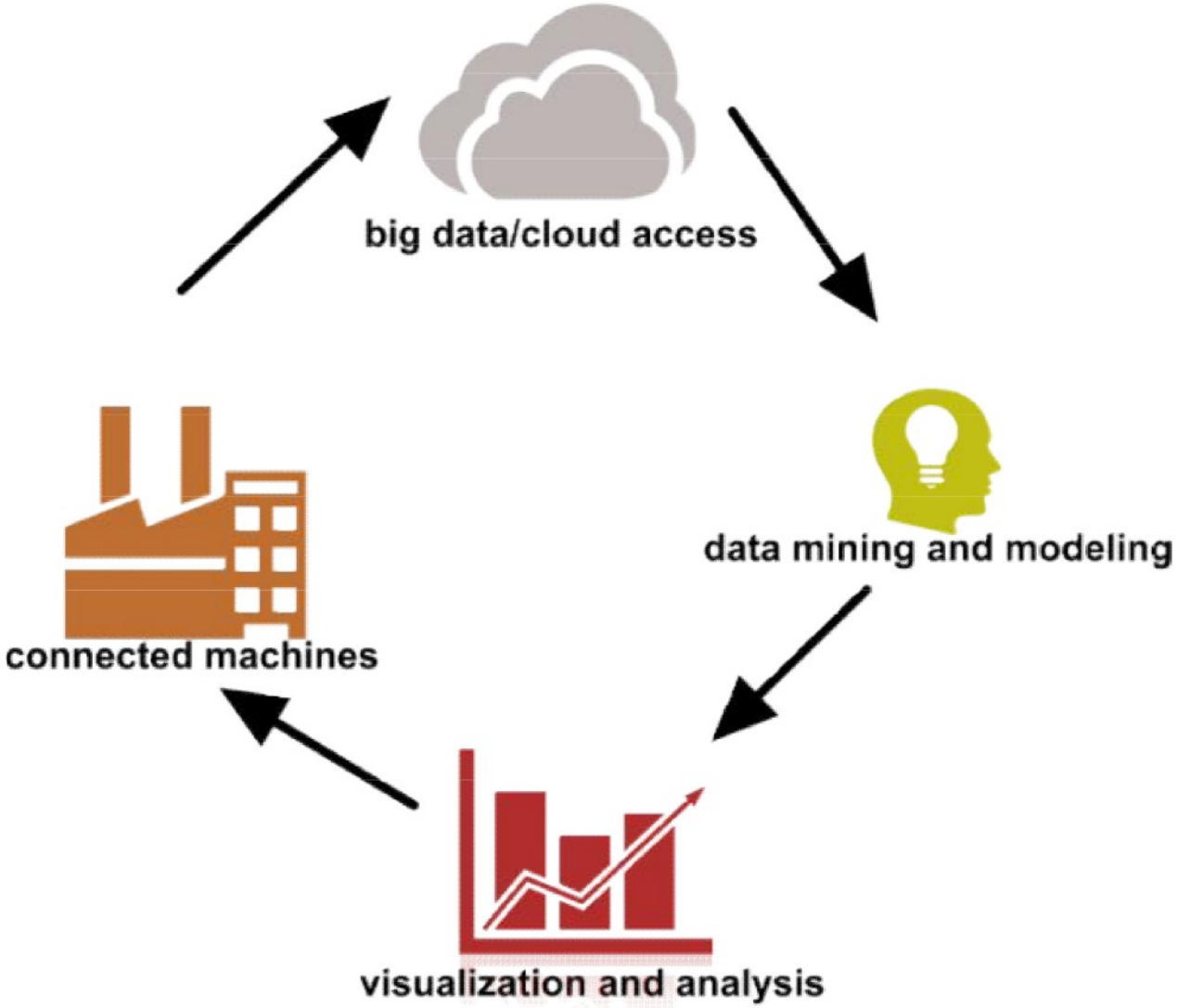
Principais Desafios da IoT



Principais Desafios da IoT

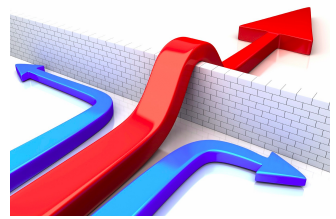
Excesso de informações





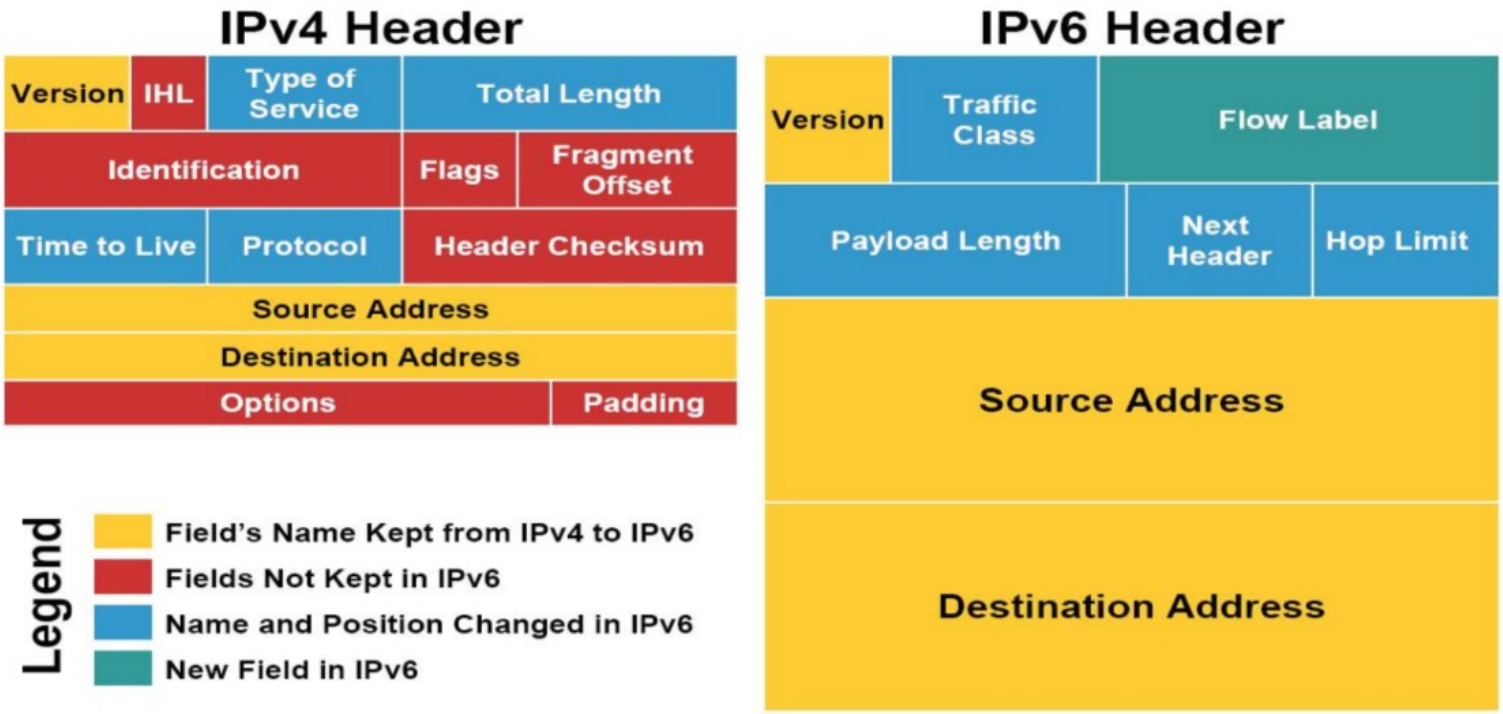
Principais Desafios da IoT

Implantação do IPv6



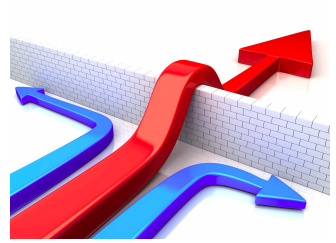
	IPv4	IPv6
Standard since Developed by	1974 IETF	1998 IETF
Length in bits Amount of addresses	32 2^{32} = 4,294,967,296	128 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456
Address format	Dotted decimal 192.168.100.1	Hexadecimal Notation
Dynamic addressing	DHCP	
IPSec	Optional	
Header length	Variable	
Minimal packet size	576 bytes (fragmente	
Header checksum	Yes	
Header options	Yes	
Flow	No	

IPv4 and IPv6 are very similar in terms of function



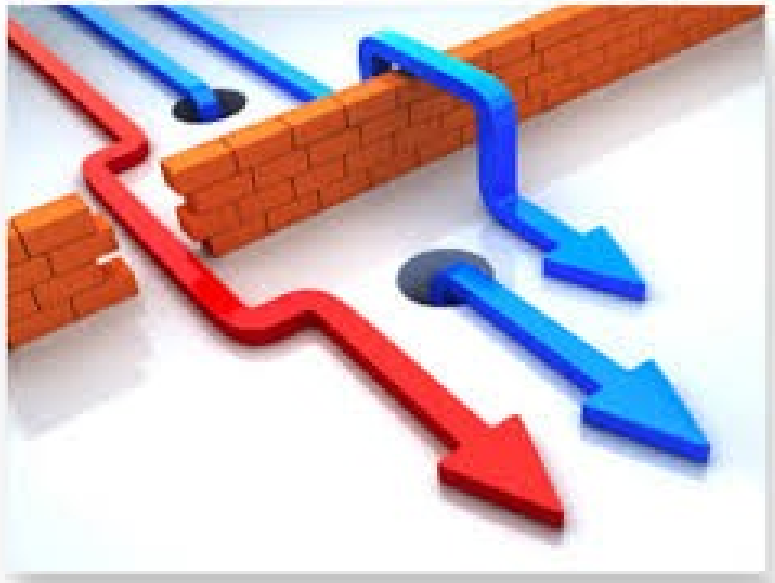
Principais Desafios da IoT

Segurança Digital



- Comportamento autônomo dos objetos
- Recursos computacionais restritos
- Comunicação sem fio
- Cuidados com as Propriedades de Segurança
  - Confidencialidade, Integridade, Disponibilidade, Autenticidade e **Privacidade**
- Segurança é um grande obstáculo !

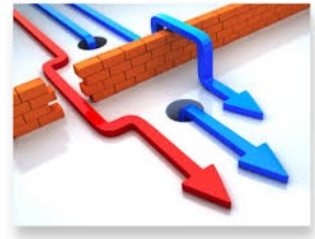
Riscos da IoT



Riscos da IoT (I)

- Ataques baseados em Botnets e Malwares
- Enfraquecimento do perímetro de segurança
  - Corporativo ou pessoal (doméstico)
  - Por objetos que não estão preparados para serem conectados a Internet
- Vazamento de informações privadas
- Falhas de segurança

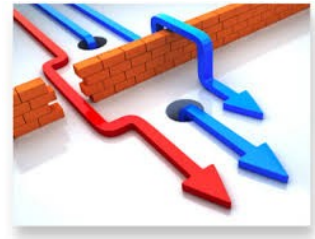
Riscos da IoT (II)



- Dispositivos vestíveis coletam muitas informações pessoais assim como do ambiente onde estão
- Dispositivos relacionados a saúde possuem dados sensíveis
- Exposição da Privacidade ou Segurança pessoal
  - Risco de vida

Riscos da IoT

Qualquer coisa pode ser invadida!



SOFTPEDIA®

Updated one minute ago

WINDOWS | GAMES | DRIVERS | MAC | LINUX | SCRIPTS | MOBILE | HANDHELD | NEWS

NEWS CATEGORIES:

- Google I/O 2014
- NSA & Edward Snowden
- Latest News
- Oddiverse
- Laptops & Tablets
- NEW! 3D Printing

Home > News > Editorials

May 4th, 2014, 01:29 GMT · By Eduard Kovacs

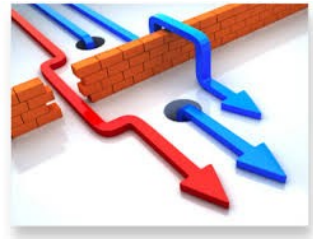
Everything Can Be Hacked, It's Just a Matter of Time Until Things Get More Serious

Researchers have demonstrated that routers, set-top boxes, security cameras, TVs, and even fridges can be hijacked and abused by cybercriminals for various purposes, including sending spam, mining for crypto-currencies, and spreading malware. Medical devices can also be hijacked, and the consequences can be deadly.

On the other hand, experts have also demonstrated that **cars**, **ships**, **airplanes**, **satellites** and even the **sensors used for traffic control systems** can be hacked.

Riscos da IoT

Qualquer coisa pode ser invadida!



Hackers find security weaknesses with the Lifx smart LED

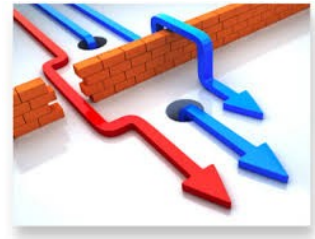
A team of British security consultants hacked their way into a private Wi-Fi network -- using Lifx bulbs as the backdoor.

by Ry Crist @rycrist / July 7, 2014 2:12 PM PDT

1 / 14 / 203 / 87 / / more +

Riscos da IoT

Qualquer coisa pode ser invadida!



Chinese hackers take command of Tesla Model S

Security firm Qihoo 360 says hackers gained control of some Tesla Model S functions -- but skimps on details of how the car was hacked.

by Seth Rosenblatt @sethr / July 17, 2014 12:47 PM PDT

THIS WEEK'S MUST READS /

1 Chinese hackers take command of Tesla Model S
Security

2 How fear and self-preservation are driving a cyber arms race
Security

Riscos da IoT

Qualquer coisa pode ser invadida!

InfoSec Community Forums

Keyword, Domain, Port, IP or Header Search

← Previous Threa

Multi Platform *Coin Miner Attacking Routers on Port 32764

Thanks to reader Gary for sending us in a sample of a *Coin miner that he found attacking Port 32764. Port 32764 was recently found to offer yet another backdoor on Sercomm equipped devices. We covered this backdoor before [1]

The bot itself appears to be a variant of the "zollard" worm sean before by Symantec [2]. Symantec's writeup describes the worm as attacking a php-cgi vulnerability, not the Sercomm backdoor. But this worm has been seen using various exploits.

Here some quick, very preliminary, details:

The reason I call it *Coin vs. Bitcoin is that in the past, we found these miners to mostly attack non-Bitcoin crypto-currencies to make use of the limited capabilities of these devices. I do not have sufficient detail yet about this variant.

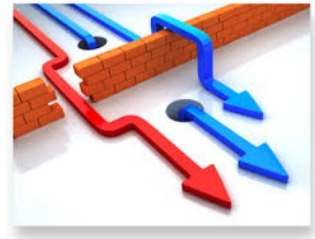
Interestingly, Gary found what looks like 5 binaries with identical functionality, but compiled for 4 different architecture providing for larger coverage across possible vulnerable devices. The binaries are named according to the architecture they support.

Name	Size	"file" output

GILBERTO SUI TECNOLOGI

Riscos da IoT

Qualquer coisa pode ser invadida!



Home / Security

Widely used wireless IP cameras open to hijacking over the Internet, researchers say

Lucian Constantin
IDG News Service

Apr 11, 2013 6:29 AM

Thousands of wireless IP cameras connected to the Internet have serious security weaknesses that allow attackers to hijack them and alter their firmware, according to two researchers from security firm Qualys.

The cameras are sold under the Foscam brand in the U.S., but the same devices can be found in Europe and elsewhere with different branding, said Qualys researchers Sergey Shekyan and Artem Harutyunyan, who analyzed the security of the devices and are scheduled to present their findings at the Hack in the Box security conference in Amsterdam on Thursday.

Tutorials provided by the camera vendor contain instructions on how to make the devices accessible from the Internet by setting up port-forwarding rules in routers. Because of this, many such devices are exposed to the Internet and can be attacked remotely, the researchers said.

Finding the cameras is easy and can be done in several ways. One method involves using the Shodan search engine to search for an HTTP header specific to the Web-

Câmeras IP e Babás eletrônicas

Riscos da IoT

E usada para disparar ataques !

NETWORKWORLD | Most read:

Home > Security

Bot-herders can launch DDoS attacks from dryers, refrigerators, other Internet of Things devices

Spike malware toolkit can infect Windows, Linux and ARM-based Linux devices

215 Gbps
150 Mpps

By Tim Greene | Follow
Network World | Sep 24, 2014 11:31 AM PT

RELATED TOPICS
Security
Malware/Cybercrime
Security Malware

A new malware kit called Spike can infect not only traditional desktops but also routers, smart thermostats, smart dryers and a host of other Internet of Things devices to herd them into massive botnets.

Spike botnets have carried out various forms of DDoS attacks including SYN, UDP, DNS query and GET floods, according to Akamai's Prolexic Security Engineering & Response Team (PLXsert).

GILBERTO SUDRÉ TECNOLOGIA

Riscos da IoT

E usada para disparar ataques !

IoT – Discovered first Internet of Things cyberattack on large-scale

January 19, 2014 By Pierluigi Paganini

Proofpoint discovered more Than 750,000 Phishing and SPAM Emails Launched From "Thingbots" Including Televisions, Fridge

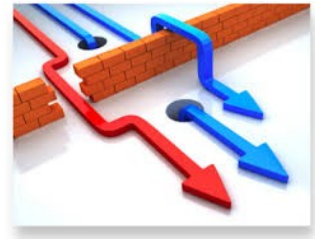
Recently security researchers from *Proofpoint* uncovered a cyber attack against the Internet of Things (IoT), more than 100,000 Refrigerators, Smart TVs and other smart household appliances have been hacked to send out 750,000 malicious spam emails.

The nightmare comes true, dozens of Zombies are already in our house! In the past weeks I wrote about a Linux worm specifically designed to hit the Internet of Things, unfortunately this is just the beginning because according the forecasts the attacks will increase in the next months.

Smart TVs
Geladeiras

Riscos da IoT

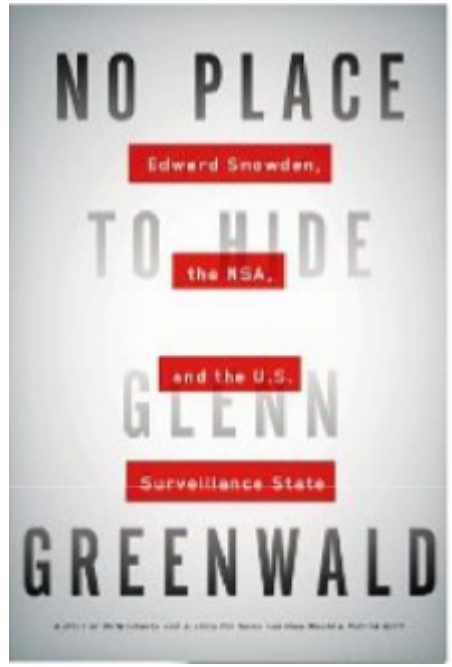
ou espionar !!!!

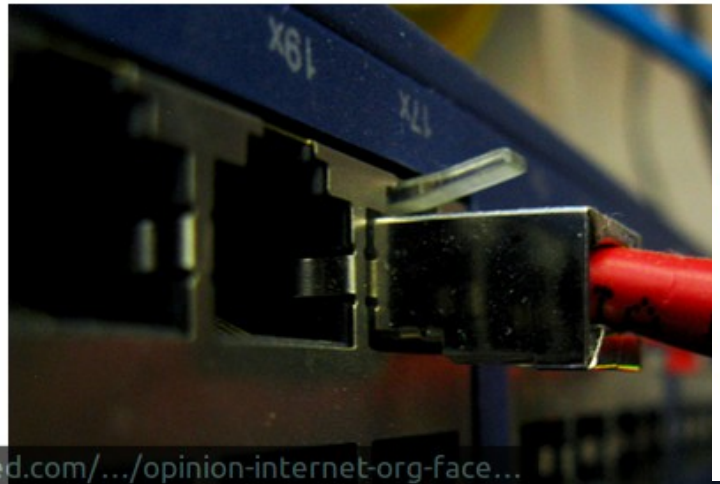


WIRED NSA Laughs at PCs, Prefers Hacking Routers and Switches

KIM ZETTER 09.04.13 6:30 AM

NSA LAUGHS AT PCS, PREFERS HACKING ROUTERS AND SWITCHES





TECH'S BOTTOM LINE

By Bill Snyder | Follow

Snowden: The NSA planted backdoors in Cisco products

'No Place to Hide,' the new book by Glenn Greenwald, says the NSA eavesdrops on 20 billion communications a day -- and planted bugs in Cisco equipment headed overseas

InfoWorld | May 15, 2014

MORE LIKE THIS

Reported NSA backdoors might open up networks to more threats

There are no secrets: What Edward Snowden taught us about privacy

Vulnerabilidades da IoT

Vulnerabilidades da IoT

25 vulnerabilidades por objeto

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Radio | Reports | White Papers | Event

ATTACKS/BREACHES | APP SEC | CLOUD | ENDPOINT | MOBILE | PERIMETER | RISK

VULNERABILITIES / THREATS

7/29/2014
09:15 AM

Ericka Chickowski
News

Connect Directly

Internet Of Things Contains Average Of 25 Vulnerabilities Per Device

New study finds high volume of security flaws in such IoT devices as webcams, home thermostats, remote power outlets, sprinkler controllers, home alarms, and garage door openers.

A new study published this week found that among even among just a small sample of some of the most popular and prevalent Internet of Things (IoT) devices, researchers uncovered 250 vulnerabilities -- many of which were severe and resulted in remote code execution, including vulnerabilities to Heartbleed, denial of service, and cross-site scripting.

Conducted by researchers at HP Fortify, the study was meant to

Por que? (I)

- Sistemas operacionais simples
  - não possuem mecanismos adequados de proteção e não sofrem atualizações
- Inúmeras vulnerabilidades nos softwares embarcados
- Monitoramento governamental em larga escala à Internet
  - Portas que os fabricantes de hardware e software foram “obrigados” a deixar abertas para que as agências americanas possam ter acesso a dados

Vulnerabilidades da IoT

Por que? (II)

» Desejo das empresas fabricantes de equipamentos de querer conhecer seus consumidores

- Criam mecanismos que coletam informações sobre utilização, sobre o que foi acessado, assistido, comprado etc.

- “Big Brother” virtual

Vulnerabilidades da IoT

Top 10 OWASP IoT

OWASP
Open Web Application Security Project

1. Interface WEB insegura
2. Autenticação / Autorização insuficiente
3. Serviços de rede inseguros
4. Falta de transporte criptografado
5. Problemas de privacidade
6. Interface com a Nuvem insegura
7. Interface móvel insegura
8. Configurações insuficientes de segurança
9. Software / Firmware inseguros
10. Segurança física insuficiente

Ataques

Tipos de Ataques (I)

- Ataques físicos
  - Violam o hardware, difíceis de executar
- Ataques no canal de comunicação
  - Dados de dispositivos criptográficos (análise de temporização, radiação emitida, potência consumida)
- Ataques de análise de criptografia
  - Análise do texto cifrado (ataque Man-in-the-Middle)

Tipos de Ataques (II)

- Ataques de software
  - Vulnerabilidades nos softwares embarcados (buffer overflows, aplicativos maliciosos)
- Ataques de rede (sem fio)
  - Análise de tráfego, negação de serviço, corrupção de mensagens, ataques de roteamento, mascaramento
- Ataques contra a Cloud
  - Mascaramento, negação de serviço, aplicativos maliciosos

Defesas

Como se defender? (I)

- Garantir as propriedades de segurança
  - Atualização dos softwares embarcados (firmware)
  - Rever políticas de segurança
  - Uso de senhas e criptografias fortes
  - Desativar portas não utilizadas
  - Não expor dados pessoais
  - Conscientização pessoal por segurança

Como se defender? (II)

- Gestão de identidades
  - Acesso seguro
  - Identificação única e autenticação de objetos
  - Autenticação de usuários
- Comunicação e armazenamento seguro de Dados
- Dispositivos resistentes à violação
- Uso de tecnologia nacional
  - Conhecer o código que está sendo executado

Conclusão

Mais Informações

http://blogs.gazetaonline.com.br/conexaodigital/

Aparelhos em Stand By e o consumo de energia

Gilberto Sudré · 04/mai/2015 · 0 Comentários

Luz vermelha acesa, indica que o eletrodoméstico está ligado na tomada mas mais do que isto, significa mais gastos para o consumidor. Aparelhos desligados em modo stand by também consomem energia. Apesar do consumo ser pequeno, a soma

GILBERTO SUDRÉ

Professor, escritor, consultor e pesquisador da área de Segurança Digital e Perícia Forense do Ifes. Comentarista de Tecnologia da Rádio CBN e TV Gazeta.

http://gilberto.sudre.com.br

GILBERTO SUDRÉ
TECNOLOGIA

CURRÍCULO PALESTRAS CURSOS CONSULTORIA ARTIGOS WEBCASTS BLOGS E PROGRAMAS LIVROS FOTOGRAFIA CONTATOS

SEGURANÇA DIGITAL

Manter o ambiente corporativo seguro não é uma tarefa fácil pois não existe uma solução única e definitiva. Cada empresa necessita de ferramentas e procedimentos específicos para atender o nível de segurança desejado.

- Administração Segura de Servidores

PESQUISAR

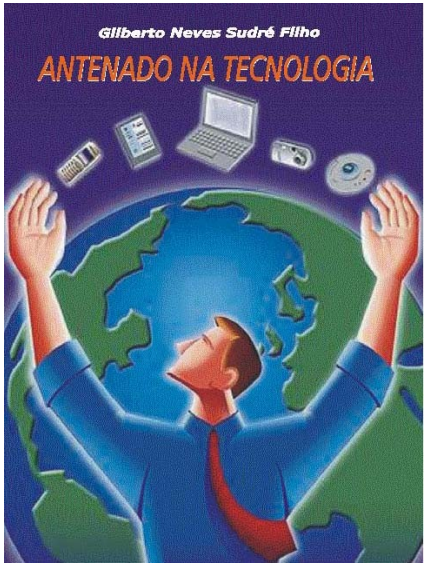
FIQUE POR DENTRO DAS NOVIDADES

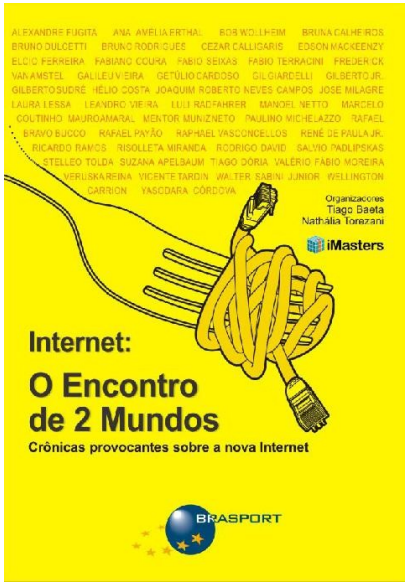
Digite seu e-mail:

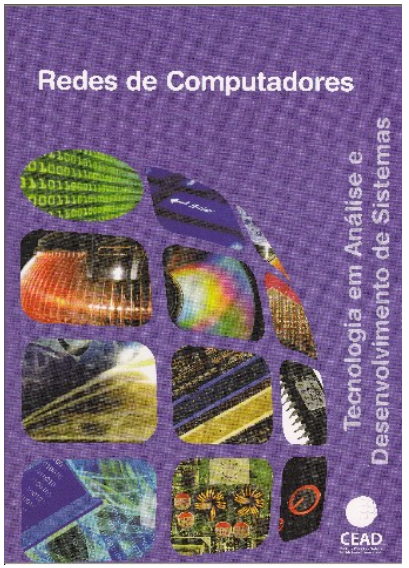
Enviar

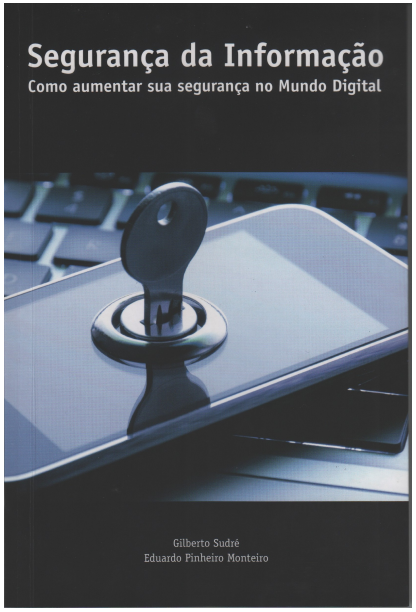
Tecnologia FeedBurner

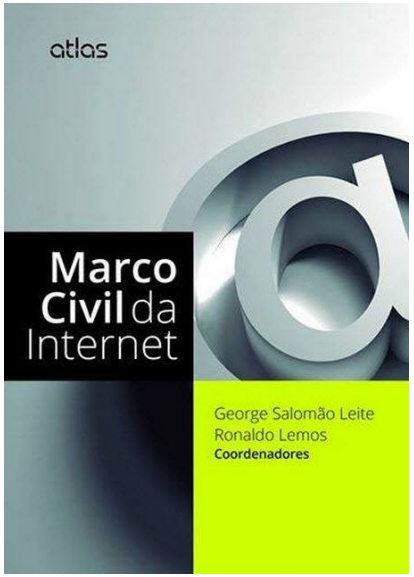
http://gilberto.sudre.com.br











http://labseg.ifes.edu.br

LabSeg

Laboratório de Segurança Digital e Perícia Computacional Forense

INSTITUTO FEDERAL
ESPÍRITO SANTO
Campus Serra

Home | O LABSEG | Projetos | Trabalhos e Publicações | Pesquisadores | Downloads

Bem vindo

Posted on 29/11/2011 by gilbertosudre

Bem vindo a página do LABSEG – Laboratório de Segurança da Informação do IFES – Campus Serra.

Posted in Uncategorized | Leave a comment | Edit

Search

Agenda / Eventos

Calendario

Links

- Coordenadoria de Informática – Ifes Serra
- IFES – Campus Serra

Últimas publicações

- Bem vindo

GILBERTO SUDRÉ TECNOLOGIA

gilbertosudretecnologia

@gilbertosudre

gilbertosudre

gilberto.sudre.com.br

gilberto@sudre.com.br