
egi
Escola de Governança
da Internet no Brasil

Fundamentos de Segurança da Informação

Cristine Hoepers, D.Sc.
Klaus Steding-Jessen, D.Sc.

02/08/2016 – 10:30 às 12:00h

Objetivos

Discutir os conceitos técnicos relacionados com segurança, privacidade e resiliência

De forma não exaustiva

Subsidiar os participantes para as crescentes discussões sobre privacidade, segurança, estabilidade e resiliência nos fóruns nacionais e internacionais de governança da Internet

Embasamento técnico para identificar e questionar falácias, mitos e artigos não embasados

Segurança e Governança da Internet

egi

WSIS:
Declaration of Principles

Document WSIS-03/GENEVA/DOC/4-E

12 December 2003

[...]

B5) Building confidence and security in the use of ICTs

35. Strengthening the trust framework, **including information security and network security, authentication, privacy and consumer protection**, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

[...]

http://www.itu.int/wsis/docs/geneva/official/dop.html

CGI.br:
Princípios para a Governança e Uso da Internet no Brasil

CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL

Fevereiro de 2009

[...]

8. Funcionalidade, segurança e estabilidade
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa **através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas**.

[...]

http://www.cgi.br/resolucoes/documento/2009/003

NETmundial:
Internet Governance Principles

NETmundial Multistakeholder Statement

April, 24th 2014, 19:31 BRT

[...]

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a **secure, stable, resilient, reliable and trustworthy network**. **Effectiveness** in addressing risks and threats to security and stability of the Internet **depends on strong cooperation among different stakeholders**.

[...]

http://www.netmundial.org/references/

Foco de Hoje:

Discutir
Questões Emergentes

Dinâmica ("*Rules of Engagement*")

Um tema emergente nas discussões em Fóruns de Governança de Internet é apresentado

- **incluindo *quotes* sobre algumas das posições predominantes**

Seguem-se 10 minutos de debate aberto

- **apresentem argumentos pró/contra**
- **sejam sucintos, para termos o maior número possível de contribuições**

Segue-se uma pontuação nossa sobre

- **aspectos técnicos**
- **aspectos de segurança**

Segurança vs. Privacidade

Quotes:
Segurança vs. Privacidade

"*Para ter segurança é preciso abrir mão da privacidade*"

"*Na Internet, não se deve analisar nem os cabeçalhos dos pacotes*"

"*Órgãos investigativos precisam ter acesso a comunicações criptografadas para serem efetivos*"

"*Para ter privacidade deve-se eliminar*

- *logs*
- *cookies*"

"*Usar criptografia em tudo garante privacidade*"

Considerações:
Controle vs. Segurança vs. Privacidade

Medidas de Segurança

- criptografia
- controle de acesso
  - garantir que só você acessa sua conta de *e-mail*; que ninguém invade seu perfil do *twitter,* etc
  - garantir que só você acessa seu *Internet banking*
- amazenar *logs* de acordo com políticas bem definidas e para fins específicos de segurança e funcionamento da rede

Medidas de Controle

- armazenar 100% do tráfego
- armazenar, inspecionar e processar de forma centralizada *logs*, consultas DNS, acessos, conteúdo, etc
  - de múltiplas redes
  - correlacionando estas informações
  - com motivações diversas e difusas

Considerações:
Controle vs. Segurança

Supostas medidas de segurança, mas usadas para controle, podem gerar reações contra a segurança como um todo

- uso indiscriminado da biometria em escolas, academias, acesso a edifícios, etc
- RFID (*Radio Frequency Identification*) em carros, cartões de crédito e passaportes

Quem tem acesso? Com que finalidade?

Como estes dados estão protegidos?

Seu uso traz mesmo mais segurança no contexto em que estão sendo usados?

Considerações:
Privacidade *Online*

Um grande risco à privacidade pode ser simplesmente não entender a tecnologia

- As informações que um navegador fornece a um *site*, permitem identificação mais únivoca que um endereço IP válido
- Medidas de segurança não são contra a privacidade, mas sim essenciais para mantê-la

É necessário que modelos de negócio e regras sejam claros

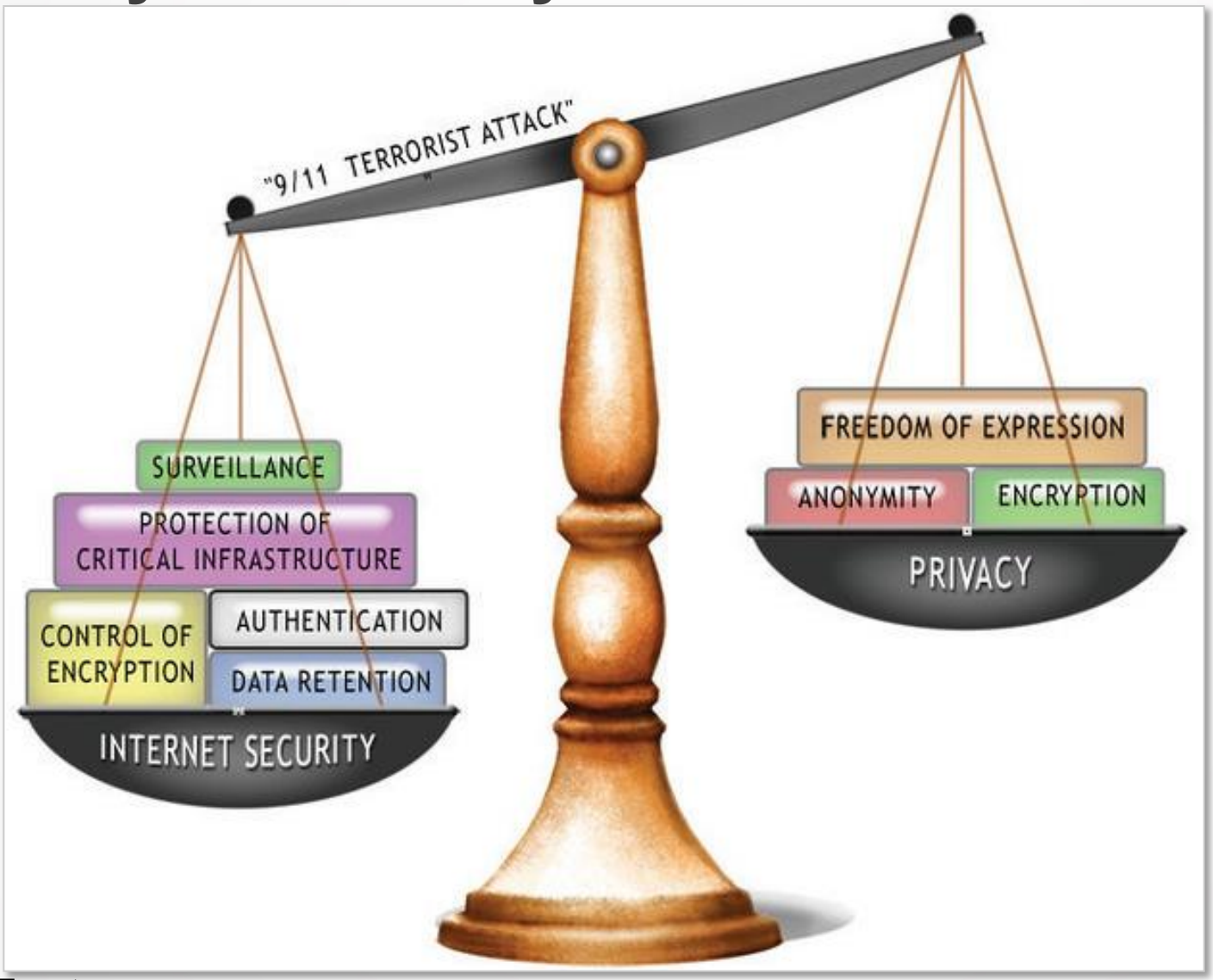
- Serviços não são gratuitos, são pagos com informações providas por seus usuários

DPI é um *buzzword* criado pela indústria para vender "caixas"

- Sem "olhar" os cabeçalhos e os IPs, os pacotes não chegam ao destino
- Antivírus, *antispam*, IDS e alguns *firewalls* necessitam inspecionar o "conteúdo" à busca de assinaturas de ataques
- O importante é isto ocorrer com políticas bem definidas e para fins específicos de segurança ou funcionamento da rede

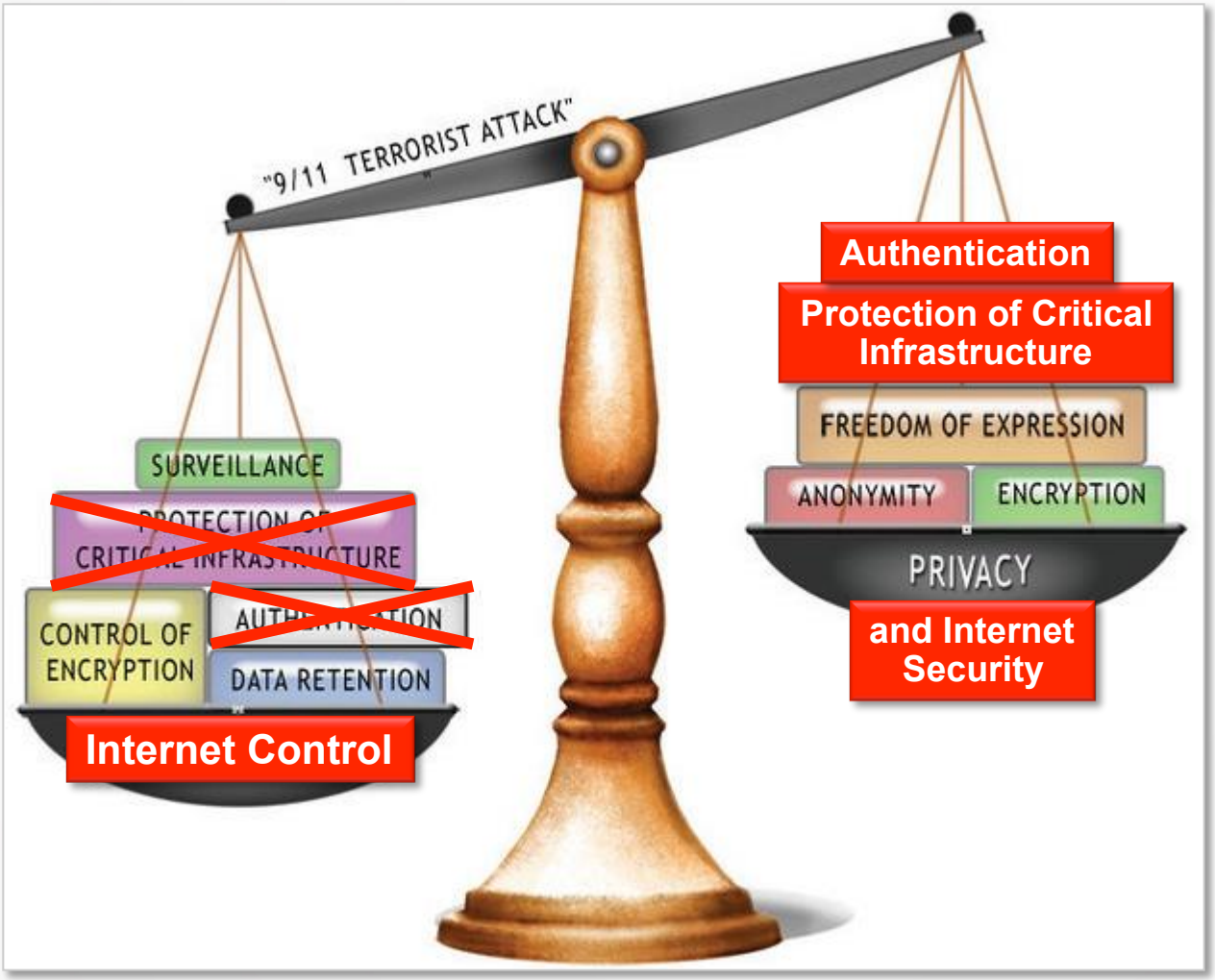
Mais
Segurança vs. Privacidade

Visão da Diplo Foundation: **Security vs. Privacy**



Fonte:
http://pt.slideshare.net/DiploFoundation/gic-introduction-to-ig

Como poderia ser uma balança 2.0:
~~Security~~Control vs. Privacy and Security



Fonte:
http://pt.slideshare.net/DiploFoundation/gic-introduction-to-ig

Considerações:
Leitura Complementar Recomendada

Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications

http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

"*This report's analysis of law enforcement demands for exceptional access to private communications and data shows that such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend.*"

NAT e IPv6

Quotes:
NAT e IPv6

"*IPv6 permite rastrear todos os passos de uma pessoa na Internet*"

"*IP público é inseguro, sem NAT não tenho como me proteger*"

Considerações:

IPv6

A Internet poderá voltar a ser ponto-a-ponto

Já há extensões de privacidade para vários sistemas (RFC 4941)

A segurança é implementada via ferramentas e cuidados ao utilizar a rede

IoT: será possível acessar os dispositivos diretamente

NAT

Dá uma falsa sensação de segurança

Dificulta o tratamento de incidentes de segurança

Todos os *malwares* tem "*connect back*"

- ou seja, mandam dados para fora
- se conectam ao atacante

Dispositivos IoT mandam dados para a "nuvem" porque estão atrás de NAT

Internet das Coisas (IoT)

As “coisas” já estão conectadas

- carros, lâmpadas, TVs, câmeras de segurança, equipamentos médicos
- são sistemas complexos e completos (tem um sistema operacional, aplicações Web, permitem acesso remoto, etc)

(In)Segurança em IoT

Empresas de áreas sem experiência com Internet

- Estão repetindo os erros dos desenvolvedores de 30 anos atrás
  - contas e senhas padrão, protocolos inseguros, falta de autenticação, furos básicos de programação, serviços desnecessários ligados, etc
- Não estão prevendo updates para corrigir problemas

Problemas já estão acontecendo:

- Lâmpadas Phillips e Osram (cripto fraca permite descobrir senha do wi-fi; vulnerabilidades permitem controlar remotamente)
- TVs Samsumg mandam todo o som ambiente para sede; TVs da LG enviam nomes de arquivos, filmes, inclusive dos drives de rede, que são ativamente procurados pela TV
- Carros da *Fiat Chrysler* permitindo controle do veículo via 3G/4G, via vulnerabilidades do sistema de entretenimento Uconnect
- Aviões potencialmente vulneráveis via sistemas de entretenimento
- Dispositivos médicos

Infusion Pumps

www.hospira.com/en/products_and_services/infusion_pumps

Reader

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Our focused line of infusion systems includes general infusion and pain management pumps:

Contact Hospira

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities | ICS-CERT

https ics-cert.us-cert.gov/advisories/ICSA-15-161-01 Reader

Advisory (ICSA-15-161-01)

More Advisories

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

Ataques DDoS usando dispositivos IoT

Atacantes exploram senhas fracas ou padrão

Foco em dispositivos com versões "enxutas" de Linux

- para sistemas embarcados
- arquiteturas ARM, MIPS, PowerPC
- exemplos: CCTV, DVR, CPE, Disco Externo (NAS), etc.

Malware se instala e conecta no comando e controle de uma *botnet*

Atacante envia comandos

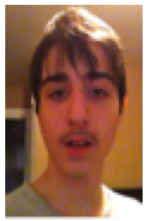
- alvo do ataque
- tipo do ataque (TCP, UDP, grande volume, grande número de conexões, etc)

Para pensar:

Se houver franquia, como será considerado

- *o tráfego de ataques*
- *o tráfego necessário para instalar updates*

DIAMOND MODEL OF DDOS (IOT) BRAZIL



@iceman4391

@bc2fast

@iceman4391 (aka Brandon) ←→ ¿@bc2fast?
- http://ddos.yt
- http://www.geocities.jp/arc_ocd/log0x40.html

- **Distribuido geográficamente**

Más de 1351 fuentes únicas
774 Vietnam
128 Brasil
81 Turquía
80 Rumanía
67 Taiwan

Adversario

usos

desarrolla

Implantada a través de

Infraestructura

- **Infraestructura Bots (IoT)**
  - Admin de Cámaras (Linux Recortado)
- **Botnet IRC**
  - Variante de Lizard Stresser
    - https://github.com/gh0std4ncer/lizkebab
  - 2 Servidores de botmasters usando comandos por IRC
    - Holanda Quasi Networks

Capacidades (TTP)

- **Ciber adversario mediano**
  - C2 Comandos de ataque de DDoS (HOLD/JUNK/UDP/TCP)
    - UDP 443 → bankline.itau.com.br: 443: 1400 bytes (chr) RND

```
2016-04-22 12:41:33.276686: !* HOLD 200.*.*.* 443 120
2016-04-22 12:49:27.487482: !* UDP 200.*.*.* 80 120 32 1400 10
2016-04-22 13:11:28.938349: !* TCP 200.*.*.* 443 120 32 syn 1 10
```

  - Escaner para encontrar otros dispositivos IoT vulnerables con root como contraseña de superusuario
  - Mecanismos para ejecutar comandos de shell

Se conecta a

explota

Víctima

Instituciones financieras, gubernamentales e ISP's en Brasil principalmente

> 300 Gbps ¡No amplificados!

ARBOR NETWORKS

Fonte: Arbor Worldwide Infrastructure Security Report
http://www.lacnic.net/web/eventos/lacnic25-agenda-lacsec#viernes

Colocando em Prática os Príncipios de Governança

CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL - Fevereiro de 2009

8. Funcionalidade, segurança e estabilidade
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de **medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas**.

NETmundial Multistakeholder Statement - April, 24th 2014, 19:31 BRT

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. **Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.**

Stakeholders e Seus Papéis na Redução dos Ataques de Negação de Serviço (DDoS)

Boas práticas para reduzir o "poder de fogo":

- **Detentores de ASN:** implementar anti-spoofing (BCP 38)
- **Provedores de Serviços:** (NTP, DNS, etc): configurar corretamente os serviços para evitar amplificação
- **Usuários:** manter sistemas atualizados, prevenir-se de infecções (*hardening*), "limpar" dispositivos infectados
- **Desenvolvedores de sistemas:** considerar riscos no projeto, desenvolver código mais seguro, ter configuração padrão mais segura

Prevenção por parte das vítimas:

- Aumentar os recursos (mais banda, processamento, disco)
- Usar serviços ou ferramentas de mitigação

Repressão por parte dos operadores da justiça:

- Investigar e punir os atacantes

Obrigado

Cristine Hoepers, D.Sc.
cristine@cert.br

Klaus Steding-Jessen, D.Sc.
jessen@cert.br

nic.br cgi.br

www.nic.br | www.cgi.br