nic.br cgi.br | 20 anos cert.br

Internet: Desafios Jurídicos e Técnicos

Escola Nacional de Magistratura
Associação dos Magistrados Brasileiros

Brasília, DF – 07 de novembro de 2017

Segurança, Privacidade e Criptografia

Dra. Cristine Hoepers
Gerente Geral, CERT.br
cristine@cert.br

cert.br nic.br cgi.br

Agenda

Revendo conceitos

- Segurança da Informação
- Confidencialidade e Privacidade
- Riscos, ameaças e vulnerabilidades
- Importância da Criptografia

Acesso excepcional a conteúdos cifrados

- Possíveis implementações
- Riscos

Revendo Conceitos

Propriedades da Segurança da Informação

Confidencialidade – é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda

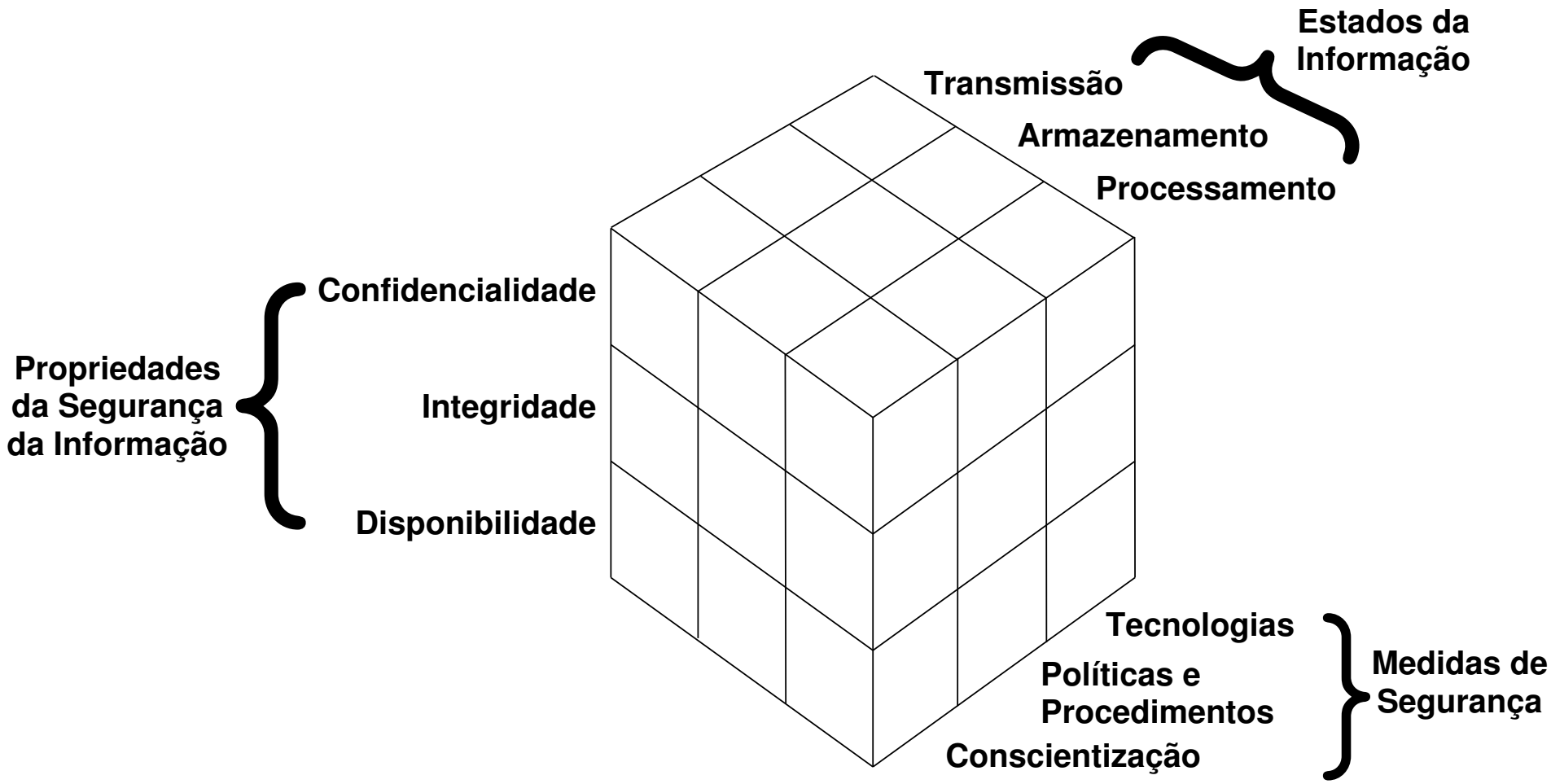
Integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

Disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

Ex. de quebra: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

As informações estão em diversos locais e a segurança depende de múltiplos fatores



McCumber Information Security Model

http://www.ibm.com/developerworks/security/library/s-confnotes2/

Privacidade vs. Confidencialidade

Do ponto de vista de Segurança da Informação:

Privacidade – habilidade e/ou direito de proteger suas informações pessoais, extende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal.

Confidencialidade – envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles.

Fonte: ***Security Engineering, 2nd Edition*****, 2008, Ross Anderson**
http://www.cl.cam.ac.uk/~rja14/book.html

Riscos a Sistemas Conectados à Internet

- indisponibilidade de serviços
- furto/vazamento de dados
- perda de privacidade
- perdas financeiras
- danos à imagem
- **perda de confiança na tecnologia**

Sistemas na Internet

Riscos

Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

Importância da Criptografia

Criptografia

- ciência e a arte de escrever mensagens em forma cifrada ou em código
- é um dos principais mecanismos de segurança

É a base para o funcionamento de:

- certificados e assinaturas digitais
- mecanismos de autenticação
- conexão segura na Web (HTTPS)
- conexão segura para outras aplicações na Internet (SSL/TLS, IPSec)
- proteção de dados armazenados em disco, em mídias removíveis e dispositivos móveis
- integridade de consultas DNS (DNSSEC)

Cartilha de Segurança para a Internet, Capítulo 9
ISBN: 978-85-60062-54-6 **–** https://cartilha.cert.br/livro/

Resiliência

Um sistema 100% seguro é muito difícil de atingir

Novo paradigma: Resiliência

Continuar funcionando mesmo na presença de falhas ou ataques

- Definir políticas (de uso aceitável, acesso, segurança, etc)
- Treinar profissionais para implementar as estratégias e políticas de segurança e conscientizar os usuários sobre os riscos e medidas de segurança necessários
- Implantar medidas de segurança que implementem as políticas e estratégias de segurança, como:
  - aplicar correções ou instalar ferramentas de segurança
  - utilizar criptografia forte, que não dependa somente da segurança das chaves privadas – e.g: ***Forward Secrecy***
    - **protege transações passadas contra um comprometimento ou espionagem**
- Formular estratégias para gestão de incidentes de segurança e formalizar grupos de tratamento de incidentes

Exemplos Concretos da Dificuldade de Impedir a Invasão de Sistemas

Comprometimento da RSA/EMC, para furto de material criptográfico – levou ao comprometimento do DoD
https://www.sec.gov/Archives/edgar/data/790070/000119312511070159/dex991.htm

Comprometimento do *Office of Personnel Management*, para furto dos antecedentes de todos os funcionários do Governo Americano
https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Comprometimento da Autoridade Certificadora da Holanda – usada para gerar chaves falsas do Google, usadas em espionagem no Irã
http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html

Alegado comprometimento da empresa Kaspersky para acesso a documentos sensíveis em sua nuvem – citado o vazamento de documentos da NSA para a Rússia – em tese, a NSA foi alertada por Israel (que admitiu publicamente ter invadido a Kaspersky)
https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

Acesso Excepcional a Conteúdos Cifrados

20anos cert.br nic.br cgi.br

Acesso Excepcional a Conteúdos Cifrados
Possíveis Implementações

Uso de algoritmos “enfraquecidos” que permitam alguns atores a quebrar a criptografia

Uso de chaves mestras (*key escrow*)

- sob guarda das empresas que implementam os produtos ou serviços
- sob guarda de terceiros (polícias, órgãos de governo, agências, etc)

"... the real security challenge is not the mathematics of cryptosystems; it is engineering, specifically the design and implementation of complex software systems."

– Abelson et. al

Keys Under Doormats

Riscos:
No uso de chaves mestras (1/2)

Vazamento da chave

- não intencional
  - sistemas comprometidos ficarem expostos, falhas nas configurações de sistemas, perda de mídia, erro humano, etc
- intencional

Quem tem a guarda da chave vira alvo e ponto único de falha

- atacantes passam a ter maior incentivo para
  - comprometer a organização
  - recrutar funcionários

Riscos:
No uso de chaves mestras (2/2)

Retroceder a segurança dos sistemas

- inviabiliza o uso da técnica de *Forward Secrecy*
  - hoje é uma técnica amplamente utilizada para garantir que um invasor ou espião não tenha acesso a comunicações anteriores, em caso de comprometimento da chave privada
  - sem *forward secrecy*, se qualquer das chaves privadas for comprometida, imediatamente todos os dados já trocados estão comprometidos

Desafios procedimentais

- Quem terá acesso às chaves mestras?
- Quantas chaves mestras existirão em um país?
- Quais países terão acesso às chaves?
- Como saber se um país não está abusando do acesso para espionar cidadãos de outro país?

Risco adicional:
Criminosos pararem de usar sistemas legítimos

Hoje utilizam os sistemas de mercado

- incentivo para os criminosos: facilidade de uso e de adoção
- vantagem para as autoridades: rapidamente se chega nos meta-dados

Facilmente podem desenvolver seus próprios sistemas

- contratando bons programadores
- usando algoritmos fortes e públicos de criptografia
- mercado "*underground*" online já oferece serviços de programação
  - *Russian Underground 101 – Trend Micro*
    http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
  - *2016 Underground Hacker Markets – Secureworks*
    https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report

Considerações Finais:
Possíveis Consequências Não Intencionais da Implantação de Acesso Excepcional

Cria-se uma nova superfície de ataque

Incentiva-se o crime organizado a criar seus próprios aplicativos de comunicação, utilizando criptografia forte

Põe-se todos os usuários em risco

- Não é uma questão de "**se**" atores maliciosos terão acesso aos sistemas que guardam as chaves ou o texto em claro
- Mas sim de o que fazer "**quando**" eles tiverem acesso

A sociedade perde a confiança na tecnologia

- Inibe-se a inovação
- Reduz-se a qualidade de vida

Leitura Complementar Recomendada

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

"*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.*"

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

Referências:
Fontes dos Conceitos Apresentados

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

The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)

https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30310

Cartilha de Segurança para a Internet

https://cartilha.cert.br/

Security Engineering, 2nd Edition, 2008, Ross Anderson

http://www.cl.cam.ac.uk/~rja14/book.html

Cyber Risk and Resilience Management, CERT/CC

http://www.cert.org/resilience/

Obrigada

www.cert.br

cristine@cert.br

@certbr

07 de novembro de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br