Segurança,Ética e Privacidade na Internet

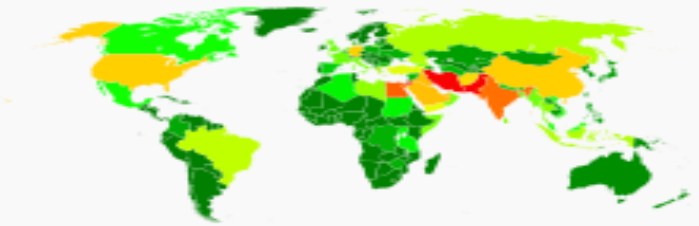
III Encontro de Segurança em Informática do CERT.Bahia

Alexandro Silva
alexos@alexos.org
http://alexos.org

Who Am I?

Alexos Core Labs

National Security Agency surveillance



Map of global **NSA data collection**

Programs [hide]

Pre-2001

ECHELON · Main Core · MINARET · SHAMROCK · PROMIS

2001

BLARNEY · RAGTIME · Turbulence · PINWALE (NSA internet database) · MAINWAY (NSA call database) · Upstream (incl. Room 641A)

2007

PRISM · **Boundless Informant** · X-Keyscore · Dropmire · Fairview · Surveillance Detection Unit · Bullrun

GCHQ collaboration

IMP · Tempora (Mastering the Internet · Global Telecoms Exploitation)

Discontinued

Trailblazer Project · ThinThread · President's Surveillance Program (Terrorist Surveillance Program · STELLARWIND)

Fonte: https://en.wikipedia.org/wiki/Boundless_Informant

Você realmente sabe o que está acontecendo?

Estados Unidos

A agência de segurança nacional (NSA) dos Estados Unidos mantém, desde 2007, um programa secreto de vigilância eletrônica capaz de interceptar uma proporção substancial da internet global e de vigiar as comunicações em tempo real, o PRISM (Performance and Registration Information Systems Management). Segundo as denúncias de Edward Snowden, nove das grandes corporações e serviços de internet participam do programa fornecendo dados de usuários: Microsoft, Google, Facebook, Yahoo!, Apple, YouTube, AOL, Paltalk e Skype.

Fonte: http://www.ibliss.com.br/blog/a-espionagem-governamental-e-mais-comum-do-que-se-imagina/

Reino Unido

Segundo denúncias de Edward Snowden, o Reino Unido seria responsável pelo maior programa de vigilância da história, ainda mais poderoso do que o da NSA: o Tempora, mantido pela agência Government Communications Headquarters (GCHQ).

O programa monitora dados através de cabos de fibra ótica que passam em grande quantidade pelo território britânico a caminho de outros países e continentes, viabilizando o monitoramento do tráfico global da internet e ligações telefônicas. Esses dados seriam armazenados e analisados em parceria secreta entre a GCHQ e a NSA.

Segundo levantamento do *The Guardian*, a GCHQ monitorou 600 milhões de telefonemas por dia e mais de 200 cabos de fibra ótica no último ano. Cada cabo carrega 10 gigabites por segundo, o equivalente ao envio de todas as informações sobre todos os livros da Biblioteca Britânica, 192 vezes, a cada 24 horas.

Fonte: http://www.ibliss.com.br/blog/a-espionagem-governamental-e-mais-comum-do-que-se-imagina/

França

"Não apenas o Estado americano desenvolveu um gigantesco aparato que permite espionar todos os cidadãos e além. Paris faz o mesmo", afirmou o diário francês Le Monde no início de julho.

Segundo o jornal, a inteligência francesa Direção Geral de Segurança Externa (DGSE) armazena sistematicamente os sinais eletromagnéticos emitidos por computadores na França, assim como informações que circulam entre a França e o exterior. "Todas as nossas comunicações são espionadas", denuncia o diário. E-mails, mensagens de texto, registros telefônicos, mensagens de redes sociais, entre outras informações são armazenadas durante anos na sede do serviço de inteligência francês.

O gabinete do primeiro-ministro Jean-Marc Ayrault chamou de inexatas as afirmações do jornal.

Fonte: http://www.ibliss.com.br/blog/a-espionagem-governamental-e-mais-comum-do-que-se-imagina/

INTERNET

27 de Agosto de 2013 • 12h58 • atualizado às 13h38

Brasil pediu dados de 857 usuários do Facebook, diz relatório

O Facebook lançou seu primeiro relatório de transparência, que mostra os países que mais requisitaram informações sobre os usuários da rede social

44 Tweetar

928 Curtir

Facebook é uma das empresas envolvidas no escândalo de espionagem dos Estados Unidos

Foto: Robert Galbraith / Reuters

O Facebook divulgou nesta terça-feira seu primeiro relatório de transparência, que mostra o número de pedidos de informações de usuários feitos por autoridades de diversos países. O relatório mostra que o Brasil fez 715 solicitações de informações sobre 857 usuários brasileiros no primeiro semestre do ano. Em 33% delas, foi revelada alguma informação.

O país que mais pediu informações sobre usuários no período foi os Estados Unidos, com cerca de 12 mil solicitações de quase 21 mil usuários. Em 79% dos casos foram revelados algum tipo de informação. No total, autoridades de 74 países pediram dados de cerca de 38 mil usuários da rede social.

Fonte: http://tecnologia.terra.com.br/internet/brasil-pediu-dados-de-857-usuarios-do-facebook-diz-relatorio

British blogger revealed that his LG Smart TV collects and sends details about the owners' viewing habits even if the users have activated a privacy setting.

Exactly one year ago we discussed about the possibility to exploit a vulnerability in Samsung Smart TV to penetrate our domestic network to spy on us or to serve a malware.

The British Developer and blogger DoctorBeet, announced to have discovered that hi LG Smart TV is sending data about his family's viewing habits back to the South Korean manufacturer.

It seems that the Smart TV, model LG 42LN575V, sends data back to LG servers even if the blogger has disabled the option "Collection of watching info" in the TV settings menu.

Fonte: http://securityaffairs.co/wordpress/19860/hacking/lg-smart-tv-spying-users.html

NSA infected 50,000 computer networks with malicious software

Photo Corbis

NEWS The American intelligence service - NSA - infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive information. Documents provided by former NSA-employee Edward Snowden and seen by this newspaper, prove this.

by Floor Boon, Steven Derix and Huib Modderkolk

A management presentation dating from 2012 explains how the NSA collects information worldwide. In addition, the presentation shows that the intelligence service uses 'Computer Network Exploitation' (CNE) in more than 50,000 locations. CNE is the secret infiltration of computer systems achieved by installing malware, malicious software.

http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/

Confidencialidade

Serviços de Armazenamento na Nuvem (Cloud)

- Google Drive
- Dropbox
- Box
- Skydrive

Educação

Cartilhas

Cert.br

http://cartilha.cert.br/

Instituto Coaliza

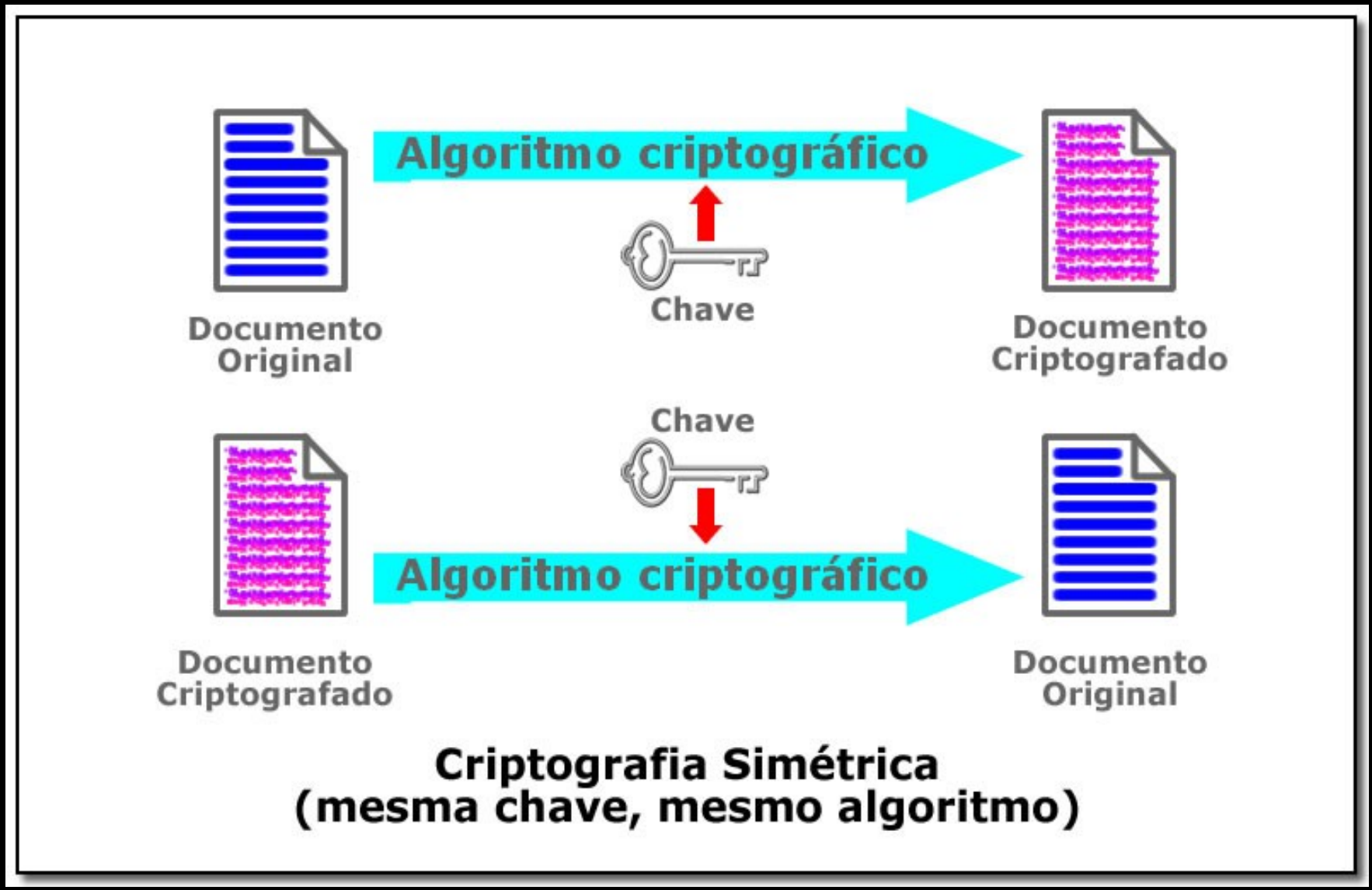
http://www.coaliza.org.br/cartilhas1.html

Criptografia

http://cartilha.cert.br/criptografia/

Simétrica

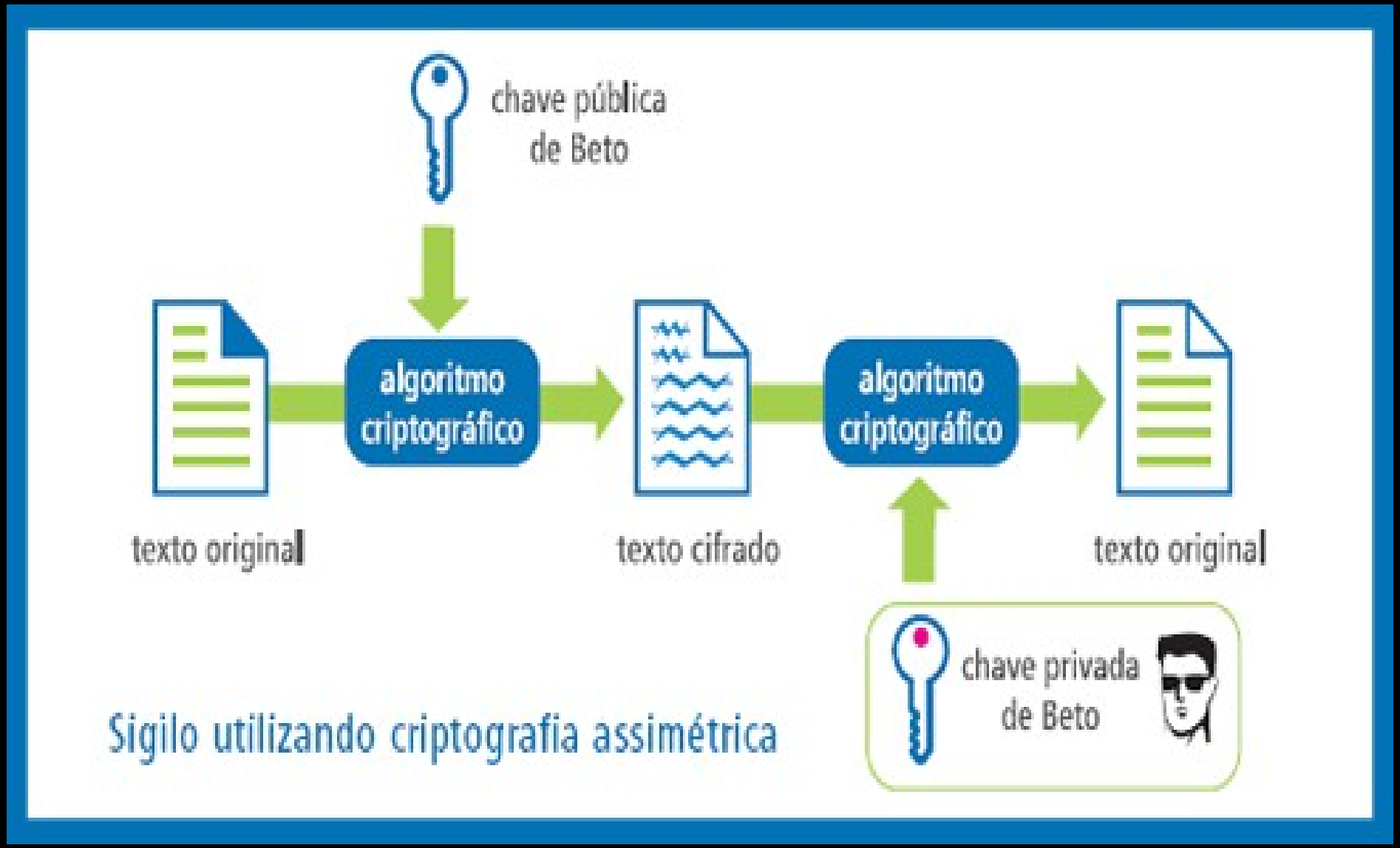
Criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados.



Criptografia Simétrica
(mesma chave, mesmo algoritmo)

Assimétrica

Criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la.



Sigilo utilizando criptografia assimétrica

Navegação Segura (HttpsEverywhere)

http://tinyurl.com/ensihttps

Email e arquivos (GPG)

http://tinyurl.com/ensigpg1
http://tinyurl.com/ensigpg2

Sistema de Arquivos (Truecrypt)

http://tinyurl.com/ensitruecrypt1
http://tinyurl.com/ensitruecrypt2

Cloud (BoxCryptor)

http://tinyurl.com/ensiboxcryptor

Transferência de Arquivos (BTSync)

http://tinyurl.com/ensibtsync1
http://tinyurl.com/ensibtsync2

Navegação Anônima (TOR)

http://tinyurl.com/ensitor1
http://tinyurl.com/ensitor2

Configuração Segura

Gestão Contínuada de Ameaças

Pesquisa e Desenvolvimento Tecnológico

Links

- PRISM-Proof Security Considerations - http://www.ietf.org/id/draft-hallambaker-prismproof-req-00.txt
- Privacidade na internet x segurança pública. Uma relação polêmica - http://www.ibliss.com.br/blog/privacidade-na-internet-x-seguranca-publica-uma-relacao-polemica/
- Como a NSA traiu a confiança de todo o mundo - http://anchisesbr.blogspot.com.br/2013/11/seguranca-como-nsa-traiu-confianca-de.html

Alexandro Silva
alexos@alexos.org
http://alexos.org