

Segurança, aonde?!

Leslie H. Watter

Outline

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Uma pergunta para vocês. . .



A BatCaverna é segura?



O que é segurança ?

- ▶ O que é segurança?

Segurança



Segurança ??



O que é segurança ?

Segurança da Informação

A segurança da informação está diretamente relacionada com **proteção de um conjunto de informações**, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

São características básicas da segurança da informação os atributos de **confidencialidade, integridade, disponibilidade e autenticidade**, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.

O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

O que é Segurança ?

segurança é sempre uma escolha entre:

facilidade de uso \times ***proteção***

Segurança da Informação ?

1. O que proteger?
2. Quando?
3. Como?
4. Onde?
5. De quem?
6. Por quê?

Exemplo



Figura 1 : Backup

Por quê ?



SHIT HAPPENS

(shut up and deal with it)

Por quê!?



Segurança, Ogros e semelhanças . . .



Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Camadas da Segurança de TI



Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Física

- ▶ Cercas / Portões
- ▶ Portas e Portarias
 - ▶ Catracas
 - ▶ Detectores de Metais
 - ▶ Crachás
- ▶ Sensores de Invasão em Paredes e Janelas
- ▶ Seguranças
- ▶ CFTV
- ▶ Sistemas de Climatização
- ▶ Documentação (eng. civil/elétrica/hidráulica)
- ▶ Sistemas de Detecção/Combate a incêndio
- ▶ Compartimentalização de Ambientes

Datacenter

- ▶ Terreno: Muro, Controle de Acesso, Guaritas e Seguranças
- ▶ Prédio: Paredes, controle de acesso: recepção, seguranças, catracas
- ▶ Callcenter: 2 portas de vidro, controle de acesso: crachá, segurança
- ▶ Datacenter: 2 portas de aço: controle de acesso: crachá + biometria
 - ▶ Racks com chave e Câmeras
 - ▶ Sala Cofre: + biometria

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Operações

- ▶ Controles
 - ▶ Hardware e Equipamentos
 - ▶ Software
 - ▶ Pessoal (Gestão de RH)
- ▶ Manejo de Mídia
 - ▶ Armazenamento
 - ▶ Descarte
- ▶ Mesas e Quadros *Limpos*
- ▶ CSIRT
- ▶ Mecanismos de controle e Verificação
 - ▶ Recuperação de Desastres
 - ▶ Análises de Vulnerabilidades/ Testes de Invasão
 - ▶ Controle de Logs

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

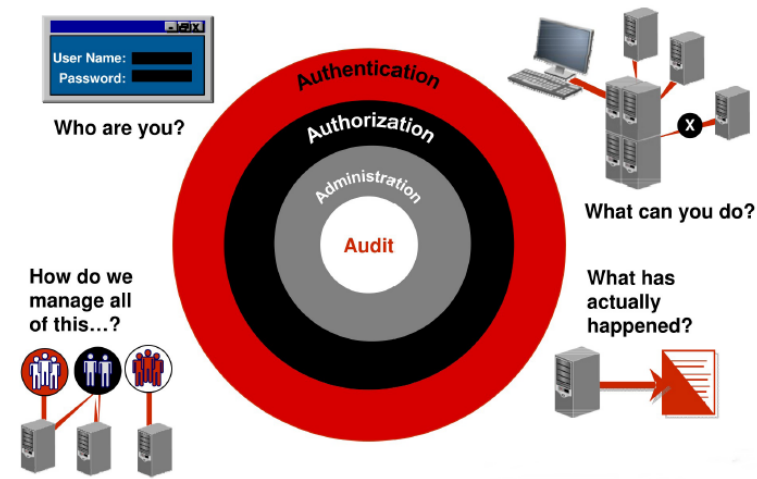
Atualização

Conclusão

Controle de Acesso

- ▶ Ambientes
 - ▶ Biometria
 - ▶ Crachás
- ▶ Sistemas
 - ▶ ACLs
 - ▶ Biometria, tokens, smartcards, etc
 - ▶ SSO (Single SignOn)
 - ▶ Serviços de Autenticação AAA
- ▶ Os mecanismos de autenticação de usuários dividem-se em três categorias: baseados
 - ▶ no conhecimento (o que se sabe)
 - ▶ em propriedade (o que se possui)
 - ▶ em características (o que se é)

O AAAA da Segurança



Problemas ?!

- ▶ Sistema Operacional
 - ▶ Auto login !?!
- ▶ Controle de Acesso
 - ▶ Senhas 'padrão' para acesso aos servidores
- ▶ Aplicação
 - ▶ Aplicações com 'páginas de execução de SQL' direto em produção porque a infraestrutura restringe o acesso.
 - ▶ Perfis de usuário com superpoderes e senhas fracas (admin/admin)

Problemas ?!

- ▶ Sistema Operacional
 - ▶ Auto login !?!
- ▶ Controle de Acesso
 - ▶ Senhas 'padrão' para acesso aos servidores
- ▶ Aplicação
 - ▶ Aplicações com 'páginas de execução de SQL' direto em produção porque a infraestrutura restringe o acesso.
 - ▶ Perfis de usuário com superpoderes e senhas fracas (admin/admin)

Problemas ?!

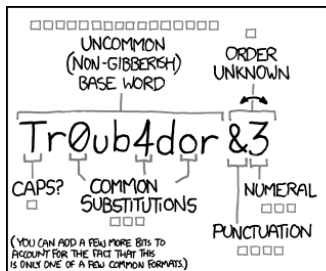
- ▶ Sistema Operacional
 - ▶ Auto login !?!
- ▶ Controle de Acesso
 - ▶ Senhas 'padrão' para acesso aos servidores
- ▶ Aplicação
 - ▶ Aplicações com 'páginas de execução de SQL' direto em produção porque a infraestrutura restringe o acesso.
 - ▶ Perfis de usuário com superpoderes e senhas fracas (admin/admin)

Problemas ?!

- ▶ Sistema Operacional
 - ▶ Auto login !?!
- ▶ Controle de Acesso
 - ▶ Senhas 'padrão' para acesso aos servidores
- ▶ Aplicação
 - ▶ Aplicações com 'páginas de execução de SQL' direto em produção porque a infraestrutura restringe o acesso.
 - ▶ Perfis de usuário com superpoderes e senhas fracas (admin/admin)

Problemas ?!

- ▶ Sistema Operacional
 - ▶ Auto login !?!
- ▶ Controle de Acesso
 - ▶ Senhas 'padrão' para acesso aos servidores
- ▶ Aplicação
 - ▶ Aplicações com 'páginas de execução de SQL' direto em produção porque a infraestrutura restringe o acesso.
 - ▶ Perfis de usuário com superpoderes e senhas fracas (admin/admin)



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

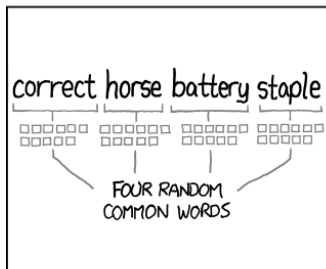
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HIGH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Segurança de Redes

- ▶ Arquitetura
 - ▶ Segmentação de Rede
 - ▶ DMZ
 - ▶ Honey Nets
 - ▶ Segregação de Serviços e Máquinas
- ▶ Controles
 - ▶ Firewall
 - ▶ IDS/IPS
 - ▶ Controle de Banda
 - ▶ Gerência de Conteúdo
 - ▶ VPN Criptografada
 - ▶ 802.1X
- ▶ Extras
 - ▶ Redundância de link
 - ▶ Balanceamento de carga

Segurança de Redes

Necessidade

- ▶ A segurança de redes é necessária pelo fato de sistemas computacionais interagirem
 - ▶ Mensagens confidenciais são enviadas entre os sistemas (p.ex. transações bancárias)
 - ▶ Instruções são enviadas de um sistema para outro
 - ▶ Serviços são fornecidos de um sistema para outros pela Internet

Objetivos

- ▶ Estabelecer protocolos seguros que garantam
 - ▶ Confidencialidade
 - ▶ Integridade
 - ▶ Disponibilidade

Segurança de Redes

Necessidade

- ▶ A segurança de redes é necessária pelo fato de sistemas computacionais interagirem
 - ▶ Mensagens confidenciais são enviadas entre os sistemas (p.ex. transações bancárias)
 - ▶ Instruções são enviadas de um sistema para outro
 - ▶ Serviços são fornecidos de um sistema para outros pela Internet

Objetivos

- ▶ Estabelecer protocolos seguros que garantam
 - ▶ Confidencialidade
 - ▶ Integridade
 - ▶ Disponibilidade

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Arquitetura de Segurança

- ▶ Segurança nativa dos sistemas
- ▶ RFCs de segurança
- ▶ Classificação da Informação
- ▶ Homologação de Produtos

"Pior que não ter um sistema de segurança, é ter um e não usar."

Arquitetura de Segurança

- ▶ Segurança nativa dos sistemas
- ▶ RFCs de segurança
- ▶ Classificação da Informação
- ▶ Homologação de Produtos

"Pior que não ter um sistema de segurança, é ter um e não usar."

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

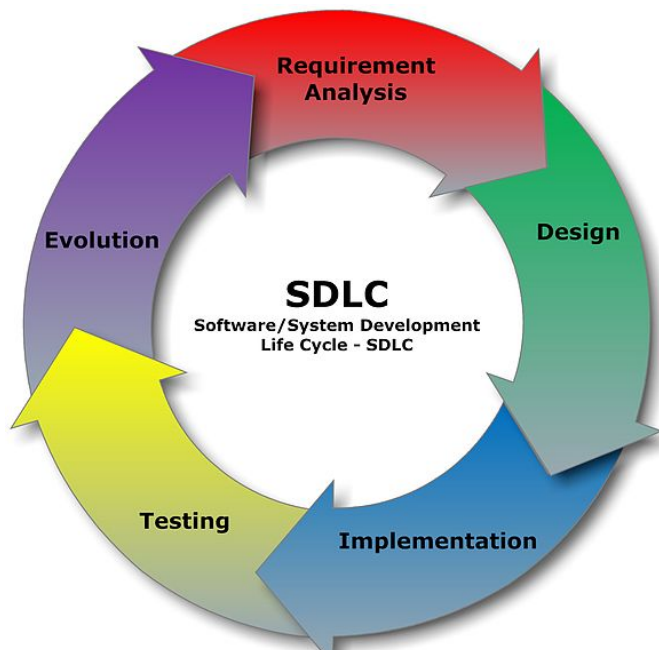
Atualização

Conclusão

Segurança de Aplicações

- ▶ Uso de Metodologias de Produção (*SDLC - software development life cycle*)
- ▶ Implantação de segurança em Desenvolvimento
- ▶ Mecanismos de Backup e Auditoria
- ▶ Políticas anti-malware
- ▶ Controle de licenciamento
- ▶ Controle de versão

Segurança de Aplicações



Segurança e Metodologias



How the customer explained it



How the Project Leader understood it



How the System Analyst designed it



How the Programmer wrote it



How the Business Consultant described it



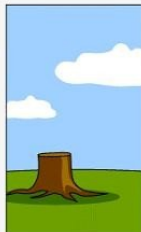
How the project was documented



What operations installed



How the customer was billed



How it was supported

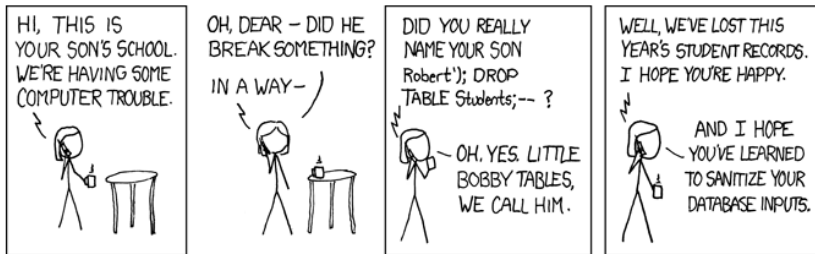


What the customer really needed

Falhas comuns em Aplicações WEB

1. Cross-Site Scripting (XSS)
 - ▶ [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
2. Cross-Site Request Forgery (CSRF)
 - ▶ [https://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))
3. Click-Jacking
 - ▶ <https://www.owasp.org/index.php/Clickjacking>
4. SQL Injection
5. Shell Injection / Command Injection
 - ▶ https://www.owasp.org/index.php/Command_Injection
6. Phishing / Fraude

SQL Injection



Desenvolvimento vs Infraestrutura

- ▶ Existem situações em que ser apenas **desenvolvedor** não basta.
- ▶ A arquitetura das aplicações depende de muitos fatores que nem sempre (pra não falar *nunca*) são levados em conta pelos desenvolvedores no momento da codificação.
- ▶ Principalmente aplicações de alto desempenho, onde cada operação no banco de dados conta e cada ciclo do processador deve ser levado em conta para o dimensionamento de hardware e conexões de rede.

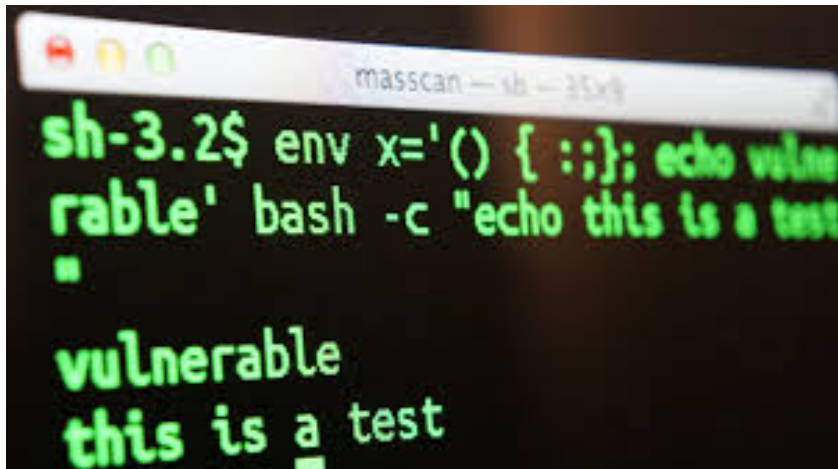
Aplicações são como gremlins, quando menos você espera elas crescem e viram monstros fora de controle...

Desenvolvimento vs Infraestrutura

- ▶ Existem situações em que ser apenas **desenvolvedor** não basta.
- ▶ A arquitetura das aplicações depende de muitos fatores que nem sempre (pra não falar *nunca*) são levados em conta pelos desenvolvedores no momento da codificação.
- ▶ Principalmente aplicações de alto desempenho, onde cada operação no banco de dados conta e cada ciclo do processador deve ser levado em conta para o dimensionamento de hardware e conexões de rede.

Aplicações são como gremlins, quando menos você espera elas crescem e viram monstros fora de controle...

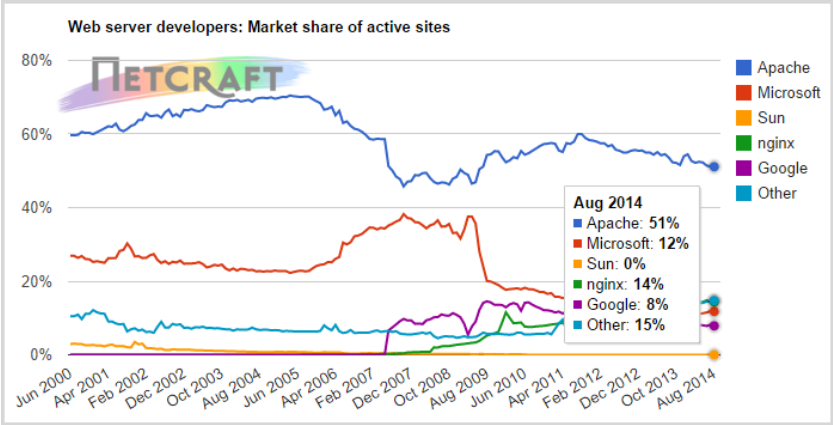
Bash Bug

A photograph of a terminal window with a dark background and green text. The window title bar shows 'masscan — sh — 35x9'. The prompt is 'sh-3.2\$'. The command entered is 'env x='() { :; }; echo vulnerable' bash -c "echo this is a test"'. The output shows 'vulnerable' on one line and 'this is a test' on the next line, with a cursor at the end of the second line.

```
sh-3.2$ env x='() { :; }; echo vulnerable' bash -c "echo this is a test"  
vulnerable  
this is a test
```

env x='() { :; }; echo vulnerable' bash -c "echo this is a test"

Bash Bug



Bash Bug

It's super simple to solve this problem.

Many software developers have already issued patches and more are being released by the hour.

Two of the most popular Linux distributions, Red Hat and Ubuntu, already have patches available, and we suspect Apple will soon release its fix. Updating a system takes almost no time.

*It's a simple process and it's a common task for most users. **The problem is with systems that are not often updated.***

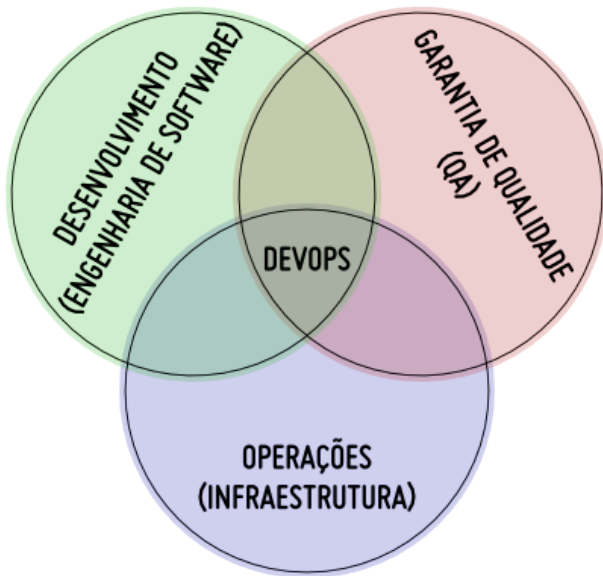
DevOPS

*DevOps (conjunção de Desenvolvedor e Operações) é uma **metodologia de desenvolvimento de software** que explora a **comunicação, colaboração e integração** entre desenvolvedores de software e profissionais de TI (Tecnologia da Informação).*

*DevOps é a reação à **interdependência entre desenvolvimento de software e operações de TI.***

Wikipédia

DevOPS



Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Criptografia

- ▶ Última linha de Defesa
- ▶ Proteção dos dados
 - ▶ Em repouso
 - ▶ Em Trânsito
- ▶ Segurança de Comunicações
 - ▶ IPSec
 - ▶ SSL

Desenvolvimento

- ▶ Mesmo utilizando criptografia, não temos como fazer tudo.
- ▶ Invariavelmente algum trabalho tem que ser terceirizado ou alguma biblioteca é utilizada. O que acaba levando a outros problemas . . .

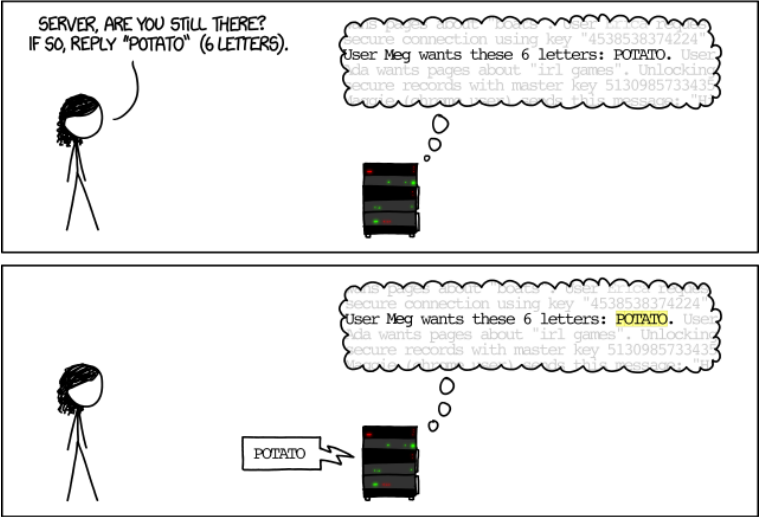
HeartBleed

*The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness **allows stealing** the **information protected**, under normal conditions, **by the SSL/TLS encryption** used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).*



HeartBleed comics

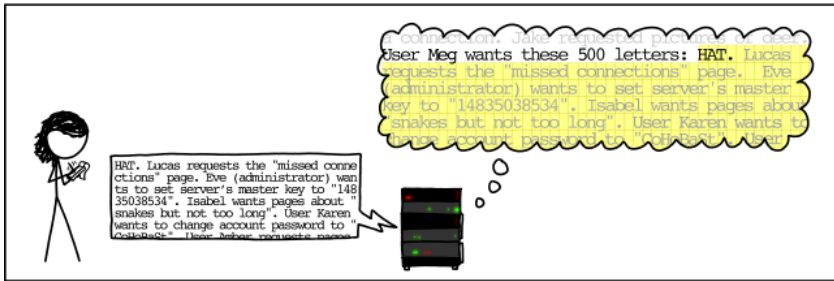
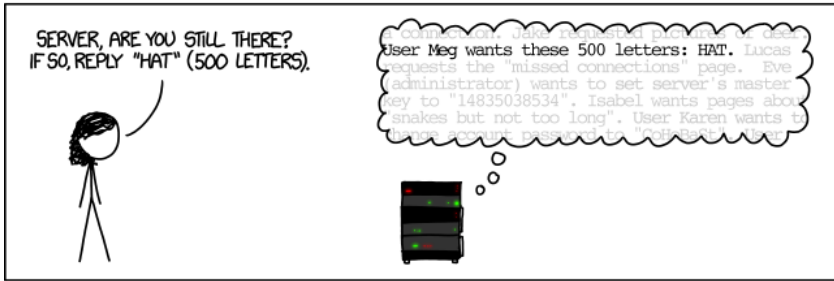
HOW THE HEARTBLEED BUG WORKS:



HeartBleed comics



HeartBleed comics



HeartBleed

Tudo isso por quê ?

- ▶ confiança no 'outro lado'
- ▶ falta de validação simples

Criptografia

- ▶ ... mesmo com tudo isso ainda usamos criptografia ?
- ▶ Sim! Ainda queremos proteger nossas informações
- ▶ e também o nosso dinheiro ;-)

Criptografia

- ▶ ... mesmo com tudo isso ainda usamos criptografia ?
- ▶ Sim! Ainda queremos proteger nossas informações
- ▶ e também o nosso dinheiro ;-)

Criptografia

- ▶ ... mesmo com tudo isso ainda usamos criptografia ?
- ▶ Sim! Ainda queremos proteger nossas informações
- ▶ e também o nosso dinheiro ;-)

Criptografia

Entre as diferentes aplicações de criptografia que podemos citar está a criptomoeda (*cryptocurrency*).

A cryptocurrency (or crypto currency) is a medium of exchange using cryptography to secure the transactions and to control the creation of new units. Cryptocurrencies are a subset of alternative currencies, or specifically of digital currencies.

Criptografia e Dinheiro



Bitcoin ?!

"Bitcoin é uma forma de dinheiro, com a diferença de ser digital e não ser emitido por nenhum governo. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro. É uma tecnologia inovadora."

Mercado Bitcoin

Bitcoin é um software de código-fonte aberto, sustentado por uma rede de computadores distribuída (peer-to-peer) em que cada nó é simultaneamente cliente e servidor. Não há um servidor central nem qualquer entidade controlando a rede. O protocolo do Bitcoin, baseado em criptografia avançada, define as regras de funcionamento do sistema, às quais todos os nós da rede aquiescem, assegurando um consenso generalizado acerca da veracidade das transações realizadas e evitando qualquer violação do protocolo.

Por que Bitcoin ?

- ▶ Moeda Virtual com muita exposição na mídia
- ▶ Várias instituições de diversos países aceitam
- ▶ "Não é para os fracos" . . .

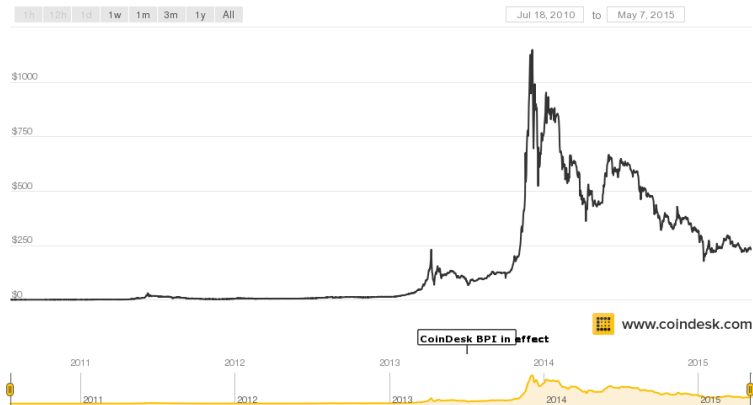


Figura 4 : Variação na cotação do bitcoin

Bitcoin ?!

No que a moeda virtual pode influenciar o desenvolvimento de Software ?

Quem aceita bitcoins hoje ?

- ▶ WordPress.com
- ▶ Overstock.com
- ▶ Amazon
- ▶ Target
- ▶ CVS
- ▶ Subway
- ▶ Victoria's Secret

Qual o risco ?

- ▶ Variabilidade do câmbio
- ▶ Dificuldade em gerar novos bitcoins, exigindo mais poder computacional.

Bitcoin ?!

No que a moeda virtual pode influenciar o desenvolvimento de Software ?

Quem aceita bitcoins hoje ?

- ▶ WordPress.com
- ▶ Overstock.com
- ▶ Amazon
- ▶ Target
- ▶ CVS
- ▶ Subway
- ▶ Victoria's Secret

Qual o risco ?

- ▶ Variabilidade do câmbio
- ▶ Dificuldade em gerar novos bitcoins, exigindo mais poder computacional.

Bitcoin

Viabilidade

- ▶ Você saberia avaliar se é viável a utilização de bitcoins no seu negócio ?

Bitcoin Argentina

- ▶ Mercados em crise como o da Argentina viram no BTC uma moeda mais estável que a local.

And so Argentines, at least the most technologically savvy of them, are turning to bitcoin as a way to exchange their pesos for what they're actually worth, rather than what the government says they should be worth. Bitcoin, in other words, is simply a way for Argentines to make an end-run around the banking system, which works with the Argentine government to force its citizens to use the ever-devaluing peso.

Bitcoin

Viabilidade

- ▶ Você saberia avaliar se é viável a utilização de bitcoins no seu negócio ?

Bitcoin Argentina


- ▶ Mercados em crise como o da Argentina viram no BTC uma moeda mais estável que a local.

And so Argentines, at least the most technologically savvy of them, are turning to bitcoin as a way to exchange their pesos for what they're actually worth, rather than what the government says they should be worth. Bitcoin, in other words, is simply a way for Argentines to make an end-run around the banking system, which works with the Argentine government to force its citizens to use the ever-devaluing peso.

Popularidade

- ▶ E como o bitcoin se tornou tão popular ?

Silk Road

**Silk Road**
anonymous market


messages 1 | orders 0 | account \$0.00

Search

Go

Hi,



logout




Shop by Category

- Food 5
- Beverages 2
- Apparel 168
- Art 4
- Books 865
- Collectibles 8
- Computer equipment 30
- Custom Orders 47
- Digital goods 365
- Drug paraphernalia 174
- Drugs 4,217
- Electronics 37
- Erotica 369
- Forgeries 92
- Hardware 3
- Herbs & Supplements 14
- Home & Garden 3
- Jewelry 52
- Lab Supplies 29
- Lotteries & games 30
- Medical 31
- Money 100
- Packaging 25
- Services 37
- Weight loss 19
- Writing 2
- Yubikeys 3


sort by: ☐ Domestic only




Cocaine Energy Drink - Banned
seller: nameddeclined(100)
ships from: United States of America
\$0.74
add to cart




Kefir grains - water kefir
seller: etizolam(97)
ships from: United States of America
\$0.83
add to cart



3Jane Stealth Listing Feedback
seller: 3Jane(100)
ships from: Canada
\$0.00
add to cart



Kefir grains - milk kefir
seller: etizolam(97)
ships from: United States of America
\$0.90
add to cart





THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York



Silk Road



Figura 5 : Efeitos no Bitcoin após fechamento Silk Road

Silk Road - tecnologias

1 - Bitcoin

If you assume your bitcoins can't be traced back to you, think again. Like cash, bitcoins aren't tied to a person's identity. But unlike cash, a detailed public ledger called the blockchain keeps track of each wallet a bitcoin passes through.

2 - Chat logs

So much chatter. Thousands of pages of chat logs helped prosecutors trace the growth of Silk Road.

Silk Road - tecnologias

3 - Encryption

Encryption puts a digital padlock on information so it can't be viewed. But eventually the person with the keys has to unlock the information in order to see it. That's why law enforcement agents had to catch Ulbricht while he was logged into the Silk Road's admin console.

4 - Facebook and other public websites

Ulbricht sowed the seeds of his demise the very first time he publicized the Silk Road. To get people interested in the the new site in January 2011, Ulbricht posted a message on the Bitcointalk.org forum, under the username Altoid, asking if anyone had tried the site.

Silk Road - tecnologias

5 - Automated server log-ins

The Silk Road servers were maintained in large part through ssh (Secure Shell), a tool that allows administrators to log into remote machines in a way that the communication is encrypted. Users can set up ssh hosts such that trusted parties can log in automatically without providing a password. A list of trusted parties is kept in a file on the server, along with their encrypted passkeys.

Bancos

Toda moeda precisa de um 'banco' para ser armazenada de forma 'segura'.

MtGox - história

Mt. Gox was a Bitcoin exchange based in Tokyo, Japan. It was launched in July 2010, and **by 2013 was handling 70%** of all Bitcoin transactions.

In **February 2014**, the Mt. Gox company suspended trading, closed its website and exchange service, and **filed** for a form of **bankruptcy** protection from creditors called minji saisei, or civil rehabilitation, to allow courts to seek a buyer.

In April 2014, the company began liquidation proceedings.

It announced that around **850,000 bitcoins** belonging to customers and the company were missing and likely **stolen**, an amount valued at more than **\$450 million** at the time.

Although 200,000 bitcoins have since been "found", the reason(s) for the disappearance – **theft, fraud, mismanagement**, or a combination of these – are unclear as of March 2014.

Problemas de segurança no código causam estragos problemas ao MtGox:



Yesterday, the bitcoin exchange MtGox – riddled by problems – issued a press release saying the bitcoin protocol was to blame for its ongoing problems. That statement, which caused the markets to nosedive temporarily, is outright false. **The problem is, and was, bad code hygiene** in the MtGox exchange itself. Here are the details.

(...)

Here's the real problem: **MtGox is running its own homebuilt bitcoin software, and has not cared to update and upgrade that software along with the developments of the bitcoin protocol.** Recently, after a very long grace period, the bitcoin protocol tightened slightly in order to disallow unnecessary information in transaction records, and did this to fix the malleability problem that MtGox blamed.

E não foi só Mt. Gox que se foi . . .

www.ibtimes.co.uk/chinese-bitcoin-exchange-gbl-vanishes-takes-coins-521557

IBT

News

World

Business

Politics

Technology

Science

Sport

Entertainment



Technology

Bitcoin

Hong Kong

Chinese Bitcoin Exchange Vanishes Taking £2.5m of Coins With It

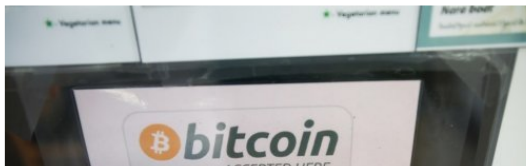


By **Alistair Charlton**

November 12, 2013 09:57 GMT





A Chinese Bitcoin exchange has vanished without trace, taking more than \$4 million of the virtual currency with it and leaving profit-hungry investors out of pocket.



E não foi só Mt. Gox que se foi . . .

Topic: *Security*

Follow via:  

MyCoin closes its doors, \$387 million in investor funds vanishes

Summary: *Bitcoin exchange MyCoin has vanished -- leaving up to \$387 million in investor funds unaccounted for.*



By [Charlie Osborne](#) for [Zero Day](#) | February 10, 2015 -- 11:40 GMT (03:40 PST)



Follow [@ZDNetCharlie](#)

6,397 followers

[Get the ZDNet Security newsletter now](#)



Silk Road II Hacked

SILK ROAD 2 HACKED, ALL BITCOINS STOLEN – \$2.7 MILLION

POSTED BY: DEEPPDOTWEB FEBRUARY 13, 2014 IN FEATURED, NEWS UPDATES 60 COMMENTS

 Like  Tweet 1,143  +1 104  Share 23  7

Update 5: [Alleged Silk Road 2.0 Hacker Doxxed!?](#)

Update 4: Defcon's Latest post: We Will Repay The Stolen Funds

Update 3: Silk Road 2 Admin – Silk Road is not dead!

Update 2: As the time passes there are more and more suspicions that this was in fact a **SCAM** by the Silk Road staff – and not a hack, we will post more details about it once, and if we get the full picture.



Looking for new marketplace? Try this [List of hidden markets](#)

Must Read: [Leave the Scammer-Op Behind!](#)

Update: The amount of BTC that was stolen was calculated by Nicholas Weaver @NCWeaver – Computer Security Researcher, to be around: 4474.266369160003BTC that are with the value of about \$2.7 Million.

Em resumo

- ▶ Manter atualizado o código com a evolução dos protocolos (nesse caso bitcoin) é algo mais que necessário, é imprescindível.
- ▶ Estar atualizado com o que acontece é deveras importante, independente de qual a sua função.

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Centros de Tratamento de Incidentes - CERTs

- ▶ <http://www.cert.br/>
- ▶ <http://www.cert.org/>
- ▶ <http://www.apcert.org/about/structure/members.html>
(lista de diversos CERTs)

Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs)

- ▶ <http://www.cert.br/csirts/>
- ▶ <http://www.first.org/>
- ▶ <https://www.trusted-introducer.org/>

Listas de E-mail

- ▶ <http://seclists.org/>
 - ▶ Full Disclosure
 - ▶ Secure Coding
 - ▶ Data Loss
 - ▶ Open Source Security
 - ▶ Bugtraq
- ▶ <https://www.defcon.org/html/links/mailling-lists.html>
 - ▶ NT Security
 - ▶ Info Sec News [ISN]

Benefícios ...

A parte boa da lista é que a informação 'vem' até você...

Twitter I

- ▶ @securityfocus
- ▶ @NakedSecurity
- ▶ @CiscoSecurity
- ▶ @SearchSecurity
- ▶ @msftsecurity – microsoft
- ▶ @debian__security
- ▶ @fedorasecurity
- ▶ @IntelSecurity
- ▶ @VisaSecurity – tecnologia nos cartões de crédito
- ▶ @SecureTips
- ▶ @nodesecurity – node.js
- ▶ @CAsSecurity

Twitter II

- ▶ @Snort
- ▶ @mozsec – Mozilla Firefox Security Team
- ▶ @secprods
- ▶ @SecurityXploded
- ▶ @SecurityTube
- ▶ @TheHackersNews
- ▶ @SANSInstitute
- ▶ @owasp
- ▶ @Kasperskybrasil
 - ▶ entre outros

Sites de Notícias

Informações Técnicas

- ▶ <http://www.securityfocus.com/>
- ▶ <https://nakedsecurity.sophos.com>
- ▶ <http://searchsecurity.techtarget.com/>
- ▶ <https://securelist.com/>
- ▶ <https://cve.mitre.org/news/index.html>

Notícias para Gestores

- ▶ <http://computerworld.com.br/seguranca>

Segurança é responsabilidade

De quem é a responsabilidade por garantir a segurança ?

- ▶ ... de todos os envolvidos!

Segurança é responsabilidade

De quem é a responsabilidade por garantir a segurança ?

- ▶ ... de todos os envolvidos!

Tópico

Segurança, aonde ?!

Segurança em TI

Física

Operações

Acesso

Redes

Básica

Aplicações

Criptografia

Atualização

Conclusão

Então ...

... a Batcaverna é Segura ?

E aí, a Batcaverna é Segura ?



Contato

Leslie H. Watter
watter@gmail.com
<http://github.com/watter>

Referências

1. <http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html>
2. <https://fortune.com/2015/05/04/bitcoin-argentina/>
3. <http://pt.wikipedia.org/wiki/DevOps>
4. http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o
5. <http://www.smashingmagazine.com/2010/10/18/common-security-mistakes-in-web-applications/>
6. <http://www.infomoney.com.br/blogs/moeda-na-era-digital/post/3160782/dez-formas-explicar-que-bitcoin>
7. <http://explainextended.com/2014/07/09/top-5-xkcd-comics-which-can-illustrate-programming-questions/>
8. http://en.wikipedia.org/wiki/Kaspersky_Lab
9. <http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html>
10. <http://sdlc.uconn.edu/>
11. <https://cve.mitre.org/news/index.html>
12. <https://nvd.nist.gov/home.cfm>
13. <http://falkvinge.net/2014/02/11/the-embarrassing-fact-mtgox-left-out-of-their-press-release/>
14. <http://www.deepdotweb.com/2014/02/13/silk-road-2-hacked-bitcoins-stolen-unknown-amount/>
15. <http://www.engadget.com/2014/09/25/what-is-the-shellshock/>