Pilares da Segurança e Chaves criptográficas

Marcus Botacin[1]

[1]Assistant Professor
Texas A&M University (TAMU), USA
botacin@tamu.edu
@MarcusBotacin

Tópicos

Agenda

As Propriedades da Segurança: Introdução

Propriedades ACID

- Autenticidade
- Confidencialidade
- Integridade
- Disponibilidade

As Propriedades **A**CID

Autenticidade

- Quem é você?
- Você é você mesmo?

Onde você vê:

- Formulários de *login*.
- Autenticação por chaves.

Não confundir com: Autorização

- Você pode fazer isso?

As Propriedades A**C**ID

Confidencialidade

- Apenas as partes sabem sobre isso?
- Nenhum terceiro pode ficar sabendo sobre isso?

Onde você vê:

- Formulários de submissão criptografados.
- Conexões encriptadas.

Não confundir com: Anonimidade

- Ninguém sabe quem você é!

As Propriedades ACID

Integridade

- Os dados são o que deviam ser?
- Os dados continuam como estavam?

Onde você vê:

- Permissões de leitura/escrita.
- Controles de acesso.
- Soluções de backup.

Quando e violado:

- Ataques por *Ransomware*

As Propriedades ACI**D**

Disponibilidade

- Eu ainda consigo acessar os dados?
- Quando eu precisar, os dados estarão la?

Violações de Disponibilidade: Onde você vê:

- Eventos tipo *Black Friday* (benigno)
- Ataques do tipo Negação de Serviço (DoS) (malicioso)

As Propriedades da Segurança: Resumo

Propriedades ACID

- Autenticidade
- Confidencialidade
- Integridade
- Disponibilidade

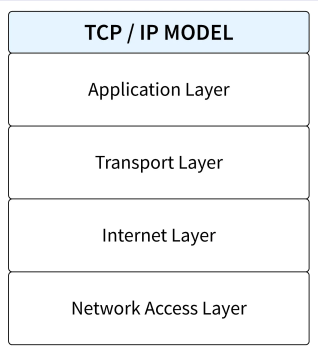
Propriedades Derivadas

- Privacidade
- Anonimidade
- Não-Repúdio

Agenda

Onde vai a segurança?

A Pilha TCP/IP



Agenda

O Problema: Man-In-The-Middle

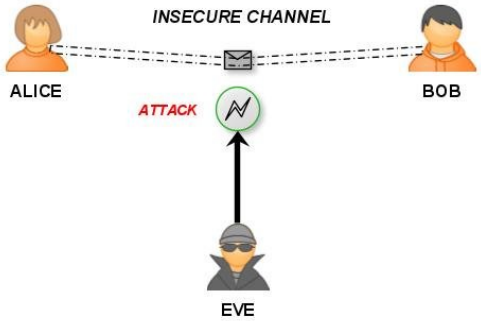


Figure: **Fonte:** `https://tinyurl.com/5dekpu74`

A Solução: Criptografia

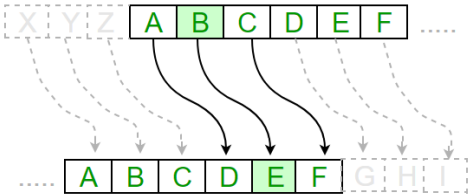


Figure: **Fonte:** https://tinyurl.com/df8ubpht

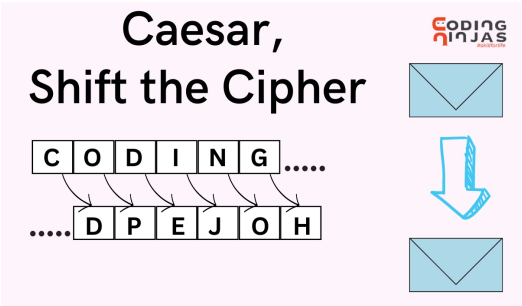


Figure: **Fonte:** https://tinyurl.com/mrx8p3ms

Criptografia “de verdade”

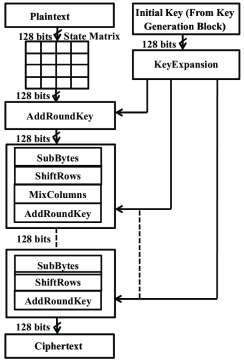


Figure: **Fonte:** `https://tinyurl.com/3zjnremx`

Criptografia de Chave Simétrica

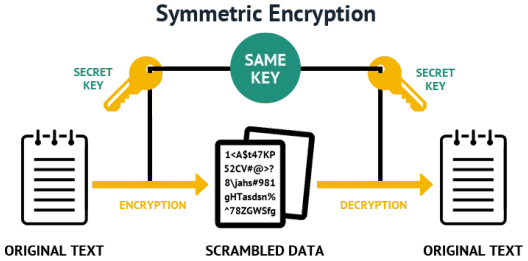


Figure: **Fonte:** `https://tinyurl.com/mttstkmv`

Criptografia de Chave Assimétrica

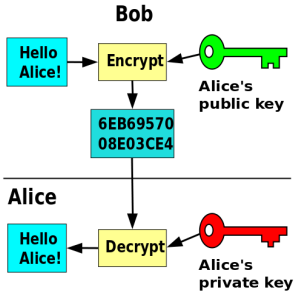


Figure: **Fonte:** `https://tinyurl.com/yb4956rc`

Negociação de Chaves

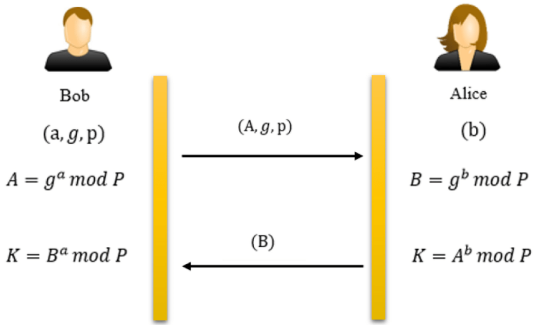


Figure: **Fonte:** `https://tinyurl.com/y6pm592m`

Figure: **Video:** `https://youtu.be/qgzpJnStGto`

Resumo

Tipos de Criptografia

- Simétrica: Onde todas as partes utilizam a mesma chave.
- Assimétrica: Onde as partes utilizam chaves diferentes.

Criptografia Assimétrica: Tipos de Chaves

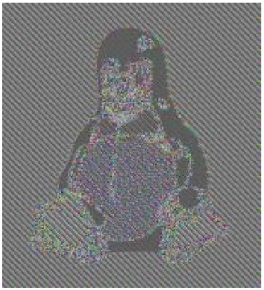
- Pública: A chave visível no canal inseguro.
- Privada: A chave mantida sob controle exclusivo da parte.

Criptografia na Internet

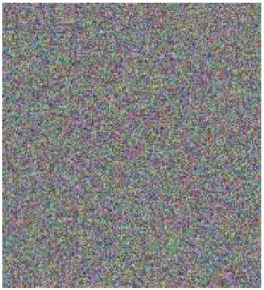
1. Estabelecimento de chave via Diffie-Hellman.
2. Troca de dados via chave simétrica compartilhada.

Desafio: Configuração Adequada

(a) Original image



(b) Encrypted with AES only



(c) Encrypted with AES using CBC mode

Figure: **Fonte:** `https://tinyurl.com/39ezvxf5`

Agenda

Publicação

RESEARCH-ARTICLE

The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study

Authors Marcus Botacin, Anatoli Kalysch, and André Grégio | Authors Info & Claims

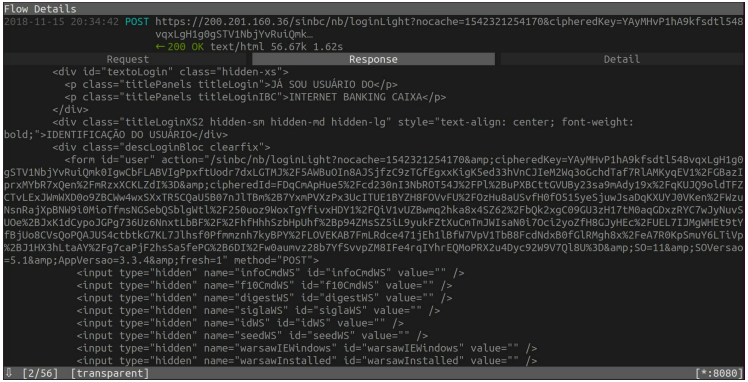
ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security • August 2019
Article No.: 49, Pages 1 - 10 • https://doi.org/10.1145/3339252.3340103

Published: 26 August 2019 Publication History | Check for updates

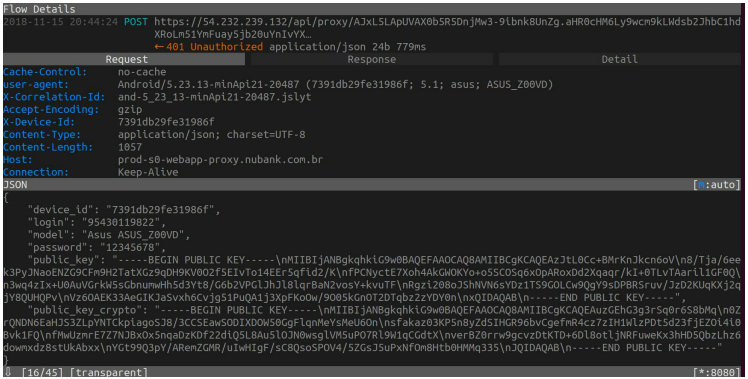
2 421 | PDF | eReader

Figure: **Fonte:** `https://dl.acm.org/doi/10.1145/3339252.3340103`

Man-In-The-Middle (Banco 1)



Man-In-The-Middle (Banco 2)

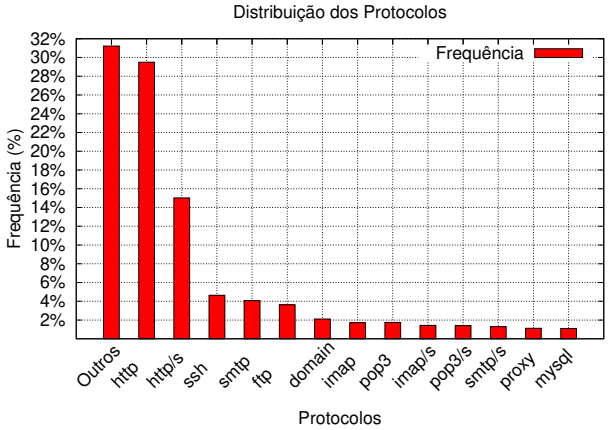


Agenda

Publicação

Figure: **Fonte:** `https://arxiv.org/abs/2109.06068`

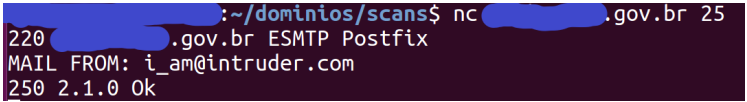
Escaneamento do domínios .gov



Possíveis Falhas de Segurança (1/2)

```
[redacted]:~/dominios/scans$ dig @[redacted].gov.br google.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @[redacted].gov.br google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6764
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             273     IN      A       172.217.29.174

;; AUTHORITY SECTION:
google.com.             7134    IN      NS      ns3.google.com.
google.com.             7134    IN      NS      ns2.google.com.
google.com.             7134    IN      NS      ns1.google.com.
google.com.             7134    IN      NS      ns4.google.com.
```

Possíveis Falhas de Segurança (2/2)



Agenda

Resumo

Problema

- Os protocolos de Internet não foram projetados com segurança em mente.

Solução

- Soluções de segurança propostas na camada de aplicação: e.g., Criptografia.

Desafio

1. Configuração adequada de serviços e protocolos criptográficos.

Obrigado!

Dúvidas? Comentários?

botacin@tamu.edu
@MarcusBotacin