Análise e implementação de um método para prover integridade a sistemas de banco de dados

Gabriel Garcia Becker, Lucas Pandolfo Perin, Anderson Luiz Silvério,
Marcelo Carlomagno Carlos, Ricardo Felipe Custódio

Laboratório de Segurança em Computação
Universidade Federal de Santa Catarina

{gabrielbecker, lucasperin, anderson.luiz, custodio}@inf.ufsc.br
marcelo.carlos.2009@rhul.ac.uk

19 de Novembro de 2012

LabSEC
Laboratório de Segurança em Computação

Sumário

LabSEC
Laboratório de Segurança em Computação

Introdução

LabSEC
Laboratório de Segurança em Computação

Motivação

- *Modificação não autorizada*
- Adição não autorizada
- Remoção não autorizada
- Consulta não autorizada

id	nome	email	salário
41	João	joao@labsec.ufsc.br	3000
42	Maria	maria@labsec.ufsc.br	45000

LabSEC
Laboratório de Segurança em Computação

Motivação

- Modificação não autorizada
- *Adição não autorizada*
- Remoção não autorizada
- Consulta não autorizada

id	nome	email	salário
41	João	joao@labsec.ufsc.br	3000
42	Maria	maria@labsec.ufsc.br	4500
43	Roberto	roberto@labsec.ufsc.br	10000

LabSEC
Laboratório de Segurança em Computação

Motivação

- Modificação não autorizada
- Adição não autorizada
- *Remoção não autorizada*
- Consulta não autorizada

id	nome	email	salário
41	João	joao@labsec.ufsc.br	3000
~~42~~	~~Maria~~	~~maria@labsec.ufsc.br~~	~~4500~~

LabSEC
Laboratório de Segurança em Computação

Motivação

- Modificação não autorizada
- Adição não autorizada
- Remoção não autorizada
- *Consulta não autorizada*

id	nome	email	salário
41	João	joao@labsec.ufsc.br	3000
42	Maria	maria@labsec.ufsc.br	4500

LabSEC
Laboratório de Segurança em Computação

Objetivos

- Confidencialidade
- Integridade
- Autenticidade
- Rastreabilidade

LabSEC
Laboratório de Segurança em Computação

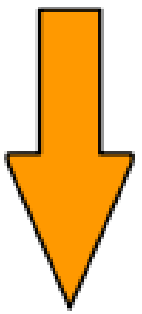
Proposta

LabSEC
Laboratório de Segurança em Computação

Sigilo

- **Confidencialidade**
- Integridade
- Autenticidade
- Rastreabilidade

Encrypt (chave, salario)



id	nome	email	salário
41	João	joao@labsec.ufsc.br	7dk2dk
42	Maria	maria@labsec.ufsc.br	dyrn73

Figura: Sigilo

LabSEC
Laboratório de Segurança em Computação

HMac

- Evitar a modificação não autorizada de registros contidos na base de dados.
- Permite identificar as modificaçãos não autorizadas.

HMac

- Confidencialidade
- **Integridade**
- **Autenticidade**
- Rastreabilidade

HMAC(K, m) = H (K || H (K || m))

HMAC(chave, id||nome||email)

id	nome	email	salário	hmac
41	João	joao@labsec.ufsc.br	7dk2dk	aqw2s3
42	Maria	maria@labsec.ufsc.br	dyrn73	kjh43kj

Figura: HMac

LabSEC
Laboratório de Segurança em Computação

Histórico cifrado

- Com o HMac, não é possivel identificar remoções não autorizadas.
- O Histórico Cifrado permite identificar as modificaçãos não autorizadas.
- Permite relacionar dois ou mais registros de forma que possa se detectar a ausência de um deles.

LabSEC
Laboratório de Segurança em Computação

Histórico cifrado

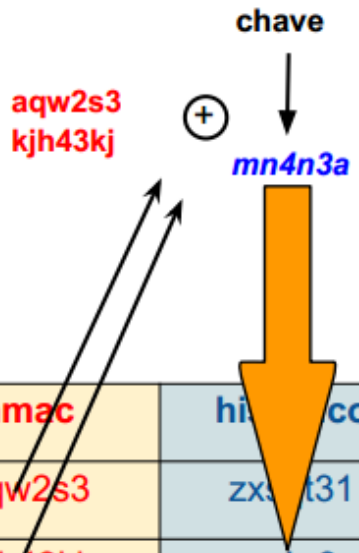
- Não permitir que uma terceira parte possa calcular o "histórico cifrado" sem conhecer as chaves de cifração.
- Utilização de operações de baixo custo computacional: criptografia simétrica e a operação lógica "ou exclusivo" (XOR);

LabSEC
Laboratório de Segurança em Computação

Histórico cifrado

- Confidencialidade
- **Integridade**
- **Autenticidade**
- **Rastreabilidade**

Hist(K, List<HMAC>) = E (K, xor (List<HMAC>)))



id	nome	email	salário	hmac	hi co
41	João	joao@labsec.ufsc.br	7dk2dk	aqw2s3	zx t31
42	Maria	maria@labsec.ufsc.br	dyrn73	kjh43kj	nm4n3a

Figura: Histórico Cifrado

LabSEC
Laboratório de Segurança em Computação

Desempenho

Desempenho

Tabela: Descrição do ambiente de simulação

Processador	Intel Core 2 Duo 2.53Mhz
Memória RAM	4GB
Sistema Operacional	Mac OS X 10.6.4
Linguagem	PHP 5.3
SGDB	MySQL 5.1
Algoritmo de Hash	SHA-1
Tamanho de Chave HMAC	128 bits
Algoritmo de cifração	AES 128 bits
Tamanho de chave simétrica	128 bits

LabSEC
Laboratório de Segurança em Computação

Select, Insert, Updade e Delete

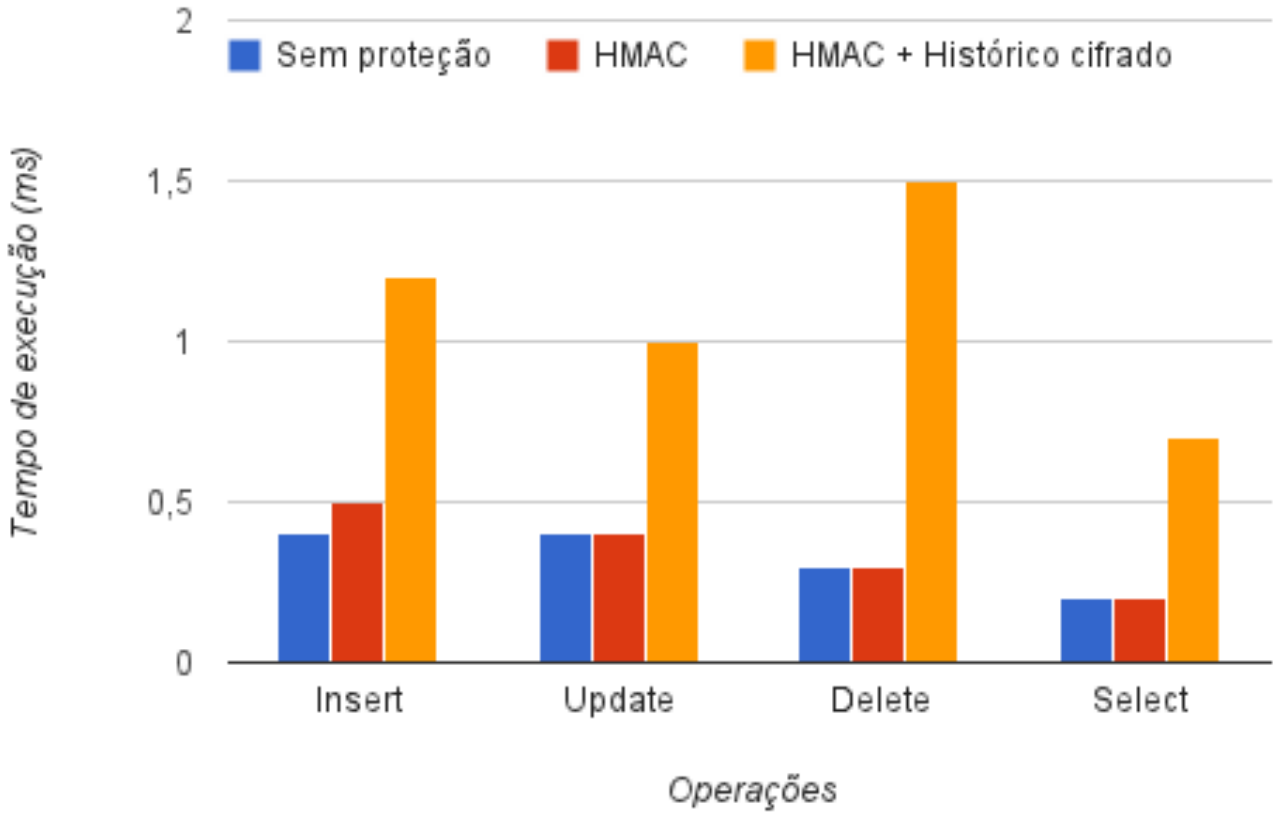


Figura: Tempo de execução em segundos.

LabSEC
Laboratório de Segurança em Computação

Calculo em tabelas ja existentes

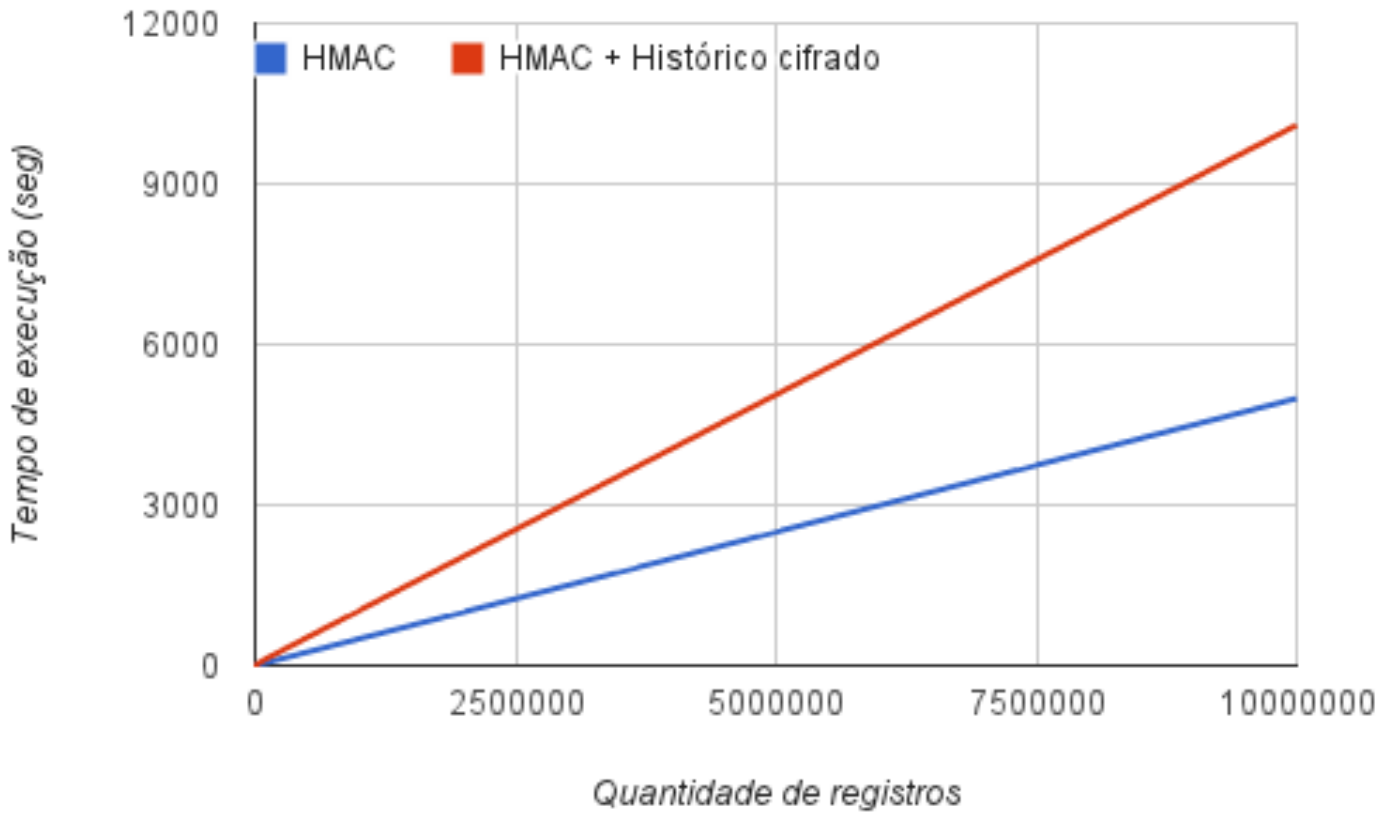


Figura: Tempo de execução em segundos.

LabSEC
Laboratório de Segurança em Computação

Verificar integridade

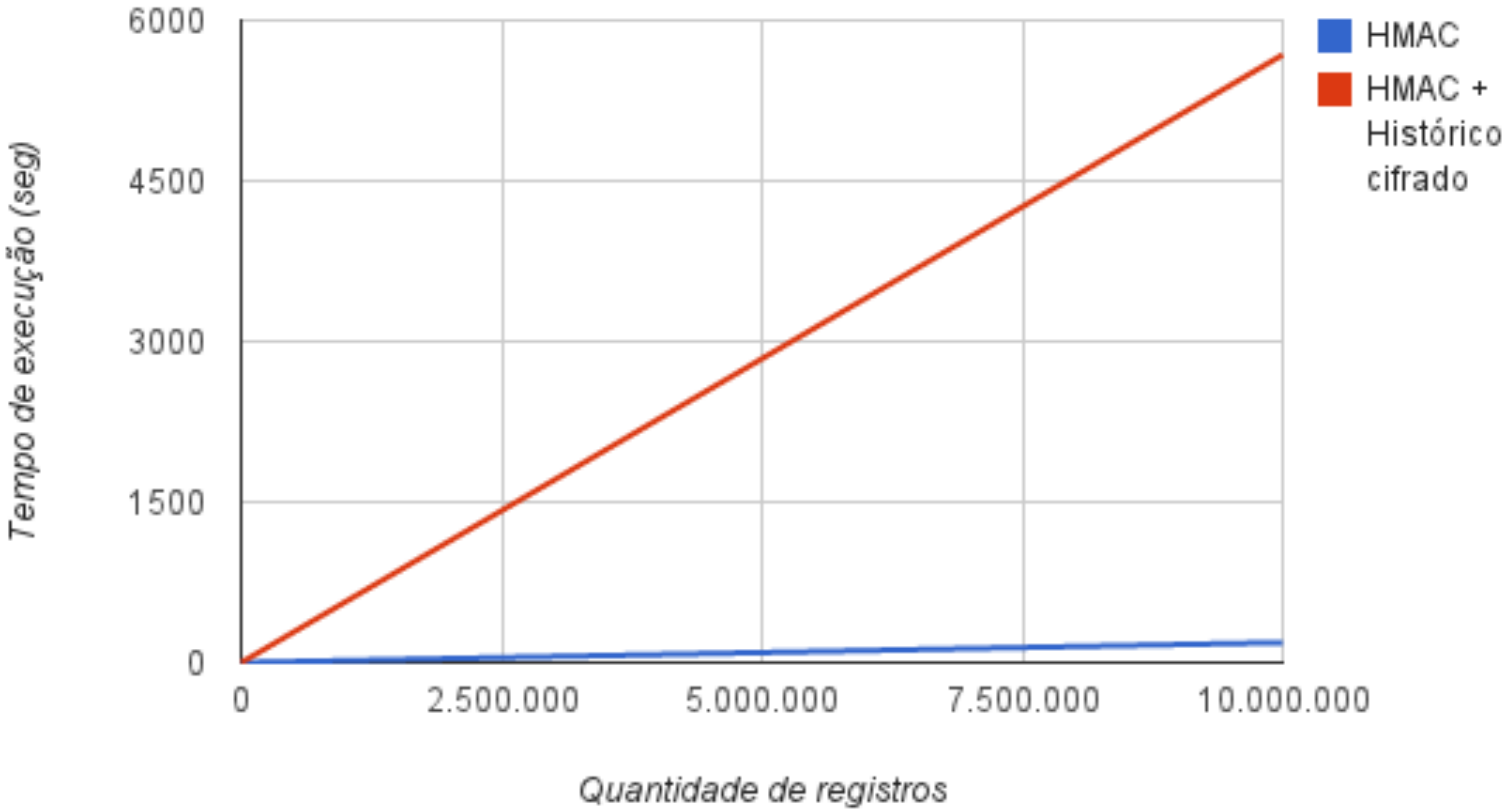


Figura: Tempo de execução em segundos.

LabSEC
Laboratório de Segurança em Computação

Implementação

Biblioteca

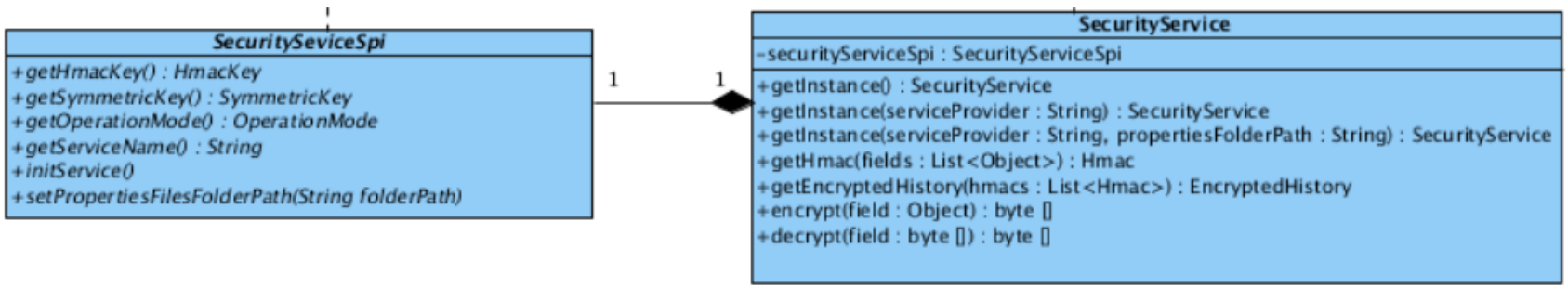


Figura: Representação do *provider* da biblioteca

LabSEC
Laboratório de Segurança em Computação

Considerações finais

LabSEC
Laboratório de Segurança em Computação

Considerações finais

- Desenvolvimento de método independente de SGBD.
- Testes mostram que o uso do HMAC é imperceptível na execução das operações básicas.
- Testes de operações em lote com tempos satisfatórios.
- Implementação de uma biblioteca.

LabSEC
Laboratório de Segurança em Computação

Perguntas?

LabSEC
Laboratório de Segurança em Computação