

GBC083 - Segurança da Informação

Aula 2 - Sigilo Perfeito

Construção de melhores cifras

- ▶ Vigenère foi considerado segura por muito tempo
- ▶ Em criptografia antiga: uso de métodos empíricos sem garantias
 - ▶ Criptografia era uma **arte**: ciclo projeto–quebra–correção
 - ▶ Em 1970, criptografia começou usar método científico
- ▶ Como provar que esquema criptográfico é seguro?
- ▶ O que é um esquema **seguro**?

Princípios da criptografia moderna

- ▶ Evitar **ciclo projeto–quebra–correção**
- ▶ Princípio 1 - Definições formais
 - ▶ Modelo matemático precisão e definição do que é segurança
- ▶ Princípio 2 - Premissas mínimas
 - ▶ Definidas sem ambiguidades
- ▶ Princípio 3 - Provas de segurança
 - ▶ Provas formuladas de acordo com as definições formais e relativas às premissas

Princípio - Importância de definições

- ▶ *Como conseguir alguma coisa se você não sabe o que quer?
Como saber se já conseguiu?*
- ▶ Exemplo
 - ▶ “Não vamos colocar uma meta: deixaremos em aberto e quando atingirmos ela, nós dobraremos a meta”, *Presidenta Dilma Rousseff*
- ▶ O uso de definições precisas força o projetista a organizar seu trabalho em torno do que realmente deve ser feito
 - ▶ Reconhecer o que é essencial, o que é mais importante e o que não é importante

Princípio 1 - Importância de definições

- ▶ Definições permitem avaliações significativas e comparações entre esquemas distintos
- ▶ Uma definição clara permite que outros entendam as garantias de segurança provida por um esquema
 - ▶ Permite que esquemas sejam usados como componentes de um sistema maior

Princípio 2 - Premissas

- ▶ Criptografia moderna exige o uso de premissas computacionais
 - ▶ Pelo menos até provarem que $P \neq NP$
- ▶ Princípio: qualquer premissa de segurança deve ser feita de maneira explícita

Princípio 2 - Importância de premissas claras

- ▶ Permite que pesquisadores tentem validar tais premissas
- ▶ Permite comparação entre esquemas baseados em diferentes condições
- ▶ Explicita implicações práticas caso premissas sejam julgadas como errôneas
- ▶ Permite a condução de provas de segurança

Princípio 3 - Provas de segurança

- ▶ Provêm uma prova rigorosa que uma construção satisfaz uma dada definição supondo um conjunto de premissas
- ▶ Provas são cruciais em criptografia, onde existem atacantes ativamente tentando quebrar o seu esquema de segurança

Limitações?

- ▶ Parte da criptografia continua sendo em parte arte
- ▶ Dada prova de segurança baseada em alguma premissa, ainda é preciso **instanciar** a premissa.
 - ▶ Verificar a validade de premissas é uma área de pesquisa ativa

Limitações?

- ▶ Provas dão uma garantia firme de segurança
 - ▶ relativa à definição e às premissas
- ▶ Mas mesmo esquemas com provas de segurança podem ser quebrados
 - ▶ Se definição não corresponde à realidade
 - ▶ Se premissa é inválida
- ▶ Definições formais e provas continuam sendo importantes e são a base da segurança

Criptografia – Sigilo Perfeito

- ▶ Garantia de segurança/meta
 - ▶ O que queremos evitar que o atacante consiga?
 - ▶ Princípio 1
- ▶ Modelo de ameaça
 - ▶ Quais capacidades assume-se que o atacante tem?
 - ▶ Princípio 2

Criptografia de chave simétrica/privada

Texto
claro
 $m =$
“oi bob
como
vai”

chave k



Texto cifrado:
 $c =$ “alkshdaioshfahr”

chave k



Encriptação:
 $c \leftarrow Enc_k(m)$

Decriptação:
 $m \leftarrow Dec_k(c)$

Modelos de ameaça

- ▶ Ataque usando somente texto cifrado
 - ▶ Somente um ou vários?
- ▶ Ataque usando texto em claro conhecido
 - ▶ Atacante conhece o texto sendo enviado
 - ▶ Exemplo: mensagem começa com "Bom dia ..."
- ▶ Ataque escolhendo texto em claro
 - ▶ Atacante consegue encriptar mensagens
 - ▶ Midway
- ▶ Ataque escolhendo texto (de)cifrado
 - ▶ Atacante consegue decriptar mensagens
 - ▶ Exemplo: obter a chave e continuar decriptando mesmo depois capacidade de decriptar termina

Encriptação segura

- ▶ O que queremos como “segurança”?
- ▶ Opção 1: “ser impossível que o atacante descubra a chave”
 - ▶ A chave é somente um **meio** para segurança, não a parte mais importante
 - ▶ Necessário mas não suficiente
 - ▶ Fácil de projetar um esquema de encriptação que esconde a chave completamente que é inseguro

Encriptação segura

- ▶ O que queremos como “segurança”?
- ▶ Opção 2: “ser impossível para atacante descobrir o texto em claro enviado a partir do cifrado”

Encriptação segura

- ▶ O que queremos como “segurança”?
- ▶ Opção 3: “ser impossível para atacante descobrir qualquer caractere do texto em claro a partir do cifrado”
 - ▶ E se atacante obtém informação parcial sobre o conteúdo transmitido?
 - ▶ E se atacante *adivinha* um caractere?

Encriptação segura

- ▶ O que queremos como “segurança”?
- ▶ Opção 4: “Independentemente de qualquer informação prévia que o atacante tem sobre o texto em claro, o texto cifrado não pode vaziar nenhuma informação adicional sobre o texto em claro”

Encriptação segura

- ▶ Meta: “Independentemente de qualquer informação prévia que o atacante tem sobre o texto em claro, o texto cifrado não pode vaziar nenhuma informação adicional sobre o texto em claro
- ▶ Cenário: ataque usando somente um texto cifrado