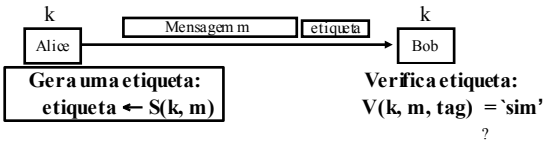
MAC
Código de Autenticação de Mensagem

Prof. Dr. Avelino Francisco Zorzo
Faculdade de Informática – PUCRS

Integridade de mensagens

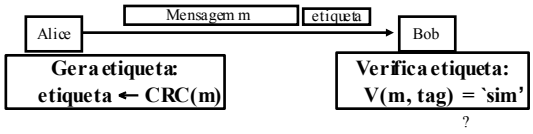
- Meta: **Integridade**, não confidencialidade
- Exemplos:
  - Proteger o código de um Sistema Operacional
  - Proteger propagandas em páginas *web*

Integridade da mensagem: MACs



- Def: MAC I = (S, V) definido sobre (K,M,T)
  - S(k,m) gera t em T
  - V(k,m,t) gera "Sim" ou "Não"

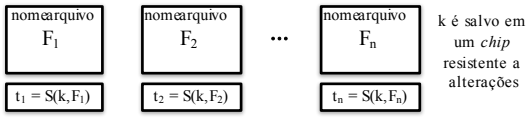
Integridade requer uma chave secreta



- *Cyclic Redundancy Code* (CRC)
  - Projetado para detectar erros **aleatórios**, não erros maliciosos.
- CRC não pode ser usado para verificar integridade
  - Atacante pode facilmente modificar a mensagem e calcular um novo CRC

Exemplo: protegendo arquivos

Suponha que no momento da instalação seja computado:

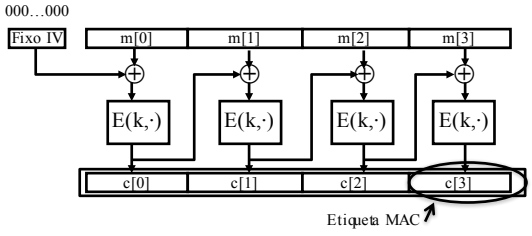


- Mais tarde um vírus infecta o sistema e modifica os arquivos
  - Se o MAC é seguro, o vírus não consegue forjar uma etiqueta válida
- O usuário reinicializa o SO não infectado
  - Todos os arquivos serão detectados pela chave que está no *chip*

Como construir um MAC?

- Em geral, duas formas
  1. Baseado em uma cifra de bloco (e.g., CBC-MAC)
  2. Baseado em uma função *Hash* (e.g., HMAC)

Construção 1: CBC-MAC

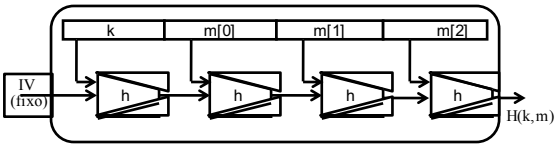


- Pergunta:
  - Por que não pode ser usado um IV aleatório?

Construção 2: *Hash-MAC*

- Construir um MAC baseado em uma função *Hash*
  - Por exemplo SHA-256
- Um exemplo
  - Assuma uma chave k e uma mensagem m
  - Construa um MAC usando: **H(k, m)**
- Isto é seguro?

MAC não seguro: H(k, m)



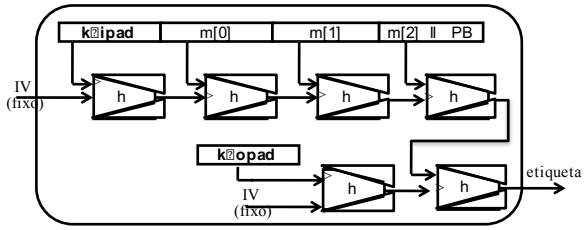
- Suponha etiqueta MAC = H(k, m[0]||m[1]||m[2])
  - Mallory pode facilment adicionar outro bloco m[3] e computar H(k, m[0]||m[1]||m[2]||m[3])
- Uma construção alternativa de etiqueta MAC = H(m, k)
  - Ainda assim insegura

HMAC

- Intuição básica
  - Precisa uma chave para proteger o início
  - Precisa uma chave para proteger o final
- Exemplo de uma construção segura
  - H(k1, H(k2, m)) onde k1 and k2 são duas chaves diferentes
- HMAC
  - Usa somente umachave secreta (assim mais eficiente)
  - Define ipad e opad como constantes

$$HMAC(k,m) = H(k \oplus opad \;||\; \mathbf{H(k \oplus ipad \;||\; m)})$$

HMAC



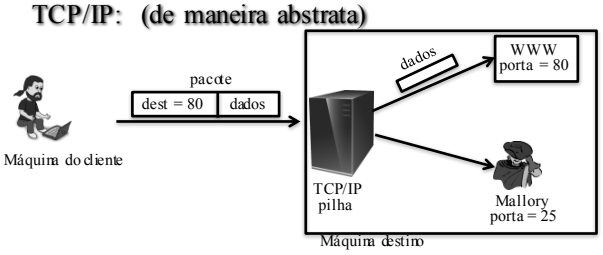
$$HAMC(k,m) = H(k \oplus opad \;||\; \mathbf{H(k \oplus ipad \;||\; m)})$$

Criptografia autenticada

- Em segurança no mundo real, criptografia geralmente é feita em um modo **autenticado**
  - Produz um MAC como parte do processo de criptografia
  - Provê confidencialidade e integridade
- Exemplos de criptografia autenticada
  - Cifrar com CBC + CBC-MAC
  - Cifrar com CTR + CBC-MAC (IEEE802.11i)

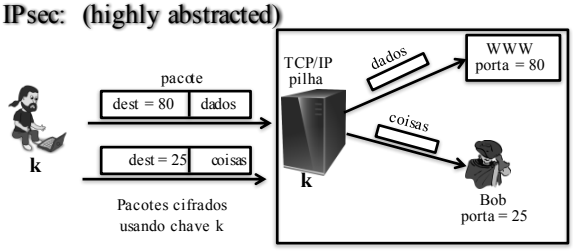
Exemplo de ataque

TCP/IP: (de maneira abstrata)



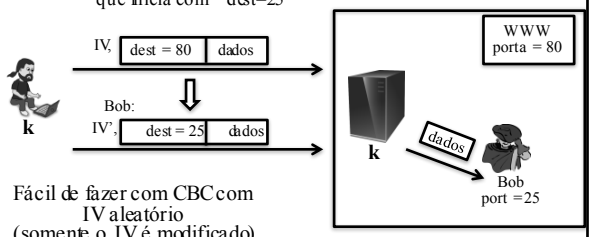
Exemplo de ataque

IPsec: (highly abstracted)



Lendo dados de outros

Note: atacante decifra qualquer texto cifrado que inicia com "dest=25"



Fácil de fazer com CBC com IV aleatório (somente o IV é modificado)

Criptografia é feita com CBC usando IV aleatório.

Qual deve ser o IV'? $m[0] = D(k, c[0]) \oplus IV$ = "dest=80…"

a) IV' = IV ⊕ (…25…)
b) IV' = IV ⊕ (…80…)
c) IV' = IV ⊕ (…80…) ⊕ (…25…)
d) Não pode ser feito