Encriptação Negável

Mostrando somente aquilo que você quer mostrar

ENIGMA

Universidade de Campinas

17 de Outubro de 2019

Sumário

O que é?

O que é?

Tipo de criptografia que pode ser negada de existir

Por que?

- Negar a existência de conteúdo criptografado de forma convincente

ou

- Negar a habilidade de decriptar um conteudo criptografado

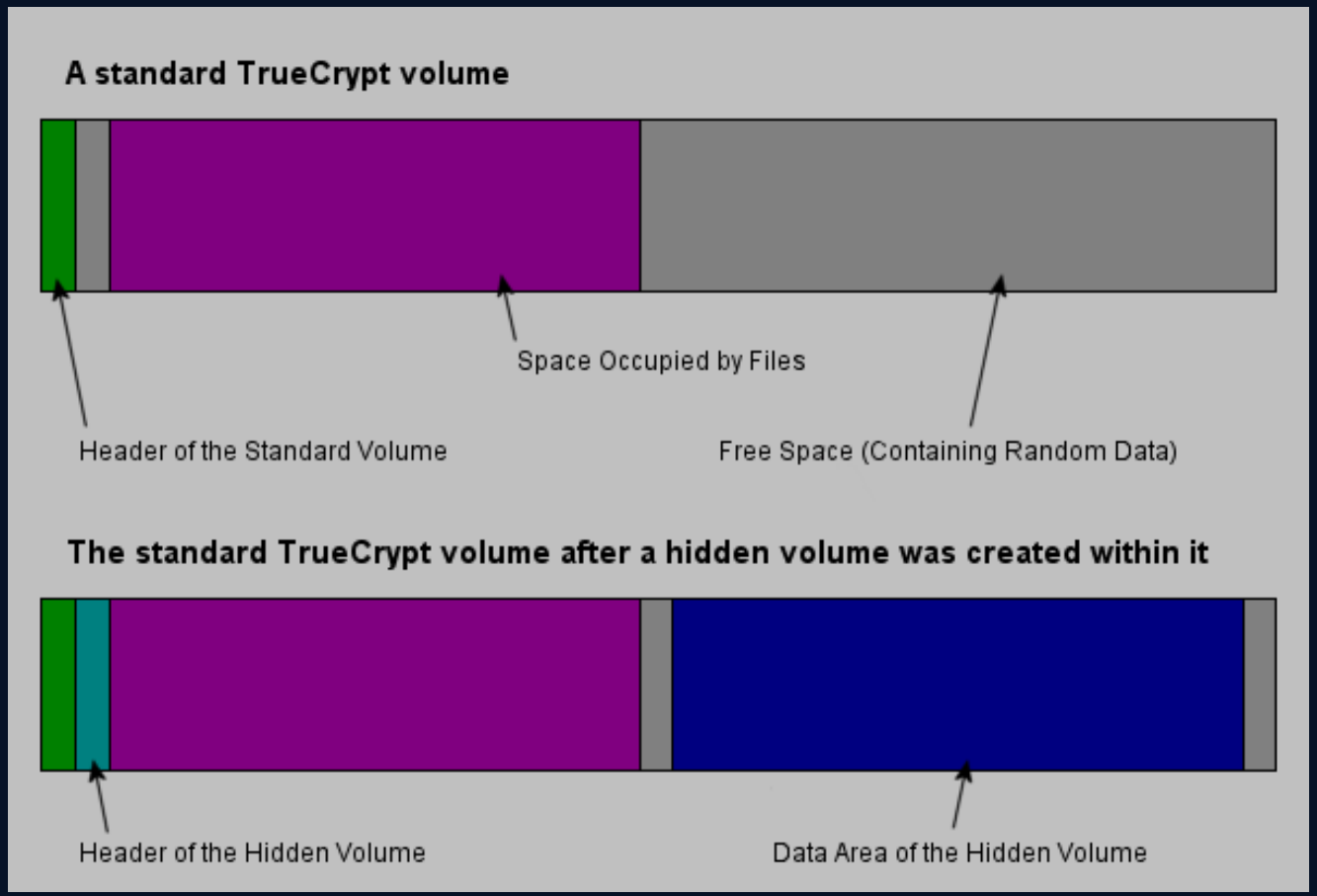
Usos Práticos

Criptografia de Disco

- Truecrypt Plausible Deniability [1]
  - Conteúdo completamente aleatório
  - Não pode ser discernido entre conteúdo seguramente apagado ou conteúdo criptografado

Criptografia de Disco

- Truecrypt Hidden Volumes [2]



ENIGMA
CRYPTO ANSWERS

Situações Plausíveis [3]

- Viajando com conteúdo sensível
  - Decriptar conteudo modificado que nao seja perigoso
- Comunicação observada
  - Manter uma chave pública que decripta todas as mensagens para algo não secreto
- Votação
  - Existência de duas chaves
  - Uma de posse do governo para conhecer seu voto
  - Uma segunda para mostrar um voto irreal para outra pessoa

Implementação em Python

Como Funciona?

Encriptação

- Salva as mensagens e chaves em um dict
- Utiliza "Password-Based Key Derivation Function 2 (PBKDF2)"[4] nas chaves
- Cifra cada mensagem com sua chave (AES)
- Escreve a concatenação das mensagens cifradas em um arquivo

Como Funciona?

Decriptação

- Le o arquivo e a chave digitada
- Aplica a mesma função que foi utilizada durante a criptografia na chave
- Decifra todo o arquivo, busca pelo header e então imprime aquilo que seria a mensagem buscada

Referências I


Truecrypt. *Truecrypt Plausible Deniability*. https://www.truecrypt71a.com/documentation/plausible-deniability/. "Acessado em: 01/10/2019".


Truecrypt. *Truecrypt Hidden Volumes*. https://www.truecrypt71a.com/documentation/plausible-deniability/hidden-volume/. "Acessado em: 01/10/2019".


Ari Trachtenberg. *Say it ain't so - an implementation of deniable encryption*.


PBKDF2. *Public Beta Key Derivation Function 2*. https://www.pbkdf2.com/. "Acessado em: 09/10/2019".

ENIGMA

Venham hackear com a gente!

https://enigma.ic.unicamp.br/