Geocryptark: arca digital segura, associada a uma coordenada geográfica e protegida por criptografia.

Patrick
patrick-mns@hotmail.com

Junho 2025

Resumo

Apresentando uma arquitetura de criptografia que permite que apenas usuários que conheçam a localização correta (latitude e longitude) e uma senha comum possam descriptografar um conteúdo protegido. Esta abordagem é ideal para aplicações que dependem de restrição geográfica de acesso, como jogos de caça ao tesouro, experiências de realidade aumentada e narrativas interativas baseadas em mapas.

1 Introdução

Sistemas tradicionais de controle de acesso por localização geralmente dependem de coordenadas geográficas, tokens ou outros mecanismos centralizados de autenticação — o que implica confiar em terceiros para validação. Essa abordagem apresenta limitações importantes, especialmente quando o objetivo é garantir autonomia, privacidade e resistência à censura ou manipulação externa.

Proponho uma alternativa descentralizada, onde o acesso a um conteúdo esteja vinculado a um ponto geográfico específico, e a validação possa ocorrer diretamente entre pares (*peer-to-peer*), sem a necessidade de servidores confiáveis. Para isso, combino coordenadas geográficas com senha para derivar chaves criptográficas capazes de desbloquear os dados protegidos apenas em localizações autorizadas.

Não se trata de um artigo acadêmico formal, mas sim da apresentação de uma proposta prática, que chamei de **Geocryptark**. O nome é formado por três elementos centrais: *Geo*, de geografia; *crypt*, de criptografia; e *ark*, remetendo à ideia de uma arca ou baú seguro onde os dados são protegidos.

2 Formalização

Dado um objeto sigiloso O a ser armazenado de forma protegida, utilizamos uma abordagem criptográfica baseada em localizações autorizadas L_i, combinadas com uma senha comum P e um valor de entropia adicional *salt*. A seguir, descrevo o procedimento completo:

Entradas

- O: dados para armazenar no baú.
- $L_i = (lat, lng)$: representa um ou mais pontos no mapa.
- P: senha comum (análoga à chave do baú).
- *salt*: valor para aumentar a entropia.

Geração do Hash

Para cada localização L_i, concatenamos suas coordenadas com o *salt* e a senha P, formando a mensagem m:

$$m = L_i \parallel salt \parallel P$$

Aplicamos a função de hash:

$$h = \text{SHA256}(m)$$

Derivação da Chave

A chave simétrica K_{L_i} é derivada por:

$$K_{L_i} = \text{PBKDF2}(h, salt_{\text{const}}, n, \text{SHA256})$$

Criptografia dos Dados

Antes de aplicarmos a criptografia baseada em localização e distribuição, protegemos a mensagem original O com uma camada inicial de cifragem simétrica

utilizando apenas a senha comum P e um *salt*:

$$O = \text{AES\_Encrypt}\left(O, \text{KDF}(P \parallel \mathit{salt})\right)$$

Geramos uma chave de sessão aleatória:

$$K_{\text{sess}} \xleftarrow{R} \{0,1\}^{256}$$

E ciframos a mensagem O novamente:

$$C = \text{AES-GCM\_Encrypt}(O, K_{\text{sess}}, IV)$$

Envelopamento da Chave de Sessão

Para cada localização autorizada L_i, ciframos a chave de sessão com sua respectiva chave derivada:

$$W_i = \text{AES-GCM\_Encrypt}(K_{\text{sess}}, K_{L_i}, IV_i)$$

Descriptografia

Um cliente que possua:

- A coordenada correta L_i,
- A senha comum P,

poderá gerar a chave K_{L_i}, decifrar W_i para obter K_{sess} e finalmente recuperar a mensagem O a partir de C.

3 Distribuição dos Artefatos

- O *salt* utilizado;
- O dado cifrado C e seu vetor de inicialização (IV);
- A lista de chaves envelopadas W_i e seus respectivos IVs.

Formas de Distribuição

Existem duas abordagens principais para distribuir os artefatos criptografados:

1. Modelo servidor intermediário: `peer → servidor ← peer`

Nessa abordagem, o servidor atua como repositório dos dados criptografados gerados por um peer. Ele armazena o artefato e compara hashes recebidos de outros peers para validar acessos. O ponto essencial aqui é que o servidor nunca tem acesso à latitude, longitude ou à senha secreta — apenas ao hash derivado desses dados. Mesmo que o hash seja interceptado, ele não permite acesso ao conteúdo, pois a mensagem ainda depende da chave de sessão e da senha. Essa estratégia remove a necessidade de confiança no servidor, mantendo a segurança do sistema. Em uma analogia simples: o servidor reconhece que você sabe onde está o baú e entrega o baú, mas para abri-lo você ainda precisa da chave.

2. Modelo peer-to-peer: Nesta abordagem, o peer pode gerar todos os dados criptografados localmente e distribuí-los diretamente por qualquer canal (redes P2P, QR Codes, arquivos, etc.), sem necessidade de um servidor.

Nesse cenário, o principal desafio passa a ser a proteção contra ataques de força bruta. Como não há um servidor intermediando, não há controle direto de tentativas de desbloqueio. Em contextos híbridos, o servidor pode atuar apenas para aplicar *rate limiting* (limite de tentativas) ou mecanismos de travamento temporário, ajudando a proteger o artefato.

Essa arquitetura adota o princípio de que o "baú" pode ser acessado por múltiplos peers simultaneamente. Uma vez descoberto o segredo, o conteúdo pode ser "saqueado" — o que, dependendo do objetivo da aplicação (por exemplo, jogos ou desafios), pode ser desejável.

4 Conclusão

O sistema proposto combina criptografia simétrica de alta segurança com restrições geográficas, criando um mecanismo de controle de acesso que depende tanto de conhecimento (a senha) quanto de presença (a localização). Essa abordagem elimina a necessidade de confiança em terceiros, permitindo implementações totalmente peer-to-peer, onde os dados permanecem protegidos mesmo diante de servidores maliciosos ou comprometidos.

A proposta, nomeada de **Geocryptark**, oferece uma solução versátil para contextos em que o acesso deve ser condicionado à presença em uma determinada coordenada — seja em aplicações lúdicas como jogos, distribuição de conteúdos secretos em locais físicos, ou mesmo em sistemas de autenticação em ambientes controlados.

Embora este trabalho não tenha caráter acadêmico formal, ele serve como base para experimentação prática e futuros aprimoramentos. A ideia central é demonstrar que é possível vincular espaço, segredo e criptografia de forma simples, mas eficaz.

Referências

[1] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley Publishing, 2010.

[2] Jonathan Katz, Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, 2ª edição, 2014.

[3] National Institute of Standards and Technology (NIST). *Recommendation for Password-Based Key Derivation: Part 1 – PBKDF2*. NIST Special Publication 800-132, 2010. `https://doi.org/10.6028/NIST.SP.800-132`

[4] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. NIST Special Publication 800-38D, 2007. `https://doi.org/10.6028/NIST.SP.800-38D`

[5] Internet Engineering Task Force (IETF). *JSON Web Encryption (JWE)* — RFC 7516. `https://tools.ietf.org/html/rfc7516`

[6] ISO/IEC 18033-3:2010. *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*. (Define o conceito de envelopamento de chaves via criptografia simétrica.)