Best Practice in Crittografia

Riccardo Longo

Non improvvisare

- La sicurezza è un problema serio
- È molto facile sbagliare
- Soluzioni apparentemente sicure possono essere totalmente rotte
- Non inventare nuove primitive/protocolli, evitare di implementare da sé
- Fare sempre riferimento agli standard più recenti e supportati dalla comunità scientifica
- Preferire sempre implementazioni Open Source ampiamente revisionate, scrutinate e controllate dalla comunità

Prospettiva

- Valutare sempre il contesto d'uso
- Non esiste una soluzione perfetta per ogni situazione
- Considerare in maniera realistica gli aspetti di sicurezza
  - Necessità di protezione, importanza delle informazioni
  - Tipologia e risorse degli avversari
  - Scenari di attacco
- Non strafare con i parametri

Sicurezza pratica

- L'utente umano è quasi sempre l'anello debole
- Non scaricare troppa responsabilità sull'utente
- Cercare di prevedere e proteggersi il più possibile da abusi e usi impropri

Sicurezza continua

- Gli attacchi sono in continua evoluzione
- Tecniche e strumenti diventano sempre più potenti
- Bisogna restare costantemente aggiornati
- In caso di errori/bug paga di più essere aperti ed onesti
- È importante collaborare con la comunità
  - Condividere informazioni
  - Segnalare bug e problemi
  - Coordinarsi per mettere in sicurezza

Consiglio d'oro

- Librerie specializzate si prendono cura di implementare correttamente i vari protocolli
- Parametri e primitive sono accuratamente selezionati ed aggiornati
- Uso a più alto livello, dettagli di sicurezza lasciati agli esperti
- Consiglio: se possibile usare

  NaCl (`https://nacl.cr.yp.to/`)

Cifratura Simmetrica

- Se possibile usare soluzioni integrate di **Key Management System**
- Usare cifratura autenticata (**AEAD**)
  - suite CAESAR (`competitions.cr.yp.to/caesar-submissions.html`)
  - Chacha20-Poly1305
  - AES-GCM
- Evitare AES-CBC, cifrari vecchi.
- Usare chiavi di lunghezza 128 - 256 bit

MAC e Hash

- Se serve autenticare o controllare l'integrità ma non cifrare
- Evitare soluzioni troppo complesse
- Per MAC:
  - HMAC-SHA-512/256
  - Altre varianti di HMAC-SHA-2
  - BLAKE2s o BLAKE2b con chiave
  - SHA3 con chiave
- Per hash:
  - SHA-2: veloce, standard
  - BLAKE2: il più veloce, moderno
  - SHA-3: più lento, standard, moderno
- **Evitare SHA1, MD5**

Random

- Generare sempre i parametri che devono essere random con fonti appropriate
- Usare CSPRNG (Cryptographically Secure Pseudo-Random Number Generator)
- Su sistemi GNU/Linux (incluso Android), BSD, o Mac (incluso iOS) usare

  `/dev/urandom`
- Su sistemi Windows usare

  `CryptGenRandom`

Password

- Ricordarsi che gli umani non sono bravi a generare buone password
- La lunghezza è il fattore più importante
- Cambiarle troppo spesso è controproducente
- Fare riferimento ai nuovi standard NIST (vedi lezione 3)
- Mai conservarle in chiaro per l'autenticazione di utenti, usare:
  - Argon2
  - scrypt (con $p = 1, r = 8, N \geq 2^{14}$, o $p = 1, r = 1, N \geq 2^{17}$)
  - bcrypt (con costo ≥ 5, usato con hash per password lunghe)
  - PBKDF2 (almeno 1000 round)

Crittografia Asimmetrica

- Evitare RSA favorendo ECC
- Se bisogna usare RSA:
  - Usare chiavi di almeno 2048 bit
  - Usare KEM (Key Encapsulation Mechanism)
  - Non usarlo per la firma
- Per ECC:
  - Chiavi di almeno 256 bit
  - Fare molta attenzione alla curva e parametri usati, nel dubbio usare *Curve25519*
  - Per la firma usare schemi deterministici: *EdDSA* o *RFC6979*

Riferimenti sulle Best practice

- Raccolta di vari consigli:

`https://gist.github.com/atoponce/07d8d4c833873be2f68c34f9afc5a78a`

- Guida pratica e abbastanza completa:
  `https://cryptodoneright.org`

Altre risorse

- Riferimento sulla sicurezza di varie curve ellittiche:
  `https://safecurves.cr.yp.to`
- Importante risorsa per dubbi in crittografia:
  `https://crypto.stackexchange.com`
- Wikipedia (in inglese) fornisce molte informazioni su pratiche, protocolli e primitive crittografiche
  - A volte il livello di dettaglio richiede competenza di un certo livello per capire

Per restare aggiornati

- Blog su cybersecurity in generale di un famoso crittografo: `https://www.schneier.com/`
- Raccolta di vari blog che offrono news in tema di cybersecurity:
  - `https://blog.marketingenvy.com/best-cyber-security-resources`
  - `https://www.smartbrief.com/original/2020/07/top-cybersecurity-news-sources-you-should-be-reading`