Integrity and Authenticity

Table of Contents:

Background Noise: Youtube
this loop EVAPORATES all ADHD atoms

Data Integrity Methods

- Manipulation Detection Codes (MDC): Hashes
- Message Authentication Codes (MAC): Hash with key

Digital Signatures

> Authorship - Integrity - Non-Repudiation

```
Relies on Public Key Cryptography
```

Possible Attacks:

1. Key-Only Attack: Public key PK is known
2. Known Signature Attack: Message and PK are known
3. Chosen Message Attack: PK and Signing algorithm are known

Types of Forgery:

1. Existential Forgery: forges one message without selection
2. Selective Forgery
3. Universal Forgery: forge any signature without knowing SK
4. Total Break: forge signatures by computing SK

Simple RSA signature is forger-able because of the *multiplicative property*, to fix it apply *probabilistic signature scheme*.

A) Hash then Sign

What this fixes:

1. Break the above attack and the algebraic attacks
2. Allow for bigger message size, not bounded by modulus N anymore

B) Schnorr signature scheme

- Simple
- Easy sign/verify
- Suitable for small devices

Public Key Infrastructure (PKI)

Certificate Authority
issued certificate:

- User name
- User public key (encryption or verification)
- Name of CA
- Expiry date
- Serial Number of Certificate

When is the certificate revoked?

1. Period of time is out
2. Bad use
3. PK is compromised

HTTPS authentication

This is done in two steps

1. Website & Browser do a handshake
2. Website & Browser do a TLS/SSL *tunnel* (if 1 passes)

Who are the stakeholders?

> Website owners - CAs - Browsers - End-users

The security of the entire ecosystem suffers if any of the hundreds of CAs is compromised (weakest link)