III. Authentication - identification protocols

Definition 3.1 **Entity authentication is a process whereby one party B is assured of the identity of a second party A involved in a protocol.**

Processes called identification protocols.

Examples

1. **Passwords**
2. **Passports**
3. **PINs**

Goals of identification protocols

1. If A and B are honest, B will accept A's identity.

2. B cannot reuse an identification exchange to impersonate A to a third party C.

3. Only with negligible probability a party C distinct from A is able to cause B to accept C as A's identity.

4. The previous points remain true even if

    - a large number of authentications between A and B have been observed;
    - C has participated in previous executions of the protocol (either as A or B).

Challenge-response protocols

In a challenge-response protocol A proves its identity to B by demonstrating knowledge of a secret known to be associated to A without revealing the secret itself to B.

Structure

1. commitment (to a secret)
2. challenge
3. response

Simple identification based on signatures

$\Pi = (\text{Gen}, \text{Sign}, \text{Vrfy})$ signature scheme with message length,

(pk_A, sk_A) A's key pair.

A		B
		$r \leftarrow \{0,1\}^n$
	$\xleftarrow{\quad r \quad}$	
	challenge	
$\sigma \leftarrow \text{Sign}_{sk_A}(r)$		
	$\xrightarrow{\quad c \quad}$	
	response	return 1 iff
		$\text{Vrfy}_{pk_A}(r, \sigma)$

r is called nonce. Chosen for each execution. Guarantees time dependence.

Trusted authorities

- Trusted authorities (TA) are entities trusted by all parties involved in a protocol,
- can sign messages (Sig_{TA}, Ver_{TA}),
- associates identities to entities (id(A) for entity A).

Fiat-Shamir identification – setup

TA chooses 2 random primes $p, q \in \left[2^{n-1}, 2^n - 1\right]$,

$N := p \cdot q$

A chooses $s_A \leftarrow \mathbb{Z}_N^*$, sets $v_A := s_A^2 \bmod N$.

TA sets $\mathrm{cert}(A) := \left(\mathrm{id}(A), v_A, \mathrm{Sign}_{TA}\left(\mathrm{id}(A), v_A\right)\right)$

Fiat-Shamir identification protocol

A		B
$r \leftarrow \mathbb{Z}_N^*, x := r^2 \bmod N$		
	cert(A), x $\longrightarrow$	
		verifies cert(A)
	challenge	$b \leftarrow \{0,1\}$
	$\xleftarrow{\quad b \quad}$	
$t := r \cdot s_A^b \bmod N$		
	$\xrightarrow{\quad t \quad}$	
	response	accepts iff
		$t^2 = x \cdot v_A^b \bmod N$

Factoring and modular square roots

Theorem 3.2 For any $\delta > 0$ and any algorithm C there exists an algorithm C' with the following properties:

1. If on input $N = p \cdot q$, p,q prime, and $a \leftarrow \mathbb{Z}_N^*$, C finds $b \in \mathbb{Z}_N$ satisfying $b^2 = a \bmod N$ with probability δ, then C' on input N computes p,q with probability $\delta/2$;

2. If C runs in time T, then C' runs in time $\mathcal{O}\left(T + \log^2(N)\right)$.

Chinese Remainder Theorem

Chinese Remainder Theorem Let $m_1,\ldots,m_r \in \mathbb{N}$ be pairwise relatively prime, i.e. $\gcd(m_i,m_j)=1$ for $i \neq j$. Let $b_1,\ldots,b_r \in \mathbb{N}$ be arbitrary integers. Then the system of congruences

$$\begin{aligned} x &= b_1 \bmod m_1 \\ &\vdots \\ x &= b_r \bmod m_r \end{aligned}$$

has a unique solution modulo $m = m_1 \cdots m_r$.

Corollary 3.3 Let $N = p \cdot q$ be the product of two distinct odd primes. For every $a \in \mathbb{Z}_N^*$ the equation $x^2 = a \bmod N$ has either 0 or 4 solutions. In case of 4 solutions, these solutions are of the form $\pm s_1, \pm s_2, s_2 \not\pm s_1$.

From C to C ‘

C′ on input N

1. choose $b \leftarrow \mathbb{Z}_N$
2. if $d = \gcd(b, N) \neq 1$, output $d, N/d$
3. $a := b^2 \bmod N$
4. simulate C with input N,a to obtain $w \in \mathbb{Z}_N^*$
5. if $w^2 = a \bmod N$ and $w \neq \pm b \bmod N$, compute $d = \gcd(w - b, N)$ and output $d, N/d$

Fiat-Shamir identification - security

Theorem 3.4 For any $\varepsilon > 0$ and any algorithm C there exists an algorithm C′ with the following properties:

1. If on input N, v_A C impersonates A with probability $1/2 + \varepsilon, \varepsilon > 0,$ then C′ on input N, v_A computes a square root of $v_A \bmod N$ with probability 1/2;

2. If C runs in time T, then C′ runs in time $\mathcal{O}(T/\varepsilon)$.

Fiat-Shamir is a proof of knowledge!

From C to C ‘

C′ on input N,v_A

1. repeat $1/(2\varepsilon)$ – times
   a) simulate C to obtain $x \in \mathbb{Z}_N^*$
   b) simulate C with $x, b = 0$ and $x, b = 1$
   c) if C succeeds for both choices of b, let t_0, t_1 be C's responses, output $t_1 \cdot t_0^{-1} \bmod N$.

Fiat-Shamir identification protocol

1. For i=1 to l A and B do:

A		B
$r_i \leftarrow Z_N^*, x_i := r^2 \bmod N$		
	$\xrightarrow{x_i}$	
		$b_i \leftarrow \{0,1\}$
	$\xleftarrow{b_i}$	
$t_i := r_i \cdot s_A^{b_i} \bmod N$		
	$\xrightarrow{t_i}$	
		rejects if $t_i^2 \neq x_i \cdot v_A^{b_i} \bmod N$

2. B accepts.

Fiat-Shamir identification - security

Theorem 3.5 For any $\delta \geq 2^{-l+2}$ and any algorithm C there exists an algorithm C' with the following properties:

1. If on input N, v_A C impersonates A with probability $\geq \delta$, then C' on input N, v_A computes a square root of v_A mod N with probability 0.03;

2. If C runs in time T, then C' runs in time $\mathcal{O}(T/\delta)$.

From C to C ‘

C′ on input N,v_A

1. repeat at most $1/\delta-$times
   a) $z\leftarrow\{0,1\}^R, b\leftarrow\{0,1\}^l$
   b) simulate C with random bits z and b
   c) if C succeeds set $b^{(1)}:=b$ and goto 2)
2. repeat at most $1/\delta-$times
   a) $b\leftarrow\{0,1\}^l$
   b) simulate C with random bits z and b
   c) if C succeeds set $b^{(2)}:=b$ and goto 3)
3. if $b^{(1)}\neq b^{(2)}$, output $b^{(1)},b^{(2)}$ and corresponding $t^{(1)},t^{(2)}$.

Security against (cheating) B

Can B gain information from FS-protocol that will enable him to impersonate A?

– B sees triples (x, b, t) with $t^2 = x \cdot v_A^b \bmod N$
– B can generate these triples (x, b, t) by himself

a) $b \leftarrow \{0,1\}$

b) $t \leftarrow \mathbb{Z}_N^*$

c) $x := v_A^{-b} \cdot t^2 \bmod N$

– triples have same distribution as in FS-protocol

B learns nothing in FS-protocol.

Formalized and strenthened by zero-knowledge protocols.