

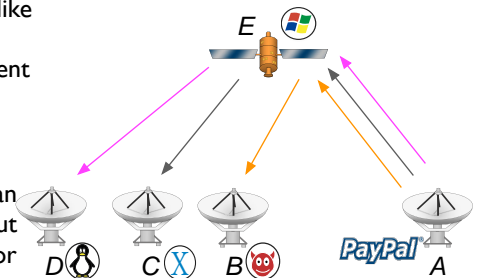
(Public Key) Digital Signatures

Digital Signatures

Prof. Zeph Grunschlag

PROBLEM: Alice would like to prove to Bob, Carla, David, ... that has really sent them a claimed message.

GOAL: Alice signs each message so individuals can verify authenticity without pre-agreed secret keys for MAC's and no interaction



2

Digital Signatures

DEF: A **digital signature scheme** consists of a tuple (M, K, G, S, V) where

- M - message space
- K - key space with each key = (pk, sk)
- G - PPT key generator picks key k of security parameter l : $k \xleftarrow{R} G(1^l)$
- S - PPT algorithm for signature $S_{sk}(m)$ from secret key and message. Write:
- V - verifier which is a Las-Vegas PPT decider s.t. $V_{pk}(m, S_{sk}(m)) = 1$ if (pk, sk) is a valid key.

3

Security Definition

Note: Security *not* built-in to above. Haven't even defined conditions for V rejecting by returning 0.

DEF: A signature scheme (M, K, G, S, V) is **existentially unforgeable** under adaptive chosen message attack if no adversarial PPT algorithm A with access to a signing oracle can output a valid signature for a message that was not signed by the oracle with non negligible probability of success. In other words, the following probability should be negligible:

$$\Pr[V_{sk}(A^{O_v}(pk)) = 1]$$

4

First Attempts

- RSA signature scheme:
 - Alice signs using private key, public verifies by using public key
- Rabin signature scheme:
 - Alice signs messages in $QR(n)$ by sending square root of message
- El-Gamal randomized signature scheme:
 - Dlog based
 - $sk = (\text{prime } p, \text{primitive } \alpha, \text{exponent } x)$
 - $pk = (p, \alpha, \beta = \alpha^x \bmod p)$
 - Signature: $[r = g^k, k^{-1}(m - rx) \bmod (p - 1)]$
 - DSS standard is similar to El-Gamal

5

Impossibility “Proof”

Many cryptographers believed that provably secure signature schemes could not exist because any security proof could be used to actually break the scheme...

7

First Attempts Fail

- RSA:
 - as defined, existentially forgeable
- Rabin:
 - as defined, existentially forgeable and total break under chosen message attack
- El-Gamal:
 - existentially forgeable if no hash function applied to message
 - DSS standard is similar to El-Gamal

6

Cramer-Shoup Stateless DSA

... next time

8