IBE vs Traditional Public Key

Radia Perlman
Radia.perlman@sun.com

1

Notes

- I'm not talking about details of particular implementations
- I'm talking about intrinsic properties of IBE vs traditional concepts of public key-based authentication

2

On-line vs off-line trusted box

- With public key, CA can be off-line – not as vulnerable a target as an IBE Private Key Generator (PKG)
- Yes, revocation server might be on-line, but:
  - > It's not as security sensitive a box as a CA or IBE-KS
  - > With CRLs, it could be "mostly" off-line
  - > Revocation server doesn't have to have the same public key as the CA, so the revocation server can at most unrevoke, not:
    - Issue bogus certs
    - Impersonate all users
    - Decrypt all encrypted files

3

How trusted

- CA cannot decrypt messages to correctly registered users
  - > Though if CA were compromised, someone could issue bogus certs, and trick users into encrypting with a key a bad guy knows

4

How easy to bootstrap

- *"With IBE, all you need to know is the other side's name, whereas with PKI you have to know the other side's public key"*

5

How easy to bootstrap

- *"With IBE, all you need to know is the other side's name, whereas with PKI you have to know the other side's public key"*
  - > No! In any sensible PKI-based system, you'd only see the other side's name
  - > And in IBE you need to know the domain parameters
- Also, you need a way of authenticating to the PKG

6

Revocation

- Issues with IBE
  - > Compromise of user's private key
  - > Compromise of PKG's secret

Escrow

- "With IBE, escrow is built-in"
- Yes…but you have the option of doing it any of several ways with traditional public key
  - > CC'ing escrow agent
  - > Storing private key with escrow agent

There are definitely ways of screwing up PKI

- Putting way too much stuff into certs (privacy issues, etc.)
- Charging lots of money for certs, and needing to get certs from distant entities
- But these aren't intrinsic to PKI

9