

Challenges in User Authentication: Are we there yet?

Radia Perlman
(radia.perlman@sun.com)

Panelists

- Stefan Brands
 - Founder/president Credentica
- Charlie Kaufman
 - Security architect, Microsoft
- Aryn Ukani
 - Identity and access management, IBM

So, are we there yet?

Spoiler alert!!!

No!!!

What's wrong?

- A million names/passwords
- Phishing
- Takes forever to do something simple like give an employee an account to access the net, get into the building, etc.
- Backup authentication, e.g., to reset password, works for bad guys and not me!

What do I want?

- “The network is the computer”
 - Aka, single sign-on
- I want to log in without it being a disaster if there’s a keyboard logger, or I’m talking to the wrong site

Pitch for PKI

Compared to Secret-key solution

- Secret key involves KDC
 - On-line box that knows all secrets
 - Introduces Alice to Bob on demand
- PKI involves CA
 - Certifies public keys in advance

PKI vs KDC

- Cost: PKI solution should be cheaper
 - KDC complex, must be fast, replicated
 - CA glorified calculator, off-line, OK if down for a few hours

But cross-organizational trust is
tricky

PKI Models

- Monopoly
- Anarchy
- Name-based, Bottom-up

Monopoly

- Choose one universally trusted organization
- Embed their public key in everything
- Give them universal monopoly to issue certificates
- Make everyone get certificates from them
- Simple to understand and implement

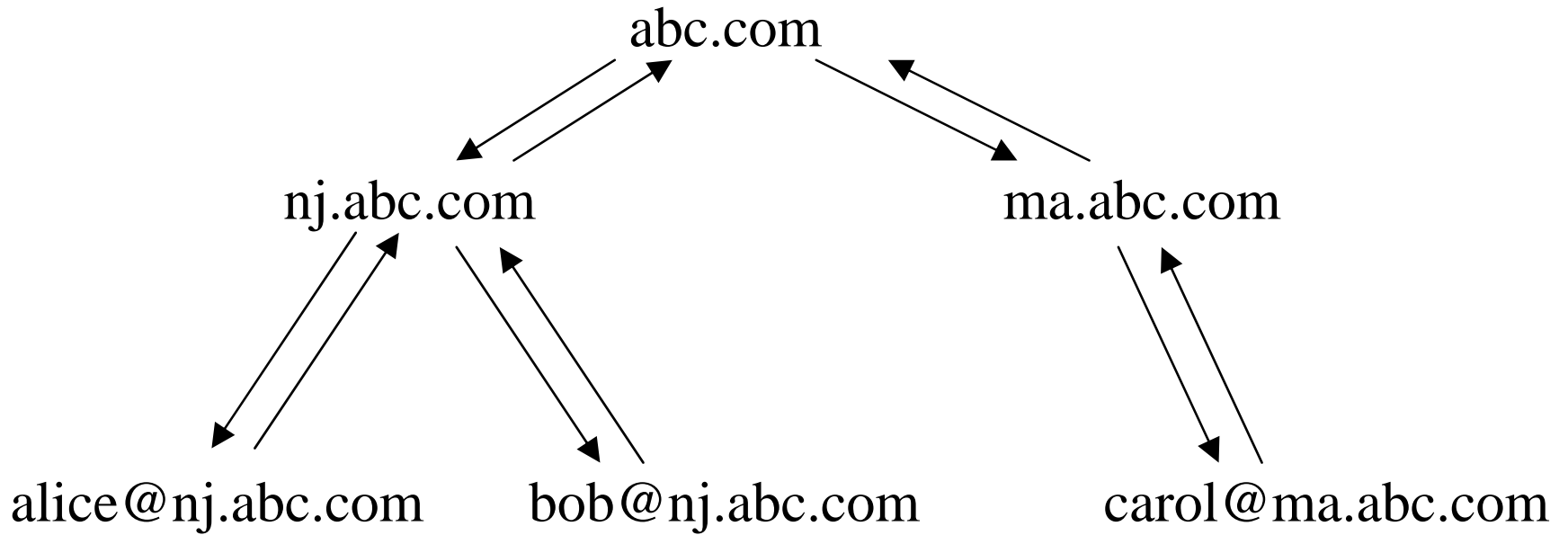
Anarchy

- User personally configures trust anchors
- Anyone signs certificate for anyone else
- Public databases of certs (read and write)
- Problems
 - won't scale (too many certs, computationally too difficult to find path)
 - no practical way to tell if path should be trusted
 - too much work and too many decisions for user

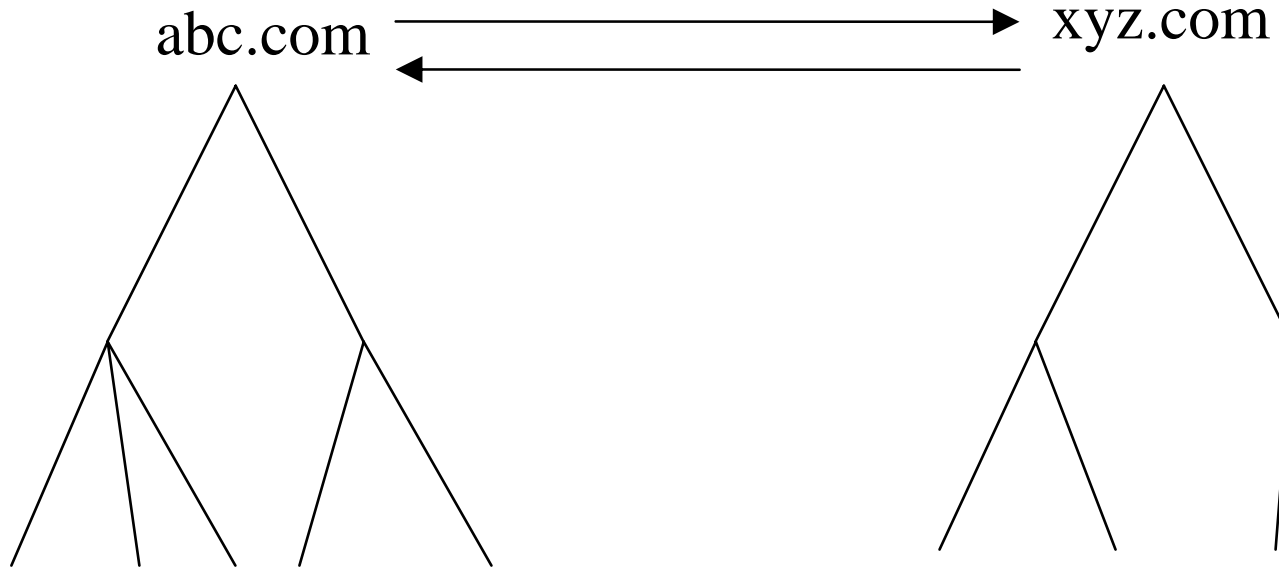
Name-based

- Name by which I know you implies who I trust to certify your key
- Well-defined path through name space

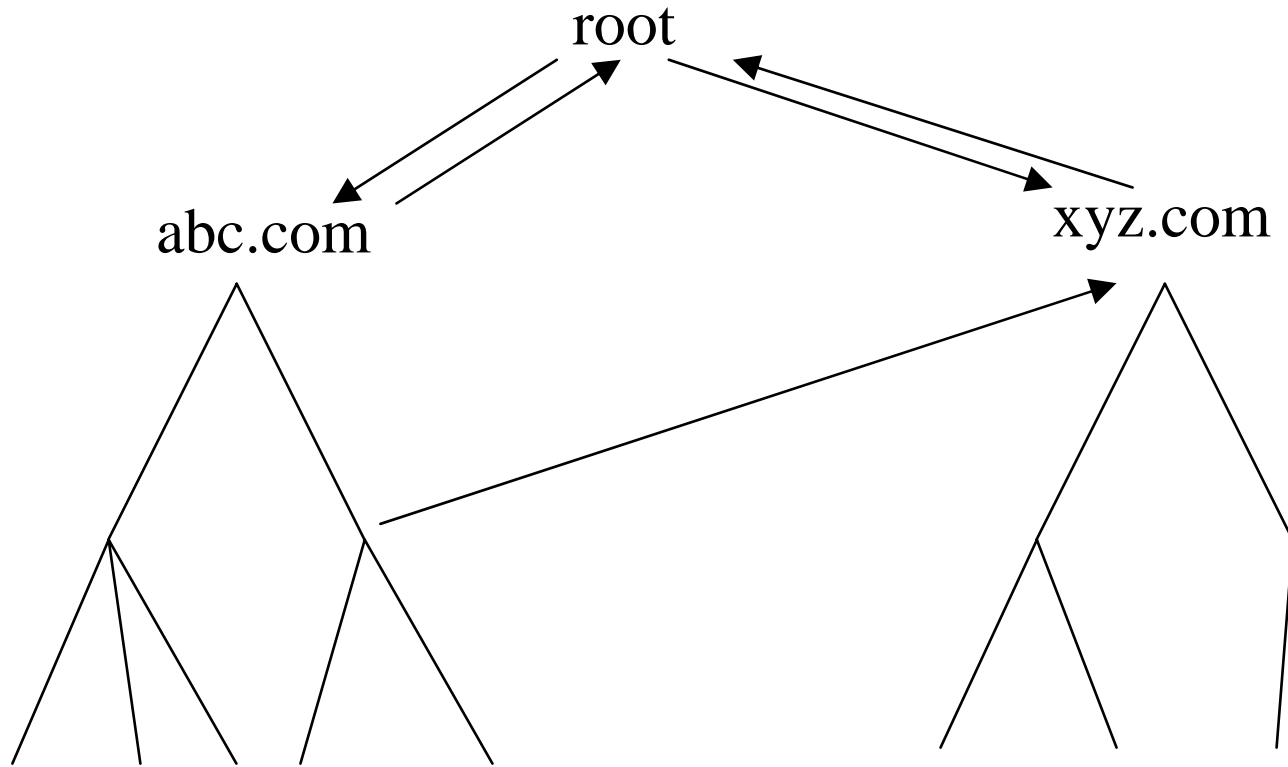
Intranet



Extranets: Crosslinks



Cross-link for added security



Advantages of Bottom-Up

- For intranet, no need for outside organization
- Security within your organization is controlled by your organization
- No single compromised key requires massive reconfiguration
- Easy configuration: public key you start with is your own

Now what?

- Panelists will each talk about some facet of authentication, hopefully saying at least something that will be heretical
- We get to debate with each other and the audience