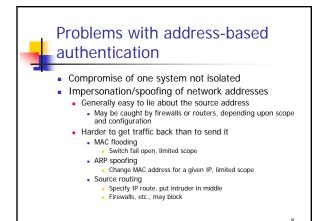


Address-based authentication Infer the identity using network location Trust the network for source information UNIX rtools implement this "Equivalent machines" – access if username matches (/etc/hosts.equiv)

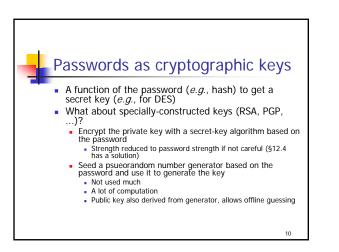
- Mappings from remote machine, account name pairs to local accounts (per-user .rhosts)
- Safe from eavesdropping
 - Passwords not sent

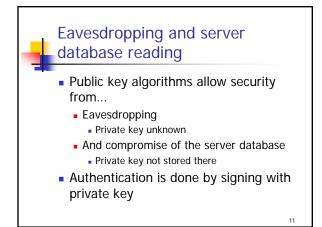


Cryptographic authentication protocols

- Improvement on password-based and address-based authentication
- Prove identity by performing cryptographic operation on supplied data
 - E.g., based on shared secret
- We wish to authenticate both systems and people

9

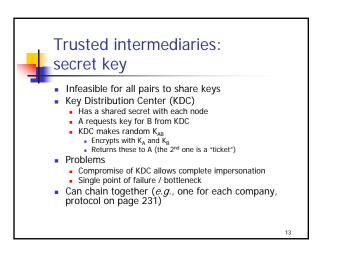


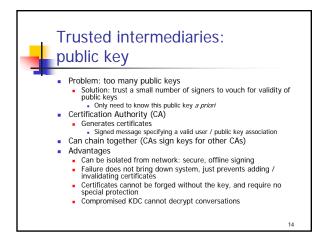


Eavesdropping and server database reading

- Hard to protect against both without PK
- Transmit clear passwords but compare to hash
 - Vulnerable to eavesdropping
- Challenge to encrypt a random number
 - Vulnerable to server database reading
- Can do both with Lamport's hash (§12.2), with some limitations

12







- Charge card good for 2 years, and then you cancel it...
- Similar solution with CAs
 - Revocation list
 - All unexpired certificates that are no longer valid

15

Authentication of people

- Humans cannot feasibly
 - Remember very high-quality secrets
 - Perform cryptographic calculations
- Solution: combine multiple techniques
 - What you know (*e.g.*, password)
 - What you have (e.g., key, ID card)
 - What you are (biometrics; *e.g.*, fingerprint, voice, iris, retina)

Off-line password guessing: dictionary attack

- Consider a large number of users and their captured, hashed passwords
- Encrypt every word in dictionary and other likely passwords; search for matches
- Overhead is typically in the hashing of each word
 - Not searching through the long list of users

17

18

16

Foiling the dictionary attack: salting the hash

- Put the complexity back in favor of the good guys
- Concatenate passwords with a random "salt" value before hashing
 - Salt stored in the clear in the password system
- For N accounts
 - the work of off-line guessing was increased by about N
 - but the increase is negligible for legitimate use

© Eric A. Durant, PhD

