

# User-centric PKI

Radia Perlman                      Charlie Kaufman  
Radia.Pperlman@sun.com      charliek@microsoft.com

1

# Motivation

- Why can't things be simple?

2

## Motivation

- Why can't things be simple?
- I can't cope with username/pwds
  - I'm not alone...
- The federated identity things seem really complicated to me

3

## I don't care about formats

- "Certificate" is any signed thing

4

## My view of federated things

- Microsoft created the “Passport” vision, with Microsoft the center of the world
- Others said, “Hey, let’s not anoint one organization to be an eternal monopoly
- So, the notion of lots of IDPs, and a federation is the set of SPs that trust that IDP

5

## If there is just one IDP

- User authenticates to that IDP
- That IDP vouches for the user at all the affiliated sites

6

## But what if there are hundreds?

- And what if the SPs the user wants to use affiliate with different subsets of them?

7

And what value does the IDP  
give, anyway?

8

## Downside of IDP (vs. peer-to-peer mutual authentication)

- Security (on-line IDP can impersonate all users)
- Availability (if IDP is down, nothing works)
- Performance (bouncing around between boxes)
- Privacy (IDP knows everyone you talk to)

9

## Upside of IDP

- ?

10

## Quick rant on today's web

11

## Perils of Perlman

12

## Buying something

- Scenario: Buy something from a merchant you haven't bought from recently
- All prepared with your info, credit card, etc.
- It asks you for your email address...

13

## You're a returning user!

- Type your username and password!

14

## You're a returning user!

- Type your username and password
- Of course you can't remember it, so...

15

## You're a returning user!

- Type your username and password
- Of course you can't remember it, so...
  - you manage to find “recover username”

16

## You're a returning user!

- Type your username and password
- Of course you can't remember it, so...
  - you manage to find “recover username”
  - suddenly you are in a Monty Python movie
    - Answer the following questions three:
      - Telephone number
      - Address
      - Mother's maiden name

17

## *New Rule*

- **It should be no more onerous to be a returning user than a new user**

18

## Security questions for password/username recovery

- Favorite sports team
- 2<sup>nd</sup> grade teacher's name
- Pet's name
- Father's middle name
- My middle name

19

## *New Rule*

- Security questions must be specifiable by the user
- I'd say "or selectable from a very large list", but I'm sure they can come up with an arbitrarily long list of questions I can't answer

20

## Security question in comedy routine

(Q&A Chosen by user, to be asked by the bank  
for phone verification of customer)

21

## Security question in comedy routine

- Question: “Are you wearing underwear”?

22

## Security question in comedy routine

- Question: “Are you wearing underwear”?
- Answer: “I don’t think that’s an appropriate question”

23

## Keeping customer information

- I do not want to do “single click ordering”
- I do not mind typing in my address
- I do not mind typing in my credit card number
- Merchants insist on keeping all of this information
- And eventually this information gets stolen

24

## *New Rule*

- After a merchant is paid, any subset of information about a customer (including all of the information) must be expunged by the merchant at the customer's request

25

## Simple intra-organizational PKI

26

## Within an organization

- Should be trivial, single CA
- To create an account
  - Sysadmin told username and initial pwd
  - Types that into “create new account” tool
  - Tool generates key pair, certifies public key, encrypts private key with pwd, stores cert in dir
- User logs in
  - Types name and pwd, retrieves private key
  - Accesses resource: authenticates with public key

27

## Better with smart cards

- Badges have smart cards. What’s the problem?
- Doesn’t do mutual authentication, but could, by having everything (including client machine) know CA’s public key

28

## And, IDP and Kerberos also work

- Within an organization, also easy to have everything trust the same KDC, or IDP
- But better without having an online trusted box

29

## Online vs offline trusted box

- Performance, availability
- Security
  - Can impersonate all users
  - More likely to be compromised vs offline box
  - Knows who is talking to who
  - May have database that if stolen, can compromise users

30

But our talk is really about  
individuals

31

How about individuals?

- Think of this as just doing what we do with username/pwd, but more securely, and without torturing the user
- Assume first the user has a smart card with a secret (private key, or secret key)

32

## “Wallet”

- A bunch of data cryptographically protected with the user’s smart card secret
- Downloadable from one or more places
- Contains, for instance, public keys of various merchants, perhaps private keys to use with that merchant, information such as passport number and credit card numbers

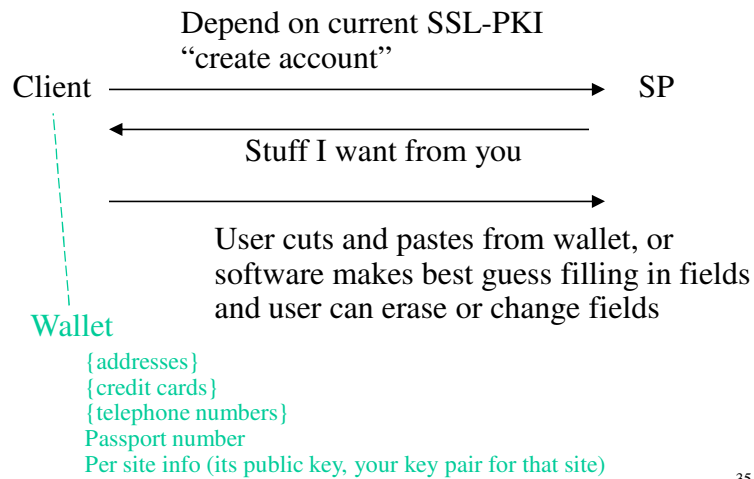
33

## Enrolling at a site

- Just like today, except username/pwd is replaced by “public key”
- The wallet information (such as address) can be filled into the form, to save the user typing, or the user could drag info she wants into the form
- The SP sends the user its public key

34

## Enrolling



## Note

- Instead of enrolling with a username and password, your account name is your public key, and you authenticate with your public key
- And by saving the SP's public key (a la SSH), you can do mutual authentication, knowing you are again reaching the same site as before

36

## Revisiting the site

- Mutual authentication using public keys (e.g., SSL with client certs)

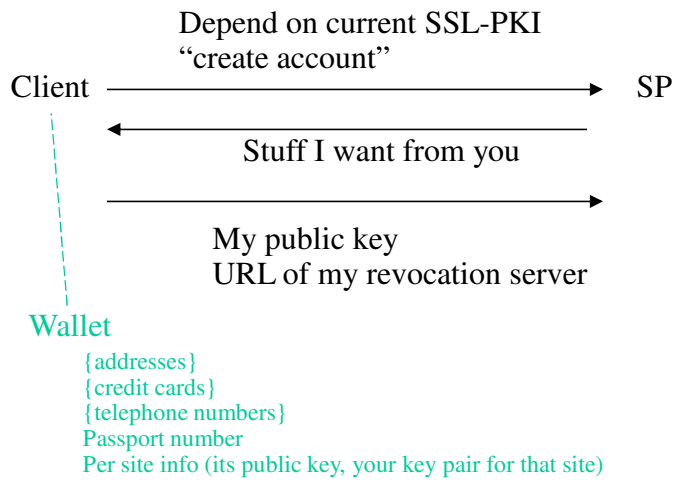
37

## One-step revocation

- Suppose you are using your public key at lots of sites
  - (not sure how useful different keys for each site is)
- And someone steals it
- Use “revocation service”

38

## Enrolling



## Revocation service

- SP learns user's revocation server along with the user's public key
- SP can "enroll" with that revocation service, to be notified in case of revocation
- Or SP can check periodically
- User has to have some sort of out-of-band mechanism to authenticate and revoke the key
- User can store { next keys } signed by current key, and escrow the future private keys

## Authenticated attributes

- User can have, in wallet, certs signed by whoever is trusted to assert the attribute, that a public key associated with the user is over 18, a citizen, whatever
- Can send such certs to SP when needed, along with proof of knowledge of the private key

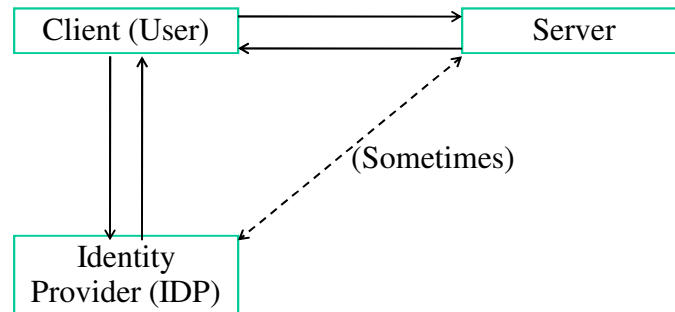
41

## Yes, things can go wrong

- Establish trust, then after increasingly large purchases, skip town
- Credit cards today somehow work “well enough” – certainly could be improved, but banks seem to think it’s not worth the bother

42

## Federated Identity: What is it?



Many variations on this theme: IDP holds secret information needed by client to authenticate to server.

43

## Federated Identity: What problems are we trying to solve?

- Something more convenient for the user than username/password?
- Something more secure than username/password?
- Reducing aggregate administrative costs of maintenance?

44

## Federated Identity: What problems are we trying to solve?

- Something more convenient for the user than username/password?
- Something more secure than username/password?
- Reducing aggregate administrative costs of maintenance?
- Something new we can implement, publish papers about, and use to excite customers?

45

## What do users want?

- Don't want to remember so many usernames and passwords
- Don't want to type usernames and passwords as often
- Don't have to type address/phone number/email address as often
- Less hassle when I forget a password or someone steals it

46

## What do users not want to give up?

- Sign-on from anywhere
- Not needing to carry smart cards or other hardware
- Ability to have lots of accounts at a single vendor, share some accounts (without sharing all of them)
- Having more than one credit card
- Having more than one email address, phone number, etc. and choosing which to give to a site

47

## Users' Security Goals?

- For most, vaguely understood worries about 'identity theft' or 'stolen credit card numbers'
- For a few of us geeks:
  - Servers can't correlate identities
  - Some degree of anonymity
  - No authority can know all the things I do
  - Not putting 'all eggs in one basket' in case of kiosk or hijacked machine

48

## Reducing Administrative Costs

- Users forget usernames & passwords
  - Centralize password reset
  - Less often if fewer to remember
- Recovery when passwords are stolen
  - Revocation in bulk rather than site by site
  - Correlate suspicious activity
- A wallet full of smart cards is impractical
  - A single hardware token should work with many services

49

## Service Provider Security Goals

- Authentication that's harder to compromise
  - Get users to choose hard to guess passwords and not use the same ones on multiple sites
  - Make phishing attacks and other network based attacks harder to mount
- Discourage users from sharing subscriptions
- Make it easier to track down users who misbehave

50

## Special Cases

- My credit card number should not be secret
  - Purchases should be authorized through some strong protocol
  - Issuing banks or alternate intermediaries like PayPal should deploy this – should not be linked to other aspects of federation
- If I get a AAA or AARP or ACM discount, proof of membership should be partly automated

51

## The Allure of Federated Identity

- Authenticated attributes (sometimes with anonymity)
  - Classic examples:
    - Age > 21
    - Employee of Microsoft
    - Member of IEEE
    - Paid attendee of IDTrust 2008
- What is the end-to-end scenario in which this is useful?

52

## Bottom Line

- Current State of the Art is awful!
- Something simple based on roaming credentials and SSL client certificates could solve the most important problems
- Federated identities could potentially solve those same problems, but they are harder to deploy and no better

53

## Bottom Line

- Current State of the Art is awful!
- Something simple based on roaming credentials and SSL client certificates could solve the most important problems
- Federated identities could potentially solve those same problems, but they are harder to deploy and no better
- Why is the world so excited about them?

54