The Murky Tangle of Web Authentication

Russ Allbery

June 2, 2011

You finished site-wide web authentication

People can use one login for multiple sites

You're now running a web authentication service

Now what?

Password Fail

Users give their passwords to anyone who asks

Legal business, salaries, health care done on the web

Regulatory requirements are growing

People can't remember good enough passwords

Solution: Multifactor

What Multifactor Method?

Smart Cards

- X.509 plus PIN is well-understood and fairly secure
- Integrates well with Kerberos
- PIV is a standard... sort of
- It works on Linux... sort of
- Provisioning systems are available... sort of
- Expensive
- Awkward (need readers, what about phones, ...)
- For 50,000 people, REALLY EXPENSIVE

SecurID

- Proven (?) track record
- Hardware devices or smart phone applications
- If eBay and World of Warcraft can do it, why not us?
- Looks less and less appealing the deeper you look
- Expensive (surprisingly) and proprietary
- Pay RSA for random numbers?

OATH

- Google solved your problem for you
- Standardized IETF OTP protocol (with good libraries!)
- Already available on most mobile platforms (except Blackberry)
- Nearly everyone already has a phone
- You can print them if you have to (Luddites supported)
- No Kerberos integration... yet

Stanford's Approach

- Choose: Smart phone, SMS, printed list
- SMS is cents per message
- Expose factors used via web authentication protocol
- Expose LoA via web authentication protocol
- Central WebLogin server handles (complex!) user interaction
- Web only (for now), but web-only solves 90% of problem
- Is the phone a good enough second factor?
- "Weak" multifactor, with "strong" multifactor coming

Not ready for multifactor always...

Abused Accounts

- Huge, HUGE increase in spear phishing
- Mostly used for spam (but no guarantees)
- Attackers willing to do extensive work to duplicate your login screens and automate attacks on your systems
- User education and filtering are insufficient
- Constantly closing the barn door after the horses

Horse Watcher

Advance warning: Creepy, scary techniques to use to stalk your users

Faster Than Sound

- Feed all authentication events into one system with time, IP
- Look up the IP in a GeoIP database
- Is the user moving faster than the speed of sound?
- Is the user out of the expected countries?
- How many places are they coming from?
- False positives? Oh, my, yes. But too many? Maybe not.

Abuse Plus Multifactor

- Tell the user about strange logins
- Require multifactor for suspicious logins
- Encourage users to set up multifactor
- Similar to techniques used by financial institutions
- Side bonus (for schools): Finding lost students in emergencies

Terrifying Privacy Issues

Do you want to have this data at all?

Do you have a policy about how you're going to use it?

Can you keep small the number of people who can see it?

Others are already doing this... food for thought.

Other things to think about...

Federation

- SAML won
- You'll end up running Shibboleth and/or ADFS
- Authentication parts not particularly difficult
- Data release is a complicated and tricky mess
- Document standards as early as possible
- Invest in audit and management tools as early as possible

Mobile and Web Services

- Growth of web services with mobile client
- Central web authentication systems play poorly with programs
- Browsers and web services need different interfaces
- Solution: REST version of central login server
- Still has weird bits around the edges
- Kerberos on mobile plus better auth stacking would be nice
- Hard problem