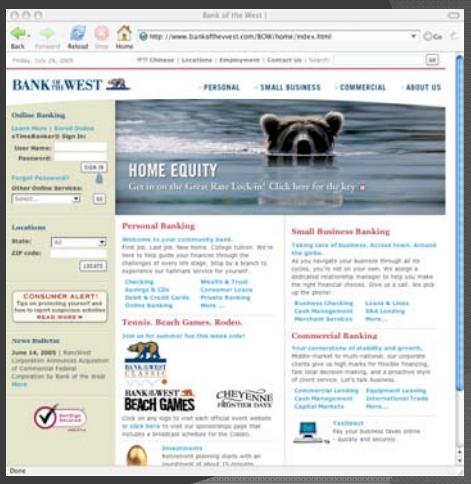
Mobile Web Phishing Defense

Francis Hsu, Yuan Niu, Hao Chen
{fhsu, niu, hchen}@cs.ucdavis.edu
Computer Science, UC Davis

UCDAVIS
UNIVERSITY OF CALIFORNIA

Phishing

- Human factors problem – users give up credentials to the wrong party
- 2 million victims and $1.2 billion in losses for US banks in 2003



Goal: Eliminate phishing

- Problem:
  Users give up their passwords in an authentication session
- Solution:

1. *Stop users before they enter passwords*
2. Remove users and passwords from the authentication session

Mobile Device Limitations

- Physical restrictions
  - Screen size
  - Input interface
- Vendor restrictions
  - Limits on running additional software
  - Upgrades

URL Display

http://welcometo.bankofamerica.malweb.org/index.jsp

- No https indication
- Truncation from middle – lose effective second level domain
- Long URLs never fully displayed

5

Chrome

- Lack of trusted chrome elements
- Developers actively try to remove chrome from view

Chrome

Page Content

Which of these is a forgery?

6

SSL

- What can a user do here?
- Even if they wanted to, users can't
  - Examine SSL certificates
  - Diagnose invalid certificates

7

Mitigation Strategies

- Browser designer
  - Sites need to identify themselves to the user
  - Keep effective second level domain name
- Website authors
  - Site designers should shorten URLs
- Network administrators
  - Network level anti-phishing proxy filters

8

Goal: Eliminate phishing

- Problem:
  Users give up their passwords in an authentication session

- Solution:

1. Stop users before they enter passwords

2. *Remove users and passwords from the authentication session*

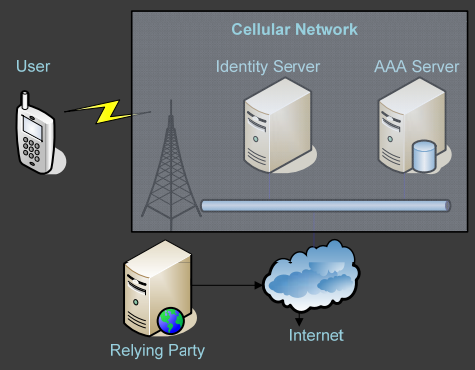
Cellular Based Authentication

- Cellular devices authenticate to network, network authenticates user to websites

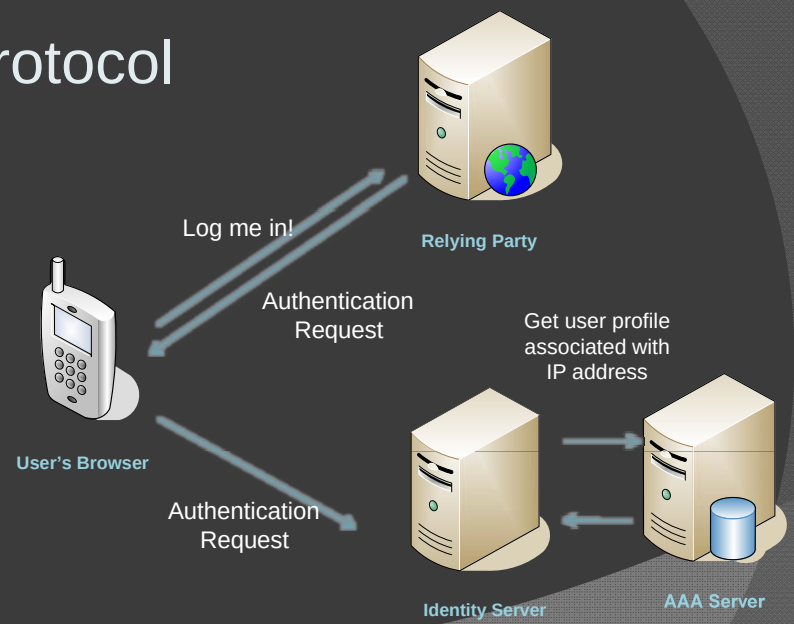
- Advantages
  - Usability – Without active user participation, users can't make security mistakes
  - Ease of deployment – Takes advantage of existing infrastructure, billions of cell phones and users
  - Trust – Wireless network authentication relatively hard to attack from the outside

10

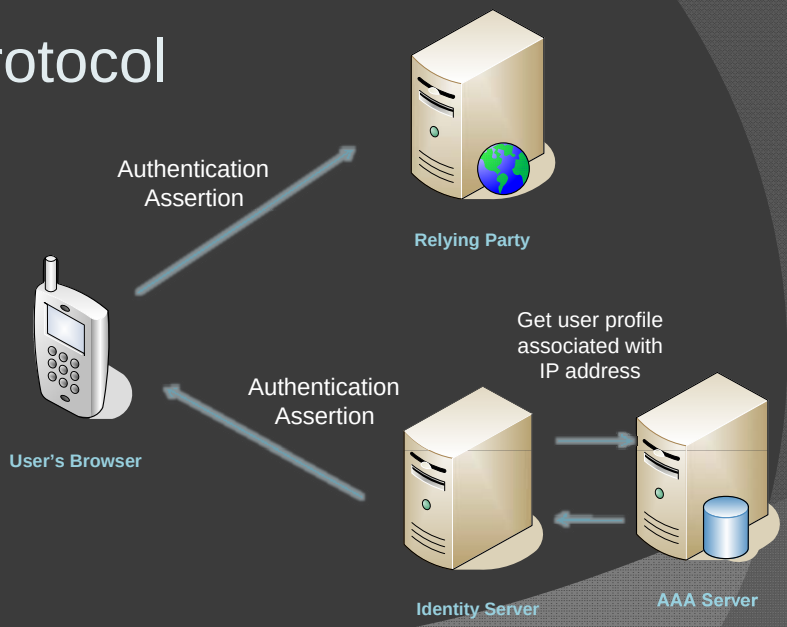
WebCallerID Architecture



Protocol



Protocol



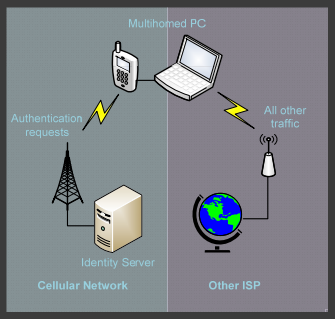
Implementation

- Based on OpenID, but could be used with other SSO systems
- AJAX client handles all authentication for user, user simply clicks "Login" and the network handles the rest
- Unique identity per RP (directed identity) prevents colluding RPs from tracking a user across sites
  Construct identity per RP via keyed hash of (user, domain)

14

Deployment

- No changes needed for user clients
- No changes needed for OpenID enabled relying parties
- Works with
  - cell phone based browsers
  - PCs with cellular modem
  - PCs with a tethered phone



Multihomed usage scenario

Security Benefits

- Users don't need to:
  - Create and remember good passwords
  - Identify malicious relying parties
  - Carry another physical token
- Websites don't need to:
  - Store and handle user authentication data
  - Worry about phishing sites stealing valid credentials

16

Mobile Device Authentication

- Multi-factor authentication
  - Many sensors – location, audio, video, wireless networks
  - Combine multiple forms of evidence to authenticate
- Passive system
  - Minimal user interaction
  - Mimics human authentication processes