Preventing Spoofing, Phishing and Spamming by Secure Usability and Cryptography

ICDCS 07/07/2006

Amir Herzberg

Computer Science Department, Bar Ilan University

http://AmirHerzberg.com

Internet Most Visible Threats

- Spam
  - Lots of junk email
  - Mostly illegal
  - Breaks email
    - But not just via email…

- Spoofing
  - Fake sites, email, etc.
  - Steal passwords, …
  - Breaks e-commerce

- Phishing
  - Spam leading to spoofed site

Can Crypto, Secure Protocols Help?

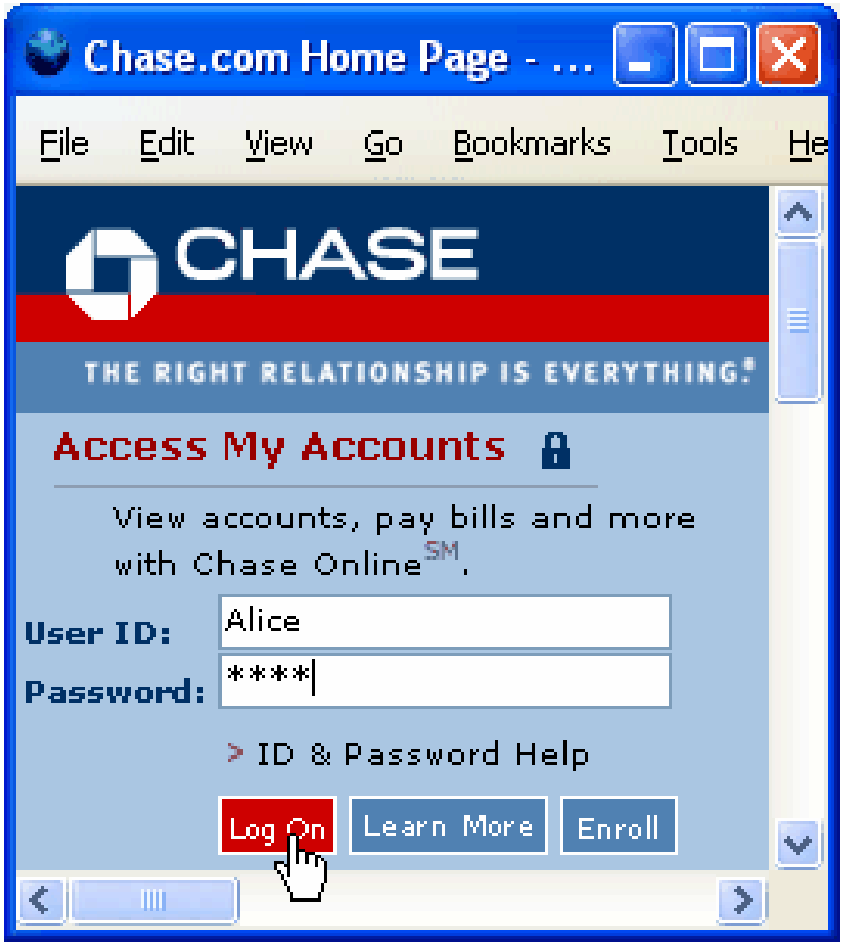
- Strong, provably-secure schemes, protocols
  - Schemes: encryption, signatures, …
  - Computation of any function
  - Protocols: SSL, IP-Sec, S/MIME,…
- But:
  - E-mail crypto (S/MIME etc.) rarely used
    - Definitely not against spam
  - SSL/TLS used… but spoofing, phishing thrives
- Why? Can't crypto help?
  - Good question…
  - Our topic, actually ☺

Outline of rest of lecture

- Why users use spoofed sites?
  - Short answer: mostly bad usability
  - Usability improvements… and beyond (crypto!)
- Spam and phishing solutions
  - Why they fail ?
- How crypto should help…
  - Accountability for e-lies (spoofing, malware, ads)
  - Secure protocols for accountability, penalties

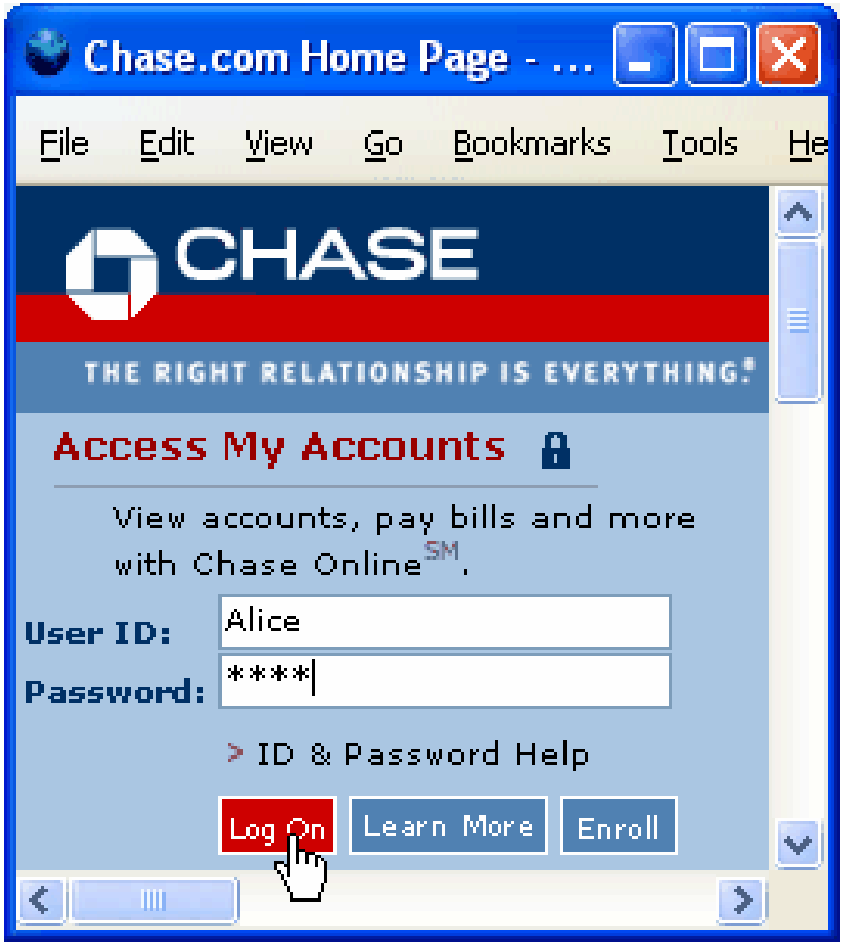
Typical Web Login Process

- Security mechanisms:
  - Username – Password
  - SSL (encrypt password)
- Simple to use
- Any problems?



Problem 1: Site Uses SSL Incorrectly

- Invokes SSL only on clicking `Log On`
- Login form itself not protected
- Spoofed form:
  - Looks the same
  - But sends PW to attacker!
- Many other such sites
  - PayPal, Bank of America, MS hotmail/passport…
  - See my `Hall of Shame`
  - See FSTC report



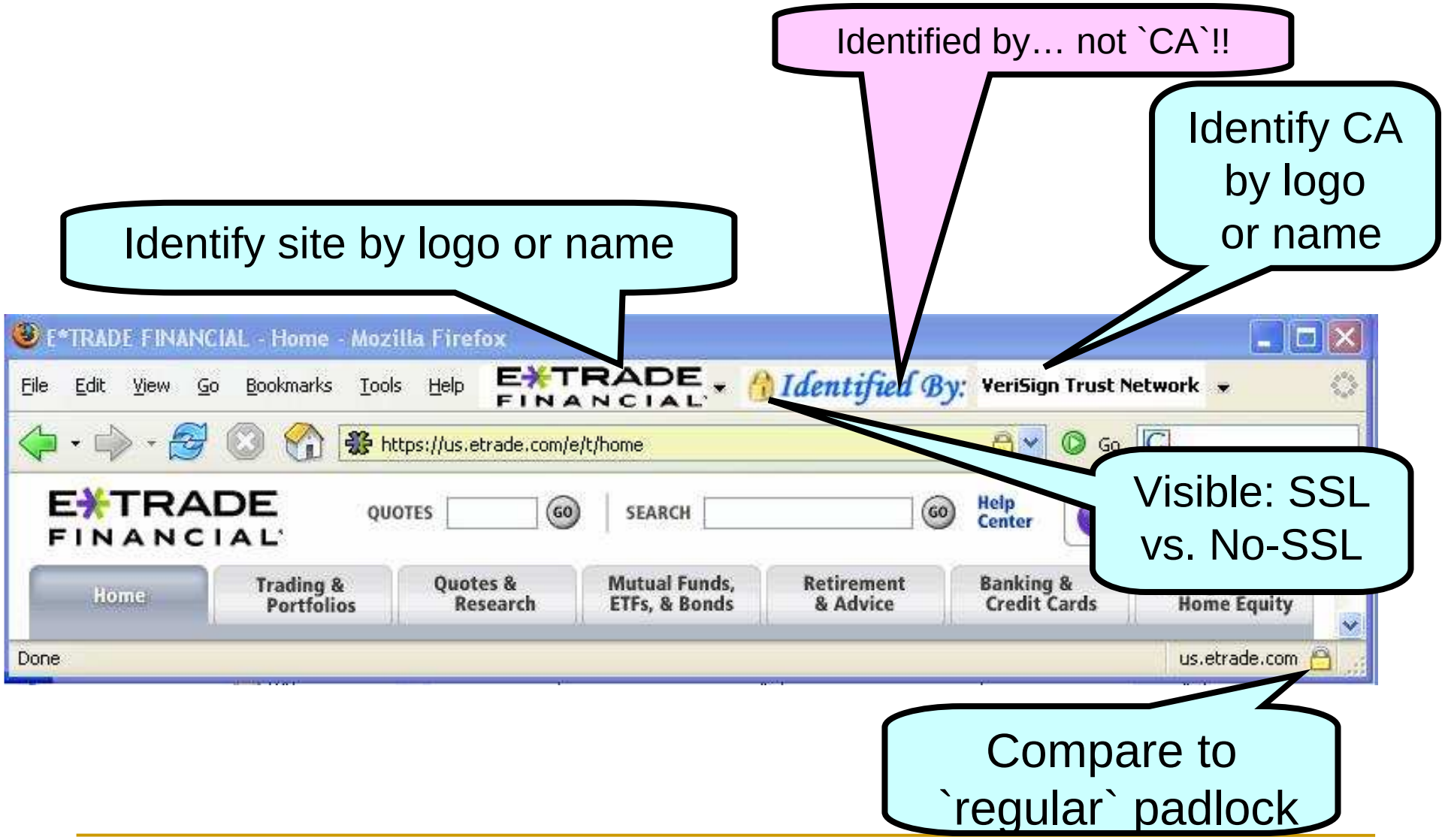
Problem 2: Users DO NOT...

- Notice SSL indicators (padlock, https)
  - E.g., few suspect Chase's site…
  - Trust based on content – e.g., padlock in page...
- Notice URL in wrong domain
  - Wrong domain login: http://BankOfAmerica.REO.com
  - Most do *not* detect wrong domain and no SSL!
  - And: sites can hide location bar, put fake instead
- Use only trusted CAs
  - Users do not know what is a CA
  - Users allow sites with bad certificate, or new CA

What went wrong? How to fix?

- `PKI is too complex`
  - Did we give it a chance?
- `Users are too dumb`
  - Did we give them a chance?
- First step: fix the User Interface !
- TrustBar: **site identification indicator**
  - Default: name/logo and `Identified by` <CA>
    - Users know whom they depend on
  - Customized: user-selected logo/icon/name
    - Petname

TrustBar: Default Identification

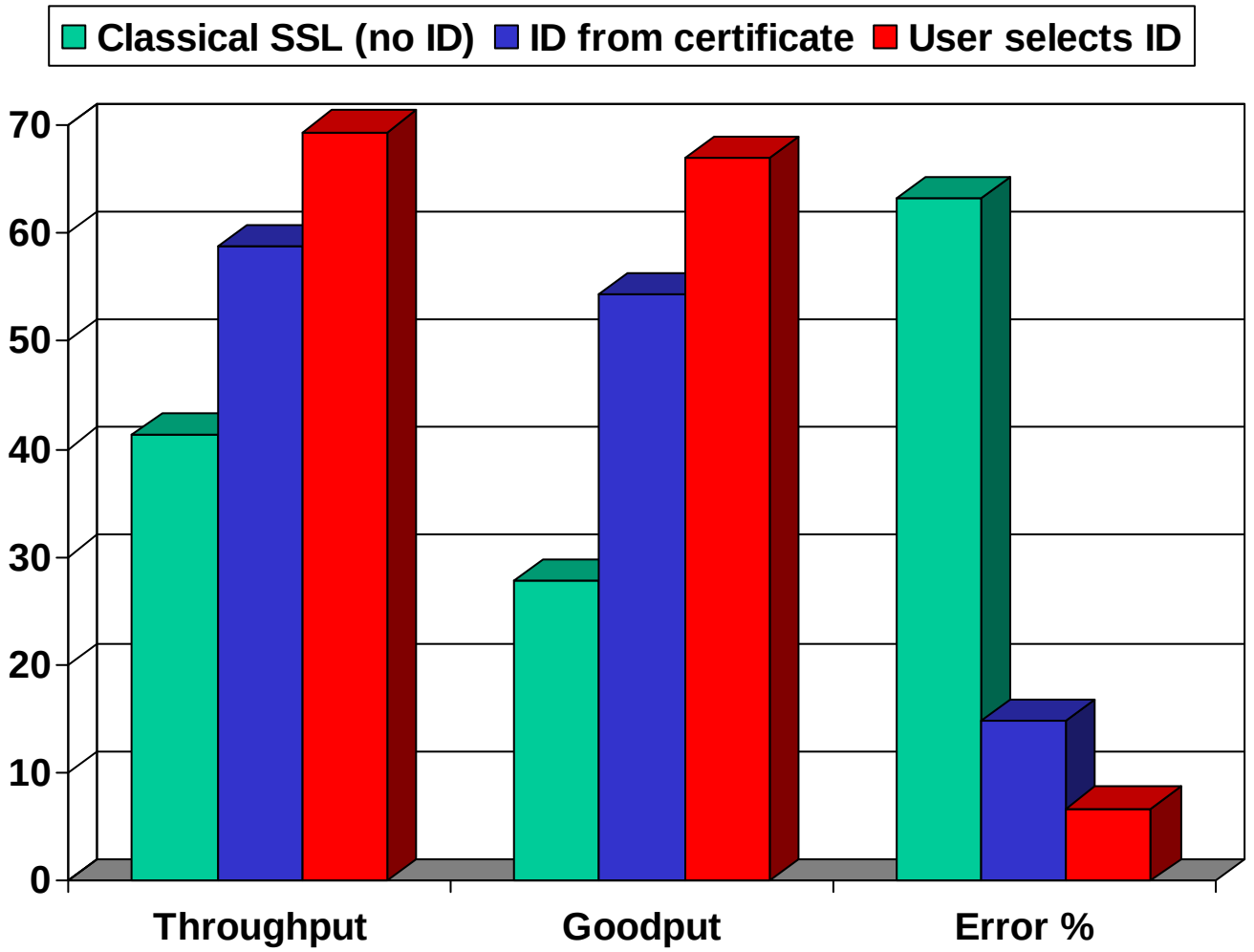


IEv7: Partial Adoption…

- Mandatory, fixed location bar
  - Color coded: red (phishing), green (`good` SSL)
  - `Blacklist` approach ☹ [new addresses are cheap]
- Contains padlock and name for SSL site:

  Name alternates with `Identified by` <CA>:
- But: only for `extended validation certificates`

Experiments: Compare ID Indicators

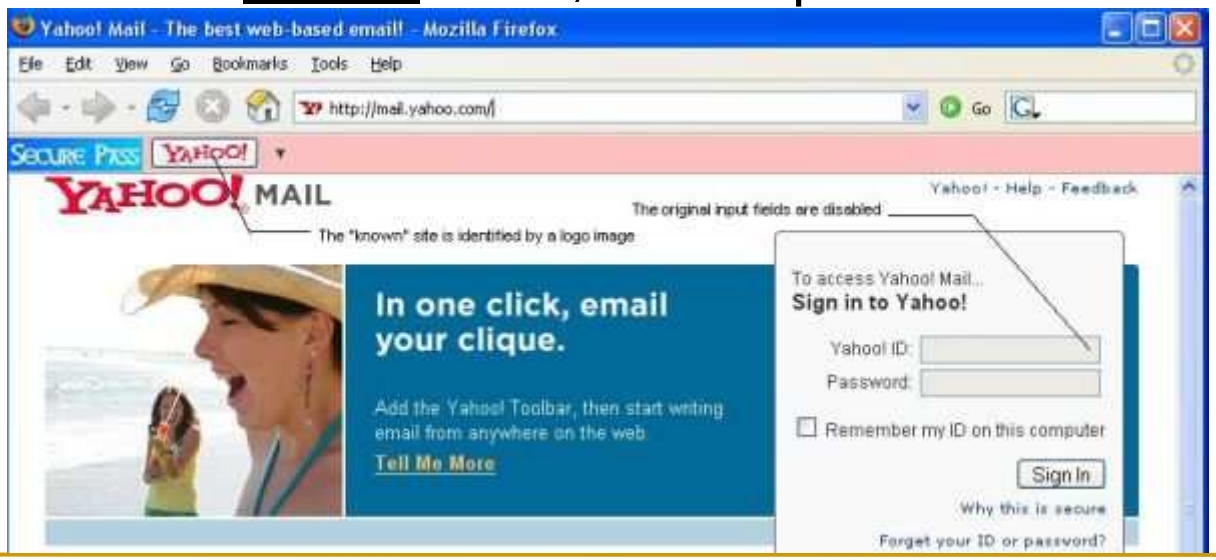


Conclusions from Experiments…

- Adding site identification helps
- User-selected identification even better
- But: significant error rates!!
  - Expect higher error rates in `real life`
- Why high error rates?
  - Users trust content of site
  - Is this stupid or what?
- Secure usability rule: **Defend, don't ask**
  - Block attacks, don't ask user to help
  - That's the role of defense forces, isn't it?
- How??
  - Single click logon (don't enter password)
  - Default blocking mode & **accountability** - using crypto!!

Single-Click Logon

- Idea: avoid entry of password by user
  - Cannot steal password if user does not enter it!
- Improved usability
  - Trivial to use: must click site identifier (logo)
    - User cannot enter, submit password via site!!



Safe-Surf Mode (Block by Default)

- Defending login process is not enough
  - E.g., does not block malware
- Proposal: safe-surf mode: allow only legit pages
  - Display only rated, signed content
  - Initially, only e-banking… future: everything rated, signed!
- Ratings:
  - This script/executable does not contain malware
  - This image does not contain any logo or trademark
  - This page contains only content owned by Foo.com Inc.
  - This video is rated PG-13
- Ensure correct ratings by reputation or penalties
  - Punish e-lies by crypto protocols

Outline of rest of lecture

- Why users use spoofed sites?
  - Short answer: mostly bad usability
  - Usability improvements… and beyond (crypto!)
- Spam and phishing solutions
  - Why they fail ?
- How crypto should help…
  - Accountability for e-lies (spoofing, malware, ads)
  - Secure protocols for accountability, penalties
- Only highlights - no time today ☹

`Isn't content filtering good enough?`

- Content filtering blocks most spam
  - By email client (e.g. Thunderbird, Outlook)
  - By mail server (e.g. spamassasin)
- But filtering…
  - is expensive (computationally)
  - is unreliable
  - fails against adaptive adversary
- Spammers are very adaptive…
  - Short messages (`Bob, see this link: xxx.com`)
  - Learn from captured messages, feedback
  - Phishing: messages emulate authentic text!!

Accountability Spam Solutions

- Most spam solutions use accountability:
  - Accept only `accountable` messages
  - Punish `accountable party` if message was spam
- Often, `accountable party`=outgoing mail server
- Validate `accountability` by…
  - Sending mail server's (SMTP-sender) IP address
  - SMTP-sender-IP vs. SPF record
    - SPF record of mail-from/HELO/PRA domain
  - Signature on email, e.g. DKIM
    - DKIM: signature format, key of domain stored in DNS
- How to punish accountable spammers?

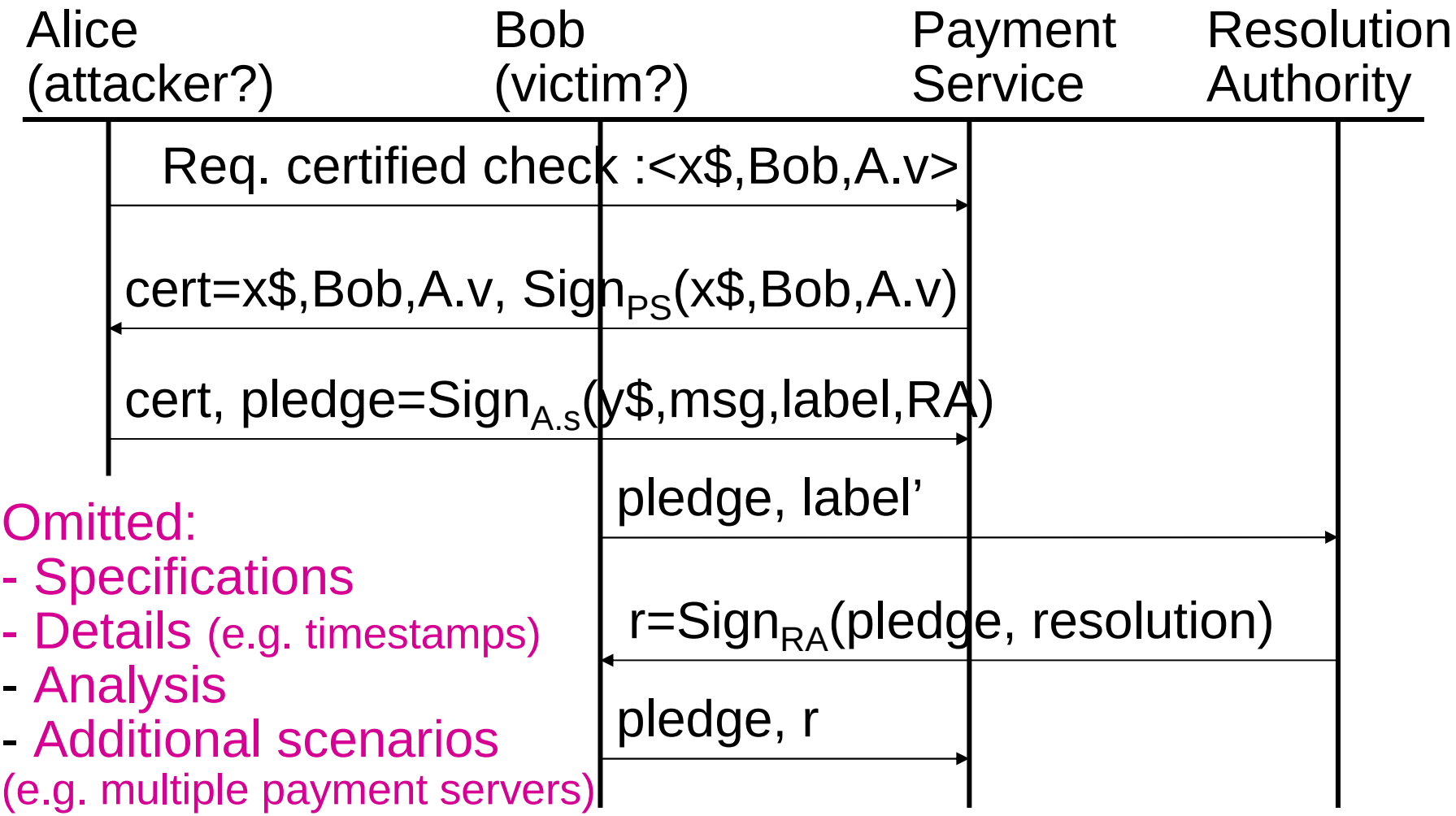
Punishing Accountable Spammers

- Blacklist (block) `bad` servers
  - Problem: easy, cheap to change `name` (IP addr)
- Whitelist known, trusted servers
  - Spammers – and unknown – delayed, filtered
  - Problem: unfair to new correspondents
- Common problem: `all or nothing` approach
  - Very few servers block all users of AOL, gmail…
- Using reputation / accreditation services
  - Spammers reported, `punished` by service
  - How can recipient be sure penalties are right?
  - How can service validate complaints?

Secure Penalties and Resolutions

- General automated resolution and penalty mechanism
- For spam
  - Mail with incorrect `label` (e.g. `not commercial`)
- For phishing
  - Mail with false sender identification
- For spoofed/scam sites
  - Sites with misleading/harmful content
- And other goals, e.g. P2P fairness (no free riders)
- How?
  - Use trusted **resolution authority (RA)** and **payment service**
  - Sign **pledge**: content, label (`no ad`), RA, penalty amount
  - Victim sends pledge to RA, receives signed **resolution**
  - Trusted **payment service** receives **pledge + resolution**

Secure Resolution and Penalty Protocol



Omitted:
- Specifications
- Details (e.g. timestamps)
- Analysis
- Additional scenarios
(e.g. multiple payment servers)

Conclusions

- We should protect `average` Net users
- Usability and accountability are keys
- Specific proposals:
  - Site Identification Indicators (customizable)
  - Single-click logon
  - Safe-Surf mode (allow only rated content)
  - Secure resolution and penalty protocol
- Validation is critical
  - Serious usability studies (hard…)
  - Modular analysis and proofs of security