SSL/TLS

- Transport-layer security protocol
  - Often used to secure reliable protocols (TCP)
  - Does not require pre-shared keys
  - Most common usage: https
    - E-commerce ($200bn/2008), Banking, etc.

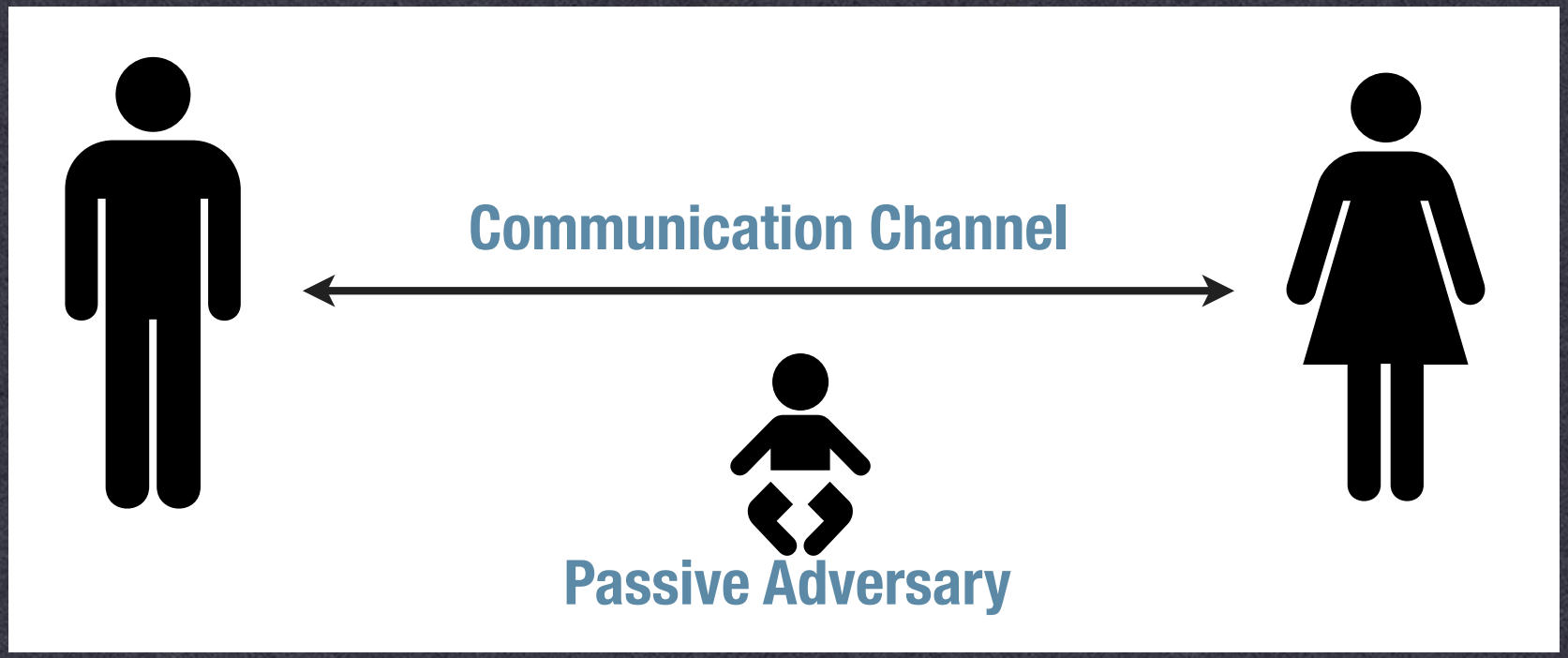
Bank of America

Bank of Opportunity™

https://bofa.com

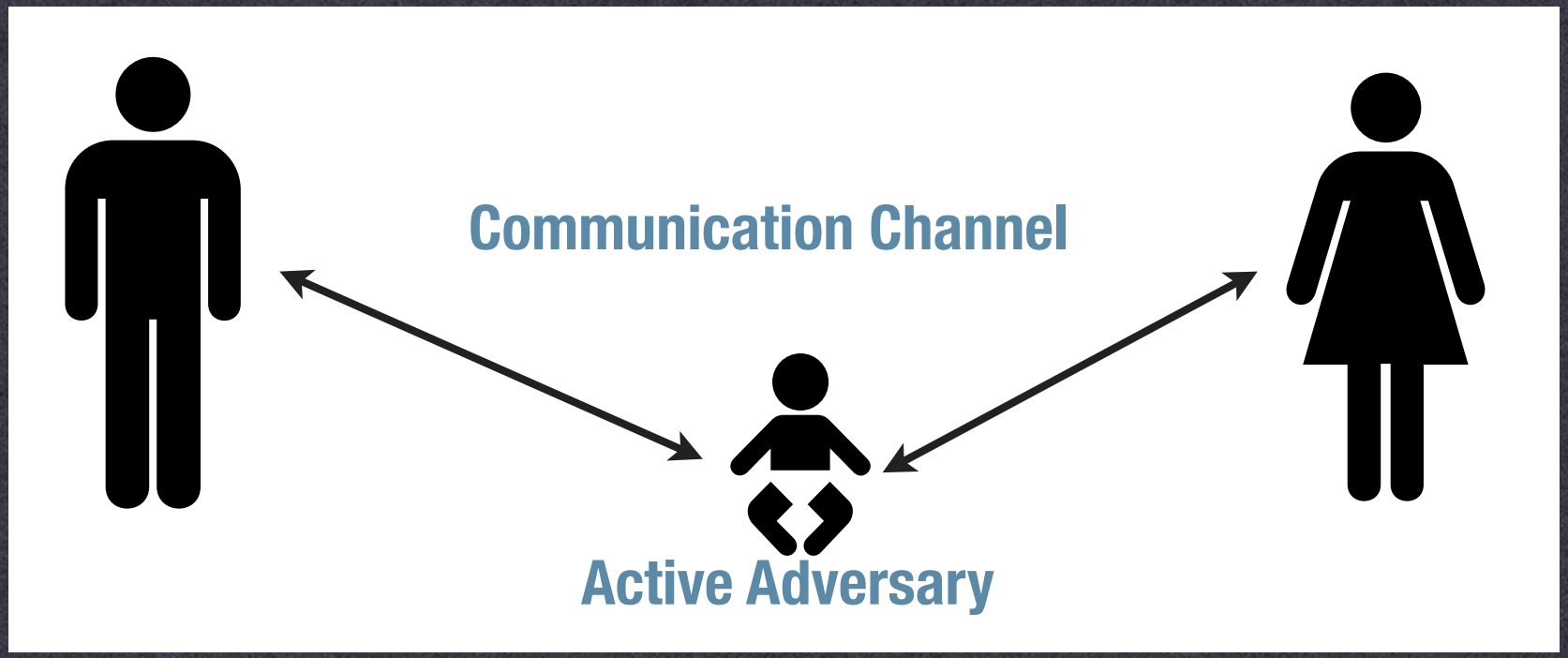
https

Threat Model



Threat Model

Q: How does an adversary run this attack?



SSL/TLS

- Version 1.0 (pre-1995)
  - Non-public Netscape protocol
- Version 2.0 (1995)
  - Many flaws: export-weakened keys, rollback
- Version 3.0 (1996)
  - Some flaws (Wagner, Schneier)
- TLS Version 1.0 (1999)
  - Version 1.2 is current standard (as of 8/08)

SSL/TLS

- Extremely flexible protocol
  - Lots of options
  - Backwards compatibility (TLS 1->SSL 3->SSL 2)

1. Negotiate peer capabilities
2. Exchange certificates
3. Session key establishment
4. Secure communications
5. Session expiration/rekeying

SSL/TLS

- **Negotiation:**

I speak SSL 2.0, 3.0.
I support ciphersuites X,Y.
I don't require a client cert.

Bank of America

Bank of Opportunity™

1. Negotiate peer capabilities

I speak SSL 3.0.
I support ciphersuite X.
I don't have a client cert.

SSL/TLS

- **Certificate Exchange**

Bank of America

Bank of Opportunity™

$seed_1$

2. Exchange certificates

Here's my cert:
{ *pk*, bofa.com,
Not a CA, Expires 10/1/2008,
signed by $pk_{Verisign}$ } &
$seed_2$

SSL/TLS

- **Session key establishment**
  - **Various options**
  - **Common approach: RSA based**

$C = \text{RSA-ENC}_{pk}(seed_3)$

1. Negotiate peer capabilities
2. Exchange certificates
3. **Session key establishment**
4. Secure communic
5. Session expirati

$seed_3 = \text{RSA-DEC}(sk, C)$

$k_s = H(seed_1 \,||\, seed_2 \,||\, seed_3)$

$k_s = H(seed_1 \,||\, seed_2 \,||\, seed_3)$

SSL/TLS

- Secure communication
  - In practice, we derive separate MAC & encryption keys

Communicate under k_S

1. Negotiate peer capabilities
2. Exchange certificates
3. Session key establishment
4. Secure communications
5. Session expiration/rekeying

SSL/TLS

- Key expiration/rekeying
  - Key has a defined lifetime
  - If session drops within that lifetime, we restart:
    - This shortcut saves PK operations

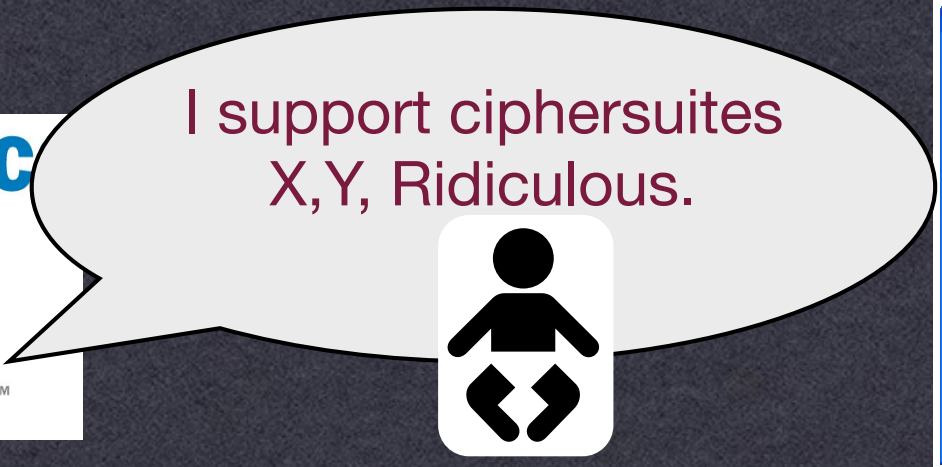
Bank of America

Bank of Opportunity™

1. Negotiate peer capabilities
2. Exchange certificates
3. Session key establishment
4. Secure communications
5. Session expiration/rekeying

Attacks on SSL2

- Many and varied...
- Major vulnerability:
  - Ciphersuite list not authenticated
  - Active attacker could modify the message to specify export-weakened ciphers

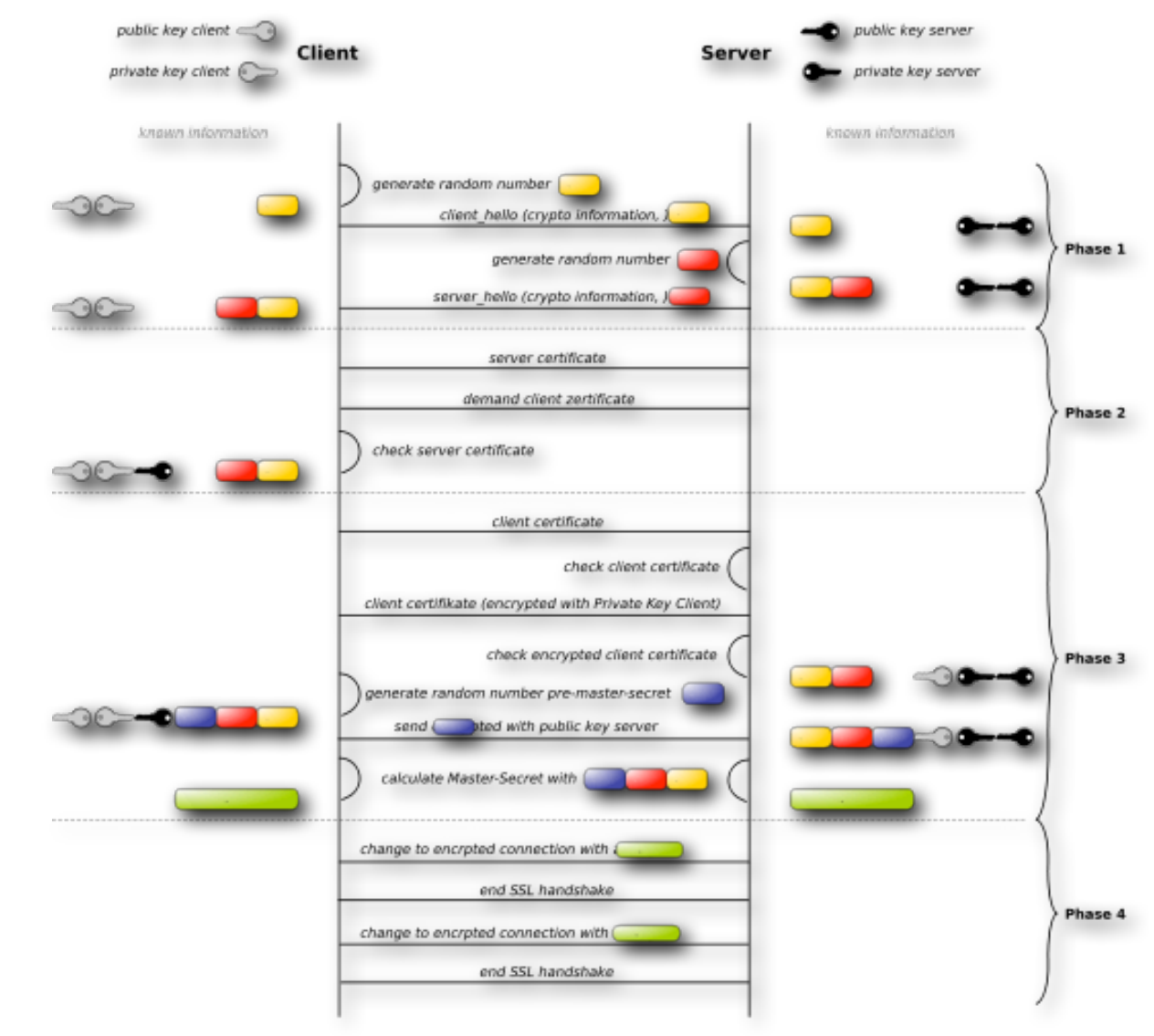


SSL3

- All of the problems with SSL2 fixed!
- Well, not quite:
  - Ciphersuite rollback attack (weaker)
  - Key-exchange algorithm rollback
  - Version rollback
  - (Weak) traffic analysis
  - Also, uses some non-standard primitives

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

SSL3 Handshake



Ciphersuite Rollback

- Most messages sent during client/server handshake are authenticated
  - Final MAC is sent at finish message
  - However, [change cipher spec] message is not included in the MAC
  - Tells the other party to start using encryption/ authentication
  - Attacker can modify/drop this message!

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

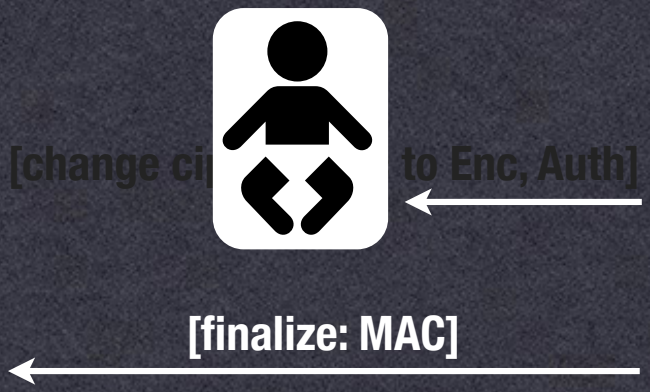
Ciphersuite Rollback

[change cipher spec to Auth] ←

[finalize: MAC] ←

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

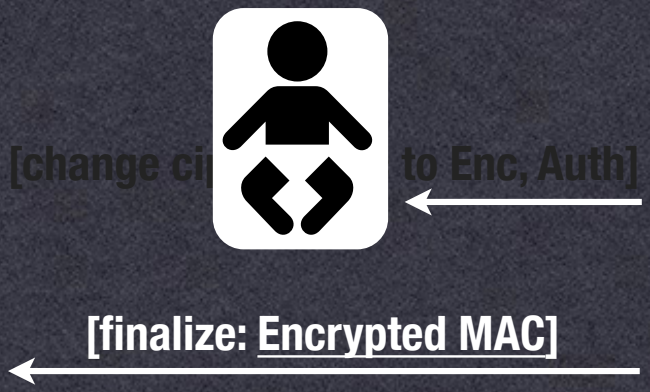
Ciphersuite Rollback



Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Ciphersuite Rollback

- **Big caveat:**
  - **Only works when client asks for authentication <u>without</u> encryption**



Server thinks encryption is disabled, but gets an encrypted MAC

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Key-Exchange Rollback

- SSL3 standard supports two ephemeral key exchange modes:
  - 1. Server publishes ephemeral RSA parameters (signed under its certified signing key)
  - 2. Server publishes ephemeral DH parameters
  - Client may be able to pick which to use
- Why ephemeral key exchange?
  - Advantages of Diffie-Hellman? RSA?

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Key Exchange - RSA

Bank of America

Bank of Opportunity™

I'd like to use RSA-ephemeral

RSA Parameters (N,e), signature

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Key Exchange - DH

Bank of America

Bank of Opportunity™

I'd like to use Diffie-Hellman

DH Parameters (p, g, g^a), signature

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Key Exchange Rollback

Bank of America

Bank of Opportunity™

I'd like to use RSA

I'd like to use DH

DH Parameters (p, g, g^a)

RSA Encrypt: k^g mod p

Normal RSA parameters: (N,e)

I assume *p* is the RSA modulus, and *g* is the RSA exponent. I ignore the extra value.

Since *p* is a prime, we can compute inverses. Recover k.

Version Rollback

- Release of SSL3 didn't make SSL2 browsers go away
  - Servers still accepted SSL2 requests
  - Attacker could modify [client hello] message to specify SSL2
  - Server continues with SSL2 connection, attacker uses SSL2 attacks

Wagner, Schneier: Analysis of the SSL 3.0 Protocol

Version Rollback

- Version rollback is a big problem!
  - SSL, SSH, IPSEC...
  - Example: PPTP
    - Can disable encryption, force use of a weaker password authentication protocol
  - Example: L2TP
    - Better! But many implementations automatically downgrade to PPTP if L2TP connection fails

Traffic Analysis: SSL3

- Example:
  - First HTTP request typically looks like:

```
GET / HTTP/1.1
Host: cnn.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel
Mac OS X 10_5_6; en-us) AppleWebKit/525.27.1
(KHTML, like Gecko) Version/3.2.1 Safari/
525.27.1
```

  - From ciphertext length, we may be able to work out URL information

Traffic Analysis++

- **Digression: The case of encrypted VoIP**
  - Some VoIP protocols use VBR encoding, size of data packets depends on signal
  - Also include “silence suppression” (VAD)
  - Therefore, total traffic is highly correlated to the contents of the line.

Good news:
Most VoIP implementations don't actually use VBR/ supression

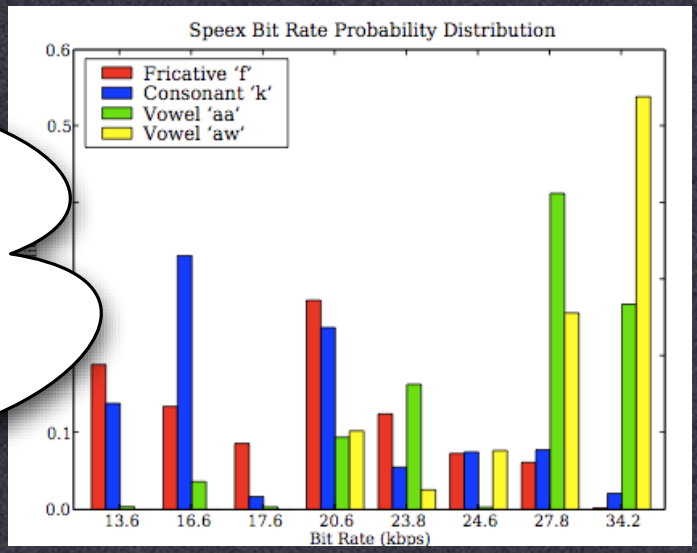


Image from Wright, Ballard, Coull, Monrose, Masson: Spot me if you Can, Uncovering spoken phrases in VoIP conversations

SSL: Current Events 2/2009

Current Events

- Black Hat Federal 2009 (last week)
  - Moxie Marlinspike: SSLStrip
    - (now in the wild)
  - Does not break SSL
  - Instead: takes advantage of the way SSL is used

HTTP->HTTPS

- Typical Banking Experience:
  - SSL URLs begin with https://
  - But users rarely type the prefix

User enters: americanexpress.com

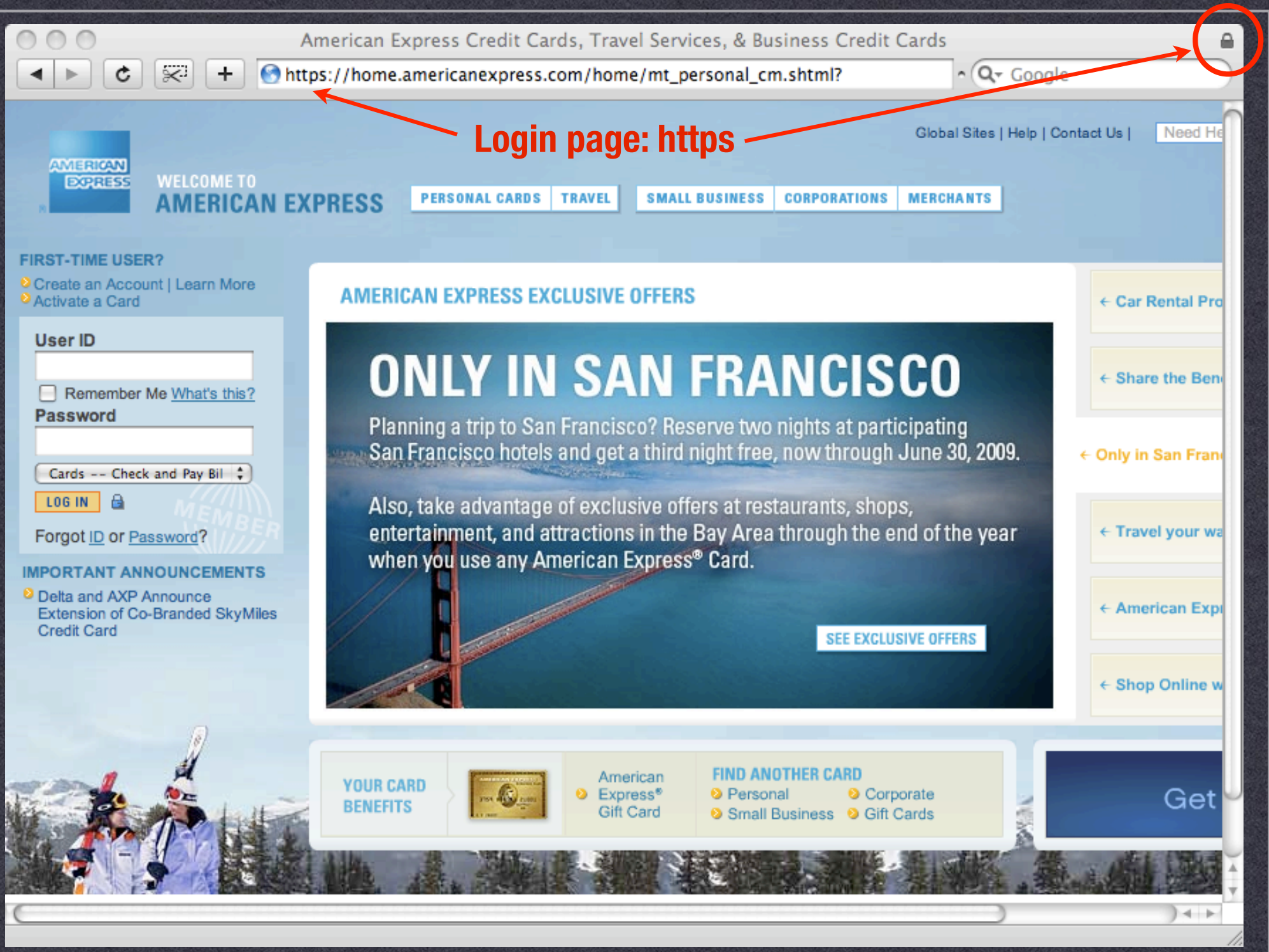
GET http://americanexpress.com

REDIRECT https://americanexpress.com

GET https://americanexpress.com

SSL secured web page

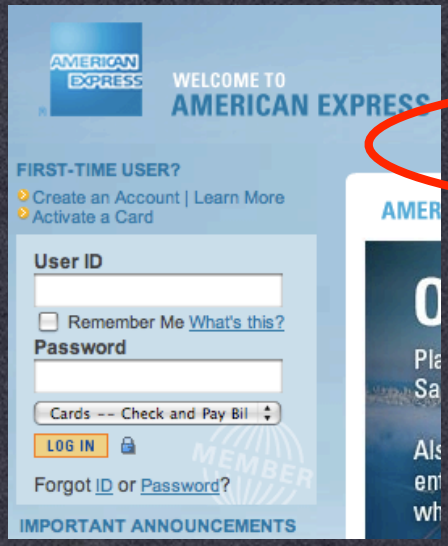
User login info


American Express Credit Cards, Travel Services, & Business Credit Cards
https://home.americanexpress.com/home/mt_personal_cm.shtml?
Google
Login page: https
Global Sites | Help | Contact Us |
WELCOME TO
AMERICAN EXPRESS
PERSONAL CARDS
TRAVEL
SMALL BUSINESS
CORPORATIONS
MERCHANTS
FIRST-TIME USER?
Create an Account | Learn More
Activate a Card
User ID
Remember Me What's this?
Password
Cards -- Check and Pay Bil
LOG IN
Forgot ID or Password?
IMPORTANT ANNOUNCEMENTS
Delta and AXP Announce Extension of Co-Branded SkyMiles Credit Card
AMERICAN EXPRESS EXCLUSIVE OFFERS
ONLY IN SAN FRANCISCO
Planning a trip to San Francisco? Reserve two nights at participating San Francisco hotels and get a third night free, now through June 30, 2009.
Also, take advantage of exclusive offers at restaurants, shops, entertainment, and attractions in the Bay Area through the end of the year when you use any American Express® Card.
SEE EXCLUSIVE OFFERS
← Car Rental Pro
← Share the Ben
← Only in San Fran
← Travel your wa
← American Expr
← Shop Online w
YOUR CARD BENEFITS
American Express® Gift Card
FIND ANOTHER CARD
Personal
Corporate
Small Business
Gift Cards
Get

HTTP->HTTPS

- If you can intercept the user's connection:
  - Don't redirect, or:
  - Redirect to malicious site, unsecured (http)

User enters: americanexpress.com



GET http://amex.com

REDIRECT http://secure.amex.com

GET https://secure.amex.com

SSL secured web page

User login info

HTTP->HTTPS

- If you can intercept the user's connection:
  - Homograph site: paypal.com (with a capital i), or:
  - Use clever IDN tricks e.g.,

    https://www.gmail.com/accounts/ServiceLogin!f.ijjk.cn

HTTP->HTTP->HTTPS

- It can be worse:
  - Some sites give an http page with a form that submits via https

User enters: americanexpress.com

GET http://americanexpress.com

Unsecured http web page

User login info

Wachovia – Personal Finance and Business Financial Services

http://wachovia.com/

Google

Login page: http

Customer Service | Contact Us | Locations

WACHOVIA

Great News
about Free Online Statements—
Now with up to 7 years of
Online Statement history.

See More >

LOGIN

User ID:

Remember my User ID

Password:

(case sensitive)

Service:

Choose a service...

Login

Forgot User ID or Password?

Retirement Plan Participants: Login
Education Loan Customers: Login

Online Security
Wachovia Security Plus℠
Online Services Guarantee

Sign Up for Online Banking
Sign Up | Learn More | Demo

LOCATIONS

ZIP:

Find

More Search Options

PERSONAL FINANCE

En español

Online Services
Online Banking with BillPay
Mobile Banking
Online Brokerage
More...

Retirement Planning
Tools & information for
Lifetime Retirement Planning

Investing
Accounts & Services
IRAs
More...

Insurance
Life, Auto, Home,
Health

Banking
Checking
Savings & CDs
Credit Cards
Check Cards
More...

Lending
Mortgage
Home Equity **New!**
Education Loans
Vehicle Loans

Rates
Mortgage Rates
Home Equity Rates
Credit Card Rates

Payment Challenges?
Explore your loan options

Save up to 30% on TurboTax.
Small Business customers save big on the #1 rated tax software.
Save Now >>

The time is now.
Mortgage rates are at an all-time low.
Refinance Today >>

Search

Search Tips

What to Expect:
Homeowner Affordability & Stability Plan
Learn More >>

WACHOVIA SECURITIES

An industry leader in investment and advisory services for individuals, corporations and institutions.

SMALL BUSINESS

The tools, services, and research to manage your company.
Small Business Login

ONLINE BANKING.
Securely manage your business finances online.
Wachovia Business Online.

CORPORATE & INSTITUTIONAL

Wachovia Securities Corporate and