Applications of Crypto: SSL/TLS

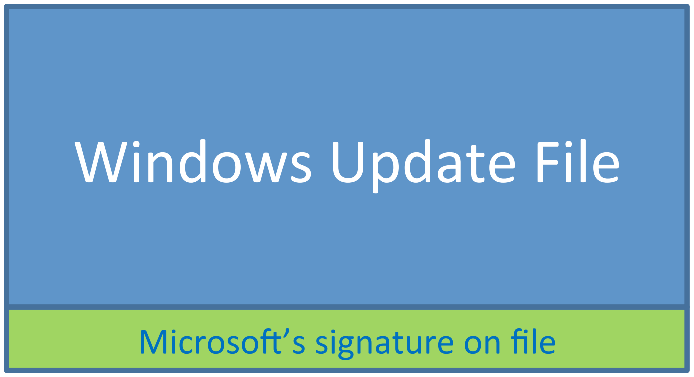
Slides credit: Dan Boneh, Doug Tygar, David Wagner

Overview

- Last lecture
  - Cryptographic hash function
  - HMAC
  - Public-key encryption
  - Digital signature
- This lecture
  - Certificate
  - SSL/TLS
  - Passwords

Review: Applications of Digital Signatures

- Software distribution



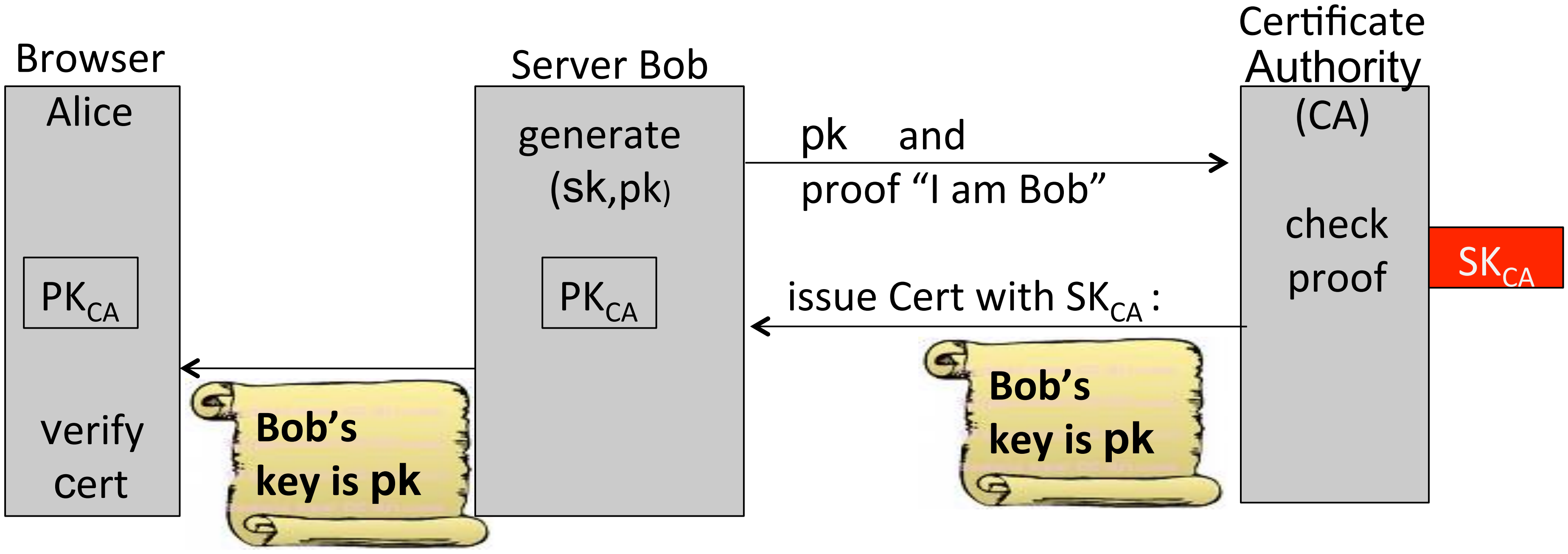
Windows Update File

Microsoft’s signature on file

- How can we get Microsoft’s public key?

Certificates: bind Bob’s ID to his PK

How does Alice (browser) obtain Bob’s public key pk_{Bob} ?



Browser Alice

PK_{CA}

verify cert

Server Bob

generate (sk,pk)

PK_{CA}

pk and proof “I am Bob”

Certificate Authority (CA)

check proof

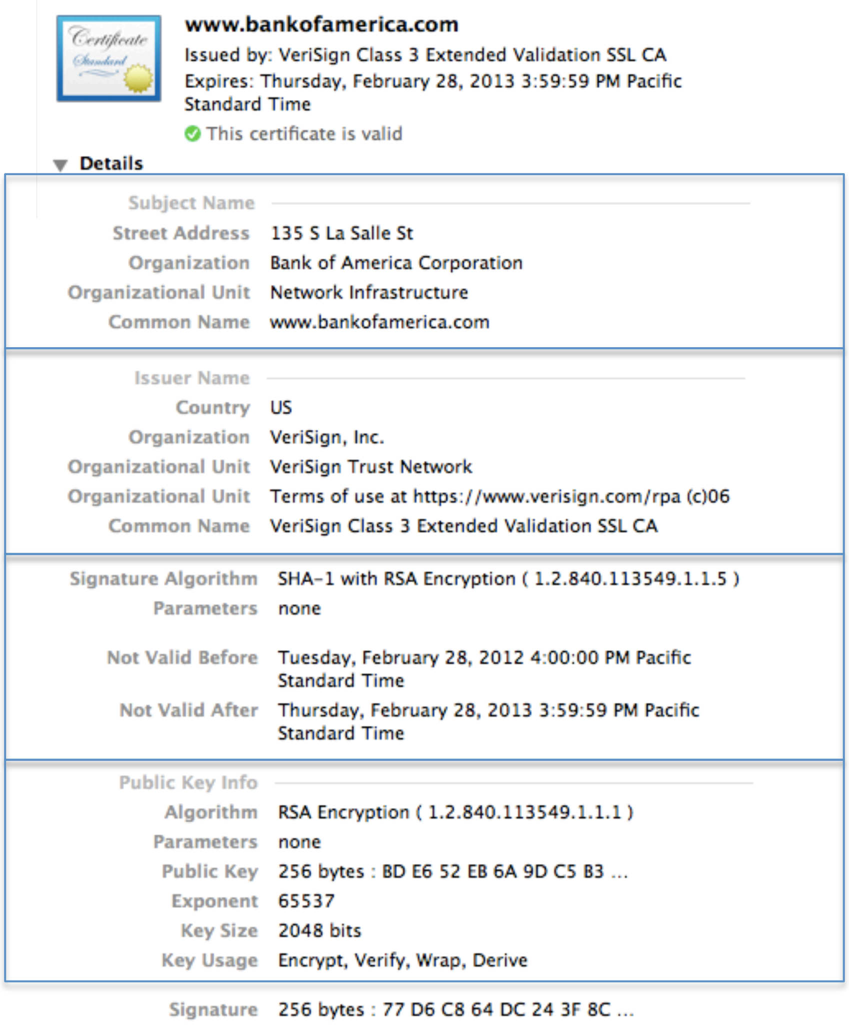
SK_{CA}

issue Cert with SK_{CA} :

Bob’s key is pk

Bob’s key is pk

Sample certificate:



www.bankofamerica.com

Issued by: VeriSign Class 3 Extended Validation SSL CA

Expires: Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time

✓ This certificate is valid

▼ **Details**

Subject Name	
Street Address	135 S La Salle St
Organization	Bank of America Corporation
Organizational Unit	Network Infrastructure
Common Name	www.bankofamerica.com
Issuer Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)06
Common Name	VeriSign Class 3 Extended Validation SSL CA
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday, February 28, 2012 4:00:00 PM Pacific Standard Time
Not Valid After	Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : BD E6 52 EB 6A 9D C5 B3 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 77 D6 C8 64 DC 24 3F 8C ...

Certificate Issuance Woes

Wrong issuance:

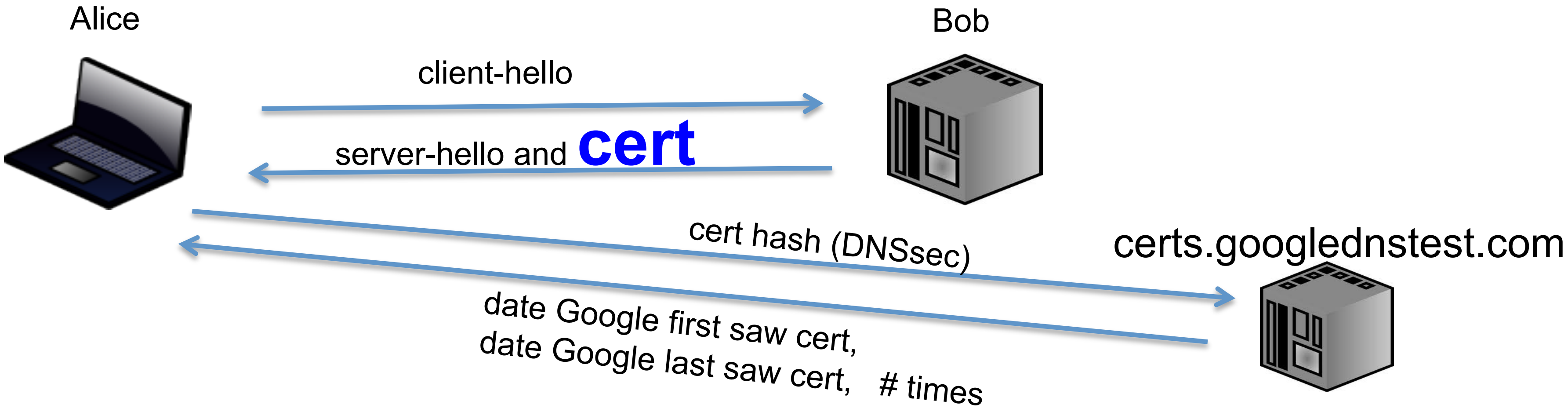
2011: Comodo and DigiNotar CAs hacked,
incorrectly issue certs for

gmail.com, yahoo.com, and many others

What to do?

Ask some other trusted 3rd party:

- examples: Perspectives [WAP'08] , Google certificate catalog, DANE



Certificate revocation

What happens if Bob loses his secret key sk?

- Certificate on pk_{bob} must be revoked

Revocation methods:

- Expiration: certificates active in fixed time window (one year)
- Certificate Revocation Lists (CRLs):

  CA publishes a list of revoked certificates
- Online Certificate Status Protocol (OCSP)

Certificate Revocation Lists (CRLs)

CA periodically publishes the serial # of revoked certs.

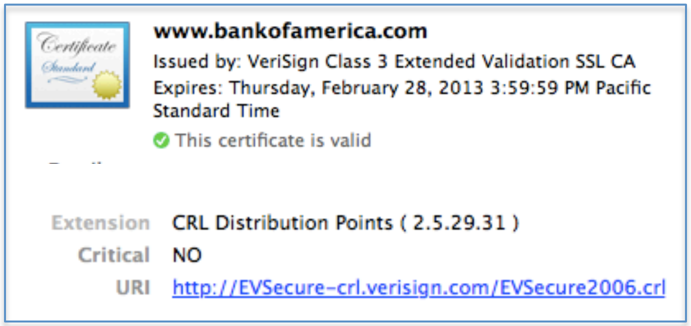
- List is signed by the CA

When browser receives cert.:

- Download latest CRL and reject cert. if serial # is on list

Problems:

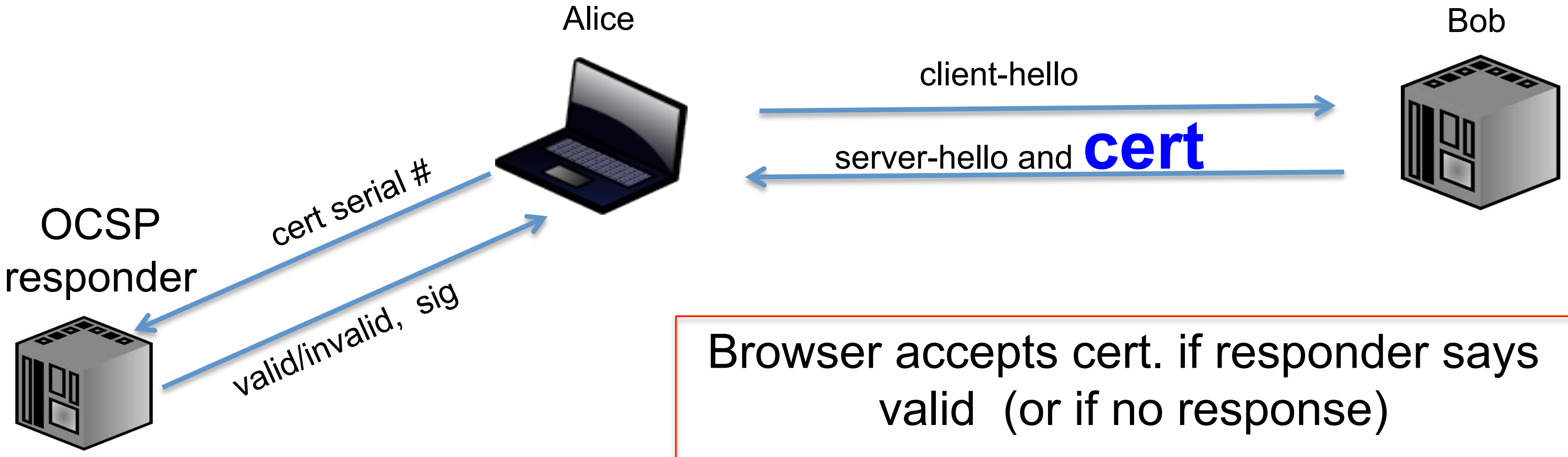
- CRLs can get large
- May reveal whose cert. is revoked



www.bankofamerica.com
Issued by: VeriSign Class 3 Extended Validation SSL CA
Expires: Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time
✓ This certificate is valid

Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://EVSecure-crl.verisign.com/EVSecure2006.crl

Online Certificate Status Protocol (OCSP)



Alice

Bob

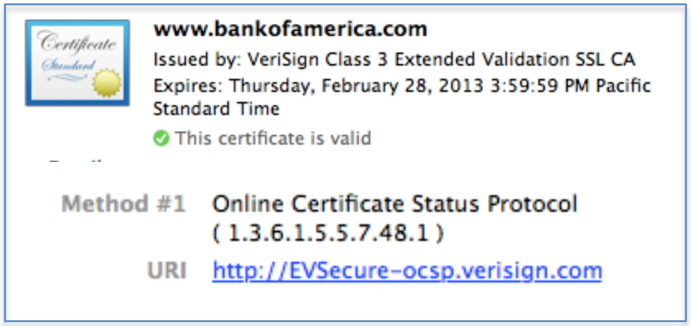
client-hello

server-hello and **cert**

OCSP responder

cert serial #

valid/invalid, sig



www.bankofamerica.com

Issued by: VeriSign Class 3 Extended Validation SSL CA

Expires: Thursday, February 28, 2013 3:59:59 PM Pacific Standard Time

✓ This certificate is valid

Method #1 Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

URI http://EVSecure-ocsp.verisign.com

Browser accepts cert. if responder says valid (or if no response)

Problems:

- Slows down HTTPS session setup
- Let responder track users

(see OCSP stapling for a solution)

Key Exchange

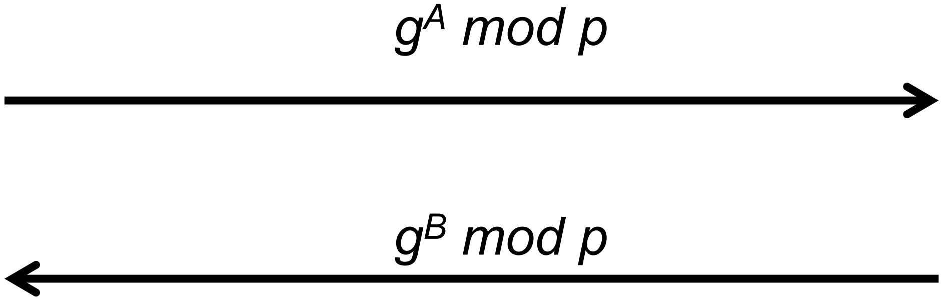
- Alice and Bob want to use symmetric-key encryption
- How can they establish a secret key?
  - Public-key encryption
  - Diffie-Hellman key exchange

Diffie-Hellman key exchange

Alice

Prime p, number g, 0< g < p

Bob



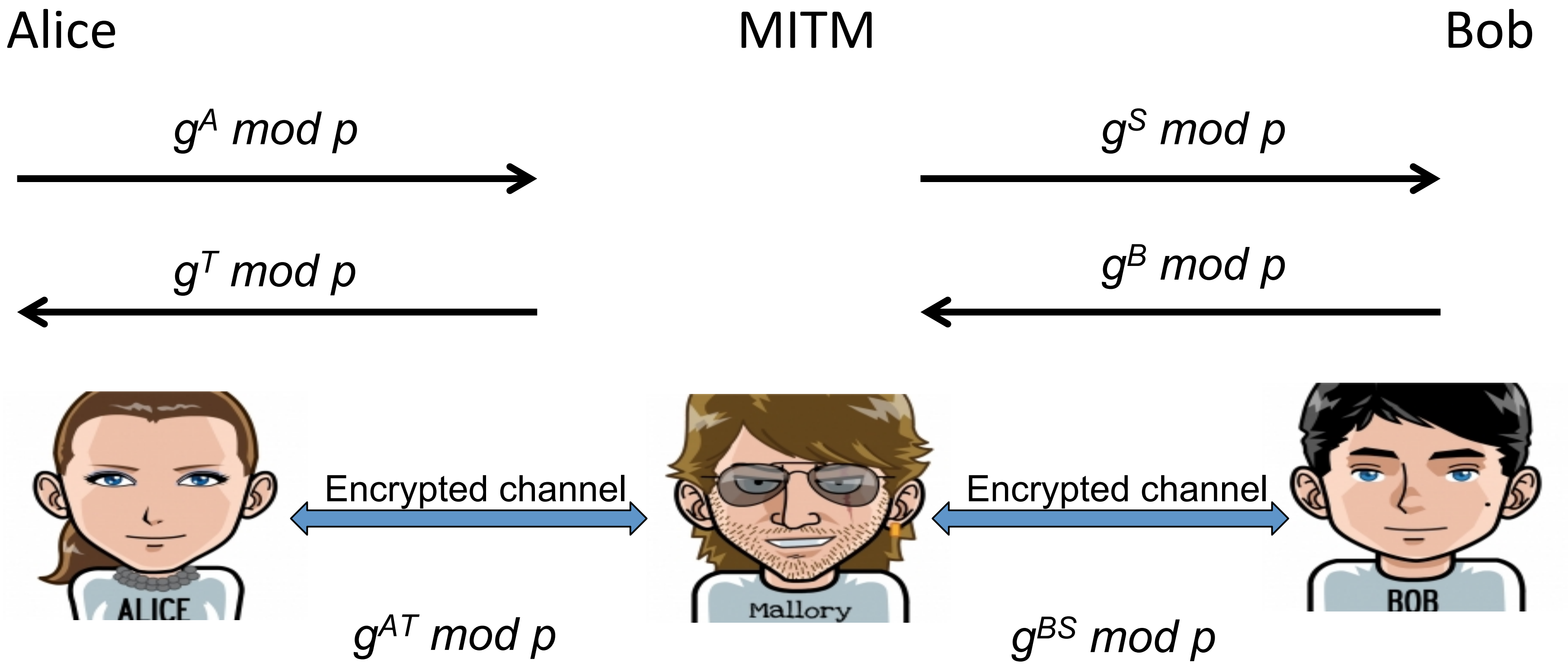
$g^A \bmod p$

$g^B \bmod p$

$(g^A)^B \bmod p$

$(g^B)^A \bmod p$

Man in the middle attack



Alice

MITM

Bob

$g^A \bmod p$

$g^S \bmod p$

$g^T \bmod p$

$g^B \bmod p$

Encrypted channel

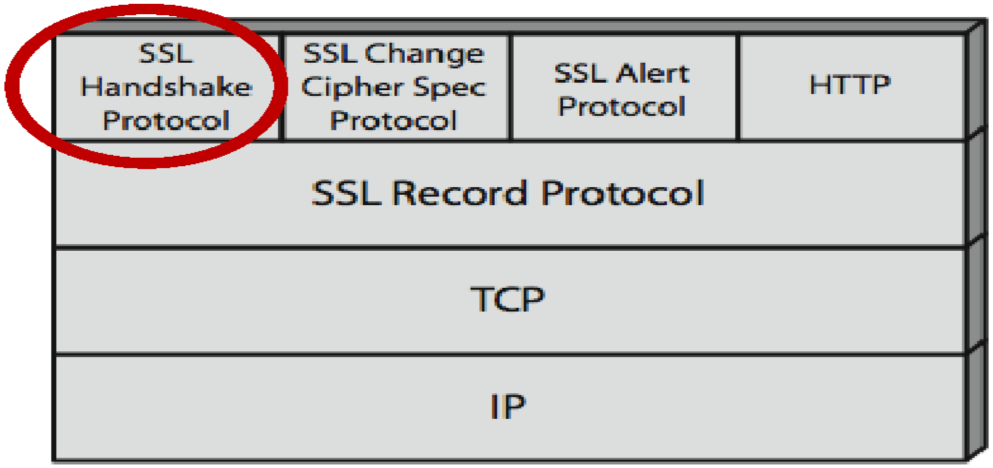
Encrypted channel

$g^{AT} \bmod p$

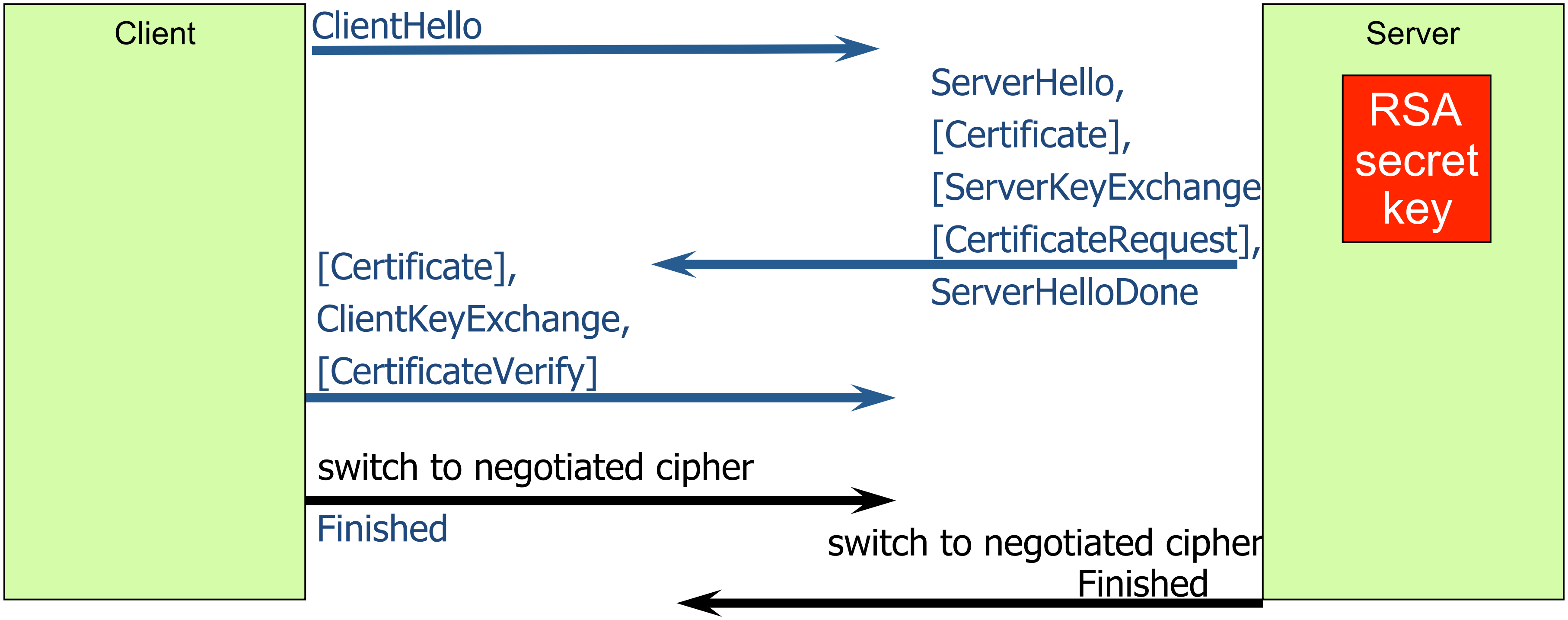
$g^{BS} \bmod p$

SSL Architecture

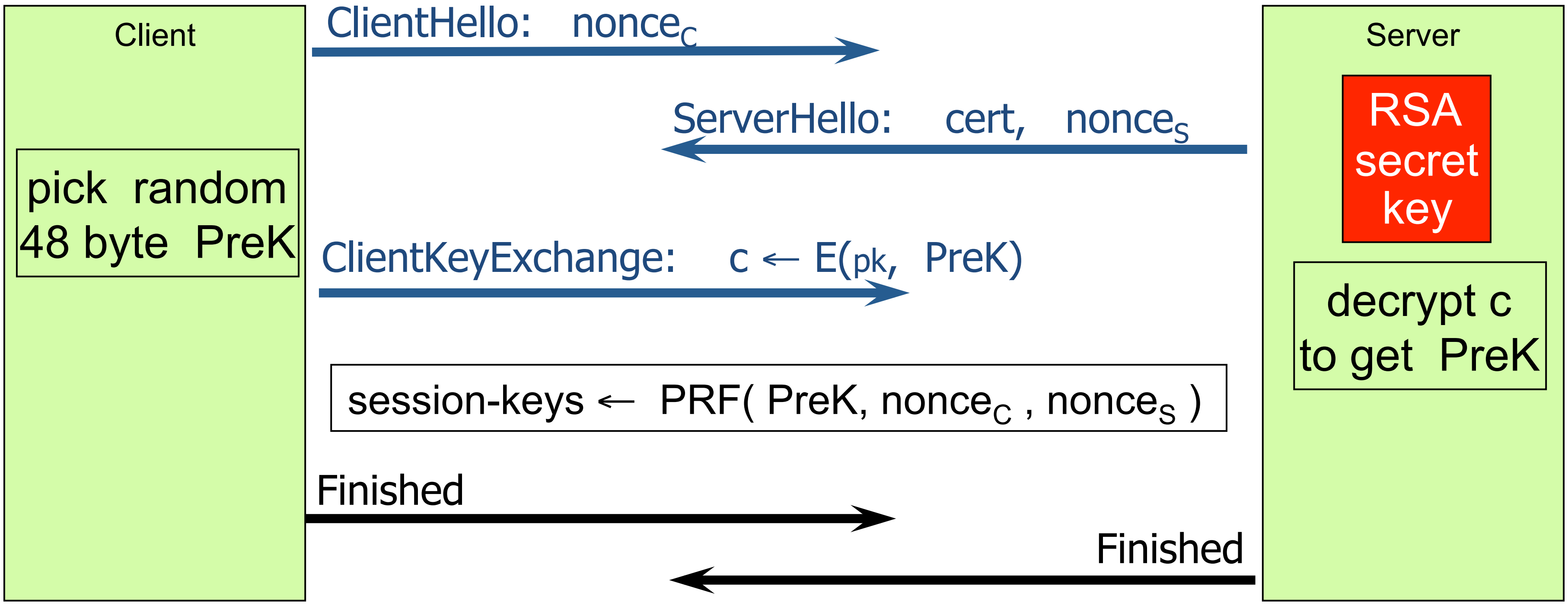
Application of crypto to secure Internet communications



SSL session setup



Abstract SSL (simplified)



Client

pick random 48 byte PreK

ClientHello: nonce_C

ServerHello: cert, nonce_S

ClientKeyExchange: $c \leftarrow E(pk, \text{PreK})$

session-keys $\leftarrow$ PRF(PreK, nonce_C , nonce_S)

Finished

Finished

Server

RSA secret key

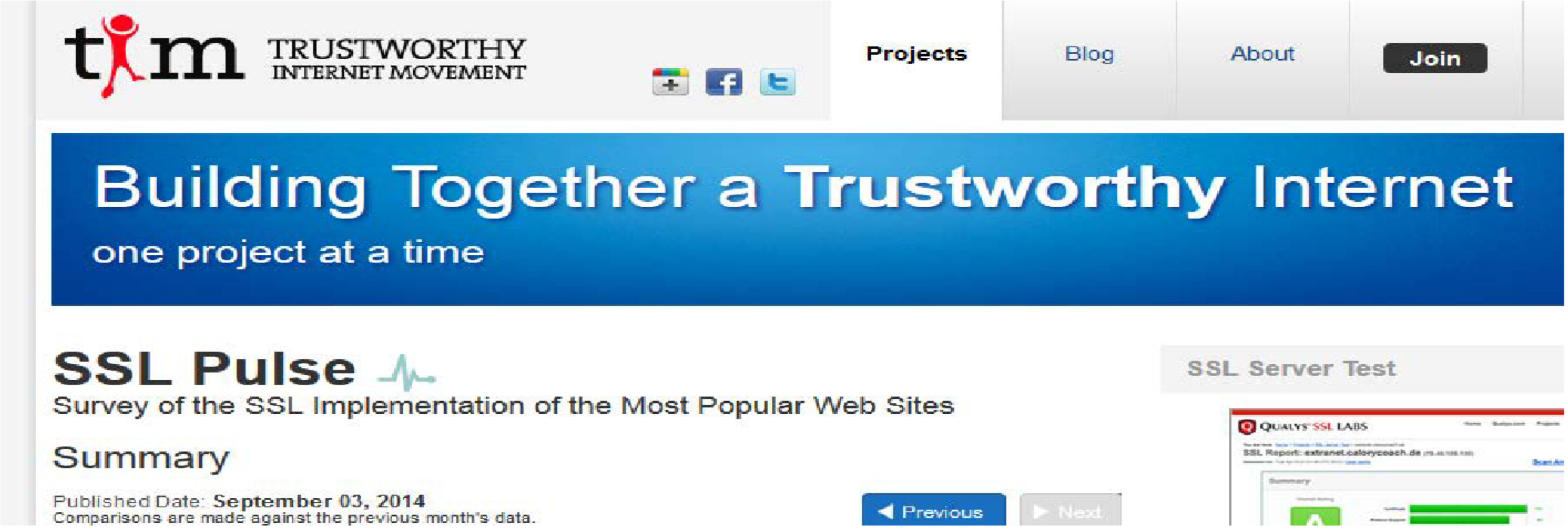
decrypt c to get PreK

SSL Problems

- SSL 2.0 broken
- SSL 3.0 broken
- TLS 1.0 broken
  - BEAST: Browser Exploit Against SSL/TLS Tool

SSL weaknesses in wild

- https://www.trustworthyinternet.org/ssl-pulse/



Building Together a Trustworthy Internet

one project at a time

SSL Pulse

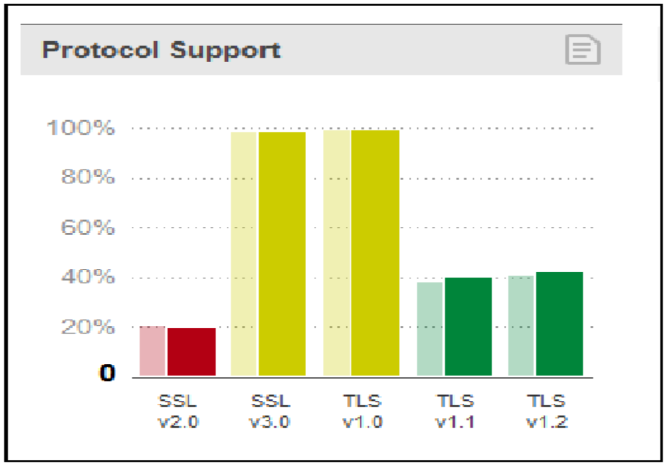
Survey of the SSL Implementation of the Most Popular Web Sites

Summary

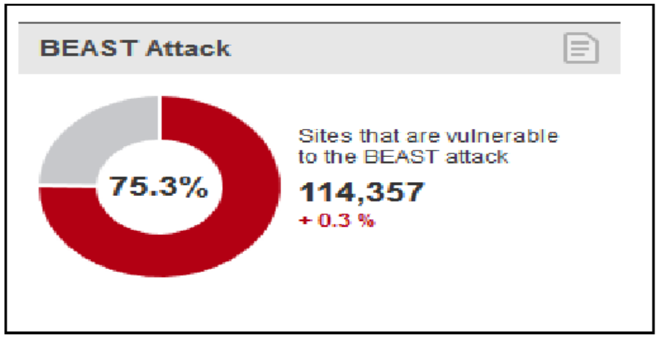
Published Date: **September 03, 2014**
Comparisons are made against the previous month's data.

Published Date: **September 03, 2014**

SSL weaknesses in wild



Protocol Support



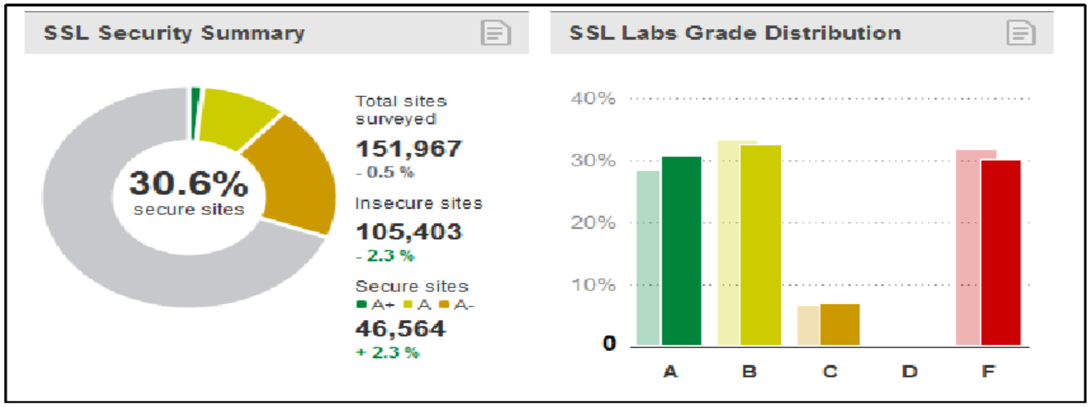
BEAST Attack

75.3%

Sites that are vulnerable to the BEAST attack

114,357

+ 0.3 %



SSL Security Summary

30.6% secure sites

Total sites surveyed

151,967

- 0.5 %

Insecure sites

105,403

- 2.3 %

Secure sites

🟩 A+ 🟨 A 🟧 A-

46,564

+ 2.3 %

SSL Labs Grade Distribution

Passwords

- The most popular authentication method
- Security & Usability issues
  - Long and random passwords are harder to remember
  - Users select memorable passwords, which are easy to guess
  - Users reuse passwords across multiple sites

Attacks to Passwords

- Online guessing attacks
- Social engineering and phishing
- Eavesdropping
- Client-side malware
- Server compromise

Online Guessing Attacks

- Repeatedly try logging in with many different guesses
  - 123456
  - password
  - 12345678
- Defenses
  - Rate limiting, e.g., 5 guesses in one day
  - CAPTCHAs
    - Vulnerable to machine learning attacks
    - Underground markets hire human workers to solve CAPTCHAs

Social Engineering and Phishing

- Fool a user to reveal his/her password
- Defenses
  - Educating users
  - Machine learning to detect phishing sites

Eavesdropping

- If plaintext passwords are sent from the client to the server, they can be eavesdropped on internet, e.g., public Wi-Fi.
- Defenses
  - SSL!

Client-side Malware

- Keyloggers to capture passwords
- Virtual keyboard
  - Malware records the locations of mouse clicks and take screen shots
- Very difficult to defend in this threat model

Server Compromise

- Get a copy of the password database
  - 32M passwords from Rockyou in 2009
- Do not store user passwords in plaintext
- Use cryptographic hash function and salt
  - Store (username, salt, H(salt, password))
  - Offline password guessing: test guesses on the attacker's own computer
  - Use slow hash function to slow down offline password guessing