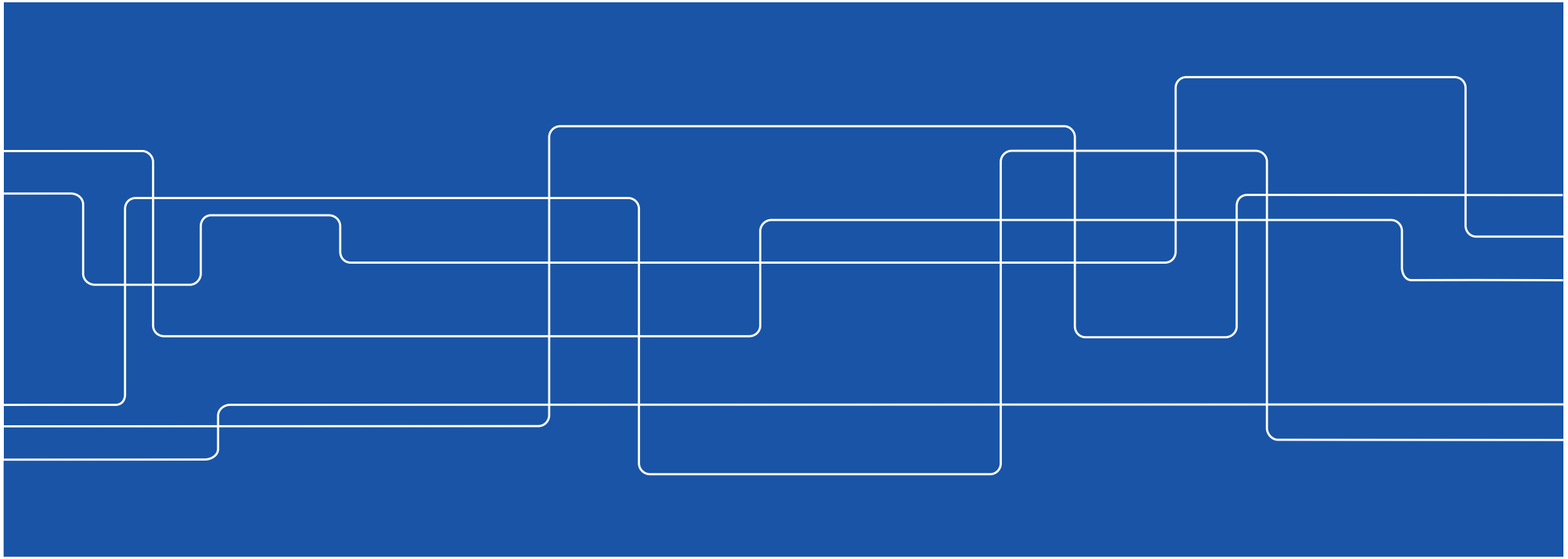
Web Security

IV1013

Peter Sjödin

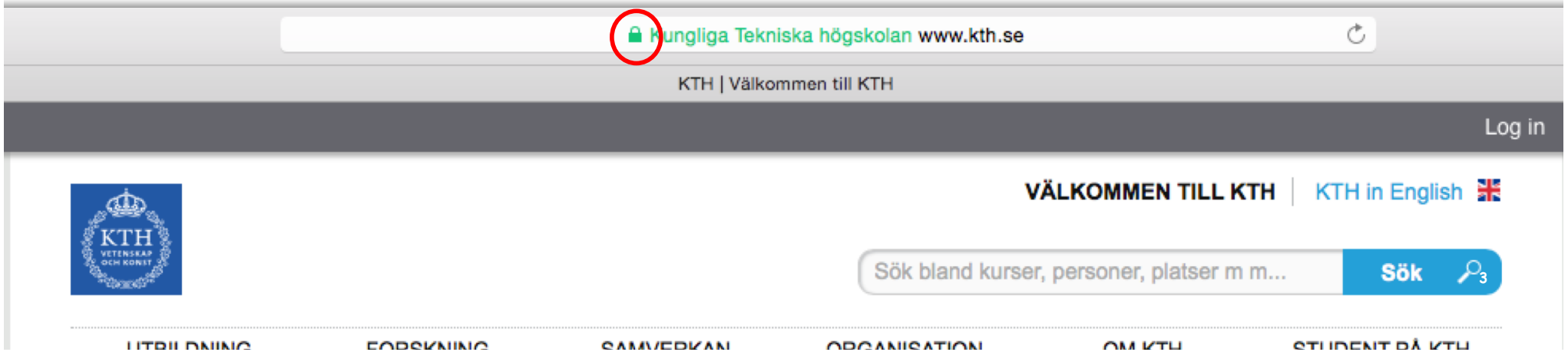


Web Security

- Securing communication between client and server
- Authentication of server and possibly client
- Encryption of HTTP communication

SSL (TLS): Secure Sockets Layer

- widely deployed security protocol (https: in URL)
  - https://www.kth.se
- SSL by Netscape
  - Standardized as TLS (Transport Layer Security), with some variations
- Encrypted communication
- Server authentication (and optionally client authentication)
- Runs over TCP
  - Encrypted data transfer over TCP



Security Protocols in Practice

- Public-key encryption is computationally expensive, and requires long keys
  - But has advantages in key management
- Public key infrastructure (PKI) for certificate management
  - Verification
  - Distribution
  - Revocation
- Symmetric key encryption is computationally efficient
  - But lacks infrastructure for key management

Security Protocols in Practice

- Use best of two worlds

With proper use of certificates, this step also authenticates Bob/Alice

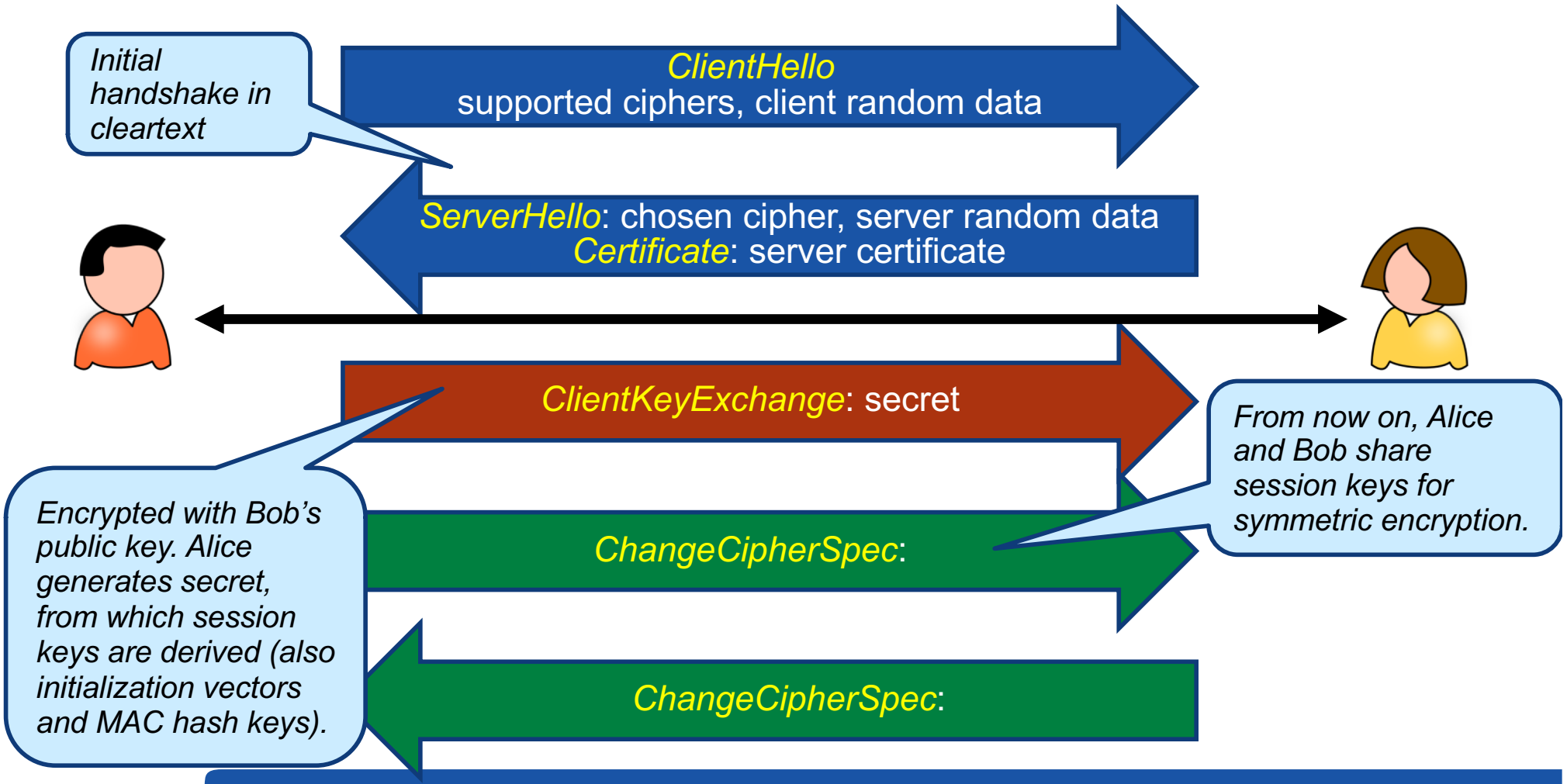
Step 1: Initial handshake using public-key cryptography

Create and exchange temporary session key for symmetric key encryption

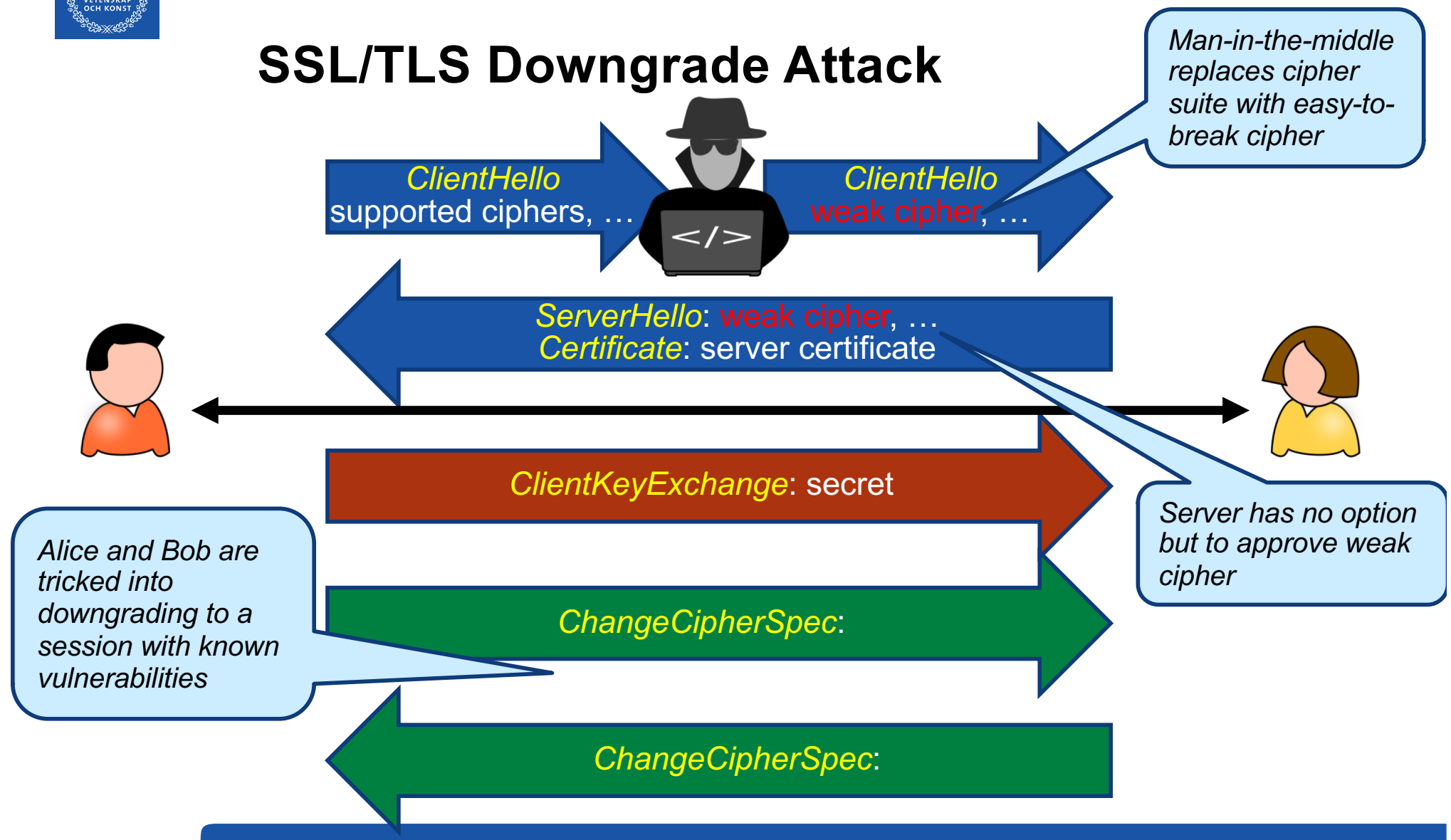
Step 2: Data transfer using symmetric-key cryptography (with temporary session key)

Transmission of bulk data

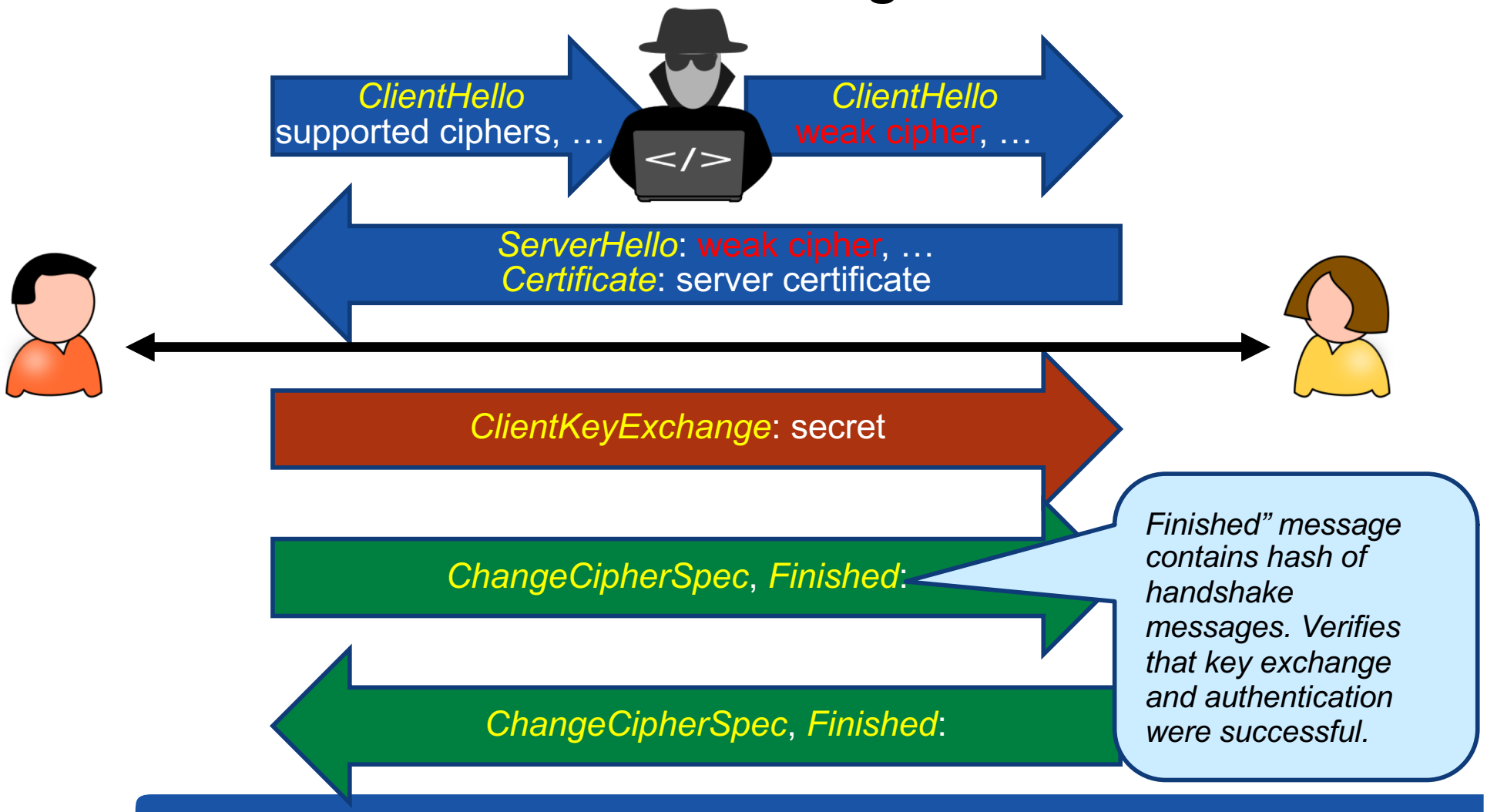
SSL/TLS Handshake Example



SSL/TLS Downgrade Attack



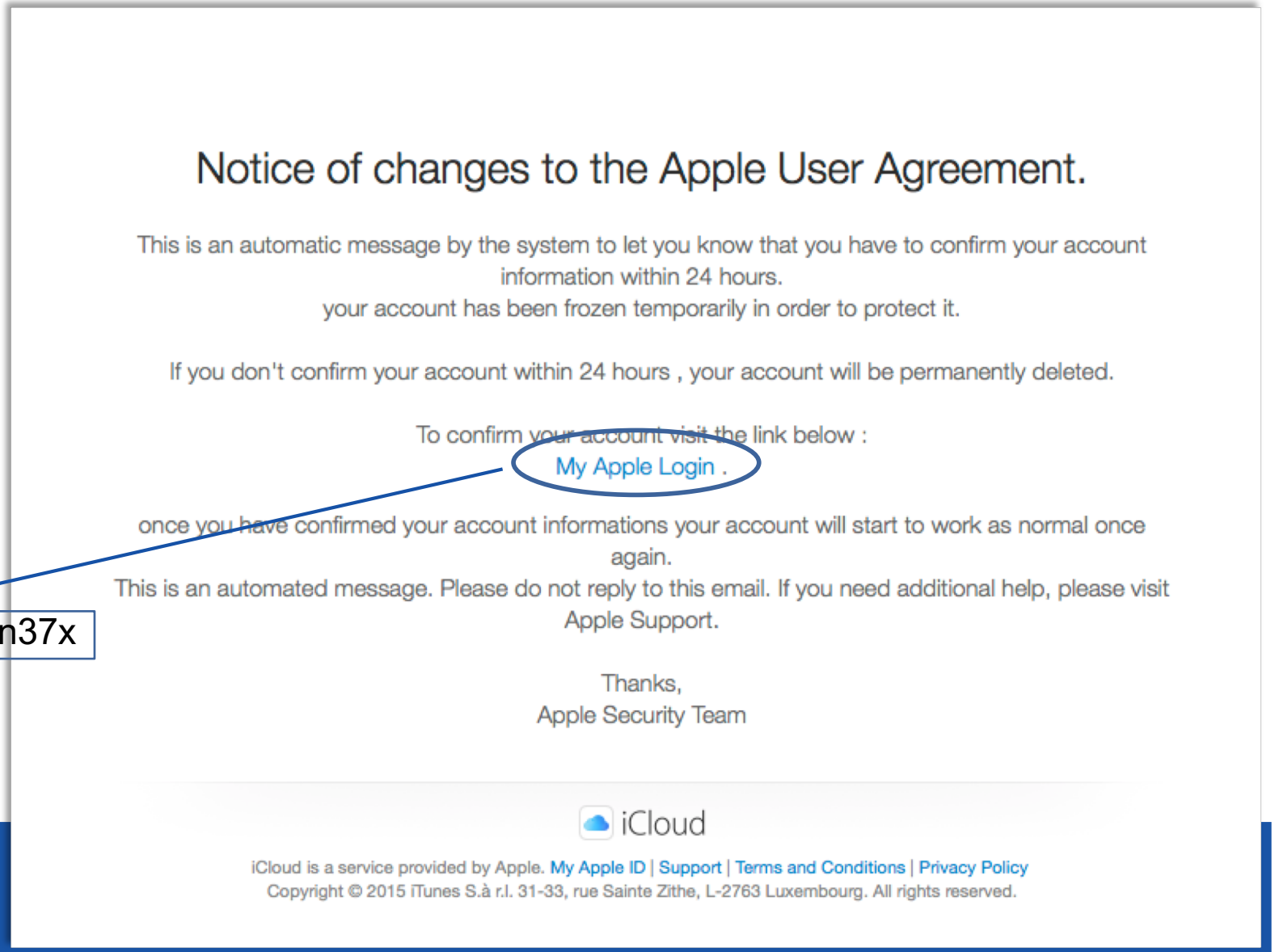
SSL/TLS Finished Messages



Web Attacks and Vulnerabilities

- Luring users to fake sites
  - Social engineering
  - URL obfuscation
- Web servers with insufficient protection
- Script injection
- …

Phishing



Notice of changes to the Apple User Agreement.

This is an automatic message by the system to let you know that you have to confirm your account information within 24 hours.
your account has been frozen temporarily in order to protect it.

If you don't confirm your account within 24 hours , your account will be permanently deleted.

To confirm your account visit the link below :
My Apple Login .

once you have confirmed your account informations your account will start to work as normal once again.
This is an automated message. Please do not reply to this email. If you need additional help, please visit Apple Support.

Thanks,
Apple Security Team

iCloud

iCloud is a service provided by Apple. My Apple ID | Support | Terms and Conditions | Privacy Policy
Copyright © 2015 iTunes S.à r.l. 31-33, rue Sainte Zithe, L-2763 Luxembourg. All rights reserved.

http://bit.ly/22mn37x

JavaScript

- Language executed by browser
  - Can run before HTML is loaded, before page is viewed, while it is being viewed or when leaving the page
- Often used to exploit other vulnerabilities
  - Attacker gets to execute some code on user's machine
  - Cross-scripting:
    - attacker inserts malicious JavaScript into a Web page or HTML email
    - when script is executed, it steals user's cookies and hands them over to attacker's site

Cross Site Scripting (XSS)

- Attacker injects scripting code into pages generated by a web application
  - Attacker uses known vulnerabilities in server or web application
- When user visits pages, the scripting code is executed in user's browser
- Script could be malicious code
  - JavaScript (AJAX), VBScript, ActiveX, HTML, or Flash
- Threats:
  - Phishing, hijacking, changing of user settings, cookie theft/poisoning, false advertising, execution of code on the client, ...

MySpace Worm (1)

http://namb.la/popular/tech.html

- Users can post HTML on their MySpace pages
- MySpace does **not** allow scripts in users' HTML
  - So no <script>, <body>, onclick, <a href=javascript://>
- … but does allow tags for CSS.
  -
- But MySpace will strip out "javascript"
  - Use "java<NEWLINE>script" instead
- But MySpace will strip out quotes
  - Convert from decimal instead:
    alert('double quote: ' + String.fromCharCode(34))

Slide by Prof. Vitaly Shmatikov, The Univ of Texas at Austin

MySpace Worm (2)

http://namb.la/popular/tech.html

- *"There were a few other complications and things to get around. This was not by any means a straight forward process, and none of this was meant to cause any damage or piss anyone off. This was in the interest of..interest. It was interesting and fun!"*
- Started on "samy" MySpace page
  - Everybody who visits an infected page, becomes infected and adds "samy" as a friend and hero
  - "but most of all, samy is my hero"
- 5 hours later "samy" has 1,005,831 friends
  - Was adding 1,000 friends per second at its peak

Slide by Prof. Vitaly Shmatikov, The Univ of Texas at Austin

Client-side XSS defenses

- Pre-process input from user before using it in HTML
- Proxy-based:
  - Analyze HTTP traffic between browser and web server
  - Look for special HTML characters
  - Encode them before executing the page on the user's web browser (i.e. NoScript - Firefox plugin)
- Application-level firewall:
  - Analyze HTML pages for hyperlinks that might lead to leakage of sensitive information
  - Stop bad requests using a set of connection rules
- Auditing system:
  - Monitor execution of JavaScript code and compare the operations against high-level policies to detect malicious behavior

Questions

Some web servers are secured with SSL/TLS even though communication with them is not confidential (such as the main page of KTH). What could be the reasons?

Does SSL/TLS help to protect against XSS attacks? Discuss.