Implementation and Simulation of SSL in Windows Presentation Foundation

Vikram Gawade

Harsh Vachharajani

ECE 646 : Cryptography and Computer Network Security

Problem!!!

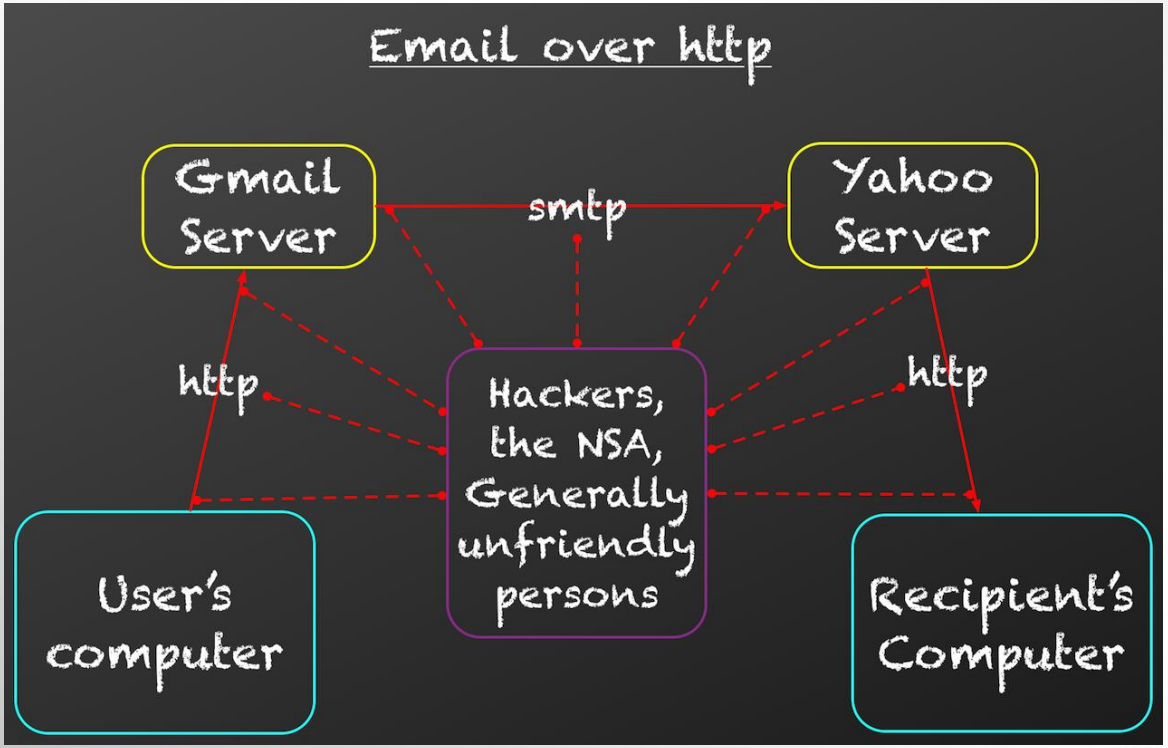
- Insecure communication between a web server and browser
- Interception/sniffing over the messages transmitted on an insecure channel

[Fig. Ref. www.goclio.com]

GEORGE MASON UNIVERSITY

Illustration

- Insecure E-mail communication over HTTP between the e-mail server and the user

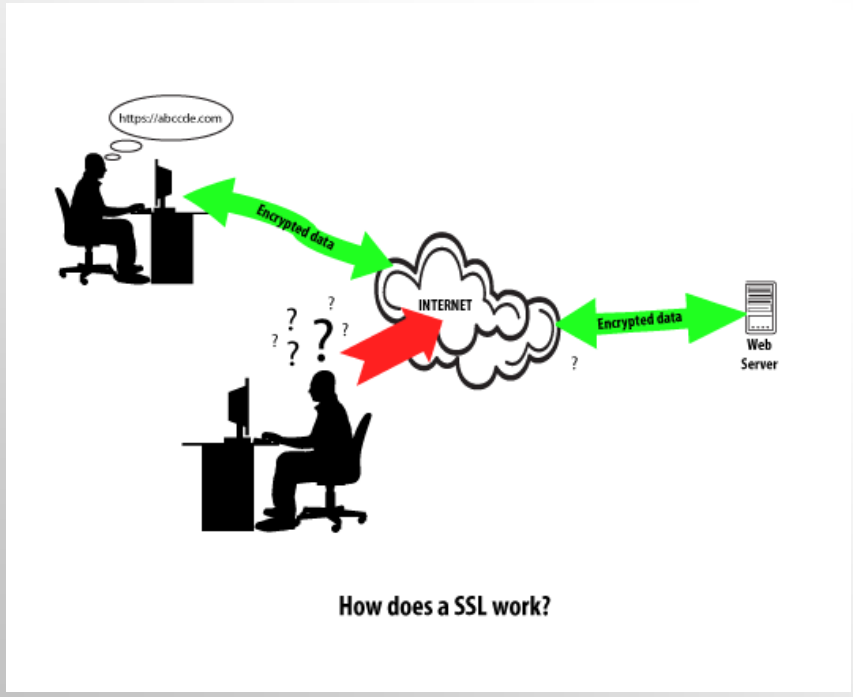


[Fig. Ref. www.kryptocake.com]

GEORGE MASON UNIVERSITY

Why SSL?

- Establishes an encrypted connection between a web server and a web browser
- Confidentiality
- Integrity



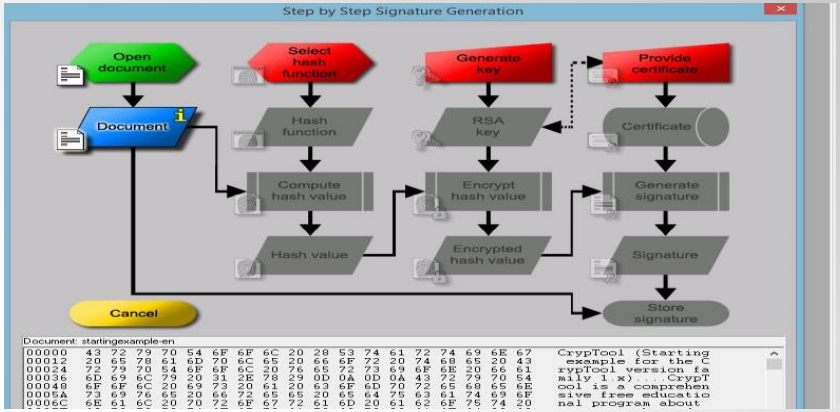
GEORGE MASON UNIVERSITY

Different perspective

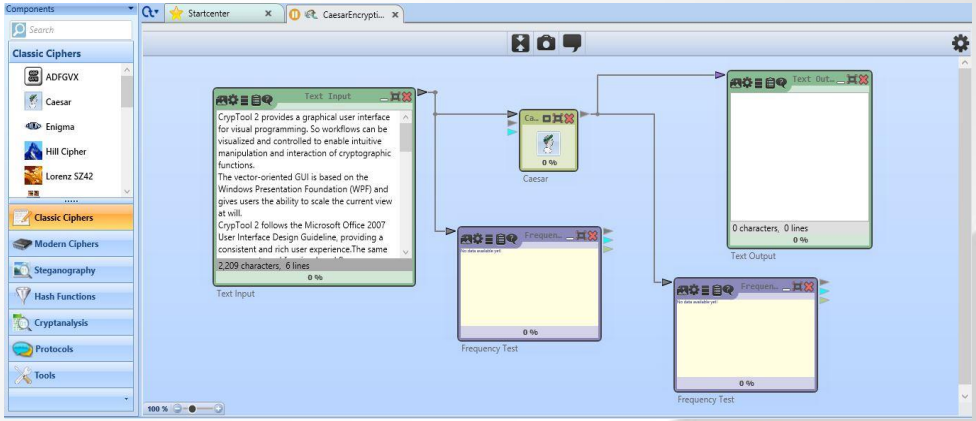
- Studied SSL theoretically but PRACTICAL understanding???

CrypTool

- CrypTool 1:
  - Free open-source program for cryptography and cryptanalysis
  - Written in C++



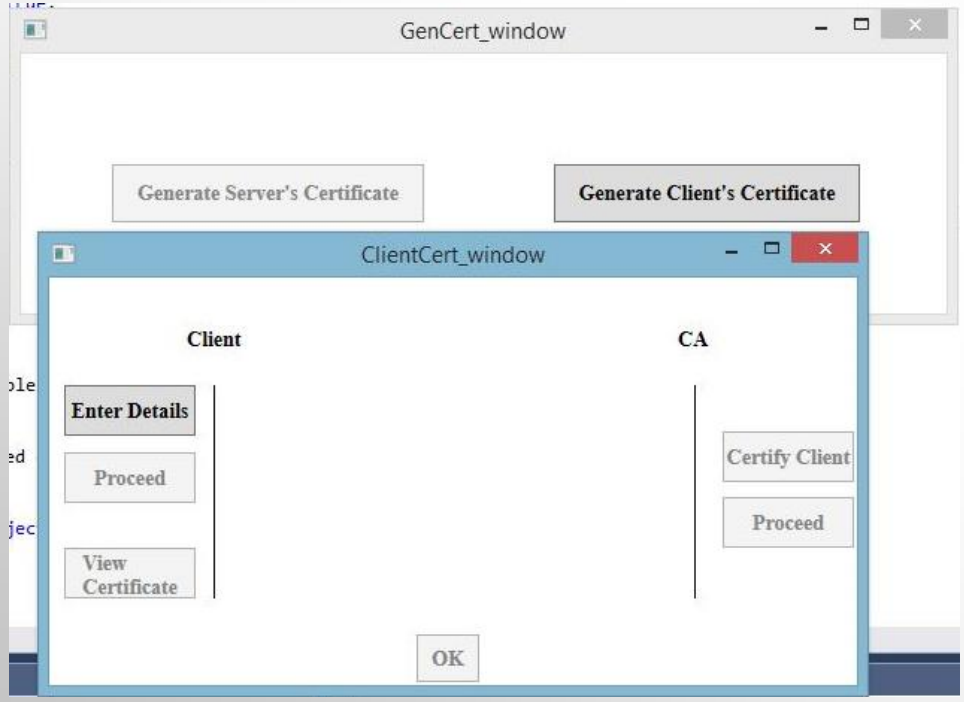
- CrypTool 2:
  - Subsequent version of CrypTool 1, developed in C#
  - Provides graphical user interface for visual programming
  - Vector-oriented GUI based on WPF



GEORGE MASON UNIVERSITY

Our Implementation

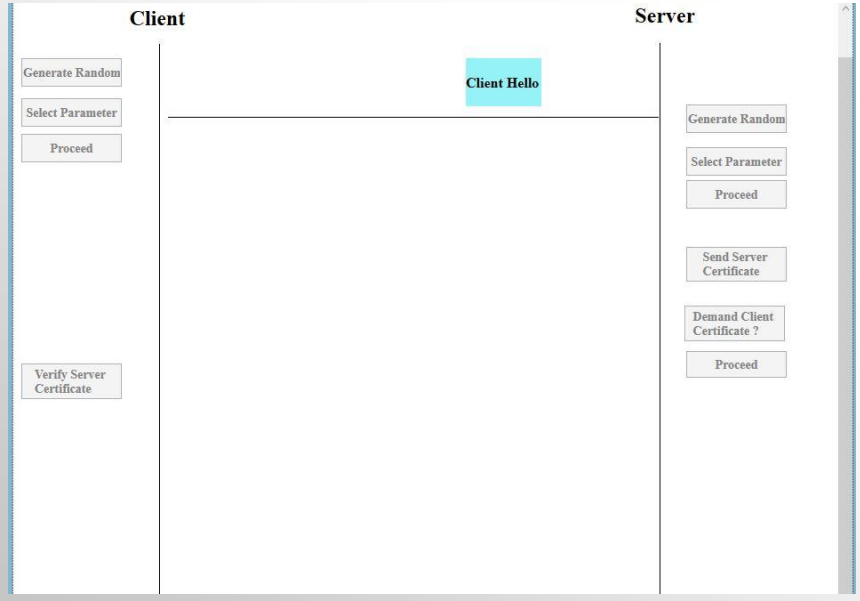
- Simulation of SSL protocol
- Visualization of its working
- Supported algorithms such as RSA, (AES, DES), (MD5, SHA-1)

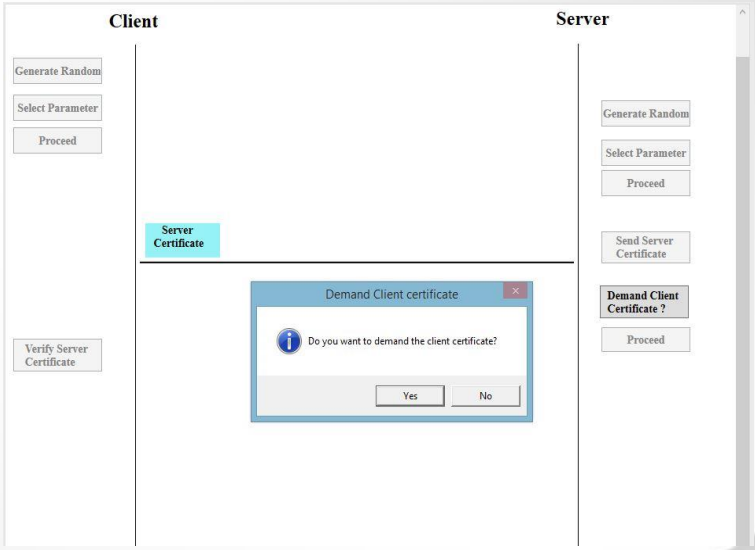


GEORGE MASON UNIVERSITY

Methodology

- Developed in C# (.NET Framework 4.0) using WPF (Windows Presentation Foundation)
- Used Cryptographic Libraries for algorithms and integrated into our implementation





GEORGE MASON UNIVERSITY

Windows Presentation Foundation

- A graphical subsystem that renders user interfaces in windows-based applications
- It’s a presentation system for building windows client applications with visual experience
- Employs XAML, an XML-based language to define various interface elements

Demonstration!!

GEORGE MASON UNIVERSITY

Limitations and Conclusions

- Limitations:
  - Could not directly develop into CrypTool 2 because of code complexity and time constraints

- Conclusions:
  - Successful implementation of Handshake
  - Better understanding through Simulation

GEORGE MASON UNIVERSITY

Future Work

- Implementing full suites of SSL/TLS and incorporating SSL/TLS libraries such as OpenSSL in the implementation
- Integrating the developed program in CrypTool 2
- Laboratory Exercises

GEORGE MASON UNIVERSITY

Questions

GEORGE MASON UNIVERSITY