

# Assignment 4: Student Research

Course 1-02-328: Communication and E-Commerce Security

Due 18 June 2011

## 1 Introduction

Your job in this assignment is to research an e-commerce or communication security topic on your own and prepare a short report on it. The goal of the assignment is for you to acquire some knowledge of your own on a topic that we didn't explain fully in the class. It is best if you choose a topic which is of interest to your interests or your work so that your research will be more meaningful.

## 2 Topics to Choose

You must choose a tool, protocol, or system which is related strongly to e-commerce or communication security. Several standard network protocols meet this requirement, but there are many others that you may choose from. Here is a list of potential topics that you may choose from:

1. Pretty Good Privacy (PGP)
2. Shibboleth
3. Wired Equivalent Privacy (WEP)
4. Wi-fi Protected Access (WPA)
5. Security Assertion Markup Language (SAML)
6. Domain Name System Security Extensions (DNSSEC)
7. Internet Protocol Security (IPsec)
8. Society for Worldwide Interbank Financial Telecommunication (SWIFT) communication system
9. Secure/Multipurpose Internet Mail Extensions (S/MIME)
10. Payment Card Industry Data Security Standard (PCI DSS)
11. Secure Electronic Transaction (SET)

## 3 What to do

**You must send an email to [mjmay@kinneret](mailto:mjmay@kinneret) with your topic.** I will allow only one group to work on each topic, so the first person to send me a message requesting a topic gets it. I will not accept oral requests - only ones submitted via email.

Your report must be at least **1600 words** (not including title, student names and summaries, and bibliography) and include information about the following aspects of the tool, protocol, or system:

- History and background of the tool, protocol, system
- Explanation of the problem the tool, protocol, or system is meant to solve
- Definition and explanation of the essential aspects of the tool, protocol, system
- Discussion of the security properties of the system: what attacks it is meant to prevent, what attacks (if any) have been successful against it

## 4 What to turn in by 18 June 2011 at 11:59:59pm

As noted in the syllabus, you may work in groups of up to 3 (three) students.

Your report must include the information about as well as the following information:

1. The names of the students in your group. In addition to the items specified below, include a one- or two-sentence description of each group members contributions to the project and an estimate of the number of hours each member contributed.
  - Your group will receive a **single grade** for the work. The information about individual contributions will be used to help gauge the *difficulty and effectiveness* of the assignment.
2. A list of all the sources which you used to write the report, including links or references to books

Each group should turn in the report in a single file. Electronic submissions should be uploaded to the Telem website, transferred to me by USB disk on key, or sent via email to the course email ([ise328@gmail](mailto:ise328@gmail.com)) in a single ZIP or RAR file. Please send your report in DOC, DOCX, HTML, or PDF.

### 4.1 Grading Criteria

I will grade your work based on the following criteria out of 100 points:

- Depth of history and background section. 10%
- Depth and clarity of explanation of the problem. 20%
- Depth and clarity of the technical description. 40%
- Depth and clarity of the discussion of the security properties. 30%

### 4.2 Sources and Copying

You may use books or online materials to help with your research, but you may not copy from any book, online resource, magazine, website, encyclopedia (including Wikipedia), or any other source without attribution. Copying includes direct copying of language or writing from another source as well as copying with minor, insignificant modification of the text.

You may copy images or code from outside sources so long as the image is properly annotated and the source listed alongside.

If you have any questions or uncertainties, it is your responsibility to clarify the issue with me before you submit your work.