CSci 4554 Final paper

Topic notifications are due Friday April 21st. Presentations are May 1, 3 in class; preliminary version is due Sunday April 30, final version due Friday May 5 at 11:59pm.

You may work in pairs or individually on this assignment.
For this problem set you are asked to research the use of cryptographic algorithms in real-life applications (for instance, HTTPS, SSH, electronic voting implementation, etc.). You may discuss specific security flaws that have since been fixed. You may also just go more in-depth into some topics that we have covered. Specifically, you should focus on:

- What algorithms are used in the application? Please relate them to the algorithms that we studied in class. For instance, if the application uses digital signatures, what kinds of signature implementations and algorithms are acceptable for this protocol (DSS, ElGamal, etc.)? If it uses key agreement, what protocols and algorithms are used (Diffie-Hellman, etc?)?

- How commonly is the application used? For instance, some secure versions of applications may be recommended or even mandated, but not commonly used, and less secure versions are used.

- What can you say about security of the application, based on the above? If there was a security fix, what was it and how effective was it?

You may also discuss legal issues related to these applications if they mandate, restrict, or regulate certain algorithms or uses. For instance, if digital signatures are accepted as legally binding signatures, what conditions are mandated and why?
Requirements:

- You need to submit an (at least) 2-3 page paper on the subject (4 pages for a group of two). The paper must introduce the topic and address all of the necessary aspects: it's not the length of the paper that matters, but the depth of the topic coverage. Don't forget a title and a bibliography (web references OK). The paper must be well-organized, well-written, and grammatically correct.

- The purpose of the application and the services it provides need to be explained. You may choose to focus on only one aspect of the application. For instance, if it provides both data integrity and encryption, you may cover only one of the two in detail.

- The work of the application should be described in detail (the algorithms used by each of the participants, in which order they are used, how are the keys determined, etc.). You may refer to algorithms and protocols covered in class without going into details.

- Give a brief history of the application.

- Make sure to justify your claims about the security of the application by the known properties of the algorithms used. It is also OK to refer to articles on security of the application, but you need to give the summary of the argument in your own words.
- You need to prepare a 5-10 minutes presentation to summarize your findings; be prepared to answer questions.

Some topic suggestions (feel free to choose your own):

- "Web of trust" systems, such as PGP and GnuPG.
- Public key infrastructure (PKI).
- LDAP (Lightweight Directory Access Protocol) authentication.
- X.509 or X.500 authentication.
- Random number generators used in practice.
- Hash functions used in practice or proposed (other than the ones we have covered in class in detail).

These are just suggestions, you may consider very different applications, as long as you you satisfy the key points of the requirements.

Please enter your topic in the google form that I send to you so that there is no duplication. **Important:** the topics have to be chosen by Friday April 21st at midnight. I will approve your topic or make a suggestion for a modification.

Final papers should be shared with me (and your group) on google docs. I will post papers on the course page (unless you would rather not have it posted). Thus make sure your name appears on the paper as you would like it listed in the public domain.

Extra credit. For extra credit on this assignment you may do one of the following:

- Implementation of a protocol or an algorithm: an actual code example that demonstrates how the algorithm works or shows a working attack on the algorithm. Statistical analysis of random number generators or hash functions works as well. Come up with something similar to the lab in approaches and the level of difficulty. I would be happy to discuss your ideas with you.
- Use a recent peer-refereed paper in ACM digital library as one of your primary sources.
- Do a detailed comparison of two different approaches to the same problem.