Projects for Foundations of Security in BiSS

Joshua D. Guttman
Worcester Polytechnic Institute and
The MITRE Corporation
guttman@wpi.edu

April 14, 2013

To receive credit for the short course on Foundations of Security given at BiSS the week of 4 March, you should choose one of the following three types of projects. Please complete it, sending me your materials at the email address above before *8 July 2013*.

There are three possible types of project. One uses CPSA for analysis; another consists of a comparison between two papers; the last is to prove or refute a variant of a result.

Do any one of the three for full credit. Do two if you can; that will consolidate many aspects of the course and build a deep understanding.

You may check with me by email whenever needed. I will reply promptly, especially if you can ask sharply focused questions. In fact, in the second project, you will need to communicate with me about the pair of papers you propose to compare.

1. Using CPSA for protocol analysis. The paper "Prudent Engineering Practice for Cryptographic Protocols," by Martìn Abadi and Roger Needham, is available at URL `http://web.cs.wpi.edu/~cs564/f12/papers/AbadiNeedham.pdf`. It has very insightful advice, supported by a lot of examples.

Read the paper.

In this exercise, you will focus on the examples. You will select six examples from the paper. You will code each example within CPSA. In each case, you want to:

1. **Demonstrate the problem** that the paper describes. To do so, you must code the protocol actions in the CPSA notation. Then you

must construct a query (a "defskeleton" form) containing one or more assumed strands, as well as assumptions about which parameters are uniquely originating and which keys are non-originating.

CPSA will then compute all of the minimal, essentially different skeletons that are compatible with that starting point.

You will include the CPSA outputs in the ⟨*protocol*⟩`_shapes.xhtml` format. You will also write a short summary of what the CPSA result tells you. Does this agree with the Abadi-Needham criticism?

2. **Check their solution.** Modify the previous analysis to reflect the fix proposed by Abadi-Needham. Include the ⟨*protocol′*⟩`_shapes.xhtml` file. Inspect it to determine whether the Abadi-Needham solution really resolves the problem. Write a short summary of your conclusion.

   There's at least one example in that paper where I believe their solution doesn't work.

Do this process for six examples. There are a few of their examples that focus on issues that don't lend themselves to a CPSA analysis. Avoid any examples that don't seem to fit within CPSA.

2. Comparing two papers. You can choose any one of the papers referenced in the syllabus at URL `http://web.cs.wpi.edu/~guttman/biss/`, i.e. any of the non-slide PDFs. For each candidate you think you might be interested in, look it up in Google Scholar to see other papers that cite it, and also look through the references in the paper.

You would like to find another paper on a closely related problem, but with a very different approach.

When you have a pair of papers that you think would make an interesting contrast, please send me email stating which pair you are proposing. Please tell me (in a couple of sentences) what the overall topic seems to be; why you are interested in this; and why the two papers seem to have an interesting contrast.

I may suggest alternatives to one or both of the papers.

When the papers are agreed, you will write a report of 5 to 10 pages discussing the following questions:

Core problem What is the main problem that both of the papers consider? Why is it practically important? Why is it theoretically interesting?

Paper summaries For each of the two papers, discuss what are the main results (and more broadly, the main contributions) of each of the two papers. What methods does each use? What weaknesses or limitations do the papers have?

In this part, discuss each paper separately.

Paper contrasts What differences do the papers have? Contrast the main results of each. Which is more informative, or more widely applicable? Does one paper's method seem more extensible or reusable than the others? More rigorous? Are the adversary models comparable?

Remaining problems Conclude by summarizing what problems raised by the papers remain open, and what the prospects for solving them seem to be.

3. Prove or refute. Read my paper (with Thayer) on Protocol Independence via Disjoint Encryption, available at URL `http://web.cs.wpi.edu/~guttman/pubs/disjoint.pdf`. In the message algebra there, the key used for an encryption is always an atomic value. Of course, in real protocols, keys are sometimes derived by putting together several ingredients, normally using hashing or encryption to generate a new key.

Claim The main results of the paper are still valid even when encryption keys are generated from complex values.

Either prove this claim by extending the methods of the paper to this wider class of cases, or else refute it by giving examples of protocols that use compound keys and do not satisfy the main results.