University of Arizona, Department of Computer Science

CSc 620 — Assignment 2 — 20%

Christian Collberg
August 28, 2008

1 Introduction

In this assignment you will read a section of the book and all the papers it is based on and prepare a 25-minute presentation to the class.

This assignment is worth 20% of your final grade. To get a good grade you need to

1. demonstrate that you've understood the material,
2. prepare a nice set of slides (using the beamer.sty LaTeX package), and
3. give a well organized, well-timed, well-rehearsed class presentation.

The presentation should be 20 minutes long plus 5 minutes for questions.

Everybody in the class is responsible for reading the material prior to the lecture and prepare reasonable questions.

The slides are due 6pm the evening before your presentation. Email them to me in LaTeX source code form.

2 The topics

Table 1 lists the topics assigned to each student. You should not only read the material in the book but all the relevant papers the section references. If there exists attacks against the algorithm you're presenting, you're expected to talk about those also.

3 OK, what should I do???

1. Read the section in the book.
2. Read the relevant papers.
3. Iterate from 1 until you understand.
4. Ask me to give you any software I may have that you can play with and which may help your understanding.
5. Ask me to give you any figures and code examples from the book that you may want to reuse in your slides.

#	section	description	student	lecture	date
1	3.3.4,3.3.5	Branch functions (including attacks)	anandp	18:1	Thu Oct 23
2	3.6.3	Destroying high-level structures	robackja	18:2	Thu Oct 23
3	6.2.3	Dynamic code merging	tpatki	18:3	Thu Oct 23
4	7.4.1,7.4.2	Oblivious hash functions	marshall	17:1	Tue Oct 21
5	7.5.3	Verification by timing	sushanth	17:2	Tue Oct 21
6	7.5.5	The Skype obfuscated protocol	mbi	17:3	Tue Oct 21
7	8.7.2	Watermarks in CFGs	kpcoogan	23:1	Thu Nov 13
8	9.2	Exploiting parallelism	qingju	23:2	Thu Nov 13
9	9.3	Expanding executions paths	jamyers	23:3	Thu Nov 13
10	11.2	Authenticated boot using a trusted platform module	ghigliom	20:1	Thu Oct 30
11	11.3	Encrypted execution	bhandari	20:2	Thu Oct 30
12	11.4	Attacks on tamperproof devices	ricarlos	20:3	Thu Oct 30

Table 1: Topic assignment

6. Get the LaTeX slides template from the website.
7. Learn LaTeX if you don't already know it.
8. Prepare your presentation. Try to tie it into other material we've talked about in class. Summarize your own impressions of the algorithm. How easy is it to attack? What's its overhead? How hard would it be to implement?
9. A week before your presentation come and see me and show me what slides you have.
10. You're of course welcome to come and talk to me about the material at any time!
11. A 20-minute talk can have no more than 20 slides.
12. Rehearse, rehearse, rehearse!