Secure electronic commerce (inte1070 1071) 2012s1

Secure Electronic Commerce (INTE1070/1071) — 2012s1 Assignment 2 Objective To explore the latest security related development in electronic commerce. Instruction - - This assignment is group based with a maximum of 3 members in a group. There are two tasks which are preferred in the same topic: Part I: Report (20 marks) Part II: Programming (15 marks) Option 1: Design a set of small client-server programs implementing a certificate scheme. Option 2: Design and Implement your own security algorithm (with extra 3 marks bonus). Submission details - - - - - Due date: Midnight Sunday (week 12), i. e., 23: 59 sharp, 27 May 2012. The assignment is submitted via Weblearn. Report must be submitted in HTML or PDF format. Programming languages HTML, JavaScript and PHP are preferred. Each submission must include the file readme. txt in the following format: StudentID: [your Student ID - without the initial " S"] Login: [your CS username] Name: [your full name] Partner Name: [your team member’s name] Partner ID: [your team member’s Student ID] Topic: [your report topic] Notes: [any other relevant information] - The name of the file must be lowercase readme. txt and the character set used must be viewable from a text viewer like VIM or VI. Note that - - - - - Each group will demonstrate (main work using ppt & programming) on weeks 11&12. Groups demonstrate on week 11 get 2 marks bonus. A penalty of 10% per day of the total marks applies for each day if submission is late. Submissions received more than five days late will receive zero marks. All work will be checked for plagiarism and incorrect referencing, and it is your responsibility to adhere to the School guidelines. See: http://www. cs. rmit. edu. au/students/integrity/ Specification: Provide a report on the security related event of electronic commerce. The minimum length is 2500 words (figure&reference are not counted). At least 10

publications on books, referred academic journals or conferences are cited. And at least 5 of them are in or later 2008. The report should take the format of IEEE. You can find the publications from Google Search and IEEE Academic Publications Database via RMIT Library. For option 1 in part II, the report should comprise: o Introduction. o Background and related work. Information needed on a certificate? Why each part is needed? Why is it important to have a revocation list? How does this work in real life implementations? Is it possible for you to manage revocation centrally? Why? What happens if someone’s private key is compromised? Is there a way to manage this theoretically? Describe how. o Experimental results (your programming part fits here). Describe and implement the certificate (should be designed from sketch). What programming language you used. You can look at OpenSSL, as most of the options can be done by it. X. 509 file formatting is not required. You should use your own simplified format — as long as you can read back what you wrote, and it is ‘ printable’. o Conclusion and future work. Note that: Use external library, e. g. java. security. cert which can generate certificate automatically, is not allowed. For option 2 in part II, choose one main reference and investigate its security related algorithms carefully. Then the report should comprise: o Introduction. o Background and related work. What is the issue investigated in the reference. What is the security problem? How the problem being solved. o Proposed algorithm. Design your own algorithm to improve on what is presented in the reference. o Experimental results (your programming part fits here). Use examples to illustrate why and how your scheme works effectively in terms of security. Security analysis. Compare your proposed algorithm with that shown in the reference. o Conclusion and future work. Suggested areas: o Secure mobile

payment process o Ubiquitous healthcare data protection o Privacy in mobile government o Security and privacy in cyber physical systems Marking guide for option 1: Part I Report (20 marks) o Report and programming are in the same topic o What is the PKI, security certificate, revocation o How it delivers security requirements (SSL, CAs) o Programming summary o Your summary and future work o Reference and format 2 marks 4 marks 4 marks 3 marks 3 marks 4 marks Part II Programming (15 marks) o Users can create their own certificate 3 marks o Read/display the contents of a certificate 2 marks o Only certificate owner manages the keys 3 marks o Certificate manager: Certifying Authority signs a certificate and sends it back to the client. This incorporates some way of managing CAs as well (ie. a central CA list somewhere, how long are certificates valid for) 4 marks o Client can display the certificate and its content to ANY user. 3 Marks Marking guide for option 2: Part I Report (20 marks) o Report and programming are in the same topic o What is the state-of-the-art in the related area o How existing research publications address the vulnerability o How your propose to improve on the security o Programming summary o Your summary and future work o Reference and format Part II Programming (15 marks+ 3 marks bonus) o Implement the algorithm in the main reference o Use examples to illustrate why/how your scheme works o Compare the results: your vs. algorithms in reference The possible improvement to consider: o Have both sides contribute to the session key o Bundle mobile, SIM card information with PIN for authentication Note that: Option 2 is prepared for potential research. Students have the knowledge of research methods are suggested to choose Option 2. You can further explore security component in the area you have investigated. The maximum possible mark is 40: o Basic report o Basic

programming o Choose to Design and Implement your own security algorithm o Demonstration on week 11 2 marks 2 marks 3 marks 3 marks 3 marks 3 marks 4 marks 5 marks 8 marks 5 marks 20 marks 15 marks 3 marks 2 marks