Quiz #2: July 29th, 2004

1. This quiz is due in class on Tuesday August 3rd at 6pm.
2. Late quizzes will not be accepted, and will count as a zero towards your grade. There will be ***no exceptions***. Therefore, you should start your quiz early.
3. If you cannot make class on August 3rd, you can email your quiz in advance of class. It is recommended that you email your quiz well in advance of class and that you confirm receipt of the quiz by your instructor, as late quizzes will not be accepted—even if the quiz is late because of circumstances beyond your control.
4. There is no collaboration allowed on this quiz. Do not discuss any aspect of this quiz with anyone until Tuesday, August 3rd, at 6pm.
5. Questions on the quiz may be sent by email to simsong@acm.org. Questions will be answered within 24 hours. In order to ensure fairness, questions will not be answered after Monday, August 2nd, at 6pm Eastern Time.
6. This quiz is open-book, open-notes. Calculators and programmable devices (including laptop computers) *are permitted*.
7. In fact, it is expected that you will *type your answers to this quiz*. *Handwritten quizzes will not be accepted.*
8. It is recommended that you download the Microsoft Word file for this quiz and use it as your template.
9. You will be graded not only on the correctness of your answer, but also on the clarity with which you express it. Unjustified answers will receive no or only partial credit, at the instructor's sole discretion. Partial credit will be given.
10. In all cases below, when you are asked to describe a technique, full credit will be given for using techniques that were discussed in class. Using techniques that were not discussed in class may result in partial or no credit being given.
11. This quiz has 100 points and 2 points of extra credit.

Good luck.

Part 1 Short Answer [200 words each]

1.1 Cipher Suites [5 points]

PGP version 1.0 encrypted files with the BassOmatic encryption algorithm and encrypted BassOmatic session keys with RSA. PGP version 2.0 switched to the IDEA encryption algorithm. Higher versions of PGP allow the selection of a variety of different encryption algorithms, implementing what is called a *cipher suite*.

Explain what a cipher suite is and why using a cipher suite is advantageous.

1.2 Hacking the Prox Card [5 points]

In October 2003 Jonathan Westhues at the University of Waterloo built a device that could clone RFID-based entry systems made by several vendors. The system works by stimulating a proximity card with an RF signal and recording the results. To simulate the presence of the proximity card the signal is simply played into a reader. Essentially, Westhues built a device that is similar to an audio tape recorder, except Westhues' device records RF. A detailed explanation of the project can be found at http://cryolite.ath.cx/perl/skin/prox.

Explain why the proximity cards that Westhues studied are vulnerable to his "tape recorder" attack. Describe engineering changes that could be made to the proximity cards, the readers, and the over-the-air protocol used by proximity cards to make them secure against this kind attack.

Part 2 Experiences Running a Web Anonymising Service

Carefully read "Experiences Running a Web Anonymising Service" by Golembiewski, Hansen and Steinbrecher. You can download this paper from http://www.inf.tu-dresden.de/~ss64/Papers/DEXA-Misuse.pdf. The paper is mirrored at http://www.simson.net/csg256/handouts/DEXA-Misuse.pdf. This paper was originally presented at the 14th International Workshop on Database and Expert Systems Applications (DEXA'03).

2.1 In section #2, the authors state that the data collected in their survey cannot be treated as representative. Why do they make this assertion? How could the survey be designed so that the data would be representative? [5 points]

2.2 In section #2, the authors state that AN.ON does not support anonymous e-mail accounts or support P2P file exchange to minimize misuse potential. Describe two techniques through which the AN.ON system could be used for anonymous e-mail or P2P file exchanges. [10 points]

2.3 In Section #3, the authors state that users are protected from corrupt mix providers because every provider has signed a commitment not to store any information about users, and AN.ON is based on Open Source Software. Unfortunately, the architecture presented does not allow users to verify that a mix provider is actually using the Open

Source Software that is available for inspection. Describe a technique that would allow users of the AN.ON service to verify that the software being used by a mix provider is actually the software that AN.ON provided. [10 points]

2.4 The authors assert in Section #2 that the main motivation of AN.ON users is to guard against profile building of surfing behavior. As described, AN.ON cannot provide this protection. Explain why, giving details of an attack that would work against AN.ON users. [5 points].

2.5 Describe what modifications would be required to AN.ON to produce the privacy assurances promised in section #2. [5 points]

Part 3 Client-side defense against web-based identity theft

Carefully read "Client-side defense against web-based identity theft" by Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh and John C. Mitchell. You can find this paper online at http://crypto.stanford.edu/SpoofGuard/webspoof.pdf/ .

3.1 At the bottom of the first column on page 2, the authors discuss "previous efforts by the Princeton Secure Internet Programming group and others [FBDW97, EY01]." The technique described in this paragraph are described as a kind of attack. In class we discussed a commercial website that uses the same approach described in [FBDW97] and [EY01]. Name that website and describe the reason that this approach is used. [5 points]

3.2 Unlike AdSubtract, which is implemented as a client-side Java proxy, SpoofGuard is implemented as an Internet Explorer Helper Object. Give an advantage and a disadvantage of each implementation strategy [4 points].

3.3 Explain three features of SpoofGuard that would be difficult if not impossible to implmenet if SpoofGuard were a client-side Java proxy. [6 points]

3.4 Why does SpoofGuard store the SHA-1 hash of passwords, instead of storing the password itself? [2 points]

3.5 Does SpoofGuard's storage of passwords as SHA-1 hashes make sense? Give two techniques that a piece of spyware running on the user's computer could use to circumvent SpoofGuard's protection. [3 points]

3.6 In Section 5.1 the authors note "Since most spoof web sites do not use https, our server used ordinary insecure [sic] http." What is not secure about http when compared with https? List 3 things. [6 points]

3.7 In section 5.3, the authors note that a simple way to disable SpoofGuard's image checks is by slicing the image and delivering two vertical slices. Suggest two other ways to defeat SpoofGuard's image checks [4 points].

3.8 Evaluate the "CONFIDENTIALITY" proposal in section 6.1. Do you think that it could work? Why or why not? [100 words] [5 points]

Part 4 Design Project [20 points]

At the top of page 3 of "Client-side defense against web-based identity theft," the authors describe a problem faced by many websites today: frequently a single username/password combination is used at multiple websites. As a result, one way to capture username/password combinations is to simply create a website that invites visitors to register. As visitors register, the website can attempt to use username/password combinations presented at the attack websites on other websites, such as E*Trade and Fidelity.com.

The authors suggest adding a new "Salt" tag to HTML in an attempt to solve this problem. Unfortunately, as the authors note, implementing this new tag would require upgrading all websites and all browsers simultaneously --- almost certainly an infeasible project.

Design and describe a better approach for counteracting the problem of web visitors selecting the same usernames and passwords at multiple websites. Describe how your approach would be implemented and deployed in 1000 words or less.

Your project will be graded on its likely effectiveness, ease-of-use, and ease-of-implementation.

Part 5 Extra Credit

5.1 Why did I put "[sic]" in the quote in section 3.6 above? [2 points]