Solution Set for CPSC 156 Exam 2
April 26, 2007

Question 1

(a) Users have the freedom to

1. run the software for any purpose
2. study how the program works and adapt it to their needs
3. redistribute copies of the program
4. improve the program and release improvements to the public

(b) If the licensee (*i.e.*, the person who acquired the program that's governed by the GPL) wants to redistribute copies of the program, he must grant those he distributes it to the same rights that he was granted.

(c) Correct answers include but are not limited to

1. support contracts
2. building customized versions of open-source programs
3. documentation and training
4. packaging and installation
5. partnerships with hardware manufacturers

Question 2

(a) See slides 13 and 14 from the April 5, 2007 Lectures Notes.

(b) Suppose to the contrary that, every time Alice signed a digital document M using her secret signing key, the same signature string σ_A was produced. Anyone to whom Alice gave a signed document (M, σ_A) could remove the string σ_A, append it to another document M', and claim that Alice had produced the signed document (M', σ_A). Note that this problem does not arise when dealing with paper documents: One cannot just tear off the signature and attach it to another piece of paper without the tampering's being apparent.

(c) Encryption protects data while they are in transit or in storage. In general, however, data are decrypted *by authorized users* before they undergo any nontrivial processing. Once the cleartext data are obtained for a legitimate purpose, there is no straightforward way to prevent their being used for an illegitimate purpose.

Question 3

(a) CAPTCHA stands for "Completely Automated Public Turing test for telling Computers and Humans Apart." To pass a CAPTCHA, a person must successfully perform a task that is easy for humans but hard for computers, *e.g.*, identifying words or finding objects in pictures. Currently, some email-service providers require people to pass CAPTCHAs in order to sign up for free email accounts.

(b) Before executing remote code that is invoked by a command in a webpage, browsers can check for a valid signature of the code publisher. If it cannot verify a valid signature by a trusted publisher, the browser can ask the user for explicit permission before executing the code. (Here, “remote code” is code that is not resident on the user’s local machine on which the browser is running.)

(c) False. WORD documents can contain executable code (such as macros). For example, the Melissa virus was a WORD-macro virus.

(d) True. See slides 28 and 29 from the April 3, 2007 Lecture Notes.

Question 4

(a) “Public records” contain facts about people, property, and organizations that are deemed to be of interest to the general public; they are, by definition, “open to inspection by any person.” Depending on State and Federal law, they can include: Birth, death, marriage, and divorce records; court documents and arrest warrants (including those of people who were acquitted); property ownership and tax-compliance records; driver’s license information; and occupational certification. Traditionally, these records were legally public but “practically obscure,” because they were stored in physical form on hard-to-search media; thus, one had to spend time, effort, or money to access them, and only highly motivated people did so. Now that many of these records are stored on public web pages in standard, searchable formats, almost no investment is required to access them, and people may do so for questionable reasons (such as blackmail or prurient curiosity). This is the source of the disruption.

(b) By demonstrating possession of knowledge (*e.g.*, a secret password), artifacts (*e.g.*, a uniform), or skills (*e.g.*, the ability to swim), a person proves that he is a member of a certain group and should be treated in a certain way. The demonstration need not involve revealing the person’s name or address, but it can if revealing this information is appropriate. This type of identification is relevant to Internet-based interaction (and, more generally, to interaction in very large, geographically distributed systems), because it provides a way to control access to valuable resources without necessarily requiring very large numbers of people to reveal personally identifying, sensitive information.

(c) Type 3: identification by unique alphabetic, numerical, or other symbols that can be linked back to a person under restricted conditions. The certificate itself is the unique string of symbols, and the CA can link this string back to Alice if presented with a compelling reason to do so.

Question 5

(a) In Solove’s words, “Under the *secrecy paradigm*, privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data [are] revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information.” Because computers and networks are increasingly prevalent, more and more ordinary, daily activity involves the capture and storage of sensitive, personal information. Thus, there is less and less sensitive information (if any) that is “completely secret,” and yet it seems intuitively clear that uncontrolled collection or dissemination of such information constitutes a privacy violation.

(b) “Increased accessibility” occurs when information that is already, in principle, available to the public is made easier to access. If this information is sensitive, then increased accessibility can lead to increased risk of a diverse set of privacy violations, including disclosure. A difference in quantity (of access to information) becomes a difference in quality. This is precisely the phenomenon that we addressed in our discussion of Internet access to public records.

(c) Intrusion. (See page 550 of Solove’s article “A Taxonomy of Privacy.”)

Question 6

(a) Information provided to or by a website should not be directly available to another website unless the user explicitly provides it.

(b) Cryptographic hash function.

(c) Correct answers include but are not limited to (1) suspicious-looking URLs and (2) non-HTTPS URLs.

(d) Correct answers include but are not limited to (1) users don't read carefully, and (2) users don't understand the indications they are given.