# Answer Key for Exams 2 in CPSC 457/557 (2013)

All presentations referred to in this answer key can be found on the course website: `http://zoo.cs.yale.edu/classes/cs457/fall13/`.

Answer 1:
a) A Tor "hidden service" is one that hides its location. Using "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity. Natural applications include censorship-resistant publishing and e-commerce in contraband goods.
b) See slide #10 of Sean Haufler's presentation on Oct. 17, 2013.

Answer 2:
Slide numbers in this answer refer to the slide deck used by Ariel Ekblaw and Alex Noonan in their Oct. 29, 2013 presentation.
a) See slide #10.
b) See slide #5.
c) False. (No explanation was needed for full credit, but note that this statement is false, because users must opt in before their personal information is shared with other companies. See slide #4.)
d) For its Street View service, Google sent vehicles into residential neighborhoods to take photographs. Without notice to or consent of the residents, these vehicles captured unencrypted data (both location and payload data) that was transmitted over these residents' WiFi networks; although Google claimed that this "wardriving" code that captured WiFi data was experimental and included by accident, there were references to it in Street View engineer Marius Milner's design document, along with predictions that people would object to it. The incident illustrates very clearly that, in a big company that encourages engineers to innovate and that regularly rolls out new services, it is extremely difficult to prevent *all* misuses of personal information *even if upper management intends to do so*. There is just too much going on, and not all of it will come to the attention of upper management or the legal department.

Answer 3:
a) False. A DN must be unique within a particular CA's domain, but the same DN can be used with multiple CAs. In particular, an individual or a company could obtain certificates from multiple CAs and use his or its "real name" as the DN in all of them.
b) False. A person could, for example, obtain a certificate from Verisign using his real name, *e.g.*, John Smith, as the DN and obtain another certificate from his employer's CA using his job title, *e.g., Vice President*, as the DN.
c) True.
d) False.
No justification was needed for full credit on parts c or d, but you can find more information

about these issues on page 7 of required reading assignment
`http://www.blackhat.com/presentations/bh-usa-99/EdGerck/certover.pdf`.

Answer 4:
Slide numbers in this answer refer to the slide deck used by Aayush Upadhyay and Naicheng Wangyu in their Nov. 14, 2013 presentation.
a) Lack of physical bank branches, lack of capital, and prevalence of low-value transactions. See slide #3. Credit was given for conditions found on Slides #6-8 as well.
b) Correct answers include: (1) In some countries in which there is considerable potential demand for M-payment systems, *e.g.*, India, the government has prohibited strong encryption; see slide #12 of Upadhyay-Wangyu. (2) As explained in Section 5 of the assigned article by Michael Paik (`http://www.cs.nyu.edu/~mpaik/pubs/stragglers.pdf`), many of these M-payments are taking place on 2G GSM systems. These are outdated systems, and the technical community is not very interested in securing and improving them at this point. In poor countries such as Kenya and Uganda, however, there is a big installed base of 2G GSM, and many users cannot afford to replace their phones soon.
c) See slides #13 and 14.

Answer 5:
a) Using automata-based pattern-recognition and other nontrivial algorithmic techniques, DPI engines permit network operators to identify (and sometimes alter) packets of interest in real time. Firewalls are also used to identify packets of interest, but they are less powerful. Notably, DPI engines inspect the payload of packets as well as the headers fields, but firewalls generally don't.
b) Potentially beneficial uses include identification and blocking of malware, network-address translation, quality-of-service management, and statistical analysis of traffic flows. More controversial uses include blocking of popular but controversial protocols such as Tor, censorship, draconian copyright enforcement, and government surveillance.

Answer 6:
See slide #1 of Jeremie Koenig's presentation on Nov. 21, 2013.

Answer 7:

a) False

b) True

c) True

d) False