CS6600 Homework 1

Matthew Whitesides

I. Chapter 1 Problems

1) a) Confidentiality and Integrity, Mary did not conceal her information correctly, and John does not have an authorized claim to the data.
   b) Availability, the system is no longer usable.
   c) Integrity, the check amount data has been improperly changed.
   d) Integrity, the authorized source of the data, is no longer valid.
   e) Availability and Integrity, the perceived rightful owner of the domain does not have access to the site and could lead to spoofing from the domain owner.
   f) Confidentiality and Integrity, the card info was not kept secure, and the thief has compromised the Integrity of the rightful card owner.
   g) Integrity, the spoofing has broken the trustworthiness of the owner's computer and IP address.

3) Security by obscurity can work well when the design or critical information about a system is inherently secret. For example, military equipment, often not only do you want to keep specific technical implementations a secret but even what features a project has should need to know only. If one person does not have the whole picture, it's more difficult to compromise the entire system or even know which avenue to begin to look for a weakness. Security by obscurity should not be used in commercial or open-source software examples, where anyone can have detailed implementation information. If there are any holes in the underlying code, anyone who uses the software will know. Proper security is also vital in closed source software and should be secured beyond keeping the vulnerabilities a secret but even more critical in open source code.

4) Compromising confidentiality can easily lead to compromised integrity. For example, suppose an attacker obtains personally authorized user information. In that case, the information was not kept confidential. They could use that to spoof that they are the trusted source and put out untrustworthy information, which would not have integrity, such as hacking into an authority email account and sending emails as them.

6) In addition to explicitly stated policy requirements, there could exist implicit ones not visible to the users. This may be done to obscure specific implementation details or security measures that all policy readers do not need to know, such as firewall settings or user authorization methods. It's implicit that if the user does not have access to these systems, they are not authorized even if it's not explicitly stated. However, like anything open to interpretation, this could lead to users unwittingly attempting to access or utilize data they should not be. Improper use could easily happen with informal policies as there's no way to prove (unlike mathematical approaches) that all cases are covered.

11) There will always be a balance between user security and privacy. System admins could better detect any bad actors or inconsistencies in user behavior if system admins have complete control and access to personal user data. However, since system admins do have access to so much user data, they have a responsibility to control, protect it and not attempt to access it unless there is a good reason.

13) A prominent example of a site that would allow users to bring in their external programs is sharing information and knowledge; websites such as StackOverflow.com. Their entire business model is on user-generated programs and content. However, corporate intranet websites sharing intellectual property with other employees would be on the opposite end of the spectrum. Corporations obviously would not want any external or unauthorized code and programs entering the site.

18) a) One easy way to detect if email traffic within a company is personal or business use without reading the email would be to see if the emails sent/received are external or internal emails based upon the sender/receiver address. Any traffic to external personal email accounts likely is not business use.
   b) Most companies probably do not ban all personal use just for employee trust and morale. It's a bit extreme for most jobs to cut off a person entirely from their personal life. Nowadays, people could use their smartphones in the office, but it creates a pretty extreme culture to cut off all personal use on a company computer.

Acknowledgment

The author would like to thank Professor Bruce McMillin with the Department of Computer Science, Missouri University of Science and Technology.

Matthew Whitesides Master's Student at Missouri University of Science and Technology.