Midterm Examination 1 CS 4235 Summer 2009

Your name / GT Account Name: ____

(1) (3 points) Circle the category that best fits the term *pretexting*: **Buffer Overflow,** [✓ **Social Engineering**]**, Countermeasure**

(2) (4 points) Which category of threat is more likely to involve user interaction: A [✓ *virus*] or a *worm*? Explain.

Worms can spread on their own without user interaction

(3) (3 points) Consider a program called `britney.exe` that a user has downloaded and is considering running. The user is able to confirm the *integrity* of the file. Should the user consider the program safe to run? Explain.

No, an unaltered viral file is unsafe but has integrity

(4) (5 points) An evil website `christina.ant` provides a link to `christina.exe` for users to download and run. Although the function of `christina.exe` is always the same, each copy of `christina.exe` has a different file size because of the addition of random, inconsequential bytes at the end of the file. Explain this situation in the context of *countermeasures* often deployed by users (and discussed in class) and hacker strategies to attempt to subvert these countermeasures.

AV programs often use file signatures that could be thrown off by random bytes

(5) (4 points) Circle all that apply: Intercepting a text file, then changing its contents and sending the changed file to the intended recipient compromises what? [✓ **Integrity**], **Polymorphism,** [✓ **Confidentiality**], **Rootkit, Availability**

(6) (6 points) Suppose your computer is running malware that enables someone to control it remotely. This person then uses your computer resources to stage a DDoS attack on `whitehouse.gov`. Barack Obama detects that `whitehouse.gov` is under attack and sends secret agents to your house. Does this situation constitute a *false positive*, a *false negative*, a *boundary condition error* and/or a *back door*? Explain for each term.

FP: Not FP, there was an attack. FN: No, no attack was missed. BCE: No. BD: Maybe part of remote control

(7) *Read the following excerpt from the popular internet tabloid Slashdot and answer the questions that follow*

New Scientist reports that a team of steganographers at the Institute of Telecommunications in Warsaw, Poland have figured out how to send hidden messages using the internet's transmission control protocol (TCP) using a method that might help people in totalitarian regimes avoid censorship. Web, file transfer, email and peer-to-peer networks all use TCP, which ensures that data packets are received securely by making the sender wait until the receiver returns a "got it" message. If no such acknowledgment arrives (on average 1 in 1000 packets gets lost or corrupted), the sender's computer sends the packet again in a system known as TCP's retransmission mechanism. The new steganographic system, dubbed retransmission steganography (RSTEG), relies on the sender and receiver using software that deliberately asks for retransmission even when email data packets are received successfully. "The receiver intentionally signals that a loss has occurred," says Wojciech Mazurczyk. "The sender then retransmits the packet but with some secret data inserted in it." Could a careful eavesdropper spot that RSTEG is being used because the first sent packet is different from the one containing the secret message? As long as the system is not over-used, apparently not, because if a packet is corrupted, the original packet and the retransmitted one will differ from each other anyway, masking the use of RSTEG.

(5 points) What term from the textbook describes the communication method above? Covert Channel

(5 points) Describe a scenario in which the above method could pose a problem for an IT environment. Identify specifically the *threats*, *assets*, *vulnerabilities* and possible *motivations*.

Threat of corporate espinage by infecting unpatched system (vuln.), sending secret file (asset) to get money (motive)

(8) (3 points) Circle **true** or [✓ **false**]: Recent cybercrime trends have seen a shift away from large criminal organizations toward lone individuals acting in isolation.

(9) (3 points) Circle **true** or **false**: Recent cybercrime trends have seen a shift away from large criminal organizations toward lone individuals acting in isolation.

(10) (4 points) Label the following scenarios as pertaining to one or more of the following: **Interception, interruption, modification, fabrication**

- A GT zimbra account is hacked in such a way that emails sent to `georgep@gatech.edu` actually arrive at the inbox of `hacker@gatech.edu` intercep.
- Hackers enter the Rich building and modify the power cables for the servers providing zimbra services by severing them interrup.
- Hackers insert an invalid student "George P. Burdell" into the central campus directory fab.
- Hackers change a previously recorded grade of a genuine student from B to C mod.

(11) (5 points) Which would be considered a more secure operating system: An operating system that ensured that arbitrary programs could not corrupt *user data* or one that ensured they could not corrupt [✓ *system code*]? Explain.

Altered system code could lead to attacks on user data, but the reverse is not nec. true