CS181S – Systems Security Fall 2020

Problem Session 2: Principles

Monday September 7, 2020

1. **Principles of Security.** The `su` command enables a UNIX user $u1$ to access the account of another user $u2$. Unless $u1$ is the superuser ("root"), `su` prompts $u1$ to enter the password of $u2$. Checking whether that password is correct requires `su` to open the password file, `/etc/passwd`. On a correctly configured UNIX system, that particular open operation will always succeed. Then `su` can proceed with checking whether the password is correct.

   A CS 181S student becomes concerned with what might happen if the UNIX system is not configured correctly—in particular, what if a misconfiguration caused the open operation to fail, and what if that led to the system becoming unusable? So the student decides to build a new version of `su` that works as follows. If the open operation succeeds, then the password is checked. If it is indeed the correct password for $u2$, then $u1$ is granted access to the account of $u2$. But if the open operation fails, then $u1$ immediately is granted access to the account of the superuser ("root"). The students intention is that $u1$ would then be able to fix the misconfiguration.

   Discuss which of the following security principles the students new version of `su` upholds, which principles it violates (and which are simply irrelevant):

   (a) Economy of Mechanism

   (b) Complete Mediation

   (c) Least Privilege

   (d) Separation of Privilege

   (e) Failsafe Defaults

   (f) Defense in Depth

   (g) Open Design

2. **Privacy.** For each of the following scenarios, to what extent has privacy been violated? Why?

   (a) Consider an enlightened company, where employees who have free time may use their office computers to access the Internet for personal tasks. A newspaper article causes management to fear that the companys secret documents are being leaked to the press, and that prompts an audit to identify which employees have electronic copies of secret documents. To implement that audit, the security officer proposes that a virus be written and used to infect all machines on the companys intranet. That virus would behave as follows. (1) This virus periodically scans the disk of any machine it infects, locating any secret documents being stored there. (2) Whenever the virus locates a secret document, it sends email containing the name of the machine and secret document to the security officer.

   (b) In the scenario above, instead of reporting all secret documents found, it simply reports the name of every document found that is not on an approved list of publicly-released corporate memos.

   (c) When the users browser opens a web page being hosted by an Internet portal (such as Google, MSN, or Yahoo), a pop-up appears containing an advertisement selected based on the last web search that user made.

   (d) When the users browser opens a web page being hosted by an Internet portal (such as Google, MSN, or Yahoo), a pop-up appears containing an advertisement selected based on the contents of the last email that user read or sent.