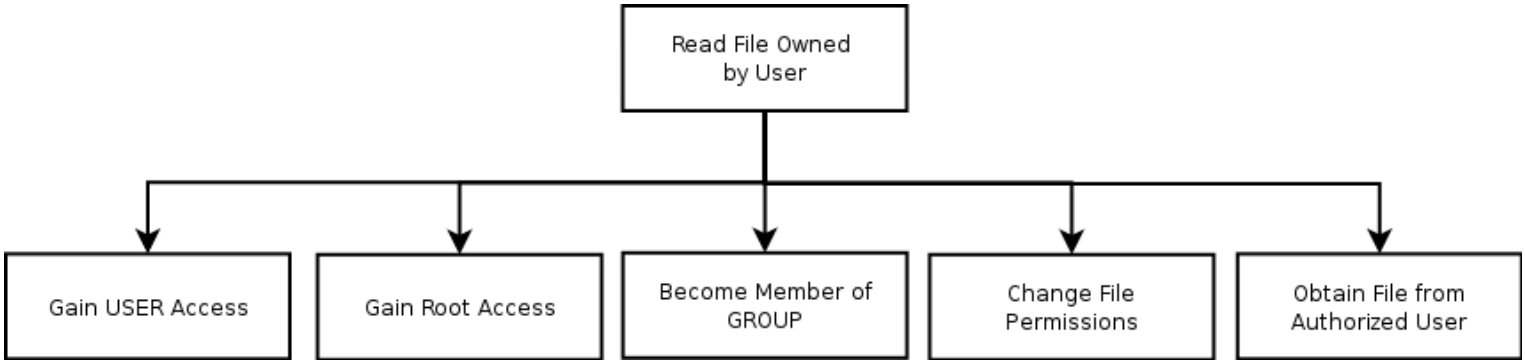
CS 161 Fall 2005 — Computer Security — Joseph/Tygar/Vazirani/Wagner — HW 1

Solutions

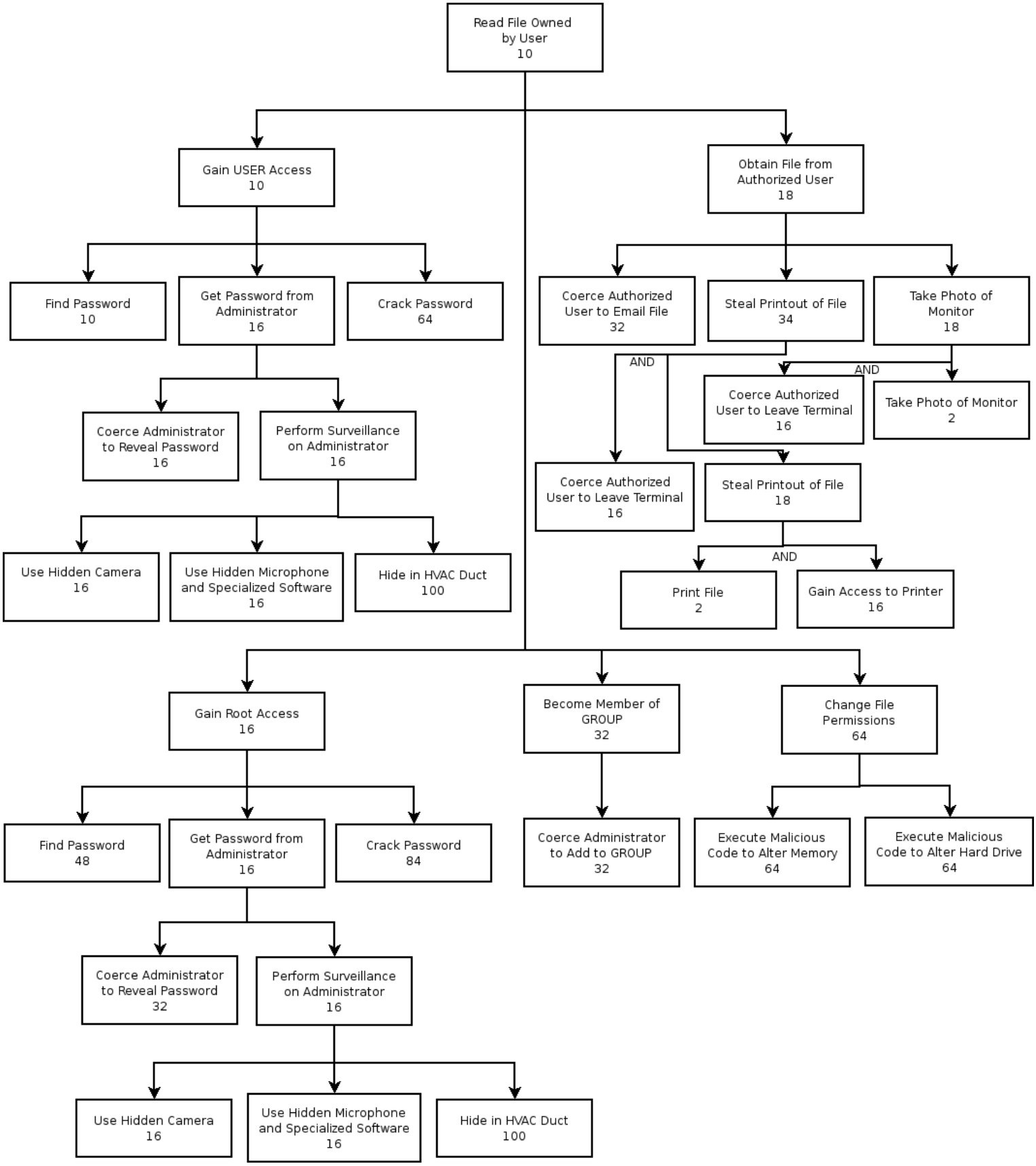
1. (1 pts.) Any questions?
All constructive responses awarded full credit.

2. (4 pts.) Getting started
(a) Sentence must be somewhere near name on the first page to receive credit.
(b) Quote from CS161 Website: "Homeworks are to be done individually, on your own (not in groups)." Additionally, "For homeworks, you **must always** write up the solutions on your own. Similarly, you may use references to help solve homework problems, but you **must** write up the solution on your own and cite your sources. You may not share written work or programs with anyone else. You may not receive help on homework assignments from students who have taken the course in previous years, and you may not review homework solutions from previous years."
(c) Registration with the grading system will be verified for credit.
(d) Quote from CS161 newsgroup: "My favorite security-related book is Bill Cheswick, Steve Bellovin, and Avi Rubin's _Firewalls and Internet Security: Repelling the Wily Hacker_. It's a classic. Even if you don't care about firewalls, it teaches a lot about network security, and there a lot one can learn about their general philosophy and approach to security that will be useful elsewhere in security. (My second favorite is Ross Anderson's _Security Engineering_, which is the optional text for this class.)

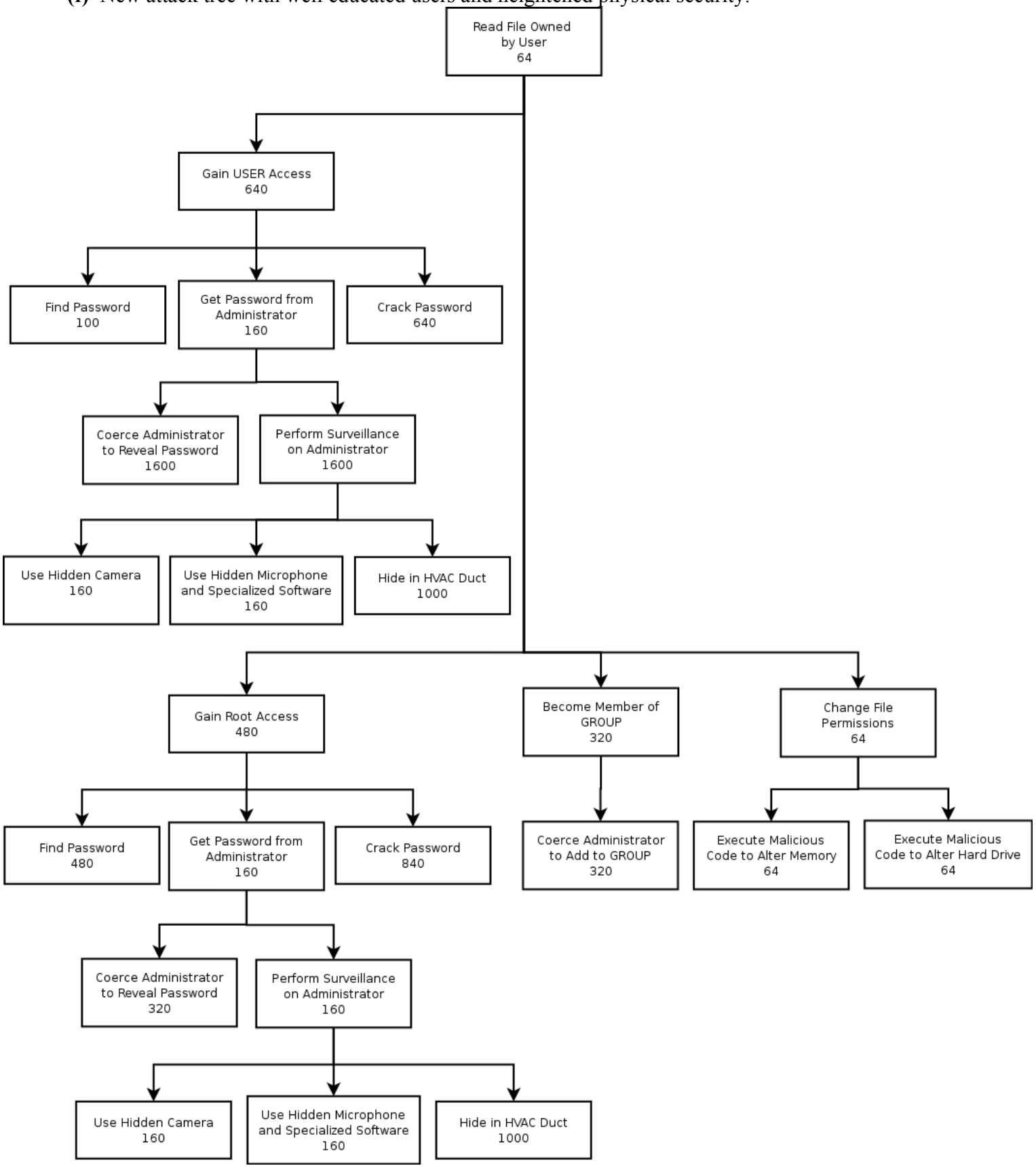
3) (45pts.) Attack Trees
(a) Express goals using an attack tree with one level.



(b) Design of successive sub-goals. **(c)** Rough costs assigned, measured in terms of t / (1 – p), where t = the time required to achieve the task and p = the chance of detection.



(d) From the sample attack tree above, the cost of the cheapest attack on the system is 10.
(e) From the sample attack tree above, the best practice to make private UNIX files more secure would be to properly educate the system users about proper password protection, physically securing the system, and periodically checking for the installation of surveillance equipment (both on the system and surrounding it).
(f) New attack tree with well educated users and heightened physical security.



(g) All constructive responses awarded full credit. Bruce Schneier: "Attack trees provide a formal methodology for analyzing the security of systems and subsystems. They provide a way to think about security, to capture and reuse expertise about security, and to respond to changes in security. Security is not a product -- it's a process. Attack trees form the basis of understanding that process."

4. (30 pts.) In-band and Out-of-band Signaling

(a) One advantage of using in-band signaling versus out-of-band signaling is that in-band signaling reduces costs by sharing the same infrastructure for both data and control information. One disadvantage of communication using in-band signaling versus out-of-band signaling is that the shared infrastructure allows a user to possibly ascertain the "secret" control protocol and take control of the entire system.

(b) Signaling System #7 (SS#7) improved the security of the telephone network when it was introduced because it featured out-of-band signaling, which prevented users from spoofing control signals over the data lines as had been seen with in-band signaling systems. However, SS#7 has no internal authentication or security, which did not initially present a problem because SS#7 was owned by a single company ("Ma Bell") that had sole control of the system. As deregulation occurred in the 1980s, anyone could become a Competitive Local ExChange (CLEC) provider and get SS#7 access. Thus, the system is inadequate today because any local exchange with access to SS#7 could spoof messages by manipulating protocols within SS#7 (spoofing CallerID, etc.).

(c) One way to improve security would be to implement an authentication protocol between Competitive Local ExChange (CLEC) providers and SS#7. Only authorized CLECs would be able to access the SS#7 system. This would require upgrades in software and hardware between CLECs and SS#7, but would not affect the phones on the system and the way people place calls.

5. (20 pts.) Default Configurations

Default configurations often have default administrative accounts and passwords that hackers the world over know. This applies to routers, hubs, switches, operating systems, e-mail systems, and other server applications, such as databases and Web servers. A good example of this is Linksys wireless routers, which contain the default administrative account named "linksys" with password "admin."

In addition to having known passwords on the computers, default configurations contain multiple security holes that you need to plug. Before you ever put any computer online, you should change the default account names and the passwords and apply all security patches. Many systems are known as "default open" and must be configured to disallow certain traffic to pass or processes to execute. A little bit more time spent on a computer at this point can save you a lot of grief later. The fewer holes you leave on a network, the harder it is for someone to break into your system. Returning back to Linksys wireless routers, the out of the box configuration has common security features such as WEP and MAC filtering disabled. Additionally, By shipping a system that is default open, you essentially guarantee that a significant percentage of installations of that system will be left open and eventually exploited. This happens because end-users may not be technically savvy enough to secure the system, or may simply not realize that the default settings are problematic.