Axioms of computer and network security **DRAFT**

Jeffrey S. Marker, CISSP
magic@jiffyscript.com

March 27, 2002

1 Acknowlegements and intoduction

If a lot of this sounds like it comes from the pen of Stephen Kent, Steven Bellovan, Gene Spafford, William Cheswick, Dan Farmer, Weitse Venma, Phil Zimmerman, or any one of a cast of information security gurus, it is because i build on the shoulders (or, prehaps, feet) of giants. It is also because these tenets are nearly universal, like unto laws of physics.

2 Rootkits

Yes, rootkits don't *really* have the much to do with network security, since they are beasts installed on single nodes, and, in fact, their name would indicate that they are rather UNIXspecific[1]. Rootkits do enter into the network security arena, though, in that they generally include a network sniffer. Besides, i'm the one doing the writing here, and i want to talk about them.

First things first: "rootkit" is a generic name applied to a number of different "hide the fact that this machine is owned"[2] groups of programs. In other words, "rootkit" is a word awfully similar to "casserole"[3] or "stew"–it describes different tools to different people.

[1] The term "rootkit" has made it's way into the Windows world as well.

[2] "Owned" is a quasi-technical term denoting the fact that the computer is no longer being run solely by it's authorized administrators, but is, in fact, infested and controlled by possibly malevolent outsiders.

[3] Make the correct reference to Steve and Sarah here.

Casseroles tend to include cream of mushroom soup, celery, and potatoes as main ingrediants; similarly, rootkits tend to include replacements for a number of standard tools which might detect them, such as *ps(1)*, *ls(1)*, sl df(1), sl netstat(1), and *ifconfig(8)*. Casseroles also tend to have some meat, which translates to the network sniffer that is often found in a rootkit.

Rootkits also tend to contain tools designed to allow the intruder to retain access to the compromised host. These tools tend to be replacements for standard tools like *login* or *sshd(8)* with magic username/password pairs embedded, or *inetd(8)* with a shell-on-a-port listening. Another tool that might be included in the rootkit is a stand-alone shell-on-a-port program. These are like carrots and peppers, adding a little color.

3 Encrypted tunnels

At the current time, attackers tend not to be well-financed employees of large corporations or governments[4]. As such, attackers tend to be less concerned with the data stored on the compromised system, and more concerned with getting and maintaining access or with completely denying access for authorized users[5].

[4] This is probably even true if the organization being protected is a government.

[5] We probably won't discuss denial of service attacks.