Clearing Up Some Misconceptions Involving MAC Numbers

by Scott Borg
with extensive editing and rewrite suggestions by Austen Borg

The biggest problem, when it comes to identifying the particular physical computer used in a cyber attack, is that computers are so profoundly generic. This is ultimately an even bigger forensic problem than the fact that computers can be used remotely. As we have already noted, computers are general-purpose machines for executing instructions. This means anything one computer can do, any other computer can do. It might take another computer a much longer or shorter time to carry out a given task. This is because different computers typically have different instructions hard-wired into them in an effort to speed up their operations. But the operations that computers carry out, at a fundamental level, are always exactly the same. Computers, in a very basic sense, are completely interchangeable. That is one of the features that make them so useful. Even the differences between computers that are due to different instruction sets being hardwired into them are not very revealing. This is because there are only a limited number of basic instruction sets—and basic operating systems—currently in use. If a cyber attack can be determined by some means to come from a Dell laptop running a Windows operating system, that is still not very forensically useful. When computers are interacting with the world as information systems, they do not have unique and lasting identities.

The one feature of computers that would seem to make them more individually distinct are their "MAC numbers." These are *identification numbers assigned to individual computers by their manufacturers before the computers are shipped to distributors*. People who have learned a bit about information technology are often under the impression that individual computers can be identified by their MAC numbers. They imagine that MAC numbers are like the serial numbers on guns or the VIN's on automobiles. They assume that because MAC numbers are used to identify hardware, they are hardwired into computers. They believe MAC numbers to be unique. They suppose that the best possible outcome of an effort to trace the computer used in a cyber attack would be to identify its MAC number. None of these things is true.

MAC numbers are simply the address numbers used to identify the individual computers within an organization's local, internal network. They are assigned to computers before shipping, so that there is a way to locate the computers on local networks when they are first plugged in. MAC numbers are not actually part of a computer's hardware, but they are automatically loaded into computers each time the computers are booted. That way, they will be immediately available for networking purposes. "MAC," in this context, stands for *Media Access Control*. MAC addresses are used for routing information within the local network and sometimes to control which computers are allowed to connect to that local network.

MAC numbers usually only matter locally. If a computer is on a local network—if it is sharing a wireless connection, for example—then that computer's MAC address will normally be visible to other computers in that same local network. But a MAC address will usually *only* be visible *within* an organization's local network. When information leaves a local network and moves onto the internet, that information will no longer contain a MAC address. Sometimes a MAC address will be used as the default identification number for establishing a secure computer-to-computer communication across the internet. But any other arbitrary number would serve that purpose just as well. This means MAC addresses are of little or no use in tracing a cyber attack that uses the internet. The purpose of MAC addresses is simply to manage electronic equipment at a local level.

MAC numbers are not the kind of unique, permanent identifiers people imagine them to be. A single computer will generally be assigned more than one MAC number. In fact, it will generally have a different MAC number for each type of local network it is using. A computer's MAC address for its ethernet connection, for example, will be different from its MAC address for its wireless connection. A single MAC number will sometimes be assigned to more than one computer. A given manufacturer will be assigned a block of MAC addresses.[1] The manufacturer will then insert a different MAC address into each successive computer coming through its production line. A manufacturer can *re-use* MAC addresses, as long as the manufacturer doesn't use the same MAC address on two computers that are likely to end up on the same local network. The way MAC addresses are assigned and re-used is governed almost entirely by practical considerations, not legal requirements.

The MAC numbers of a computer are designed to be changeable. This allows an individual computer to be replaced without changing all the local network settings. It is also sometimes necessary if two computers with the same MAC address end up by chance on the same local network. Changing a MAC address is very easy. On a Windows or Linux computer, it is usually just a matter of changing the relevant setting in the computer's network management menu.[2] On an Apple computer, the appropriate instructions need to be typed directly into the computer's general-purpose command window, but this is only slightly more difficult than using a menu. When a computer's MAC number is changed using its software, the original, default MAC number will usually remain in its firmware. But that original, default MAC number will not be visible to anyone, and, in many cases, even that firmware number can be changed. MAC numbers should never be assumed to be permanent.

The same procedure that is used to change the MAC address can be used to spoof one. Usually, when this is done, the attacker will simply assign his or her computer a MAC number that already belongs on the local network being targeted.[3] Then the attacker will connect to that network using an ethernet cable or a local wireless connection at some moment when that MAC address isn't already being used. By spoofing a MAC address that is already recognized by the network, the cyber attacker can avoid any limitations placed on new connections. This tactic will also make it appear that any actions the attacker carries out are being done by a computer that is supposed to be there. MAC addresses can be used to spoof, not just existing devices, but imaginary ones. Often the MAC number used in a local cyber attack will be the address of a ghost, no longer present anywhere after the attack communication has ended.

Understanding the uses and limitations of MAC addresses is important, because there is *no other* piece of information associated with an individual physical computer than can be used to identify it more reliably than its MAC number. There are no electronic serial numbers, electronic fingerprints, or other digital features associated with computer

[1] The Institute of Electrical and Electronics Engineers (IEEE), a non-profit professional association, does the assigning. The particular blocks of MAC numbers that are assigned to particular computer manufacturers are public knowledge and available on the internet. Since MAC numbers are generally applied to computers sequentially, knowing one number from a bulk equipment purchase will usually make it possible to deduce others.

[2] Within a Windows Device Manager, opened to the advanced settings, the MAC "Network Address" will be one of the changeable "Properties" listed for each of the "Network Adapters." Within a Linux Network Manager, the MAC address can be changed in the Edit Connections window.

[3]

hardware that can be used to distinguish one computer from other computers. Even if there were, those, too, could be electronically spoofed. In *every* situation where a computer interacts electronically with the outside world, another computer could be undetectably substituted. No investigations of a cyber target or cyber crime scene can reliably identify the specific computer used in a cyber attack.