Privacy Issues in an Insecure World

W. Timothy Strayer
BBN Technologies
10 Moulton Street, Cambridge, MA 02138
strayer@bbn.com

ABSTRACT

We all have a notion of privacy and understand that we trade some of it away in order to have normal social interactions and communal security. Networked computer systems are no different. The notion of privacy is running squarely against the need for security in an increasingly networked world. Is it possible to have secure systems that honor privacy?

There are two basic ways to secure a network: prevent bad things from happening, and watch closely for bad things and prosecute those who commit them. Since our current preventative measures like authentication and authorization seem to be failing to adequately protect the network, we have turned more toward auditing and monitoring—first as a complement, and now increasingly as a substitute—for prevention. The emphasis is on using threat of stiff penalties as the detenant, but for those perpetrators of intrusion, the auditing systems are required to collect enough forensic information for legal prosecution.

The operative questions are:

1. Is this effective?
2. What impact is this having on otherwise law abiding citizens?

Storage is very cheap, so monitoring systems can record a great deal of information, and recent legislation allows employers and the government to do so liberally. New research in data mining techniques and sophisticated analysis make them increasingly effective. And visualization tools allow investigators to notice subtle patterns that would otherwise be lost in the aggregate. Given that the vast majority of the traffic being monitored is legitimate, the very act of searching for evil-doers exposes things we have generally considered private. The new and effective monitoring tools encourage snooping, and the laws so far do little to discourage it.

In this talk I discuss the impact security concerns is having on privacy, and suggest that today’s trend of solving security by detecting intrusions through monitoring is a reaction to institutional paranoia as well as woefully inadequate software development processes. I argue that monitoring alone can’t provide sufficient protection, and that in fact the trend of relying increasingly on intrusion detection systems tells us that we are really losing ground—not gaining—on providing computer security. And it doesn’t have to be this way. Strong authentication and authorization systems do not necessarily have to rely on positive identity to work.

Yes, networked computer systems must be monitored and audited for inappropriate use, but the key phrase must be to the minimum extent possible in order to strike the proper balance between privacy and security.

Views and conclusions contained in this talk are those of the author and should not be interpreted as representing BBN official policies, either expressed or implied.