Table of Contents

True Security is Not Simple ................................................................. 3
Physical Security .................................................................................. 3
System Security .................................................................................... 3
Network Security ................................................................................... 3
Application Security ............................................................................... 4
End User Security .................................................................................. 4
UF Raises Awareness ............................................................................ 4
True Security is Not Simple

By Dr. Michael Conlon, UF Director of Data Infrastructure and PeopleSoft Implementation Officer

In today's world our complex networked enterprise systems store a wide variety of valuable and personal data. Securing these systems and our data involves effort from technical staff as well as the users of the systems. We are sometimes tempted to simplify “security” and consider only a subset of the threats to our systems and focus our thinking on defense against these threats. True security depends on a broad spectrum approach to protect our systems and data across a wide range of potential threats.

Physical Security

Physical security is the collection of processes used to insure that our physical assets can not be compromised. Alarm systems, card control systems, surveillance systems and other means are used to deter physical access to systems and data by unauthorized persons. In some cases our data our outside our systems and are present on physical media such as paper or tapes or removable disks. In some cases data have been transferred to office systems, laptops, personal digital assistants and even phones. The physical security of each location of our data must be insured.

System Security

System security has been the focus of much media attention in recent years. Unauthorized access to systems by remote users, usually to do harm to the systems and or the data in those systems has come to be known as “hacking.” Other problems are much more important than hacking in terms of data loss, but hacking has captured the imagination of the public and generates much fear and uncertainty. Most systems can be secured against hackers through rather routine countermeasures. And while there is much discussion about whether one kind of system or another is more susceptible to hacking, all systems are susceptible and all systems can be secured by adhering to well known system security. Such practices are a requirement for operating systems storing data in our networked world.

Network Security

Network security involves the practices needed to insure that data is not intercepted in transit between systems. Firewalls and encryption are two very common methods for improving network security. Networks are scanned to detect unusual traffic patterns and it is important that network access can be filtered to remove suspicious traffic as it occurs. Worms and viruses are propagated through the network by compromised systems. Good network security can mitigate the spread of malicious software. Encryption effectively removes the threat of interception of data in transit. So-called “secure sites” are merely encrypted sites – they may not possess strong system, physical or application security. Encrypted sites are particularly important for e-commerce and conduct of business over the Internet and other unsecured networks.
Application Security

Application security is the process of insuring that only the individuals authorized to perform specific functions have the permissions to perform those functions. Application security is sometimes known as access control. Password sharing is an obvious threat to application security – the individual using the shared password as access to applications they may not be personally authorized to perform.

End User Security

End user security is the collection of practices required by the users of the systems to insure that data and systems are secure. The best system and network security can not secure data from authorized end users who download and use data outside the bounds of their authorizations.

Security experts repeatedly claim that the most useful tool to the person trying to gain unauthorized access to data is the telephone. By making telephone calls, the unauthorized person can typically gain access to data via request – authorized individuals turn over passwords, create accounts, print and fax data and get access to large amounts of data in short amounts of time. Technical countermeasures do little to prevent this kind of access.

UF Raises Awareness

UF is doing a good job at raising awareness of all kinds of security threats and corresponding security measures and best practices. ITSA Day (www.itsa.ufl.edu [http://www.itsa.ufl.edu]), the HSC SPICE Project (http://security.health.ufl.edu/SPICE), the password management policies (www.it.ufl.edu/policies/passwords.html [http://www.it.ufl.edu/policies/passwords.html]) and the Access Request System for the myUFL systems (www.bridges.ufl.edu/security [http://www.bridges.ufl.edu/security]) are all efforts to bring end-to-end approaches to security to bear to protect our systems and our data.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT
2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>