|  |
| --- |
|  |

Confidentiality

|  |
| --- |
| **Information Security Environment** |
| CSC 116-71 |
|  |
| Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. |
|  |
| **Mark Hamri** |
| **4/30/2012** |
|  |

Security Mode

Integrity

Availability

**Threats in Home Environment**

[](http://www.google.com/imgres?q=home+security&um=1&hl=en&biw=1920&bih=900&tbm=isch&tbnid=zLL6BZnGw3ltCM:&imgrefurl=http://wirelesshomesecuritysystem.dealsofgift.com/&docid=iENCaJpnw4KSzM&imgurl=http://wirelesshomesecuritysystem.dealsofgift.com/wp-content/uploads/2011/12/wireless-home-security-system.jpg&w=500&h=324&ei=SG2IT-jhNMnc0QHg77HZCQ&zoom=1&iact=hc&vpx=474&vpy=288&dur=2424&hovh=181&hovw=279&tx=220&ty=100&sig=111039124019794383595&page=1&tbnh=107&tbnw=165&start=0&ndsp=42&ved=1t:429,r:2,s:0,i:143)The aim of this paper is to assess the relevance of data security in the homeenvironment and to identify the nature of vulnerability. At the time of writing most data in the home is stored manually. The widespread use of the Internet, home pcs and mobile devices now means that increasingly individuals (and families) are storing home information electronically. It is highly likely to be a trend that continues. Information on specific data security related issues is widely available in terms of how to protect your pc and there are also many products that are available to assist with this. The level of actual understanding that home users have of the general data security issues and the means that they take to protect themselves are not well documented. The approach taken in this paper is to look at many of the data security threats posed to existing ICT devices and to put them in the context of systems that are currently used or may be used in the future, in the homeenvironment. The paper clearly defines that it is not concerned with the broader topics of data assurance (which would include fire, flood etc.). The primary focus is the potential for malicious acts being committed by unauthorized use of the systems. Where the threats from and what are can be done to alleviate them? Are the main vulnerabilities in the connectivity, the systems, or both? Since technology now softens the environmental boundaries, this paper alludes to the scope of the homeenvironment. It also discusses existing solutions to perceived threats; whether they appear to be understood and whether they appear to be working. It looks for the evidence to demonstrate the significance of data security in relation to the development of intelligent homes.

[](http://www.google.com/imgres?q=home+security&um=1&hl=en&biw=1920&bih=900&tbm=isch&tbnid=PPPmQ3KIOymSEM:&imgrefurl=http://www.familyhomesecurity.com/&docid=YDcVHD1m6UOgDM&imgurl=http://www.familyhomesecurity.com/images/Family-Home-Security.jpg&w=347&h=346&ei=SG2IT-jhNMnc0QHg77HZCQ&zoom=1&iact=hc&vpx=1644&vpy=247&dur=465&hovh=224&hovw=225&tx=173&ty=128&sig=111039124019794383595&page=1&tbnh=124&tbnw=148&start=0&ndsp=42&ved=1t:429,r:9,s:0,i:157)How easy it to break into my computer, unfortunately, intruders is are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.When holes are discovered, computer vendors will usually develop patches to address the problem(s). However, it is up to you, the user, to obtain and install the patches, or correctly configure the software to operate more securely. Most of the incident reports of computer break-ins received at the CERT/CC could have been prevented if system administrators and users kept their computers up-to-date with patches and security fixes. Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure. Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

[](http://www.google.com/imgres?q=spy&um=1&hl=en&biw=1326&bih=622&tbm=isch&tbnid=8plJjDJYRwfPSM:&imgrefurl=http://weeble.net/selling-of-laptops-with-spy-software-said-to-be-false-by-samsung/2779/&docid=Z6xEmCSvJwQhnM&imgurl=http://weeble.net/wp-content/uploads/2011/04/Samsung-Spy-Software.jpg&w=293&h=288&ei=2WGUT9nbNafH6AHApPikBA&zoom=1&iact=hc&vpx=301&vpy=237&dur=142&hovh=223&hovw=226&tx=64&ty=79&sig=110354734213078086753&page=3&tbnh=136&tbnw=137&start=49&ndsp=27&ved=1t:429,r:14,s:49,i:274)Who would want to break into my computer at home, (also referred to as hackers,attackers, or crackers) may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.Having control of your computer gives them the ability to hide their true location as they launch attacks.Often against high-profile computer systems such as government or financial systems. Even if you have a computer connected to the Internet only to play the latest games or to send email to friends and family, your computer may be a target.Intruders may be able to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.What is computer security, Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

How to keep your home secure we strongly recommend the use of some type of firewall product, such as a network appliance or a personal firewall software package. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks. However, no firewall can detect or stop all attacks, so it’s not sufficient to install a firewall and then ignore all other security measures. Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs. The CERT/CC recommends the use of anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date. Many anti-virus packages support automatic updates of virus definitions. We recommend the use of these automatic updates when available. Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing they might contain a Trojan horse program. Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, but you can disable this option in order to have file extensions displayed by Windows. After disabling this option, there are still some file extensions that, by default, will continue to remain hidden. There is a registry value which, if set, will cause Windows to hide certain file extensions regardless of user configuration choices elsewhere in the operating system. The "NeverShowExt" registry value is used to hide the extensions for basic Windows file types. For example, the ".LNK" extension associated with windows shortcuts remains hidden even after a user has turned off the option to hide extensions. Vendors will usually release patches for their software when vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information. Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check periodically for updates. Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

[](http://www.google.com/imgres?q=home+security&um=1&hl=en&biw=1920&bih=900&tbm=isch&tbnid=gxOABfLsQ1CzqM:&imgrefurl=http://www.presentermedia.com/index.php?target=closeup&maincat=clipart&id=1327&docid=j5qSH-DaC-n3tM&imgurl=http://www.presentermedia.com/files/clipart/00001000/1327/home_security_md_wm.jpg&w=400&h=400&ei=SG2IT-jhNMnc0QHg77HZCQ&zoom=1)

|  |  |  |
| --- | --- | --- |
| Description | Physical Threats | Network Threats |
| Definition | Physical threats are more about accessing the data physically without any official permission. It’s even means that some outsider entering the office and accessing the secured data illegally. | A network is the most heavily used vehicle for disseminating the organization’s information. Network allows us to share information and if we are using internet it just opens the entire door to the outside world. This it could be a threat for the company and all the information stored in the companies computers and buildings. |
| Examples | Premises Access and equipment access, Mobile users and laptops, Trash Cans, Voice Mails, Old Pc’s and weak passwords etc. | Sniffers, Viruses, Backup tapes, Wire Tapping, User passwords, Administration, Share and file permission, Email administrators etc. |

Physical Threats Stay calm and attempt to assess the situation. Talk to the person who is threatening you and try to reason with him, but don't argue which can escalate the situation and increase the danger.Look for an escape route and get to a safe place as quickly as possible. If you're in a public place, run to where other people are and seek help. Try to distract the person who is threatening you to give you an opportunity to run. If you can put a physical block between yourself at the attacker, this may give you the extra few seconds needed to escape.

Network Threats, Firewall is a family of hardware and virtual appliances designed to protect network infrastructure, improve site-to-site connectivity and simplify administration of network operations. Beyond its powerful network firewall, IPS and VPN technologies, the Barracuda NG Firewall integrates a comprehensive set of next generation firewall technologies, including Layer 7 application control, WAN optimization, Web filtering, anti-virus, anti-spam and network access control enforcement.

|  |
| --- |
| Citation added: |
| "Google." *Google*. Web. 22 Apr. 2012. <http://www.google.com>.  http://www.barracudanetworks.com/ns/products/ng\_firewall\_overview.php?&a=google-na\_NGFirewall-General\_NetworkThreats&kw=%2Bnetwork%20%2Bthreats&gclid=CP3fjsbi2K8CFcXc4Aod-jK3Ag |