Comment on Student's Reading Critique (The Security Principles to Live by)

I certainly agree to the assertion "to limit the access the user has to only what is necessary and by limiting their security privileges…" Since different software is programmed using codes and while the internet is wider in scope, it is difficult to control any threat to the security of one's computer. A computer software expert can penetrate even the most top secret codes because they are programmable.

I understand that limiting the access would pose problems on the users and I could see that it is a result of this action. Anyway it would be right to give other options which are to replace the old codes with new ones. I guess, this has a lot more advantages for our future application designers than coming up with new software using old codes. First, the new codes will give the hackers who are using the old codes no opportunity to trace its path; secondly, the new codes may be programmed with more advanced security features; and, third, it will spark the new trend in software development. Likewise, old codes installed in updated software (or new developed software) may only limit further progress in terms of software development because of incompatibility issue with highly technologically advanced hardware to be invented someday.

As our technology advances, software developers must also insure security implications to the product. Coming up with new product grounded in research may be the right solution to lessen the threat in using computer. Never invent/develop product that may bring security problem to the users.

Comment #2 on Student's Reading Critique (The Problem of Cybercrime)

Computer hacking is really a serious problem for people who are using the internet especially for top government and/or organization whose security is a top most needed. For now, this is unavoidable and nothing is done with it. I agree that this condition may pose problems in the future. Hacking for this reason is a cybercrime as it can penetrate an individual's passwords, bank transactions and credit cards. As the writer noted, the internet for hackers gives them the easy way for theft to do stealing whose identity remains untraced.

As I see it, everyone was able to expound on the activity of computer hackers and the problem they bring to all internet users which include private organizations and governments around the globe. Given this issue, there must a consolidated decision coming from and represented by each country in the whole world in order to design a set of guidelines which may lead towards the formulation of cyber laws and course of actions against illegal the internet activities. Thus, restructuring and/or redesigning of operational structure of the internet should be grounded on cyber laws that will be created, because any violation committed by a hacker will be subjected to punishment. No one would be excuse from the law once enacted.

I agree with the opinion regarding prevention of cybercrime; however, individual sites may also add security features in its protocol to keep the privacy and security of the information of the subscribers. I think, in the absence of cyber laws, individual site owner and user may observe safety measures which have to be explained well, such as what messages is suspicious and which is not. I guess, security alarms may be installed in a system to prevent hackers from entering one's account.

Lecture Discussion

In my opinion, the most pervasively exploited computer system is system software which can be penetrated by viruses through an infected USB and downloaded files from the internet. The virus enters in and destroys the system while others (auto run) penetrate the system to report secret information stored in the memory. Either way, the virus is created to increase the demand for antivirus product or to steal user's information.

Viruses can be treated using antivirus software; it means, it can be prevented as long the program is updated regularly. I guess the one that poses severe problem in the future is computer hacking as it is seen operational nowadays. Not only individual persons are hacked but also important information of one's country; remember the 'I-love-you' virus which had damaged worth of billion dollars worldwide. It made The Pentagon and CIA to shut down their mail system just to get rid of it.

Week 5: Summary of the reading "Hey, You, Get Off My Cloud: Exploring Information Leakage in Third-Party Compute Clouds" by Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage

As the title suggest, the article was about a new technological innovation introduced in the market called "cloud computing" which is seen as the next infrastructure for data hosting and for deploying software services that would essentially lower capital cost. While the authors' sees this technology to provide strategic advantage for business organization, they also pointed out that this new system of data hosting present many risks and threats from attacks from the cloud provider it self in view of the fact that their clients vital information are exposed to the cloud provider. They are unprotected in their vulnerabilities against a malicious behavior by the cloud provider. The authors also noted that while the cloud computing presents many threats of attacks, they are however known and the risk they presented are understood. But these threats are not likely to occur as subscriber companies require strict guarantees of safety and confidentiality. Thus the author asserts that this threat will likely to come from mutually distrustful users. The authors discussed several ways by which information leaks or attacks might be launch.

Unfortunately, the solutions offered by the authors to address those threats were not satisfying. What they thought as the ultimate solution to the problem is quite irresponsible in the sense that it simply places the whole burden to the users how they would safeguard their system. This is not a concrete idea as there are still issues that need to be addressed. First is the cost, second it will render some of the machines under-utilized. I addressed my comment equally to the authors and the cloud provider's management. To the authors because after finding this new infrastructures presents many risks and threats of attacks offers solutions that are not worth accepting, and to the cloud provider management for introducing such unsafe infrastructure.

Comments on the students reading critique, "Hey, You, Get Off My Cloud: Exploring Information Leakage in Third-Party Compute Clouds"

I agree that the cloud computing concept presents various risks and threats of attacks yet there is no concrete idea how this technological innovation could be maintained safe from all these treats and attacks from competing companies sharing the same physical infrastructure. I think the point here is that it is too premature for these authors to say that the cloud or the virtual computing "is the wave of the future and the new infrastructure will allow for companies to out source core and software computing, resulting in lower capital costs." This is very important point because as it is, the cloud computing is laden with many areas where threats of attacks can be launch aside from the fact that the users vital information or the so-called vulnerabilities of users are exposed to cloud provider. The only principle that binds the relations between user and the cloud provider is the trust on the part of the user. So, in a sense this relationship provides no concrete guarantee that there will be no breach of trusts on the part of the cloud provider.

Besides, it is true that the cost of having and maintaining exclusive virtual space is something to really think about. Since this infrastructure has now been in the circulation of IT professionals, I think any of these experts should come up with a better idea how this technology could be used with out worrying of attacks from other competing business using the same infrastructure. It is true that the risk connected to this technological breakthrough should have to be mitigated in order for this technology to bring technological benefits to users. Unless the threat of attacks and the risks connected to this infrastructure is mitigated, this technology could probably not really serve its purpose of providing out sourcing that will lower capital cost of the particular business using this physical infrastructure.

Answers to Questions on Lecture discussion

1. The OSI which stands for *Open System Interconnection* is not a networking standard in the same sense that Ethernet and TCP/IP are. Rather, the OSI is a framework into which the various networking standard can fit. I would say that the OSI layer that proposes the greatest risk to corporate and government infrastructure is the transport layer. This is because this layer is responsible for the network's interconnectivity with other systems attached to the network. Since most businesses are engaged multi-system but is attached to just one infrastructure, the transport layer occupies very important function in order for these system to operate smoothly. This layer also facilitates LAN/WAN interconnectivity. While there are perhaps other ways of having interconnection without using transport relay such as the complicated routing tables, they are not considered as efficient as the transport relay.

2. There are quite a number of advantages of wireless network for policing and military purposes. Among these is the easy access to network infrastructures especially in areas where there are no communication facilities or when they highly mobile. They can conveniently set communication using mobile communication using the The internet Protocol (IP) or any networking technology. Another advantage is the flexibility of the physical connection to the location of the application, and it is cost efficient. However, there are great risks that out weight these advantages. Among them are the risk of large data breaches, loss of intellectual property, preying of financial assets by cyberspace criminals, and compliance failure and potential attacks from cyber criminals. This system is vulnerable to cyber criminals and is good only for use in times of national emergency. The operator of the network should draw the line where there is potential unauthorized access to the network and in areas where attacker could launch an attack. If a network operation needs to draw the line, it should be in areas where the network is

vulnerable to attackers for the purpose of detecting attempts and in defending the system against attacks.

Answers to Student's Lecture Discussion

I could not really get the point about "locking the computer equipment away until the IT guys come to fix it." I do not mean to argue on this but I think the concept is how to really secure the system from cyberspace criminals. Of course this is a serious concern as it involves valuable data and other information including financial matters. I think it is a good point to say that the advantages and disadvantages of the wireless networks for policing and military has to be weighted in terms of benefits versus dangers. I agree but I should also add a little bit, it should also include the nature and purpose. If the intended use would be to set up a system for the day to day operation, it would have different consequences than when it is set up for use due to national emergency of any circumstance of similar purpose.

At nay rate, it is right to consider important benefits that may not available when using the wireless system. It would truly be difficult to just give an opinion about the issue without carefully weighing the benefits including the possibility that the risks and dangers can be addressed while out right rejection may only lead to a tragic mistake. Yes, a system can be made secure but at a diminishing levels of usability, but I also believe that any can only be made secure but can also be improved including the usability. I entirely agree that there is indeed acceptable risk and despite the dangers associated to the wireless network, it remains a potent tool not only for policing and the military but also for business.