Computer security and therefore the prevention of potentially harmful software like virus, malware and Trojans is a grey area in computing science and an endless race between security experts [1] and black hat hackers [2] is taking place since the beginning of the 1980's. This essay will discuss on the impact of teaching both sides of security from a legal and breaching point of view, how confining the teaching reduce the possible unexpected damages and how the press faced the issue.

Viruses, malware and Trojan will be always developed even by non-professionals for generating potential profits [3] and accessing classified information like trade secrets [4]. To prevent and more often patch the issues caused by such software is based on reverse engineering the hostile code and to understand its impact and behaviour [5], only a skilled person with strong knowledge in how such programs works can be able to understand the issue used for the intrusion and then be able to fix it, that's why course in computer science should cover such matters to increase the understanding of the techniques used and the evolution over the years. It is also complicated to dissociate some types of software from malwares, if you look by example at software like DameWare NT Utilities, a software used for administrating and monitor machines by system administrators, has been used the previous decade by hackers to gain access illegally to windows machines through the IPC vulnerability [6].

The second generation of computer hackers focused not anymore on the initial definition of hacking (using a computer in a non conventional way) but on security and intrusion of remote machines through the internet, most of them like Kevin Mitnick, Mark Abene and Ian Murphy [7] were arrested and judge for their computers misdeed and served in prison after their release most of them created computer security companies. Vladimir Levin hacked Citibank's computers and shown the vulnerability in their system, now Citibank uses Dynamic Encryption Card the most secured system used by no other financial institution in the world [8]. This shows than even if the act were initially malicious this community has been more efficient in detecting and exploiting security breaches than experts in this field and the current experts of our time or the hackers of the previous generation.

It is described that the work has been carried out in a close computer laboratory without any access to the internet while the teaching was done, but this is not relevant to the accusation made by the press as the students will still receive knowledge in a domain that is considered as troublesome and malicious by non-specialist. The fact that this course was allocated a special laboratory for conducting their experiments showed that the students were limited in the potential damage they could do by mistakes during the training and therefore prevent unexpected harm to any machines over the network. The quote "no one argues that criminology student should commit a murder to understand how a murderer thinks" reflect the idea described before, ones can be able to solve the issue only if he has the capabilities to understand the issue, the problem with this quotation is that in any case criminology student can commit the murder, however in computing the equivalent of the murder would be to infect or gain unauthorized access to a machine can be done in condition were no harm is done, by using this analogy the press had a direct association of learning computer security from the hacker point of view is the same as committing a murder.

The university was criticized by the press for running such a course because I assume thought it was like teaching how to be a black hat hacker [5] and access restricted information and machines. One on the issue with the media and more generally with the press is that when they are not specialized in computing they do not understand the difference between different types of "hackers". The press use the term hacker for persons downloading illegally right protected content over the network, persons that break security systems that should be called "crackers" and not hackers and the different type of attitudes in this community [8]. By not using the proper terms and sending the idea to the general public that a so called hacker is the one installing viruses on their computers, stealing their credit card information when they buy online is the reason why the university was criticized by the press. After a presentation of a great quantity of vulnerabilities in security holes in public and private systems in front of the Committee on Governmental Affairs of the United States Senate, Senator Lieberman said "It is probably not what you came to hear, but actually, I think you are performing an act of very good citizenship and I appreciate it." and Senator Thompson added "You are performing a valuable service to your country, and we appreciate that and want you to continue" talking about l0pht a grey hat hacking community. Grey hat in the hacking scene is practicing both black and white hat hacking without any difference the only criteria is that what they have to do must be challenging.

As a conclusion I think the university first of all misnamed the course it should have been something more like "Computer Security: approach of viruses and malware" to show that the course was to give a different point of view on how to approach computer security. However the courses intends was legitimate and has been proven in previous paragraph that security experts requires skills in this domain to be able to counterhack the possible attacks. The press took action against the university because their knowledge in computer security is probably limited and does not understand that this is required to secure their information.

[1]Security expert: Computer Scientists specialized in protecting the network against attack and discovering vulnerabilities, can be referred as "ethical hackers" are "white hat hackers".

[2]Black hat hackers: An individual who attempts to gain unauthorised access to a computer system for illegal purposes

[3]The Case of the Hired Hacker: http://www.fbi.gov/news/stories/2005/april

[4]The Kevin Mitnick/Tsutomu Shimomura affair: http://www.gulker.com/ra/hack/

[5]Reverse Engineering Hostile Code: http://www.symantec.com/connect/articles/reverse-engineering-hostile-code

[6]IPC Share Vulnerability: http://www.governmentsecurity.org/articles/hack-exploit-ipc-share.html

[7]Hacking – Hall of Fame: http://www.francesfarmersrevenge.com/stuff/misc/hack/hall.htm

[8]Internet Fraud Case – Citibank – Vladimir Levin
http://www.cab.org.in/Lists/Knowledge%20Bank/Attachments/64/InternetFraud-VL.pdf

[9] Hack, CounterHack: http://www.physics.ohio-state.edu/~wilkins/html/hackers/