Computer security and prevention of potentially harmful software like virus, malware and Trojans is a grey area in computing science and therefore an endless race between security experts [1] and black hat hackers [2] is taking place since the beginning of the 1980s. 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 topics 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] in corporations and bank details for individual. To prevent and more often solve the issues caused by such software a reverse engineering approach is used to understand the hostile code and see its impact and behaviour [5] on the infected machine; only a skilled person with strong knowledge in how such programs work can be able to understand the vulnerability used for the intrusion and then be able to fix it. That is why course in computer science should cover such matters to increase the understanding of the techniques used and their evolution over the years as the computing science field is still in its early stages and it evolves quickly. It is also complicated to dissociate some types of software from malwares, if you look by example at software like DameWare NT Utilities used for administrating and monitoring machines remotely and has been used the previous decade by hackers to gain access illegally to windows machines through the IPC$ vulnerability [6] and other machine where the remote control daemon software could be installed.

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 judged for their computers misdeed and served in prison, after their release most of them created computer security companies or have been hired by big companies to audit their systems. Vladimir Levin hacked Citibank's computers in 1994 and shown the vulnerability in their system at that time in the online wire transfer service, now Citibank uses Dynamic Encryption Card the most secured system used by no other financial institution in the world [8]. This shows that even if the act were initially malicious this community has been more efficient in detecting, exploiting and repairing security breaches than experts in this field and the current experts of our time are 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 acquire knowledge in a domain that is considered 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 that could be done 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 it is impossible for a criminology student to commit the murder without any permanent harm. However, in computing the equivalent of the murder would be to infect or gain unauthorized access to a machine and this can be done in condition where no harm is done. This analogy had been used by the press to establish a direct association between learning computer

security from the hacker point of view and committing a murder, where both are at the same level of immorality.

The university was criticized by the press for running such a course because from what I can assume, the press thought it was like teaching how to be a black hat hacker [5] and access restricted information and machines. One of the issues with the press and more generally with the general population media is that when they are not specialized in the domain of interest the information can be incorrect and misleading. Media generally do not understand the difference between what they call erroneously “hackers”. The press use the term hacker for people downloading illegally right protected content over the internet, people 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 the university was criticized by the press. After a presentation in front of the Committee of Governmental Affairs of the United States Senate of a large number of vulnerabilities and security holes in public and private systems, 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 criterion is that what they have to do must be challenging.

As a conclusion, the university first of all misnamed the course it should have been something more in the line of “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 course purposes was legitimate and has been shown previously that security experts requires skills in this ethically questionable domain to be able to counter-hack possible attacks and vulnerabilities. The action initiated by the press to prevent the University of teaching such a course shows that they do not understand this topic and that if their information and articles are well protected it is related to the effort of this security experts. With the details provided in the previous points and examples of how such professionals in security have contributed to this domain of computing and based on my own understanding of this topic, I can only support the university in teaching a course about “Computer Viruses and Malware”. More competent and directly impacted people than the press like the Committee of Governmental Affairs have already stated their point of view about computer security and audit and support such practices as it helps securing systems.

[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/