Almost every morning, we read news articles about hacking and virus damage or investigation of cybercrime. Considering contemporary high technology, it is natural that we ask a question, why is the Internet so weak? Recognizing the w eaknesses of ICT will be a good start to answer the question. The computer a nd Internet entailed explosive increase of traditional crime and enabled new typ es of crime which might not have ever happened without ICT. Roughly, there ar e 2 types of crimes. Old crime using ICT, and new crime aiming at ICT. The 1st one is that criminals use ICT as in instrument to commint a crime. The latter on e is that ICT becomes a crime target.

Characteristics of the Internet and Crime

Cybercrimes seem easier to commit than other crimes. It's probably because t he 3 characteristics of the Internet make criminal attacks in the digital world mo re common and widespread. Automation, action at a distance, and technique pr opagation are the 3 characteristics. First, automation. A crimainal can attempt to blackmail millions of internet users while he or she is sleeping after inputting a line of command on his or her computer to send emails automatically. Second, action at a distance. Blackmailed targets could be living on the opposite side of the Earth. Third, technique propagation The criminal might download the mailin g software and email addresses of the targets from a public website with a Ho w-To document. For all criminal activities of the Internet, the attacker is safe be hind an electronic shield, because the attack can be passed through many other hosts in an effort to disguise the origin.

Why Is the Internet so Vulerable

Next is, why is the Internet so vulnerable? Why is the Internet so vulnerable? There are numerous causes of ICT vulnerabilities that make equipment data inse cuer. However in general, the fundamental causes of vulnerability fall into 2 part s. The 1st cause is structural security loopholes, which is an invorn weakness of the Internet. When the Internet started as a military project in the 1960s, the n etwork was disigned for openness and flexibility, not security. So theoretically, o ne connected to the Internet, a computer can be reachable from any computer with no safeguard to avoid misuse.

And any Internet packet which actually contains a content of transmission is p

otential to be intercepted by anybody in the middle of the transport. Even thou gh a number of security counter measures were implemented to cover the inbo rn weaknesses, hackers and computer virus writers found security loopholes in t he Internet, enabling them to compromise computers, and corrupt data. It is qui te difficult to find a solution, because as security technologies developed, attack ers have also developed their techniques as well.

The 2nd fundamental cause is Insecurity in Software. Hackers found that they can realize their criminal intent through some sort of software bugs. A conserva tive estimate places the number of bugs in software at 5 per 1000 lines of cod e. This means your computer might have hundreds of thousands of bugs.