Cyber Security threats in the internet world

Recap

Security threats in the internet world is a very old news, since many important network (Nuclear power plant, Gas & Oil etc.) are being connected with cyber world the severity of threats are jumping up. Everyday millions of intelligent devices, enormous amount of data are being added to network; ensuring security for this vast amount of things is a very hard job. Moreover, hackers, criminals, terrorists are inventing smart way to achieve their goal. Commission of the European Communities categorize cyber-crime into three categories, traditional forms of crime such as fraud or forgery; the publication of illegal content over electronic media ; and attacks against information systems, denial of service and hacking.

Cyber espionage becoming very popular to obtain secret information from private citizens, competitors, groups, governments and adversaries for political, military or financial gain. Often we read news regarding espionage between USA and China. Sometime government espionages its citizens cyber activity to control media. All cyber related crime's target can be put in three major group, military targets, Political targets and society targets. The pictorial depiction below shows nearly all important network of our daily life is a subject of security threat.

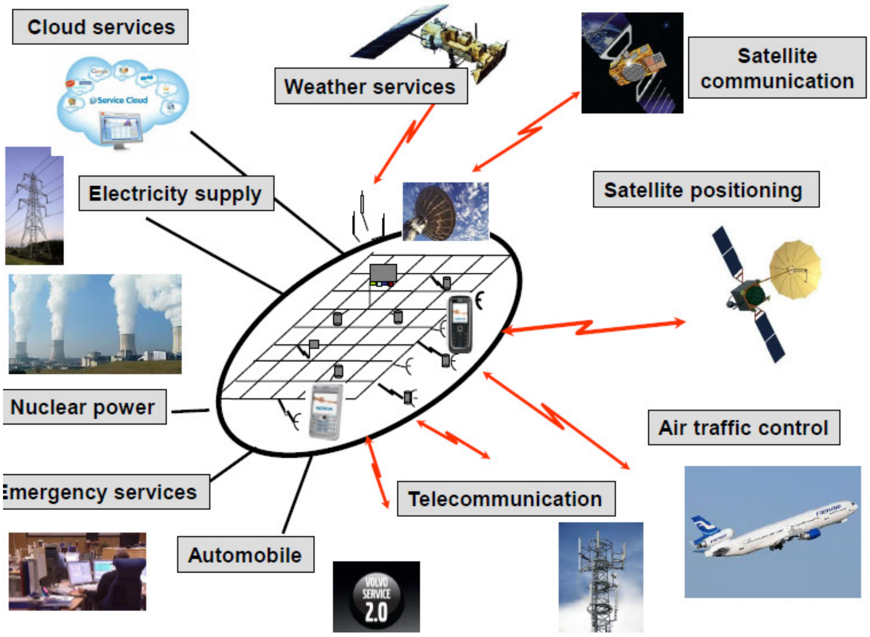


Fig1: Dimension of security threat

Since the Brain virus everyday new weapon are being added to empower attackers for cyber war, in the history of cyber attack Stuxnet worm is the most powerful one what has been used to attack opponents nuclear power plant. Production of malware has reached 200 million per year. But we should be optimistic and work on increasing security of our cyber asset to make a reliable, open and free digital society where business environment would be reliable and secure. Using advance technology, increasing competency, being tolerance, contingency planning and exercises to be able to operate under cyber-attacks could help us. Cyber threats will never be reduced; modern technology, smart human resource and precaution could be our weapon to avoid the threats.

Problem

All the concept regarding cyber threats were presented very nicely, but I felt the lack of information regarding problem of Big data threat, I mean the amount of unnecessary data what we are producing how that converting into threat to ourselves.

Perception

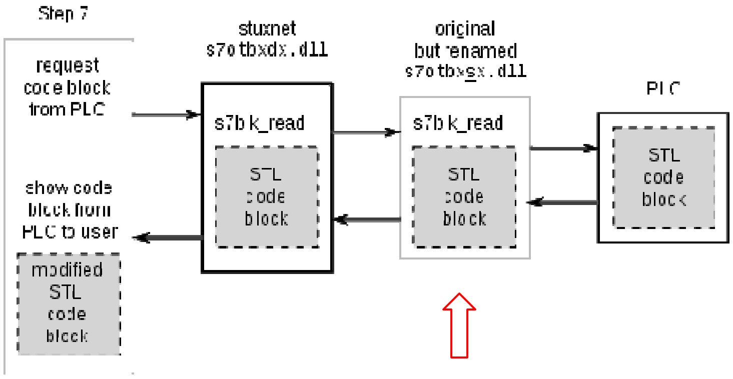
Almost all of us is victim of cyber related problem (e.g. virus, malware, spyware etc.). By some social engineering (Phishing, vishing , pertexting etc.) scammers are grapping valuable private information. January 2015, there was a heavy DDoS attack to two Finnish bank (Danske and Op) what lead to service interruption, hacker clamed 200 bitcoins. [1] Threat will be always there, we have to invent possible defence technique.

Deepening

Stuxnet malware was designed to attack industrial programmable logic controllers, Iran was the prime victim with suffered by 58% of total attack what damaged their approximately 1000 centrifuge out of 5800.[2] Stuxnet's target was Siemens step7 software in Windows operating system environment. It has three modules

- Worm , the main attack code
- Link file, to propagate copy of the worm
- Rootkit, for hiding all malicious files and process

it was exploiting by 4 zero day flaws. The worm increase operating speed of centrifuge from 1064 Hz to 1410 for 15 minute and then go for hibernate, again 27 days later it come to to attack by slowing down centrifuge speed to few hundred Hz . Once excessive stress then slower speed caused centrifugal tubes to expand, that going to fail within short time. If we look at the Stuxnet's hijacking communication it push its own code block between PLC and Step 7 software.



Siemens has released a detection and removal tool for Stuxnet and succeeded to remove this worm from 22 customers system without any adverse impact. Experts of EU and US said "Iranian engineers have succeeded in neutralizing and purging the computer virus known as Stuxnet from their country's nuclear machinery". Experts are also warning that, Iran may reengineering this cyber weapon to attack it's opponents.

Reference:

1. http://yle.fi/uutiset/op_still_under_attack_danske_bank_also_down/7720113

2. http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

Khandker, Syed Ibrahim

WISE