Information warfare

- The term information warfare refers to peace time activities
  - psychological operations (psyop)
  - cyber war/net war
- In wartime the term is Command, Control, Communications, Intelligence, Sensors Warfare(C3ISW)
  - military operations, like bombing communications infrastructure, throwing metallic fibre trash on radars
  - jamming radio communications
  - largely targeted to military command systems
  - and to communication system infrastructure
  - airplanes, trains, telecommunications
- Let us ignore C3 on this course and focus on information warfare.

Information warfare

- Who are the attackers?
  - not script kiddies, these are “harmless” hackers
  - not students/researchers hacking for curiosity and fame
  - BUT both groups of people could turn to cyber warriors
  - terrorists, the Internet can be an ideal terrorist weapon
  - activists
  - doomsday sects
  - foreign intelligence or information warfare groups
  - NONE of these groups are criminals, they all think they work for a good cause
  - can be criminals, for instance as hired cyber warriors
  - could it be some group of individuals spontaneously formed over discussion forums wanting to start a cyber war for personal reasons? (Scenario Pearl Harbor II)

Information warfare

- Goals
  - political and military goals
  - Claim: if the goals are to achieve a result,the attacker will use the easiest attacking method
  - Claim: if you have a goal, you probably know what you are looking for, there is no tourism on hacked computers
  - But: if the information warfare attack is a response to another attack, the attacker may not have any ready plans or goals.
- Notice, this may be different if the goal is
  - fame - you must use a method that impresses others
  - curiosity - you probably want to try some new method
- Notice, criminals will target banks etc. anything where there is money, probably not telecommunications. There is a difference in targets for a criminal and a terrorist.

Information warfare

- Strategies
  - This is not the same as goals, a strategy is a way to achieve a goal.
- Strategies of an attacker
  - destruction of communications infrastructure to pave way to a military operation
  - creating chaos - to prepare for a coup or revolution
  - creating losses - should be focused to crash the stock market
  - slow corruption -like to slow down technological development
  - obtaining funds to finance the activities
  - influencing the public opinion - leak to TV
  - influencing the decision makers - like by sending emails
  - use of insiders - find willing ones, buy them or spy from them

Information warfare

- Example: taken from the hypothetical Pearl Harbor II scenario
  - Send a new worm from many places at the same time, causes a global worm alert
  - Send fake emails and worms to the parties in the Middle East to have them blame each other -> crisis
  - Use insiders to mix up telephone call routing
  - Destroy satellite discs and telephone exchanges with small self-made bombs
  - Use insiders (subcontracted software development) to put bugs into products
  - Hack into credit card data bases and distribute the information to hackers, causes chaos
  - Engage other hacker groups to join into the attack
  - Use email to get people try if some stock market number has problems/ is now back in order

Information warfare

- Example: taken from the hypothetical Pearl Harbor II scenario
  - Leak the information that some company is under attack to news to add more chaos and get the shares value down
  - Cheat some employees to give passwords and mix up something, like routing, personal data, bills etc.
  - Cause a mass call to emergency numbers by mixing up routing
  - Distribute new viruses from free sex service sites
  - Reveal the sex service users to the families to create disturbance, send a copy to the police for illegal services to create more chaos
  - and so on, it is easy to add more attacks.
- The outcome: all but one of the 10 attackers were caught but they created 1 trillion dollar losses globally, but I think no real political/military goal was achieved. Pearl Harbor II not likely!

Information warfare

- Strategies of a defender:
  - more difficult for a defender: attacker only needs to find one hole, defender must succeed every time.
- BUT: usually it is true that every attack strategy can be countered by a defense strategy
- Examples:
  - If the defender uses tailored/unknown code, then the attacker must usually use insiders who have access to the code, then it is easier to find these insiders by elimination of alternatives.
  - This is an argument against open source as a method of protection. Proprietary code has more holes, only that they are typically found by insiders, not by blind walk. Then you have suspects. With open source the attacker can be anybody in the Internet.

Information warfare

- Examples:
  - A honey pot should catch any unknown viruses since they are not so clever that they would not enter the honey pot and no authorized user enters honey pots. Simply use behavior monitoring in the honey pot.
  - Now we have a detector for all viruses, compare this to detection by fingerprints (known viruses). This gives us a way to find new viruses and make an alarm.
  - Sniffing traffic is passive (like by IDS) and cannot be detected by the attacker. The defender then should detect if the traffic is odd. Maybe, the traffic is odd if it differs too much from what it normally is.
  - That is, make a predictor how traffic normally responds to cost, QoS, time of day etc. If your prediction fails, maybe it is an attack? How to do that, use a Kalman-type filter?

Information warfare

- Maybe then there are some mechanisms that can be used to build good intruder detection.
- For the time being, intruder detection is very poor.
- Example:
- US DoD tiger teams made a very large number of attacks to DoD systems.
- About 40% of the attacks were blocked by defense mechanisms (access rights, firewalls etc.)
- About 60% of the attacks succeeded, out of them only 0.7 % were detected.
- This gives some life time for an attacker: after a large number of attacks he will be noticed.
- Exercise, if a hacker is noticed by probability 0.007 each time and the attacks are independent, how many attacks he can make in average?

Information warfare

- Real examples of Information warfare:
- Psyops:
  - American solder body cruelly dragged in Somalia and shown in US television, US stopped the operation
  - Mexican Zapatists used the Web to advance their cause
  - Sri Lanka Tamil tigers spammed governmental mail boxes, an effective technique, used also later
  - In the Gulf war Americans spread the false information of a bug being planted to Irakian printers causing their LANs to be out of order.
  - In the Gulf war Americans demonstrated amphibian ability of their vehicles which they did not have.
  - In general, psyops is propaganda and influencing the public opinion. The Internet suits well to psyops.

Information warfare

- Real examples of Information warfare:
- Cyber war:
  - Hackers from the Netherlands hacked into US DoD computers, obtained masses of data and tried to sell to Irak, Saddam Hussein thought it was a trap and did not buy.
  - Spies are quite commonly used as they always were.
  - A school kid jammed the Warwick airport radar system for a prolonged time. No military goals.
  - Various hacker attacks with worms and DDoS tools.
  - American Information warfare attack in the Gulf war destroyed communication infrastructure if the Irakians, especially in Baghdad.
- We see that cyber war is not yet reality in military sense. C3 war is reality, so is intelligence and psychological operations.

Information warfare

- How information warfare differs from conventional warfare?
- asymmetric, small resources against a large army
- done already in time of peace
- no treaties or rules for this warfare
- will be one of the few ways a poor nation can attack a stronger computerized nation? then cyber war will be used
- for a terrorist cyber war may be preferred to suicide attacks
- cyber war is cheap, train the new generation of terrorist in computer science and telecommunications
- cyber war is like guerilla war, a modern army is not well prepared to fight such enemies
- less losses of lives, but not totally bloodless

Information warfare

- Consequences:
  - Good bye to the open friendly Internet?
  - Police and army will (must?) scan net sites, follow discussion groups, read emails and insert honey pots
  - More standardization in order to close the holes
  - More co-operation, like CERT teams
  - Persecution in court for computer crime, heavy punishments as deterrent
  - More traces will be left by using protocols, your activities can be tracked
  - The future views of information warfare do not make a pleasant scenario for someone just wanting to surf the web, use email and buy with credit cards from dot coms - armies and terrorist preparing strikes, other armies and police searching of offenders, but is there any choice?