# Social Security:
# Different Levels of Securities

Dulal Acharjee
Director and Professor
Applied Computer Technology, Kolkata, India.
Email: dulal@actsoft.org

## Introduction:

Providing social security is the concept of setting measures and precautions for the neighbors of a locality. When dangers come from different levels and damages are happened in any locality, then, it is very hard to trace the source of criminals. There are some attacks which come from top level and after passing many levels it finally executes to the target. This writing discusses some concept of multi level based attacks, related precautions, disinfecting the corrupted resources hired by intruders and developing awareness about multi level based attacks.

## What are multi level attacks?

When the attacker does not execute any damage directly but takes help of people (or resources) of different levels to hide the original planner is known as multi level attacks. Say, 'A' has planned to kill a person within the region of 'C', so, 'A' will hire one or more persons of 'B' region and 'B' will pass necessary information to 'C' for execution. With the help of a diagram, the concept is explained:

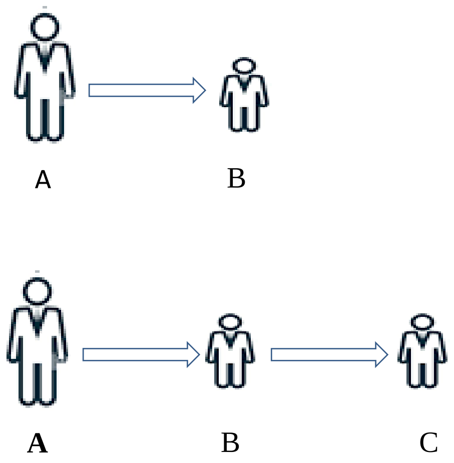

Figure-1: (a)two levels of network and (b)three levels of networks arranged by attackers.

In above figures 1(a), 'A' is known as planner and 'B' is executor. In figure 1(b) of three persons, 'A' is planner, 'B' is hired person and a sub planner, 'C' is executor. In both of cases, 'C' is executor and may be a person or an automated system like; bomb bursting remote circuit, automated firing device, car bomb with timer or any biological weapon which infects with time and weather etc. In case of automated system of 'C', it becomes harder to trace or find source of 'B' and 'A', because, after action, 'C' is fully damaged and scattered where forensic investigation may find causes of explorations but traceing network link of 'B' and 'A' is the hardest job.

**Properties of B:** he is hired or trained and motivated to do some attacks. If 'B' is a paid person, he will wait for collecting evidence of damage or explosion which will ensure his rest payment. If 'B' is a member of a political party or a member of a terror organization motivated politically, he will not wait to collect evidences of damages. He will collect information from other sources like TV, Radio, paper news etc. The most intelligent network designing depends of 'B', if 'B' is a flying man or a roaming man who changes his position time to time, then, investigation of explosion(as example) becomes hardiest.

**Delinking Netwok:** In fig-1(a) there is one link as A-B; if it is thought from the concept of communication technology, there are two channels of communication between A and B and these are A-B and B-A known as uplink and downlink. It means, before attacks, both channels remain active for setting plan of execution, but, after execution, either both channels or one channel is dislinked or destroyed for hiding information about source of attackers. In figure-1(b), there are two links A-B and B-C, it is assumed that there is no communication between A-C as because, 'A' has hired 'B' to execute with the help of 'C'. In this network 'A' wants to remain as hiding himself. When all plans and execution rights are handed over to 'C', then 'B' may delink the link B-C and A may delink A-B or they may delink both up and down channels as shown below.

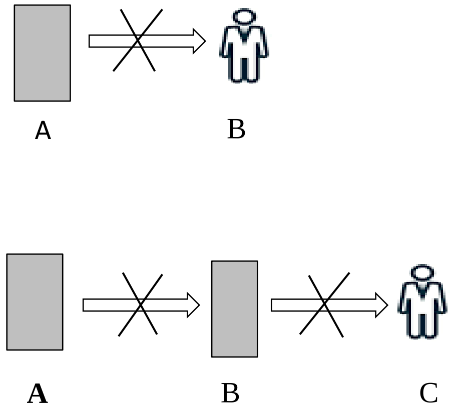

Figure 2. (a)after completion of attacks A disappears and link of A-B is disconnected. (b) a model of hiding A and B and disconnecting links of A-B and B-C.

## Gathering information:

Collecting information about suspected persons or events is a legal work. Have we permission to collect data and store in a Server of computer of a person or a locality? Can we process data for finding facts? If so, a database is required to create with many data files with different column heads. For setting precautions of any attacks or accidents which may happen over a stage or market place, some measures are suggested below. A possible schema of a data-table of stage/locality where any event will be organized is mentioned below:

Stage_type: may be at play ground, inside a open Banquet, on a permanent stage

Background: cemented wall/false wall/cloth-cover/open

Under_stage: open/covered sides/cloth-cover/

Rightside: open/cemented wall/covered sides/cloth-cover/

Leftside: open/cemented wall/covered sides/cloth-cover/

Top: open/covered sides/cloth-cover/contents of top

Outside_of_stage: gas/kerosin-oven/welding machine/open-road

Load_capacity: tested/person capacity/overload-control-by-whom/

Hanging_Fan: tested/permanent or not/temporary hanging/

## Conclusion:

Here, some information are compiled, but not limited to. These are some primary investigative points which should be checked by security personnels or volunteers before performing and event. It is suggested to gather these information either as manually or automated and structured way to storing within a computer system. Awareness starts from discussion level and then gradually takes into automated system. The organizers of the event and the participants all should be aware about their securities; if people become awared the possible dangers, then only volume of damages will be minimized.

***END***