Report of Break-Out Group 1

Network Vulnerability and Risk Assessment

Randy G. Alward
Canada

Kathleen M. Carley
Carnegie Mellon University
USA

Fredrik Madsen
Aalborg University, Esbjerg
Denmark

Vincent K. Taylor
Defence R&D Canada
Canada

Grant Vandenberghe
Defence R&D Canada
Canada

1 OVERVIEW

To help understand a network and its ability to continue operating when under attack, the break out group discussed issues that need to be considered when presenting network vulnerability information to an analyst, manager or commander in effective support of that person's "observe, orient, decide, action" (OODA) loop. The break out group discussed vulnerability presentation needs common across various application domains, particularly in support of network discovery and network analysis tasks in those domains. Finally, the break out group wished to determine whether there is a means of characterizing a vulnerability. This would take into account the potential for the vulnerability to be exploited as well as the potential impact on the operations supported by the network, and on the network structure itself, of a successful exploit of that vulnerability.

2 GENERAL

The following types of networks were considered by the working group:

- information systems
- computer/security network
- road infrastructure
- power grid
- social networks
- semantic networks
- supply chain/logistics
- knowledge networks (who knows what, when)
- precedence networks (Gantt charts)
- traffic controls - e.g. passenger flows through locations (e.g. airports)
- shop floor optimization
- software networks
- medical - e.g. disease propagation

Although these various types of networks were considered, the working group focussed mainly on computer networks and social networks; other network types were used to provide examples or counter-examples during discussion while trying to bring out general network characteristics.

In understanding a network, certain presentation issues arise. On the basis that a network consists of nodes and links, one needs to be able to represent the various characteristics, both behavioural and physical, of these elements. What is represented and how it is represented is also impacted by the role of the observer, whether analyst, manager, commander etc.

A network vulnerability is a weak point in a network that may be exploited, either by designed action of an adversary or by accident, to affect the operational capability or trustworthiness of that network. For example, a network may be vulnerable because of its architecture - e.g. the network is not designed to be robust and has one or more single points of failure. A failure at one of these points would lead to denial of service within the network. A network could have weaknesses in its engineering and implementation - e.g. a hub is designed and implemented to handle a certain volume of transactions and has not been designed to handle transient overloads. Or, there might be a security flaw or process flaw in software or hardware within the network that could allow an adversary the opportunity to compromise the network through the use of appropriate threat agents.

A network vulnerability is not important in itself, but only with respect to its potential to be an access point for a threat agent to try to compromise in some fashion the confidentiality, availability, integrity and authenticity parameters of the network or its network services. The criticality of a vulnerability, then, is some measure of the impact that a threat agent that exploited the vulnerability could have on the operations the network supports while also considering the likelihood of that vulnerability actually being exploited.

Adversaries may exploit vulnerabilities to threaten or attack a network. In some cases, the source of the threat and the target may share the same network. For example internal computers in a computer network might be vulnerable to a threat from the Internet. In contrast, there are other kinds of network where the vulnerability may be exploited from outside the network. For example, in a utilities network a terrorist who is external to the electrical grid can blow up an overhead power line at will. The threat source has a direct bearing on how vulnerabilities are employed in combinations on a network. Threats that originate inside the network tend to have the ability to exploit vulnerabilities in a serial form. This allows the attacker to traverse or "leap-frog" across the network to an advantageous position. Threats that originate outside the network tend to exploit vulnerabilities in a parallel fashion. For example a terrorist could blow up multiple sets of power lines to disrupt power to a base.

An adversary will exploit a vulnerability to achieve a desired end which could include:

- obtaining information or capability;
- withholding information or capability;
- disseminating information or capability;
- misleading/misinforming/altering information or perceived capability;
- gaining control of the network;
- Sabotaging the network - e.g. deleting/corrupting data, disabling/destroying equipment.

Although many network vulnerabilities exist, only a fraction of them will be exploited by an adversary. Risk Assessment measures the likelihood that a vulnerability will be exploited. Standard risk assessment takes into account the five key questions listed below to give the observer, whether analyst, manager, commander etc., the basis for making a situation evaluation.

- How can the network be attacked through the vulnerability?
- Why would the network be a target?
- When can one expect an attack to take place? How long would it take an attacker to develop the appropriate threat agent(s) and prepare the attack?
- What capabilities of the network can be disrupted or impacted?
- Who may be affected by an attack? What operations will be impacted? How serious may the impact be?

3 COMPUTER NETWORKS

With respect to computer networks, there are at least seven different views that can be taken: cable plant logical diagrams, topology map/logical network diagram, service map, operational diagram, geospatial view, physical network diagram and authority diagram. Links connect nodes. Links may be bidirectional - i.e. information may flow between its endpoints in either direction, unidirectional - i.e. directed or hierarchical, switchable - i.e. unidirectional with the direction switchable upon some event, time sensitive - i.e. not necessarily there all the time. There may be multiple links, each with its own characteristics, joining the same nodes. Link characteristics could include capacity, length, strength, constraints, usage cost, end point name/alias etc. Nodes could be root nodes, leaf nodes, border nodes etc. These tend to have different characteristics and may require different methods of presentation, depending on the observer's task.

Most practical networks are too complex to be presented in total at any one time and so some method of consolidating information needs to be used to allow meaningful observation of the network, while at the same time allowing specific areas of interest to be readily available. Depending on the role of the observer, consolidation could be based on routing, location, service relationships etc.

4 SOCIAL NETWORKS

A key to destabilizing a social network is to recognize that it is not a single network, but rather an overlapping set of relations. These relations might include financial - e.g. who lends money to whom - , friendship, kinship, advisorial, etc. The vulnerability of the social network depends on both how these overlap and the structure of each of these separately. For organizations, cities, states and indeed any group - the higher the overlap in these networks, the more vulnerable the group; more prone to larger, more violent disruptions. The more the networks counterbalance, the more stable the group.

For any one of these networks, vulnerabilities can be identified using social network and dynamic network techniques. In general, network destabilization depends on the type of nodes and links. Different metrics are needed for different networks to identify key vulnerabilities. At its simplest, networks can be destabilized by adding or dropping nodes or links, over- or underusing certain links or increasing or decreasing the amount of processing needed at certain nodes. Identifying which nodes or links should be added or dropped, or for which the associated activity should be increased or decreased requires knowing both what the desired effect is, what is flowing through the network and knowing the structure of the network.

For example, imagine three different flows: disease, data, money (or other physical resource). Each of these flows has different transmittal properties. Imagine two nodes - A,B. If "x" flows from A to B, then the following transmittal properties need to be defined:

- after A sends "x" to B, does A retain a copy of "x"?
- can a node, A or B, get a second copy of "x"?
- how long does it take for "x" to flow from A to B?
- what logic defines why A sends "x" to B?

Differences across flows can be seen in Table 1.

	Retain	Require	Length	Logic
Disease	yes	no	fast	contact
Data	yes	yes	moderate	homophilly[1]
Money	no	yes	fast	request

Table 1

This table is not perfect, but is just meant to indicate that even for the same structured network, the transmittal properties of the flow will impact what nodes are critical. In reality, it is even more complex as the timing, strength and the technology used for connecting nodes is also relevant.

There are at least two implications. First, structural factors alone don't determine vulnerabilities. Thus for example, one cannot assume that network hubs - i.e. highly degree central nodes - are the points of vulnerability. Second, basic research needs to be done to define those factors, e.g. characteristics of nodes, links, networks, flows that determine which nodes or links are critical to give the desired effect.

Another key aspect of social network vulnerability is that it doesn't depend on just the "social network" - i.e. the connection between actors. It also depends on the other networks to which the social network is attached - e.g. the knowledge network (who knows what) or the task network (who is doing what).

	Actors	Knowledge	Tasks
Actors	Social network	Knowledge network	Task Assignment network
Knowledge		Information network	Needs network
Tasks			Precedence network

Table 2

[1] the tendency for people with greater common knowledge to interact

The same social network will be more or less vulnerable depending on the distribution of knowledge and tasks across actors. For example, in hierarchies, the impact of removing the CEO/commander depends on the complexity of the task being done by the group and the distribution of data. When specialized data only exists at the top level in a hierarchy, removal of the commander is more devastating than when no specialized information is at the top.

Points of vulnerability for social networks also depend on where they are in their life cycle - forming the network, maintaining it (education, enculturation, recruitment), activating the network to take action, and dissolving the network. Typically, destabilization is not concerned with the last of these. At different points in its life cycle, different parts of the network are visible and the network is easier/harder to infiltrate.

Since networks interrelate, that fact can be used to identify potential vulnerabilities. For example, using the knowledge and task networks, you can identify an expected social network. This can be contrasted with the observed network. The difference suggests potential vulnerabilities - i.e. those interacting more or less than appropriate (needed) for their jobs.

As an aside, within groups, the most likely "source" to disrupt an information or computer network is a disgruntled employee or team member. The disgruntled team member can often be identified as someone interacting less with other team members than is to be expected.

5 COMMON THEMES

- Identifying vulnerabilities in one network may require understanding of how it links to other networks. Need to be able to visually tour through the networks.
- All networks are vulnerable in many ways. The issue is not where are the vulnerabilities but how to locate a particular type of vulnerability.
- Across all networks, trying to understand vulnerabilities by assuming the network is random will lead to misleading results.
- Across most networks, many critical vulnerabilities are overlooked by assuming that the network is scale free and that the hubs are the only source of vulnerability.
- Need to be able to visualize multiple types of nodes, criticality, directed/weighted links, node attributes, uncertainty, etc..
- Need to be able to visualize network dynamics dynamically.
- Need to be able to drill down in a network diagram to get additional information, see related networks and find information on sources etc..
- To control the flow of "x" through the network - e.g. goods, people, errors - you want to be able to visualize a large portion of the network, notice bottlenecks, identify key elements, characteristics etc..
- To understand, manage and/or assess vulnerabilities, you need data on the "large" network.
- Each use of the same "network" data may require a different way of visualizing the data - e.g. seeing propagation as "lights" moving through the networks or seeing critical nodes in a particular structure.
- There are a number of different ways of viewing most networks: e.g. geo-spatial, transactional, operational, logical, propagational. Whether or not one wants to see a particular view varies with the role and intent of the viewer.

There are numerous combinations of presentation and algorithmic techniques existing today that go a long way towards providing the tools to meet today's basic visualization needs. However, a lot of work still needs to be done to harness these techniques to present vulnerability and risk information in a meaningful way within the various network domains in a form immediately accessible in an interactive manner to the user, whether analyst, manager or commander etc..