

Towards System Survivability using the Single Virtual Enterprise Model and Layered Security through Information Protection Co-ordination Centres

Submitted by:

Donald MacLeod
Department of National Defence
Communications Security Establishment
Ottawa, Ontario, Canada
Donald.MacLeod@cse-cst.gc.ca

David Whyte
Department of National Defence
Communications Security Establishment
Ottawa, Ontario, Canada
David.Whyte@cse-cst.gc.ca

© Minister of National Defence, on behalf of Communications Security Establishment, Canada, 2000.

In consideration for this workshop, we submit the following position paper. This paper should not be taken or interpreted as representing the views of our employer, the Department of National Defence / Communications Security Establishment, nor those of the Government of Canada.

Donald MacLeod is a Security Architect for the Communications Security Establishment. He has a degree in Computer Science from Acadia University with eight years experience as a system administrator. His most recent work has been on researching the application of intrusion detection technologies to large cross jurisdictional systems in support of Critical Information Infrastructure Protection for the Government of Canada.

David Whyte is a Security Architect for the Communications Security Establishment. He has a degree in Computer Science from the Technical University of Nova Scotia with three years experience as a certifier for the Canadian Common Criteria Scheme. His most recent work has been participating in the development of Information Protection Centres (IPC) in support of Critical Information Infrastructure Protection for the Government of Canada.

The majority of computer networks can be characterized as unbounded heterogeneous environments, highly distributed and extremely complex. They are also becoming increasingly harder to secure. Even system owners that use the latest and best available information to protect their systems have no guarantee that they are invulnerable to attacks. History has shown us that vulnerabilities will occur in complex computing systems, often in unpredictable ways, and that malicious actors will exploit them for personal gain.

Critical Information Infrastructure Protection (CIIP) is the field of identifying and safeguarding information technology assets. A fundamental concept of CIIP is that it can be viewed as a series of security layers that are either technical or organizational in nature.

This layering is also known as layered network security. Layered network security involves the strategic deployment of a variety of security countermeasures. This reduces the risk associated with the failure or penetration of any single technology or layer. In practice, security services are not independent of one another nor do they work in isolation. The countermeasures employed to achieve layered network security can be regarded as effective if they enhance the systems ability to fulfil its mission. Although layered network security is a critical component of CIIP it is not the focus of this paper. The objective of this paper is to present an organizational framework that will aid in achieving system survivability.

A key component of system survivability is the coordination of security measures across the various components of the system. One method of achieving this coordination is through the use of an Information Protection Coordination Center (IPCC). The IPCC provides coordination services to a network comprised of all the networks under the jurisdiction of the Information Protection Centers (IPCs). In effect, this creates a Single Virtual Enterprise Network (SVEN).

The primary function of an IPCC is to coordinate security services amongst Information Protection Centers (IPC) that share some common attribute. For instance, a Federal Government could deploy an IPCC to provide coordination among its departments. Proper coordination ensures the right information reaches the right organization in a timely manner. This allows informed decisions to be made on the prevention, detection, response, and recovery options to be undertaken. The ideal solution, from an operational and timing perspective, is to have mechanisms in place to disseminate information directly to the applicable system administrators. The processes to enable this dissemination can be automated, manual or a combination of both.

The primary function of an Information Protection Center (IPC) is to provide real-time security services to the individuals directly responsible for the operation and networking of the systems. The IPC may be responsible for a single network or multiple networks.

In our model, the IPC accomplishes this by actively collecting data from a range of security technologies deployed in its networks such as of IDS, firewalls and server logs. This data is used to detect any security incidents on the network, and to initiate local response and recovery procedures. The IPC will keep the IPCC informed of all incidents within its jurisdiction, and will send all collected data to the IPCC for long-term trend analysis.

The IPC / IPCC concepts are built on an active security cycle that consists of four phases: Prevent, Detect, Respond, and Recover. The active security cycle is the underpinning of an effective security posture. Interactive real-time security is the goal of an IPC, and the active security cycle assists in achieving this objective. Examples of the type of activities that would be undertaken at each phase are:

- Prevent: the application of hardening best practices and proper user authentication methods;
- Detect: the use of data fusion to combine the logging capabilities of firewalls, intrusion detection sensors, and other logging mechanisms;
- Respond: the development and documentation of incident management procedures;
- Recover: the development and documentation of system recovery procedures.

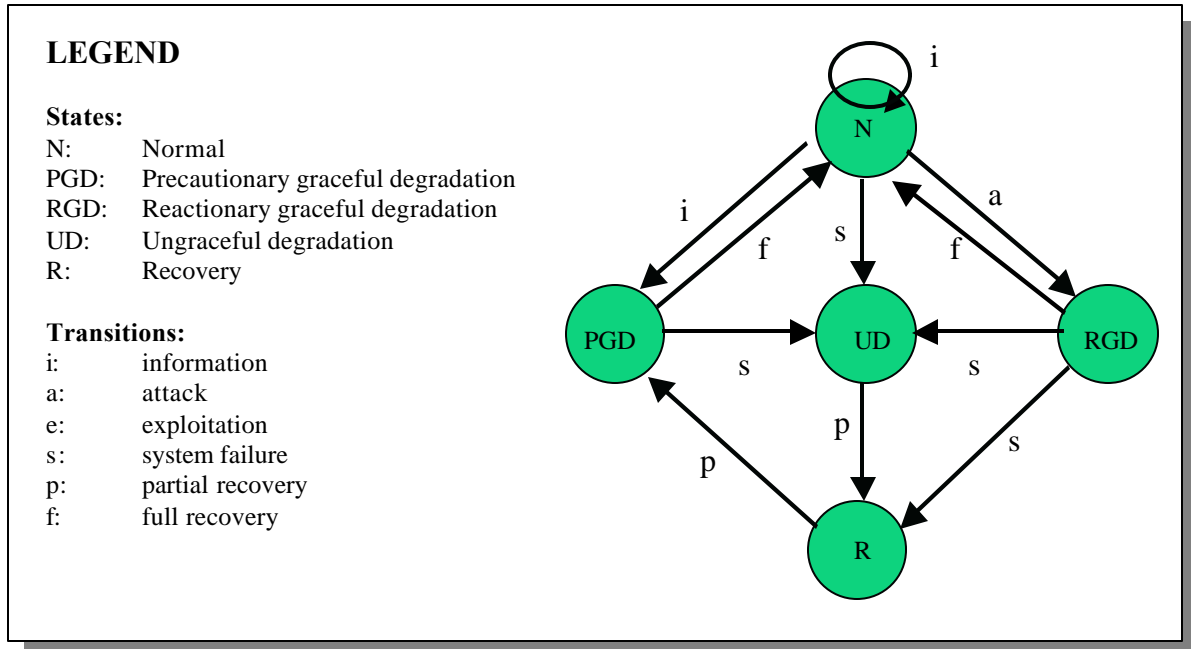
Based on the premise that vulnerabilities will always exist, the SVEN model strives to minimize the likelihood that a vulnerability will occur, the length of time that the vulnerability exists within the system and the extent to which the system is unable to fulfil its mission in the event the vulnerability is exploited.

Figure 1 exhibits the SVEN state transition model. The model can be applied to a single network, multiple networks under the auspices of an IPC, or multiple IPCs under the auspices of an IPCC.

SVEN is modeled using five distinct states:

- Normal(N): normal. The system is able to deliver its mission critical functions.
- Precautionary graceful degradation (PGD): precautionary controlled graceful degradation state. Measures are taken to address the vulnerability whilst still performing mission critical functions.
- Reactionary graceful degradation (RGD): controlled graceful degradation state. Measures are taken to fend off an attack whilst still performing mission critical functions.
- Ungraceful degradation (UD): uncontrolled degradation state. The system fails to deliver its mission critical services.
- Recovery (R): the system is repaired to remove the damage caused by the vulnerability being exercised against the node. Mission critical functions resume after recovery is completed.

Figure 1: SVEN state transition model



The normal state for the system (N) can be defined as the unimpeded fulfillment of its defined mission. From this state the IPC analyzes its security logs and the alerts, advisories, or other administrative information from its IPCC. This information is then assessed for its potential impact. If the assessment does not indicate any action be taken, the system remains in the *N* state.

If the information indicates that a new vulnerability exists that could impact the system, the state changes to the precautionary degraded state (*PGD*). Measures are taken to address the vulnerability whilst still performing mission critical functions. If the vulnerability is adequately addressed the system will return to the *N* state.

If an actual attack is directed against the system under the IPC's auspices then the system changes to the reactionary degraded state (*RGD*). Measures are taken to fend off the attack whilst still performing mission critical functions. If the attack is adequately addressed the system will return to the *N* state.

If vulnerabilities or attacks cannot be addressed and mission critical functions fail, the system will enter the ungraceful degraded state (*UG*).

Once in the *UG* state, measures must be taken to restore the system to full capabilities. These measures are implemented in the recover state (*R*). Once all capabilities are restored the system moves into the *N* state or if the threat still exists, to the *PGD* state.

A system that reports an ungraceful degradation to its IPC (or IPCC) although unable to fulfill its mission still accomplishes a greater good. Details of the event that caused this interruption in service will be shared among all constituent members of the IPCC. This will allow other IPCs to implement appropriate countermeasures to minimize the likelihood of this occurrence on their own network. The alternative to this model is non real-time information sharing that will lead to slower reactions, data interpretation issues, and thus more ungraceful degradation.

In practice the IPC/IPCC concept will minimize the amount of the network that will have to enter the recover phase. An initial compromise of any node in SVEN triggers a near real time response in all the other nodes that leads to an immediate heightened awareness. The network is able to alter its security posture in response to specific vulnerability or attack information obtained from one of its nodes. The network can correct the vulnerability or defend against the attack, and recover the compromised node(s) while maintaining the majority of its mission critical functions.

The IPC/IPCC paradigm directly supports the concept of survivable systems. System survivability can be defined as “the capability of a system to fulfill its mission in a timely manner in the presence of attacks, failures, or accidents.”¹ SVEN is an unbounded network and does not rely on centralized control; it relies on collaborative interactive information sharing. This information sharing, over time, forms a vulnerability early warning system through a centralized web of trust.

With the IPC/IPCC paradigm, network owners have the benefit provided by a service of aggregate traffic analysis from outside their perimeter. A scan that they might otherwise ignore locally could be detected as part of a larger industry sector or national wide effort. This could provide the time required to implement preventative measures. Under this model, participating system owners have the additional benefit of centralized vulnerability analysis capability.

Conclusion

As demonstrated in this position paper, the IPC/IPCC layered security concept can provide a component of survivable systems. It provides a trusted form of vulnerability prediction to allow the system or system of systems to take proactive preventive countermeasures to ensure continuation of service before a vulnerability within the system is exploited. The vulnerability can be actively defended against and the mission critical functions maintained. While the active security cycle of Prevent, Detect, Respond, Recover provides a methodology to help in effective incident response, the IPCC concept extends this by providing good technical information in a timely fashion to the system operations personnel. The initial compromise of any node in SVEN triggers a near real time response in all the other nodes. This will minimize the amount of the

¹ Survivable Network Systems: An Emerging Discipline, CMU/SEI-97-TR-013

system that has to enter the recover state thus precluding the execution of mission critical functions.

The SVEN concept accepts the fact that individual systems will be compromised despite the best security practices of its designer, administrators and users. With near real time communications among a trusted web of technical experts, the spread of the compromise can be drastically limited.