IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4213

Integrating Cooperative Engagement Capability Into Information System Security

Alexander D. Korzyk, Sr.
Department of Business, University of Idaho, Tel: (208) 885-5958, akorzyk@acm.org

ABSTRACT

The US military's concept of a Cooperative Engagement Capability should serve as a useful referent for those attempting to design/develop large scale, organization-wide information security systems. This concept involves centralizing command over the entire suite of defensive assets (naval, air, ground) available in some region or locale; whenever a threat is directed against any US force element (a ship, an infantry unit, etc.), this central authority would then be expected to direct the deployment of whatever appears to be the most efficient countermeasure…in light of prospective as well as actual threats. This is a dramatic departure from the traditional decentralized approach, whereby each force element was expected to draw on its own defensive measures to counter any threat directed at it from any source. Industrial/commercial organizations might draw on the logic of the Cooperative Engagement Capability (CEC) logic in devising a system to secure its informational assets.

COOPERATIVE ENGAGEMENT SECURITY

Macrocybernetic Security

The use of macrocybernetic theory for corporate information system security may allow the use of CEC-like logic for securing enterprise-wide informational assets of industrial/commercial organizations. A set of sensor/engagement function specific security subsystems with the macrocybernetic (supra system) [Sutherland97, p. 218] would handle the fusing of integrated multimedia data sources and invoking real-time multi-countermeasure subsystem responses without human intervention. The enterprise system protected information system boundary includes all the subsystems such as network subsystem, database subsystem, application subsystem, and security subsystems. The network boundary includes both intra- and inter-organizational networks up to and even through the Internet/Information networks. The database boundary includes client/server and Internet databases. The application boundary similarly includes client/server and Internet applications. Within each of these subsystem boundaries a microcybernetic structure handles sensor data. Interfacing subsystem's security data received from a database sensor and a network sensor requires a macrocybernetic to handle integrated sensor data. Integrating information systems security subsystems from multiple information systems within an organization necessitates a supra macrocybernetic to handle engagement data. At the inter-organizational level required for FBI and local authority coordination, humans from the corporation, FBI, and local authorities must become involved because of socio-political ramifications [Armstrong00, p.24]. This involvement may simply be the corroboration of a recommended countermeasure to be executed by the supra macrocybernetic. The result is an ensemble of interconnected sets at the supra macrocybernetic level representing cellular structures [Sutherland98, p. 166], which are the information system security subsystems.

Engagement Macrocybernetic

The corporate enterprise system would contain the engagement cybernetic, which would be based on the threat and synthesized countermeasures primarily for active and restorative countermeasures. The macrocybernetic would determine the sequence, length, and intensity of the engagement. Some rules of engagement could be mode based. A decision to engage covertly to gain counter-intelligence (industrial espionage) information prior to choosing the best course of action may only be acceptable for unknown or not recognized threats. A decision to engage by pursuit may involve calling in for reinforcements (FBI and local authorities). The CEC-like common security picture may involve other organizations such as the FBI and local law enforcement officials coordinating information security subsystem sensor data to obtain total awareness of the intruder and his intentions. The decision then could be to set an ambush with the cooperation of the FBI and local authorities [Korzyk00, p. 74]. The engagement macrocybernetic could also choose a restorative measure. The macrocybernetic could predict that the damage from the threat would be such that the best course of action is to allow the attack to proceed and use the containment rule of engagement. If the macrocybernetic uses the containment rule of engagement then the system must try to limit damage, maintain system availability, and allow recovery of full operating capabilities as soon as possible [Jajodia99, p. 73].

EFFICIENT ALLOCATION OF COUNTERMEASURES

A countermeasure is a safeguard achieved through adding a step or an improvement in system design that mitigates or eliminates the vulnerability making the threat irrelevant or reducing the damage from the threat to acceptable levels [National Research Council91, p. 13]. Countermeasures are the union of passive, active, and restorative countermeasures $C \in C_A \grave{E} C_P \grave{E} C_R$ as shown in the Enterprise System Security Planning Model [Korzyk00, p. 75]. The use of countermeasures involves a cost for each countermeasure. The maximum utility function, noted as $Utility_{max}$ $[C_1, C_2, \ldots C_n[T]]$, determines which countermeasure provides the maximum utility to counter the threat at an acceptable risk and cost. Thus, the resource or asset chosen to counter a threat would be made on efficiency criteria rather than a response from the attacked system. Each major type of countermeasure involves more than just risk and cost. The maximum utility function, $Utility_{max}$ $[C_1, C_2, \ldots C_n[T]$, uses the multi-criteria function, $f_{mc} = a + b + f + l + s$, where a = {cost of implementing $C_n[T]$}, b = {future likelihood of recurrence}, f = {known second order effects}, l = {the likelihood of concurrent SI in the enterprise}, s = {minimum exposure time}. The synthesized enterprise system security array uses the results of the multi-criteria function with the minimum expected value $E(V)_{min}$. The multi-criteria function includes the decision to use one or more of the following countermeasures.

Passive Countermeasures

A passive countermeasure, C_P, is defined as a safeguard achieved through safeguards taken to prevent the threat from exploiting the vulnerability, safeguards taken to prepare for the threat, safeguards taken to detect the threat, or safeguards taken to protect the system during the security incident. Defending is almost always less expensive than counter-attacking. Current techniques and tools require human corroboration to counter-attack. As techniques and tools for intrusion detection become adequate enough a macrocybernetic structure could determine if there was enough intelligence to switch from passive to active mode.

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference.

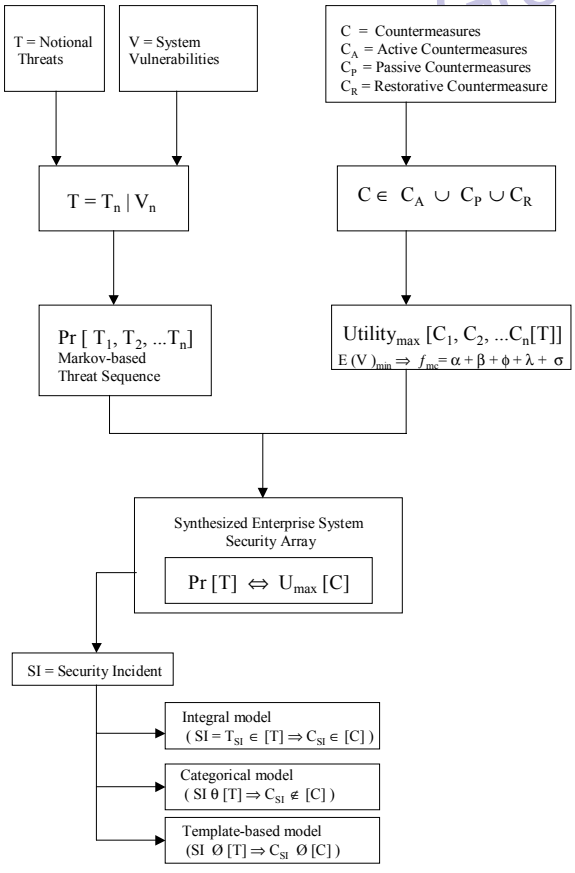
Active Countermeasures

An active countermeasure, C_A, is a safeguard achieved through safeguards taken immediately to respond to the threat upon exploitation of the vulnerability (reactive), safeguards taken to remediate or stabilize the system enough to continue information operations, safeguards taken to isolate the point of penetration and then track the attacker as long as the attacker is in the system, safeguards taken to counter-attack and if successful pursue the attacker to expose the attacker's identity to law enforcement officials. Active countermeasures also include covert security safeguards taken to confuse and expose the attacker, which enables the attacked organization to gather counter-intelligence about the attacks unknown to the attacker (proactive). This employs the military strategy of cooperative engagement capability because while the attacked company lures the attacker to a fake site or an ambush site, a cooperating agency from the National Infrastructure Protection Center, such as the FBI could be gathering real-time intelligence on the origin of the attacks. This places the cooperating agency in an advantageous position over the attacker.

Restorative Countermeasures

A restorative countermeasure, C_R, is a safeguard achieved through containing or limiting the extent of damage caused by the security incident, a safeguard achieved through quarantining or shutting down services provided by the system in order to prevent catastrophic failure (failsafe). If an enterprise system has deliberate redundancy designed into it, then the damage to the operational system can be minimized by the immediate shut down of the attacked system and instantaneous cut over to the backup or redundant system. For example, shutting down the email server to prevent the further spread of a virus, which attaches itself to email messages, a safeguard achieved through reconstituting the system with resources remaining that are still able to function or operate adequately and a safeguard achieved through recovering from the security incident as quickly as possible, e.g., installing security patches for the operating system or updating anti-virus files.

Figure 1: Enterprise system security planning model



ENTERPRISE SYSTEM SECURITY ARRAYS

The synthesized enterprise system security array consists of the threat array and the countermeasure array. The threat is assigned a probability of occurring given a vulnerability. A Markov based approach will model the threat sequence over time. Countermeasure interdiction too late in the threat cycle could lead to a serious degradation of available countermeasure at a much higher cost, possibly catastrophic. Countermeasures interdicted too early may change the attacker's strategy for the worse. Since the Markov based approach models state-level transformations, it can be used to decide which countermeasure method to use against the threat. Using high cost countermeasures against a low-level threat, which could just be a decoy, could leave the enterprise system in the horrible position of just having used all available high cost countermeasures against lower level threats when a larger threat follows with just low cost countermeasures left. Those remaining countermeasures are known to be ineffective against the larger threat, thus leaving the enterprise completely exposed to the primary attack. The cooperative engagement capability may have allowed the enterprise system to more efficiently allocate the countermeasures to produce the best performance with minimum damage and at minimum cost.

The [T] × [C] Array is the cross product of the threat array and the countermeasure array producing several combinations to be used by the cybernetic mechanisms. The countermeasures used by the macrocybernetic entity model depend upon the probability of whether the particular threat and countermeasure combination exist in the synthesized enterprise system array noted as Pr [T] $\Leftrightarrow$ U_{max} [C].

MODEL BASE SECURITY STRUCTURES

The integral model provides countermeasures for a fully predicted security incident. When the threat is known, given a certain vulnerability and the countermeasure for that threat is known given maximum utility constitutes a fully predicted security incident noted as ($SI = T_{SI} \in [T] \Rightarrow C_{SI} \in [C]$).

The categorical model provides countermeasures for a partially predicted security incident. When the threat is within a certain range or category of threats, given a certain vulnerability, but the countermeasure for that particular threat is not known for a certain threat but are known for a range or category of threat constitutes a partially predicted security incident noted as ($SI\ \theta\ [T] \Rightarrow C_{SI} \notin [C]$).

The template-based model provides countermeasures for an unpredicted security incident. When the threat is not known within a certain range or category of threats, or vulnerabilities for the unknown threat are not known and the countermeasure for the unknown threat is not known constitutes an unpredicted security incident noted as ($SI\ \varnothing\ [T] \Rightarrow C_{SI}\ \varnothing\ [C]$).

CONCLUSIONS

The use of Cooperative Engagement Capability logic clearly shows great potential for preventing the competition (enemy) from capturing the ability to control supply chain or value chain (friendly} information assets and insuring survivability of those resources (assets). CEC-like logic may increase the ability of enterprise information systems to handle increasingly complex technology.

REFERENCES

[Armstrong00] Armstrong, Illena. "Security Fights for Internet Foothold." *SC INFO Security*, Vol. 11, No. 10, October 2000, pp. 23-30.

[Jajodia99] Jajodia, Sushil; McCollum, Catherine D.; and Ammann, Paul. "Trusted Recovery." *Communications of the ACM*, Vol. 42, No. 7, July 1999, pp. 71-75.

[Korzyk00] Korzyk, Alexander D., Sr. "Towards a Cybernetic Perspective for Enterprise System Security." In the *Proceedings of the 4th World Multiconference on Systemics, Cybernetics, Informatics*, 2000, pp. 72-77.

[National Research Council91] National Research Council, System Security Study Committee Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics, and Applications. "Computers At Risk," National Academy Press, Washington, D.2., 1991.

[Sutherland98] Sutherland, John W. "Integrative Systems: Assessing Requirements and Capabilities for Intra- and Inter-Organizational Context." *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans*, Vol. 28, No. 2, March 1998, pp. 159-182.

[Sutherland97] Sutherland, John W. "A Prospective on Macrocybernetic Process Management System." *Journal of Technological Forecasting and Social Change*, Vol. 55, 1997, pp. 215-248.