Principles for Intrusion Detection

A security system is only as good as its weakest link

- By Pete Accetturo
- Feb 01, 2012

The best defense is a good offense. That often-used sports principle applies to military applications. It is an axiom that applies to the security industry, as well. When it comes to perimeter security, though, a strong offense provides a good defense, but that defense will be only as strong as its weakest link. The question to be answered is how good is that defense? Or where is the weakest link?

If there are weak links, then you have unprotected perimeters, which means unprotected assets, unprotected people and, inevitably, security breaches. The ramifications of these breaches can be disastrous, so the threat of intrusion remains a prime concern at all facilities. Because many perimeters are simply too long for conventional security patrols to cover practically or effectively, advanced perimeter intrusion detection systems (PIDS) have become the only answer.

Historically, PIDS have had some trouble clarifying between a true positive and a false positive (nuisance alarms). All too few PIDS provide sufficient analytical tracking, real-time assessment or any environmental capability, making it extremely difficult for security officers to respond to the ingress or egress point in a prompt manner. Technology has advanced to the point of offering a wide array of sensing solutions for PIDS. Those PID solutions come with an array of efficiency, costeffectiveness and precision. There are some important factors to consider when reviewing current PID technologies:

- System durability/reliability;
- Minimal nuisance alarms (false positives)
- Maximum detection capability;
- Minimal maintenance
- Ability to accurately pinpoint the location of intrusion; and
- Ability to work with other/complementary technologies.

Since the dawn of civilization, maintaining perimeter security has been a top priority. Having some form of it—whether a city wall, a moat or even trained animals—has always been critical for stopping, delaying or deterring a perimeter breach. Even with primitive perimeter security systems, having real-time intelligence and immediate response is vital. The difference between being aware of a breach and the intelligence to properly respond can truly mean life or death.

While technology has advanced over the years, the security fundamentals have not. Today we have both active and passive intrusion detection technology. Video analytics; sonic, infrared, radar and fiber optic sensing; and buried vibration and sonic or attenuation detection all have significant roles in PIDS. Fundamentally, good physical security is a combination of four defensive principles: deterrence, delay, detection and denying a breach. The first two actions are considered passive defense while the latter two are active in nature.

Deterrence

The goal of physical security is to convince potential attackers that the likely costs of attack exceed the value of making the attack (e.g., that consequences of a failed attack may well exceed the gain). The combination of layered security features establishes the presence of a security-rich deterrence system.

The initial layer of security for a campus, building, office, or other physical space uses crime prevention through environmental design to deter threats. Some of the most common examples are also the most basic— warning signs, fences, vehicle barriers, vehicle height-restrictors, restricted access points, site lighting and trenches. However, even passive things such as hedgerows may be sufficient in some circumstances.

Delay

The next layer is mechanical and includes gates, doors and locks. Key control of the locks becomes a problem with large user populations and any user turnover. Keys quickly become unmanageable, often forcing the adoption of electronic access control. Electronic access control easily manages large user populations, controlling for user lifecycle times and dates and individual access points.

For example a user’s access rights could allow access from 7 a.m. to 7 p.m., Monday through Friday, and expire in 90 days. Another form of access control includes the use of policies, processes and procedures to manage ingress into the restricted area. The deployment of security staff conducting checks for authorized entry at predetermined points of entry is usually supplemented by mechanical and electronic access control or simple devices such as physical passes, ID and RFIDs.

Detection

The third layer is intrusion detection systems or alarms. Intrusion detection monitors for unauthorized access. It is less a preventative measure and more of a response trigger, yet it has a high incidence of false alarms.

In many jurisdictions, law enforcement will not respond to alarms from intrusion detection systems. For example, a motion sensor near a door could trigger on either a person or a squirrel. A simple sensor does not do identification, and as far as it is designed, anything moving near that door is unauthorized. That is why CCTVs are the next step in a layered security system approach. Identification of the intrusion event is essential for the required intelligence detection.

Security cameras can be a deterrent in many cases, but their real power comes from incident verification and historical analysis. For example, if alarms are being generated and there is a camera in place, the camera could be viewed to verify the alarms. In instances when an attack has already occurred and a camera is in place at the point of attack, the recorded video can be reviewed.

Denying a breach

Guards have a role in all layers: in the first, as patrols and at checkpoints; in the second, to administer electronic access control; in the third, to respond to alarms. The response force must be able to arrive on site in less time than it is expected the attacker will be required to breach the barriers.

In the fourth layer of perimeter security, a guard’s role is to monitor and analyze video. Users obviously have a role also by questioning and reporting suspicious people and aiding in identifying people as known versus unknown. Often, photo ID badges are used and are frequently coupled to the electronic access control system. Visitors are often required to wear a visitor badge. Every application is unique, depending on the type of facility being protected, its operating environment, its perimeter fence construction, its intrusion and security history and the perception of threats.

Each individual site has a unique set of parameters that require a customized perimeter solution. Just as the military cannot apply a one-solution strategy for all military conflicts, neither can any perimeter apply a one-size-fits-all solution strategy. Goals need to be established that are influenced by environmental concerns (including any severe topography factors), the flow of traffic (foot and auto) and the possibility of any major weather concerns. Effective PIDS account for all of these elements and take budget into consideration. These factors weight the PID system in varying degrees that impact its overall efficiency. Again, a layered system is the best solution.

Once a PIDS solution is installed, the next critical step will involve a complete calibration of the system. This calibration must account for all environments, sensitivity and duration of any possible event breach. This ensures that any true positive alarms will provide the best intelligence for the appropriate response. Thus a proper PIDS solution provides the necessary forewarning for deterrence, delay, detection and denying a breach.

Important design considerations derived from the aforementioned factors produce a well-integrated PIDS. Design elements to be considered are: Environmental design—Having intrusion detection sensors installed in the field or on the fence.

Mechanical, electronic and procedural access control—Having an alarm processor that drives and analyzes the raw sensor signals. Intrusion detection, with appropriate response procedures—Having a security or alarm management system that notifies security staff of an alarm and the location of the intrusion.

Personnel identification—Having a communications infrastructure that ties these three elements together and connects the system to the security staff, along with an established and clearly documented site policy and alarm response procedure.

Militarily or commercially, whatever the perimeter's greatest strength is, if left ungaurded, it becomes its greatest weakness. Strengths and weaknesses of a security system require a clear definition so policies and procedures can ensure appropriate action.

Intrusion detection technology will continue to advance, but these advances will be focused more around software than hardware as manufacturers continue to pursue improved system performance, flexibility, and reliability.