

Intrusion Insights – Adapting Intrusion Prevention Functionality for Process Control/SCADA Systems

By Ernest Rakaczky

Intrusion detection systems (IDS) represent a critical piece of security infrastructure you should implement whenever you connect critical systems, such as industrial process control systems, to TCP/IP-based local and wide area networks. They can detect network activity such as hacking attempts, virus and worm attacks, and other potentially threatening traffic capable of wreaking havoc on your control system. The technology behind them is simple—detect a threat and alert you. Today, new-generation IDS, also known as intrusion prevention systems (IPS), are not only able to detect threats, but they can mitigate them by blocking the traffic from entering your network.

Intrusion prevention is a new technology category focusing on taking a proactive approach to IT and control network security by preventing attacks on multiple network resources, as opposed to similar technology that merely detects and reports on attacks that have already taken place. Intrusion prevention is gaining visibility in corporate and government organizations due to the inherent limitations in existing security technologies. The significant financial loss organizations experienced is valid proof. Think of it as the logical follow-up to signature-based technologies, such as intrusion detection and anti-virus, and to network-oriented protection solutions, such as firewalls.

Traditional security products focused on the biggest threats emerging as computer networking. Corporations adopted e-mail and Web applications and purchased products to solve the security issues inherent in these technologies, namely perimeter protection (firewalls), network protection (network-based intrusion detection), and file-based security (anti-virus). But these technologies don't address new attacks that ride over existing protocols to attack applications or new content-based attacks that attack systems before vendors are able to release and distribute signatures and other countermeasures.

Best practices

How can your organization make informed decisions when choosing intrusion prevention products? Here are some technology best practices for intrusion prevention solutions that might help.

Any organization that intends to protect itself by using intrusion prevention technology should consider a number of factors when evaluating products that address the organization's defined security requirements. Take care to choose solutions meeting corporate security, manageability, and flexibility requirements, lest the solution be a partial one, or worse, introduce a significant management burden that overshadows the security benefits.

1. Host-based protection

As more companies adopt technologies like high-speed networks, switching, and end-to-end encryption, providing desired security at the network level becomes a major challenge.

The best place to enforce security is at the desktops and servers, where you perform the actual work and where the potential for damage is greatest. Consider the value of only a host IPS solution that is not signature or role based dependent. In the control environment, one of the key current challenges is the overall deployment and execution of current security vulnerability patches for given operating software.

2. Real-time prevention decisions

To ensure the highest levels of security and minimize the ability to bypass the security policy on a host, you must intercept application calls at the kernel level, where you determine their adherence to policy. You can easily bypass implemented solutions by replacing shared libraries or analyzing system audit logs. An effective intrusion prevention strategy includes preventing violations in real-time, rather than noting attacks or system changes after the fact.

3. Defense in depth

To completely enforce a company's security policy, intrusion prevention must intercept all major points of communication between applications and the underlying system.

Network control must limit client/server communications at the port and protocol level, as well as hosts for permitted communications. File system controls must allow or deny read and write access to folders and files on an individual and group basis. Registry controls must prevent the overwriting of important registry keys that control how the system and other applications operate. And, COM controls should restrict inter-process communication to allowable access.

Attacks have multiple phases: exploiting network and application-level weaknesses, replicating and distributing themselves, and making unauthorized changes to the system. A complete intrusion prevention strategy must protect systems from all these phases, so if a new class of attack releases, you can thwart it at one or more of the stages.

4. Real-time correlation

Correlation deployed at the agent provides a level of accuracy on prevention decisions that does not exist with signature matching approaches. Correlating sequences of events within the context of an application's behavior eliminates the potential for false positives.

Correlation at the enterprise level enables security to be adaptive. By correlating the events on distributed agents, you can dynamically update intrusion prevention policies to prevent propagation of malicious code, thus preventing widespread damage to numerous resources.

5. Behavioral approach

The intrusion prevention approach must enforce appropriate system and application behavior to ensure the security implemented is proactive, not reactive. Solutions that rely on signatures only provide security to the release of the most recent signature update.

6. Flexibility

Every corporation is unique in how it configures and manages details of its systems and corporate applications. Intrusion prevention solutions considered must permit the policy customization and creation to accommodate unique applications and implementations. The solution must support automated policy creation to ease the management burden of creating policies by hand.

7. Ease of deployment

The intrusion prevention strategy should minimize the personnel overhead associated with agent deployments. Solutions considered must provide out-of-the-box functionality to allow for rapid deployment of the desired security policies, and must allow for roll out of new and custom policies as needed without additional intervention at the host level. The solution must support Web-based deployment, and allow for easy integration with standard corporate software distribution mechanisms.

8. Centralized event management

All events the agents generate must roll up into a centralized repository from which alerts and reports may be generated. Solutions considered must support standard alerting interfaces, such as SNMP, paging, e-mail, and flat files. They should also allow for custom interfaces to the alerting system to easily integrate with corporate systems.

9. Platform coverage

Solutions must provide coverage for the key operating systems the corporation wants to protect. In light of recent attacks, like Nimda, which target multiple hosts, the same management and enforcement paradigm must apply to desktop and server-based systems.

10. Administration

To ease policy management, policies must be definable centrally and automatically distributed to agents on a configurable interval. They must also be exportable for replication and archive purposes.

Behind the Byline

Ernie Rakaczky is director of Control System Security at Invensys Systems Canada, Inc., in Dollard-des-Ormeaux, QC, Canada.