

CU SECURITY: BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

Over the years, Intrusion Inc. a leading provider of data privacy protection and regulated information compliance products, has watched as Financial Institutions (FI's) increasingly relied on computer networks to improve business efficiencies and add new services for their customers. With the increased risks associated with these offerings, FI's have traditionally fortified their perimeter defenses with increasing layers of defense systems including firewalls, VPN's and intrusion detection systems. In other words, the solutions FI's have implemented center around fortifying the perimeter to keep the bad guys on the outside from getting to the private data or "good stuff" residing on the inside.

In 2005, Intrusion believes FI's will have to work more diligently to ensure the "good stuff" on the inside, is protected from the bad guys on the outside. Additionally, they will need to add to their security perspective a strong focus toward protecting internal data from inadvertent and/or intentional leakage to unauthorized persons, entities and services outside of the institution's external security perimeter.

Intrusion has spent the past year creating a new, more manageable approach that meets both of these challenges. Security systems traditionally are difficult to install, configure and maintain. One of the chief problems with intrusion detection/prevention systems, in particular, is the number of false positive alerts these systems produce. This is because all intrusion detection/prevention systems use some form of pattern matching to detect an exploit and fire an alert. Even the best protocol-decode based systems produce false positive alerts. To effectively deploy these systems requires specially trained security engineers who know how to "tune" these tools in order to reduce false positives and have a more usable system. Furthermore, interpreting the alerts and the ecommerce merchant's appropriate response to them requires special expertise.

To solve the false alarm or false positive problem, Intrusion decided last year to tackle this issue from a fundamentally different approach with the release in late 2004 of our unique Compliance Commander. Compliance Commander is an invisible sensor that sits at the customer's perimeter and monitors traffic on all ports and protocols. But, unlike traditional IDS's that simply source signatures from algorithmic patterns, Intrusion's Compliance Commander sensor utilizes our unique "middle-ware" appliance, called the Dynamic Data Dictionary (D3) server, to source the systems signatures from the actual data being protected. Additionally, to monitor multiple sites and databases, the D3 server can be coupled with one or more sensors to provide the highest accuracy for all data privacy alerts and compliance violations.

One of the truly unique features of the Compliance Commander is the capability to detect, protect and block at real-time, data privacy violations. This feature ensures, no private data is lost and no privacy regulation is violated. All alerts are logged to the Compliance Commander Web-based management system that can be accessed virtually anywhere. Once deployed, the Compliance Commander product requires no additional labor hours to the customer's staff. With its automatic updates, self-synchronization with the customer's data and automated alerts, the Compliance Commander is by far the simplest, most accurate and least expensive to own product on the market today. The real-time alert notifies the FI of the source and destination MAC and IP addresses and the specific type of privacy violation that was blocked. When coupled with Intrusion's award-winning SecureNet Provider management system, the FI can get detailed forensics information for security analysis of privacy trends. Intrusion's SecureNet Provider also includes a case file management system to completely document any specific incidents and/or policy violations for management or law enforcements attention.



Ben A. Bittle is Director of Product Development for Intrusion. Mr. Bittle joined Intrusion Inc., in March of 2003. During his 16 year career, Mr. Bittle acquired extensive experience in network security engineering, design and implementation and is currently a Certified Information Privacy Professional (CIPP). In his current role at Intrusion, Mr. Bittle is responsible for all aspects of the company's Compliance, data privacy and security product management areas. Mr. Bittle holds a Bachelor of Science degree in Electronics Engineering Technology from Oklahoma State University, and a M.B.A. in Management from Amber University.

