Identity-Based Internet Protocol (IBIP)

The Identity-Based Internet Protocol (IBIP) is a network security innovation developed at The MITRE Corporation that increases the security and resiliency of operational networks. IBIP improves network situational awareness and provides enhanced clarity regarding user, client, and server behavior.

By reducing anonymous traffic and enforcing permissible use policies, it can make an enterprise network infrastructure less accessible to attacks and unauthorized users. IBIP enables the cost-effective delivery of critical mission capabilities, even in the face of attack. It can be deployed while preserving investment in existing network infrastructure and enterprise authentication methods, and it operates with little or no impact on the users' experience.

Problem statement

Our cyber adversaries are on our networks. Opening an email attachment or visiting one wrong website is all it takes for malware to be inadvertently installed on a computer. Once an adversary has established a foothold on a host, he typically creates a back door to ensure that he can return, and then he uses that compromised host as a springboard from which to explore an entire network, stealing information and establishing additional footholds. Many such attacks may remain undetected. If they are, attempts to stop them and clean them up may be disruptive to mission-critical operations. Given this state of affairs, relying on traditional defenses like perimeter protection and antivirus software alone is insufficient. More pervasive network protection, which preserves existing investment in network infrastructure and applications, is required.

Identity-Based Internet Protocol (IBIP) solution

MITRE designed IBIP to prevent compromises from spreading to other hosts on a network, to the extent possible, and to detect these compromises by their attempts to spread. IBIP relies on the concepts of both host and user identity, as well as on defining permissible use policies within which network traffic is required to operate. IBIP inserts within each packet the identities of both the users and the hosts that are the source and destination of the packet, as well as user organization and role, ensuring that all internally-generated traffic can be evaluated for conformance to policy. Traffic that violates policy can be blocked and trigger an alert. IBIP may also reconfigure infrastructure assets to respond to detected threats in real time. IBIP's enforcement is policy based: if a user's credentials have been compromised but the traffic that he sends conforms to the permissible use policy, it will not be blocked. Nor will it generate alerts. Such authorized traffic may provide a means through which a compromise could spread. However, the user will be limited to sending traffic only as authorized by policy. Traffic that violates the policy will be blocked and will generate an alert, and its user and host identity field values will be logged for subsequent forensic analysis.

IBIP enables identity-based access

The identity information that IBIP incorporates into each packet enables all network traffic to be attributable to a specific host and user, and it determines the access control and authorization policies to which the packet will be subjected. IBIP authenticates hosts based on certificates and addresses, and it may authenticate users using passwords or smart card (e.g. CAC card). If desired, periodic re-authentication may be enforced.

IBIP reduces anonymous traffic and decreases the threat surface

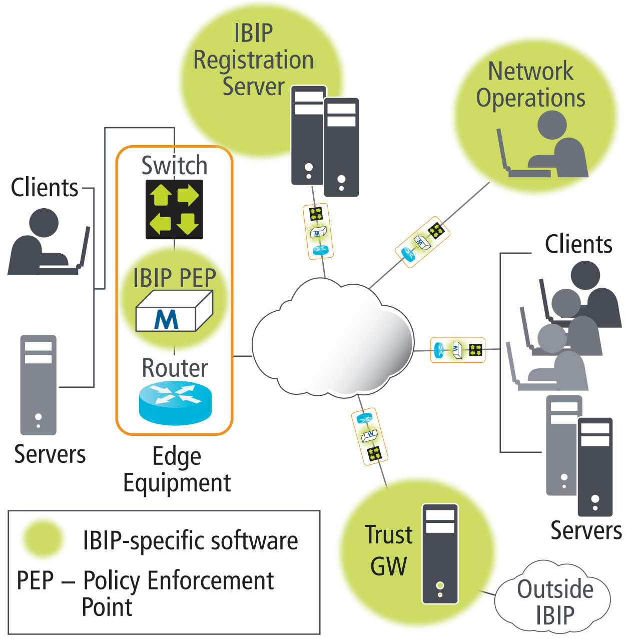
Policy Enforcement Points (PEPs) limit access to end-user systems and infrastructure devices such as routers and switches while allowing servers to be fully visible. Clients are hidden from unauthorized users, and servers are aware of clients only to the extent that they must support return traffic in response to client requests. Adversaries who use network reconnaissance to try to locate network devices to target for attack will be thwarted. IBIP will detect attempts to discover and access these hidden assets and will generate alerts. Adversaries who do not have proper credentials or

Continued on back

who attempt to send traffic from a spoofed IP address to gain access to a host and exploit a zero-day vulnerability or pre-planted back door will be prevented.

IBIP enforces permissible-use policies to prevent unauthorized network use

All identities are associated with a set of permissible use policies that define what the identified element is allowed to do on the network. These policies specify what network traffic each particular client—when used by a specific individual, and server—is permitted to send to the network. They may be based on host and user identity, role, organization, trust level, IP address, protocol, port, etc. For example, a host may be authorized only to listen on ports 80 (http) and 443 (https). If that host is compromised and generates traffic from any unauthorized ports, IBIP will block these packets, thereby preventing the attack from spreading. All client/user and server/port combinations have these policies. Any attempt to send traffic that is not permitted by policy is immediately detected and blocked and will generate an alert.



Network Infrastructure showing IBIP-specific components: Registration Server, NetOps, and PEPs

IBIP introduces the PEP to perform much of its functionality. All traffic sent into the network flows through PEPs. The source PEP encodes information such as user and host identity, user role, organization, and current trust level of the user/host, into each packet. A destination PEP removes this information prior to delivery at the final destination. Hosts are unaware of this identity information and cannot inject or examine it themselves.

IBIP software can potentially reside on other network appliances.

IBIP reconfigures network infrastructure based on threat conditions

IBIP substantially improves network situational awareness. All PEPs act as sensors to report policy violations to the IBIP Network Operations (NetOps) console. The console provides a concise, integrated view of the network, users, trust, and status, enabling malicious activity to be detected and responded to proactively, and logging network activity for later analysis. All traffic generated by hosts and users can be monitored, and user and host trust metrics can be adjusted dynamically. Infrastructure assets can dynamically and without manual intervention be reconfigured in response to triggering events and threat conditions in real time.

Existing infrastructure is preserved; user experience is minimally impacted

IBIP does not require major changes to the underlying network architecture. Legacy routers and switches can continue to be used, as long as they provide certain basic functional capabilities. User authentication relies on technologies that are familiar to users, such as passwords and Personal Identification Verification (PIV)/Common Access Control (CAC) cards. Host authentication uses standardized, widely implemented mechanisms, and detected policy violation alerts are sent to NetOps using standard syslog messages.

Contact

IBIP is available for licensing. For information, contact The MITRE Corporation | Technology Transfer Office | 7515 Colshire Drive McLean, VA 22102-7539 | Phone: 703-983-6053 | www.mitre.org/tto | Email: techtransfer@mitre.org

MITRE's Technology Transfer Office transfers innovations to the public and private sector to increase their availability, affordability, and maintainability to our government sponsors and the general public and return value to the nation's economy.