# *THE MISSING LINK IN U.S. CYBERSECURITY*

As the frequency of cyber attacks and capabilities of the attackers continue to increase, it is imperative that all government entities take every possible step to ensure that the best defenses are in place to protect sensitive data.

Increasing network complexity threatens the security and performance of networks, IT assets and resident data. Networks are constantly in flux due to numerous change vectors, such as new device deployments, network consolidations, infrastructure updates, changing business requirements, and security and compliance initiatives. Adding to the complexity, remote access and mobile device proliferation have increased the volume and variety of connections to the network.

Obtaining an accurate baseline of the large, distributed, and complex networks common to most Federal Agencies often seems a difficult task. The benefits of such an exercise, however, are game changing. With the comprehensive network intelligence such a baseline provides, Network and Security professionals can more accurately:

1. Define their true network perimeter, including the identification of unknown access points
2. Specify areas for targeted hardware deployments
3. Identify all network connections, specifically:
    a. all Internet points-of-presence, consistent with the Trusted Internet Connection (TIC) initiative
    b. rogue connectivity points, both internal and external
    c. partner and inter-agency connections
    d. legacy network drops
    e. unauthorized intra-agency leakage
4. Catalogue all active IP devices
5. Profile end nodes for non-compliant behavior
6. Build an active list of mis-configured or exposed infrastructure devices
7. Expose all collected information to other point solutions

Once armed with this information, Network and Security professionals can make the most effective decisions regarding how to proceed in executing on their cybersecurity strategy. This complete inventory of every connected IT asset helps all levels of Security professionals establish their defenses most effectively, monitor all exposed network points, and respond quickly and appropriately to any outsider threat.

Finding, identifying, and cataloguing several hundred thousand devices across a global, secure infrastructure is difficult enough. However, interpreting the data and identifying potential areas of weakness in the network defenses is a different task altogether. The first step to accomplish this is to determine which devices connected to the network <u>should</u> be there, as opposed to those that <u>should NOT</u>.

Differentiating between these authorized (or “known”) devices and unauthorized (or “unknown”) devices across a large government agency can seem another difficult, tedious, and nearly insurmountable task. With this kind of an undertaking, IT Security managers face issues like: internal segmentation blocking individual enclaves from one central management point; and IT Security tools that don’t scale to accommodate the ever-expanding IP space government networks occupy. With those hurdles at the outset, it is understandable that most agencies have difficulty getting a handle on every network connection, host, and active IP on their networks. It is in this gray area where connected devices can fall outside the watchful eye of security management. Consequently, this is where serious threats can (and often do) manifest themselves.

The remedy for this problem lies squarely within the realm of a comprehensive Network Discovery program; the simple idea being that *agencies can't secure what they can't manage, and can't manage what they don't know about.* This challenge represents a critical, but heretofore missing link for U.S. cyber security.

If Security professionals are able to collect and maintain an accurate, up-to-date inventory of every connection, device, and active IP in a given network, how much *less* likely are they to be exploited by a cyber attack? Most IT Security teams are well aware of the critical nature of developing an inventory of all Authorized and Unauthorized hardware on the network. The question remains: how are the "unauthorized" devices actually discovered?

In most cases, it appears that audit teams are usually provided with "best effort" information as a starting point regarding the assumed IP space of an agency's network. However, it appears that personnel turnover and continual requirement modifications often cause a significant disconnect between the IP ranges that are <u>believed</u> to be in use, and those that <u>actually are</u>. Therefore, agencies need a way to scan IP ranges that are provided to them, and be empowered with a solution that will dynamically "learn" more about the environment. Once all active IP space is uncovered, the next step is to automatically catalogue those address ranges that fall within the IP space provided initially (i.e. those ranges that are "known") vs. all *newly-discovered* IP space, which may contain active, but previously "unknown" IP devices.

By taking this holistic approach to the Network Discovery and baselining process, network security managers can make more far-reaching and informed decisions as to the nature of individual networks/devices within an agency--a critical first step that has been previously neglected. If a network is deemed to be authorized, that IP space can then be placed onto the authorized/known list, while networks which should not be connected can be dealt with accordingly. In most cases, simply providing intelligence about the total routed network is sufficient to allow network security managers to make an informed decision for many major security initiatives. In other instances, where the unknown networks/devices need further investigation, other measures can be taken to quarantine those networks from the rest of the agency. With comprehensive Network Discovery, these maneuvers can happen proactively, simply from the understanding of the total routed network, before a serious threat has been exploited.

Only with this true baseline of the complete IT infrastructure can agencies truly realize the benefits of a detailed cyber security strategy. Detailed and complete discovery is the foundation of all other aspects of infrastructure and device analysis. If an agency's cyber security strategy and execution is extremely thorough and effective, but is only monitoring 85% of the connected network, then how effective can it truly be? A comprehensive Network Discovery solution minimizes this inherent gap—the missing link--between the perceived network and the actual one, and as such, should be a critical component of the cyber security strategy of all Federal Agencies.

**Today's government network managers must:**

- Strive to become as informed as possible with a complete, comprehensive network topology;
- Balance change with security, availability and compliance;
- Measure network risk from a global network perspective;
- Provide an accurate view of what's connected to the network;
- Identify previously unknown devices and internet leaks;
- Validate policy compliance across the enterprise;
- Eliminate gaps between security policy and operational reality; and
- Optimize deployment and enhance the value of IT security and network management tools.

A comprehensive network view allows large enterprises and government agencies to balance the constant forces of network change with risk management and compliance initiatives such as:

- Cybersecurity and Defense Planning
- Network Mergers, Data Center Consolidation
- Data Leak Protection / Information Leak Prevention
- IT Asset Management
- Critical Infrastructure Protection & Control Systems Security
- Security Policy Compliance & Audit Programs
- Change Management

**Key requirements for advanced functionality should include:**

- **Network Discovery** – Identifies all network address spaces, routing devices and connectivity across the network (including hidden or "stealth" devices that do not respond to queries) utilizing advanced multi-protocol discovery technology, and creates a comprehensive route-based topology that identifies a network's true perimeter.
- **Host Discovery** – Detects all known and previously unknown network devices by conducting a census of IP addresses across protocols. Flags devices unrecognized by official network inventories for remediation. Additionally, address utilization reports help improve efficient use of network IP address space in the enterprise.
- **Leak Discovery** – Reveals unauthorized connections between a network and another network, sub-network, (e.g., unsecured routers exposed to the Internet or open links to former business partners). This is crucial in the proactive fight against leaks, revealing all unauthorized connections and identifying whether access is outbound, inbound, or both.
- **Device Fingerprint Discovery** – Identifies devices with active service ports that support web services and IP applications, – including those not owned by the client or its employees – pinpointing resources for which tested ports are active. Flags improperly secured wireless access points for remediation—improving security without requiring staff to scan airwaves or deploy antennae-based monitors. Additionally, matches a device's unique MAC address with its assigned IP address, providing crucial information for asset management and diagnostics.

**And beyond typical mapping or discovery solutions, today's threat environment requires that government solutions:**

- Determine empirically if devices have connectivity beyond the network perimeter or unauthorized access across secure zones;
- Provide visibility into every asset, host, node, and connection on the network
- Utilize patented technology to report on network "leaks" (unknown, unrestricted pathways into and/or out of an organizations network) that represent policy violations and security threats
- Present a comprehensive view of the entire routed infrastructure -- in a fraction of the time of other discovery tools
- Find wireless access points that are connected to the wired network, and tests those devices for inbound or outbound "leaks"
- Provide data extensible to security risk management and network management solutions
- Eliminate gaps between security policy and operational reality
- Remain lightweight, fast and non-intrusive for the world's largest and most sensitive IP networks.

## *ADVANCED METHODOLOGY AND TECHNOLOGY*

Most enterprises are doing a lot to secure and manage at the device and host level, but little attention has been typically paid to the Layer 3 (or the Network Layer on the OSI model of computer networking) itself.

All discovery tools are not the same. Unlike most tools that have a "discovery" component, advanced solutions are necessary and must perform active probes of the address space, empirically discovering everything that's on the network -- not just the IP range that is supplied for scanning. Network connections that are discovered and mapped are proven through these active probes, rather than inferred based on requested routing information.

Searches for unknown networks must utilize multi-protocol discovery to penetrate deep into the network, identifying all Layer 3 routing devices. Once these devices are discovered, one must learn all routes that these devices maintain and then compares these routes to the initially targeted routes. IPsonar then attempts to probe this newly discovered IP address space, to determine if connectivity exists. Discovery tools must explicitly prove connectivity where it exists, and report on networks for which connectivity does NOT exist. The process should be iterative for any additional Layer 3 devices that are discovered in that new space, actively continuing until every route on the network has been exercised. All network connections should be displayed providing a visualization of the network, and quickly highlight both the “known” and previously “unknown” connectivity points.

Finally, these probes should be executed using multiple protocols, effectively validating that firewalls and router access control lists (ACLs) are operating in compliance with policy.

## *HOW ADVANCED NETWORK DISCOVERY IS CRUCIAL TO FIXING OUR MOST CRITICAL NETWORK VULNERABILITIES*

The federal enterprise network faces numerous threats from intrusion by unknown foreign entities, and other well-organized and highly-sophisticated threats which are increasingly Internet-based. Situational Awareness is a critical component to an effective cybersecurity strategy. IPsonar allows you to understand how change impacts network security, availability, and compliance.

As the new administration moves to address issues of our nation’s cybersecurity with high priority, an important part of those efforts will be focused on the areas where our cyber infrastructure meets the nation’s critical infrastructure in the form of control and automation networks (including SCADA). These networks employ programmable logic controllers (PLC), direct digital control systems (DDC), distributed control systems (DCS) and IO (Input / Output) systems which are often in whole or in part IP enabled. The effort to secure these aspects of our nation’s physical infrastructure will be undertaken in the face of a new hyper-connected reality where we are all only a few hops away from the most onerous and sophisticated cyber threats.

In conclusion, a crucial part of cybersecurity is the comprehensive understanding of what is on the network so it can be properly defended. External connections, Internet points of presence, and the network perimeter represent the front-line in cyber conflict. IPsonar’s patented technology is the only tool available that scours the entire network by scanning for both known and unknown devices, and fully mapping their connectivity.