Who you gonna call… SISA Alliance

by Sam Chun

IT IS NOT GOOD enough just to capture and store information; to make all the information available to us useful, we need to share it in such a way that one piece relates to another and can be helpful in making decisions. While respecting the privacy rights of individuals, organizations need to access compiled information to build a complete picture of a situation and point to possible solutions. Governments need to better integrate their diverse systems and data stores, reduce redundancy and improve.

Secure information sharing architecture (SISA) partnership provides assurance of privacy, access, consolidation and compliance.

Mounting information overload…

Both government and the private sector are generating and storing more information than in the past. Whether it's the transformation of documents from hard to soft copies, or the massive amounts of data now being stored in searchable databases, the collection, storage, security and management of electronic information is becoming an increasing priority for almost all organizations. Compounding the challenge of storing all this new information is that much of it is private to either individuals or organizations.

The primary purpose of having information is to use it to meet organizational missions. These missions can span jurisdictions and national boundaries. For example, the National Police Services (NPS), a business line of the Royal Canadian Mounted Police (RCMP), which provides services to other Canadian law enforcement and criminal justice agencies, is well on its way to implementing the Real Time Identification (RTID) project. RTID will further mechanize and streamline the way in which fingerprint (mainly through a new automated fingerprint identification system) and criminal records are stored, shared and used by Canadian and international law enforcement communities. One of the major objectives of RTID is to be interoperable with American FBI and Interpol criminal records systems.

Global events and trends clearly demonstrate the need for a collaborative approach to solving big problems. Whether it's enabling transcontinental enterprises that serve the world's citizenry (e.g., the United Nations) or fighting global criminal elements, "doing it together" is more likely to achieve mission success than otherwise. Collaboration is critical for overcoming difficult challenges and collaboration begins with information-sharing.

Four virtues of assured information sharing

As vital as it is to share information and work collaboratively, it can't be done without context. Privacy rights of individuals need to be protected. Organizations' sensitive internal content has to be secured. Numerous information security incidents across the globe within recent months demonstrate the existence of threats from within and without. In the end, it doesn't really matter whether the information was stolen by intruders or disclosed by careless individuals. Confidentiality was lost, damage was done, and laws may have been broken.

While making information available online or to third parties outside an organization can provide clear benefits, it also forces organizations to secure that information. Collaboration is beneficial only when it won't lead to inappropriate disclosure. What organizations need to strive for is assured information sharing – the ability to share information with appropriate individuals while maintaining control over the same information within a logical community of trust. Assured information sharing has the following four virtues:

1. **Role-based access:** Access to content and services must be based not on individuals, but on roles. For example, if a user's role within an organization is finance, the user should have access to finance department service and data appropriate only to thier role. This is especially true for individuals that have orthogonal roles within their organizationslike RCMP personnel working on joint task forces. They should have access to role-appropriate data and services at national, provincial and municipal levels.
2. **Secure content within communities of trust:** Role-based access allows definitions of logical communities of trust across physical or jurisdictional boundaries. For example, a criminal investigation may involve participants from all levels of the law enforcement community including other nations. Information owners should be able to share and secure content to the participants in that community. Securing content includes important capabilities such as meta-data tagging and document-marking (technologies from Liquid Machines Titus Labs), object/file-level encryption and protection (Microsoft and Liquid Machines), and assured dissemination and redaction (with technologies from Teradact Solutions).
3. **Lower cost information ownership:** It may not be obvious, but the proliferation of data and services should not result in the exponential growth of the infrastructure to support them. More servers, storage devices and network equipment will result in higher total cost of ownership (TCO) with higher probabilities of configuration error or component failure. Assured information sharing solutions will have to be simpler, more consolidated, and have lower TCOs than existing systems. These requirements likely favour a commercial off-the-shelf-based solution, rather than a custom-developed one.
4. **Comply with appropriate laws:** Of course assured information sharing means protecting the rights of individuals, following standards, and aligning with national guidelines on privacy. This virtue is much more probable if the other virtues have been accomplished.

SISA answers the call

In 2005, three of the titans of the IT industry, Microsoft, Cisco and EMC, were challenged by a US Department of Defense customer to co-develop a solution for just this problem of "share and secure" for their coalition networks. The customer also threw down a gauntlet by requiring the solution to lower the overall TCO of the infrastructure, while conforming to the various military and US national standards and laws for system security. These seemingly difficult and conflicting functional requirements were met through the dedicated and careful collaboration of these industry leaders. The solution, referred to as the Secure Information Sharing Architecture (SISA), became the cornerstone of the formal joint venture of these companies known as the SISA Alliance.

The goal of SISA, the Alliance and its members, now numbering seven, remains true today. Its singular purpose is to meet a very large, global problem directly. The challenge of assured information sharing goes beyond nations or jurisdictions. There are privacy laws and standards in Canada (such as PIPEDA, the *Privacy Act*, and the *Municipal Freedom of Information and Protection of Privacy Act)* similar to ones that exist internationally. Through practical, proven experience, the SISA Alliance has shown that a solution that meets the multifaceted requirements of assured information sharing necessitates a disciplined, multitier, multi-vendor approach. In short, the four virtues of assured information sharing are too big and too complex to be achieved by any single technology vendor.

Although it is not the intent of the analysis to provide an in-depth review of the technologies or specific products that comprise the SISA architecture, it is important to present a brief overview of how SISA technologies can help accomplish assured information sharing:

- SISA protects internally sensitive content through its defense-in-depth approach, providing multiple layers of protection through encryption, access control and partitioning/virtualization, from endpoint to storage, supported by comprehensive auditing and integrated reporting using well-known, understood commercial off-the-shelf (COTS) technologies such as Microsoft Windows, EMC VMware and Cisco Catalyst switches.
- SISA facilitates sharing through a logical, role-based-access approach, focusing on communities of trust (CoT) rather than physical groups. For example, participants from the RCMP working with a provincial police department on a specific investigation can be logically separated and share documents and email securely. SISA allows participants from the various direct control over how their content can be distributed and accessed while using technologies that are ubiquitous and likely in line with IT investments already made.
- SISA emphasizes virtualization of infrastructures so that a community of trust within an organization can have its own private work area providing a high degree of security and isolation from other groups, without a duplicate investment in hardware. SISA can reduce an organization's TCO by providing the ability to consolidate physically separated application, network, and storage infrastructures. The consolidated, virtualized approach to data centres and IT infrastructures is becoming increasingly more important due not only to the financial benefits of consolidation but also to its ability to limit the IT industry's impact on the environment.

→ pg 12

← pg 7

For example, virtualized servers and storage consume much less power and generate less heat that needs to be dissipated via HVAC systems.

- SISA is a proven and validated solution already in use, protecting and sharing the most sensitive information of the US Department of Defense. SISA was designed to meet US intelligence community protection levels (PL3) and its design effectiveness has already been validated and is likely to be configured to meet international privacy standards.

SISA (**www.SISAalliance.com**) is ultimately a multi-vendor COTS-based approach toward assured information sharing. One of the major advantages of leveraging a COTS-based solution is the continued research and development that the technology providers will invest in the long term in continuing to update and improve their solutions to meet ever-changing demands. The SISA Alliance members invest US$12 billion annually in research and development – crucial to customer value as the road ahead continues to lead the architecture down new paths. Already under development, Release 2 of SISA plans support for cutting-edge requirements such as federated ID management (especially relevant due to the globalization of organizations and the coalition-based approach to national security issues), secure voice/video, solutions for data at rest and application virtualization. The combined strength and commitment of the members of the SISA Alliance ensures that the architecture and solution will advance and endure to achieve the four virtues of assured information sharing well into the future.

Sam Chun, CISSP, is the security architect for the Secure Information Sharing Architecture Alliance (SISA) at its joint program office at Addx, a principal provider of information and management sciences services. SISA is a formal alliance of seven companies led by Microsoft, Cisco and EMC, dedicated to collectively overcoming the challenges of assured information sharing. Chun is a regular contributor to the *Information Security Management Handbook* series. Chapters he has authored appear in the last three editions of the handbook. His articles also appear in publications such as the *Homeland Defense Journal* and *Government Security News*.