SIGNAL
AFCEA'S INTERNATIONAL JOURNAL

AFCEA

Smart Encryption Hides Data in the Open

By Henry S. Kenyon
August 2007

Technology ensures user anonymity, provides confidential messaging.

A prototype software security application encases data in an encrypted intelligent shell, allowing only an intended recipient to access the material. This software could permit warfighters, intelligence analysts and citizens to share information securely and anonymously across the Internet, popular social networking Web sites, mobile networks and security diverse infrastructure (cross domain). Users will be able to create online communities to communicate with other vetted individuals.

Developed by CYVA Research Corporation, a San Diego, California-based system integration and software development firm, the technology covers a range of applications from intelligent personal agents to network communities and virtual security tokens. According to Kevin O'Neil, the program's designer and CYVA's chairman and chief executive officer, the technology is built around the concept of information self-determination, or the ability of individuals and organizations to control their personal information directly anywhere, anytime. This security capability is possible through the use of a Self-Determining Digital Persona (SDDP) that converts data into intelligent, self-protecting software known as a Personal Information Agent (PIA). O'Neil notes that the PIA offers users the ability to protect text, video and hypermedia objects by encapsulating them within the agent.

A key feature of the Personal Information Agent (PIA) developed by CYVA Research Corporation is the ability to create varying levels of identities for users. Ranging from fully disclosed to pseudonymous and anonymous, the identities allow individuals to share information securely in trusted networks. This capability could permit local intelligence sources to provide critical data safely to coalition forces such as these U.S. soldiers conducting a house-to-house search in Iraq.

The agent's actions can be audited to track its location and to allow constant control throughout its life cycle. The PIA features certificates that enable users to confirm the agent creator's identity. Certificates also support non-repudiation, namely data authored and encapsulated within a PIA for secure exchange by a PIA owner cannot later be denied. The PIA owner cannot deny authorship of data or governing rules set to control onward data processing.

O'Neil explains that the audit function permits users to know how many times their agent interacted with other systems or was accessed by outside users and applications. For example, cell phone owners can set the system to notify them every time their phone number is scanned.

The software also features an interaction protocol allowing the SDDP to communicate with other agents. Another application is the ability to create privilege rules to control access to the data contained in the PIA. O'Neil notes that his system uses strong cryptography tools to enforce non-repudiation of authored PIAs. This function also permits users to encrypt data so only certain approved personnel can access it. He explains that this security feature can be activated via public keys or physical and virtual security tokens sent to specific individuals. The author can set the exact amount of access a token provides.

The agents can be static programs or itinerant programs that travel to a specific set of user communities. The PIAs also can be directed to go to a Web site address and can conduct preset functions or transactions. However, unlike other intelligent agent systems, CYVA's software is not designed for autonomy. "My rules are very explicit. They have to do with command and control and uses of information assets. But [the PIA] is doing exactly as it has been told. It's not using any kind of artificial intelligence algorithms to discover what I like on the fly to change its behavior. This thing is always doing what I tell it to do," O'Neil says.

Although the PIAs follow specific rules, these directives can be complex. O'Neil shares that the software is guided by established regulations about trust and relationships for information sharing. Additional security instructions may direct the agents to make data accessible for 24 hours or less, after which it is erased.

A key aspect of CYVA's software tools is their ability to form trusted network communities. Users can securely author, manage and communicate identities, information assets and rules that authorize individuals or compartmentalized communities such as intelligence analysts to process information within a distributed network. The secure information-sharing features provide varying levels of data control and choice, enabling trusted and accountable interactions and the exchange of sensitive media among community members.

With user community-controlled identities, individuals can choose their level of identity—anonymous, pseudonymous or fully disclosed. This option allows users to create a variety of personas or security levels tailored for specific missions. When engaged, the agent follows a strict protocol for assessing and authorizing identity-based exchanges. The software's administrators remain in control beyond the information transfer and continue to monitor and direct the PIA's behavior, which prevents raw and unsecured data from being introduced into a communication.

Trusted communities can range from a handful of people to thousands of individuals. O'Neil notes that these communities and their security features can be used for a variety of applications such as homeland security-related disaster response. First responders and other emergency management personnel could create trusted communities to share sensitive information and control its distribution. Health care workers could encapsulate their identities in PIAs to share victim medical information securely.

The PIA allows users to create trusted networks where vetted individuals can share information. The tool would be advantageous to warfighters, analysts and first responders, allowing them to create online communities quickly. Managers can control access to the communities or data contained in specific PIAs by sending users virtual keys or tokens with preset clearance levels.

O'Neil says that military applications also could benefit from the PIA's capacity for setting personal security levels. For example, U.S. forces operating with allies such as the United Kingdom could create trusted communities to share mission data. For security or operational reasons, the British personnel might be known only by pseudonyms. Likewise, local intelligence sources accepted by the system may be anonymous. O'Neil notes that the commander of a special operations team might not want team personnel to know the identity of an informant. He explains that the agent can differentiate anonymous, pseudonymous and fully disclosed individuals. "Agents don't necessarily need to represent real, identifiable people," he states.

By cloaking user identity and data, information also can be passed securely through commercial social networking sites such as MySpace. For instance, an intelligence officer may send a message saying "meet me for a date," which actually contains encrypted fire mission data. O'Neil adds that the agent submitting the information cannot be traced back to the person who sent it. Trusted community members also can electronically vouch for other agents and validate them. This approval process permits anonymous individuals to join trusted groups secretly.

The software also is designed for use with mobile handheld computers and communications. O'Neil notes that the need for reliability requires the agents to be small applications that do not use much memory. Much of his firm's software is built on the Java programming language because its portable code can operate on multiple platforms. "We've always targeted mobile devices as part of our environment. We also steer toward Java as an implementation language," he says.

However, many mobile systems have limited memory and bandwidth capabilities, and O'Neil admits that the software is currently a "hardened intelligent agent" that requires more bandwidth and processing than most mobile applications. He explains that the increased data demand is required for the agent's security protocols. "I'm sending the kitchen sink along with the data," he quips.

But the software's built-in security features also make it a disruptive technology. Because users control their data and whom they allow to access it, the PIAs upset a number of commercial Internet businesses that rely on collecting personal information. O'Neil notes that many social networking and search engine sites gather data without users' consent. This personal information then is provided to advertisers who use it to target demographic groups for advertising campaigns. "Right now the consumer has very little control over that [data gathering]. Most privacy policies that the Yahoo!s, Googles and eHarmonies have make you give up data," he says.

By putting individuals in control of their data, the agents challenge the status quo of the commercial Internet. "This is very disruptive to a number of existing business models. In a commercial environment, it has the potential to be very upsetting to search engine or MySpace schemes that sell personal information," he says.

O'Neil defines a disruptive technology as one that solves a problem differently than existing methods. These new solutions also can cannibalize the revenues of their predecessors. As an example, he observes that steam locomotive manufacturers resisted the introduction of diesel electric train engines, but they were ultimately driven out of business by the more efficient technology.

Because CYVA's software allows data to protect itself, the data bypasses many of the security technologies associated with the transport layer such as the secure sockets layer protocol. O'Neil explains that he designed the program to operate independently from the transport layer. Because the agents fully encrypt the data, end-to-end point encryption is unnecessary. He adds that the file transfer protocol did not have any security features when it was created. The company's secure agent-to-agent communications permits trusted information exchanges and ignores messages from nontrusted sources. "I sidestep the entire mail and spam problem. My agents only talk to other agents," he asserts.

Companies such as Sun Microsystems, Computer Associates and Hewlett-Packard have developed corporate-centric identity management systems. These products provide full identity management suites that permit firms to create employee identities and secure them in federations. O'Neil notes that few federations currently exist, but these architectures allow users to share privileges and access control mechanisms within a company network. However, he observes that federations put the company in control of personal data, not the user.

O'Neil explains that a schism exists in the identity management industry about the exact definition of user centricity and how far to take the term. He believes that in consumer-business transactions, firms may support user centricity because they could find other ways to attract business. Companies may be able to accept customers controlling their own data, but employees would not have that freedom.

CYVA currently is acquiring additional venture capital for a final round of experiments. O'Neil explains that the software requires large-scale network testing before it can be vetted for use by government and commercial clients. When he first sought venture capital for his firm, O'Neil encountered resistance to the idea of consumers controlling their data. But this attitude has changed since security challenges such as identity theft have emerged as a major threat. "We have now realized that this entire infrastructure is highly vulnerable to attacks on identity. In fact, we don't have any control over personal information like our social security numbers and addresses," he says.

Web Resource
CYVA Research Corporation: www.cyva.com