The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

Status
Laureate

Year:
2013

Organization Name:
Intelligence and Information Warfare Directorate (I2WD)

Organization URL:
Intelligence and Information Warfare Directorate (I2WD)

Project Name:
Identity Resolution Exploitation Management Services (IREMS)

Please select the category in which you are submitting your entry:
Safety & Security

Please provide an overview of the nominated project. Describe the problem it was intended to solve, the technology or approach used, how it was innovative and any technical or other challenges that had to be overcome for successful implementation and adoption. (In 300 words or less)

Identity Resolution Exploitation Management Services (IREMS) is a technical intelligence solution with the ability to integrate with, contribute to, and disseminate data from Biometrics, Forensics, Collected Material, and Document Media Exploitation. Throughout the world, a connected architecture of systems for core infrastructure support of a country does not exist. For example, in the United States, vehicles are tracked by associating license plates to a specific car that enables an association to an identity. In many other countries, it's impossible to track vehicles, promoting anonymity amongst the criminal community. IREMS provides a core fundamental service to positively identify an individual, while leveraging existing biometrics captured across multiple data repositories worldwide. With positive identification, countries can focus on building their core infrastructure for material tracking with a positive association to an identity. IREMS approached this challenge with a biometric technical solution that can be leveraged by any country/organization. The biometric capability allows a user to upload fingerprints

onto the IREMS web interface for a biometric match to be returned within minutes, when manual match requests would take weeks! IREMS implemented a streamlined workflow for fast biometric matching, supporting many customers worldwide. For capabilities expanding beyond biometrics into forensics and other domains, IREMS supports a set of services that can be configured a la carte focusing on the user's core objectives without a burden of unnecessary capabilities. IREMS provides an innovative solution for positive identification using biometrics in countries where policies, people, and the local foundation infrastructure lack the ability to track criminals or terrorists. Hurdles overcome by the IREMS team weighed more on the political relationships and agreements to leverage our services; however, once deployed and proven successful, the road was paved to establish the biometric service amongst many host nations at an incredible rate.

When was this project implemented or last updated? (Please specify month and year.) Has it incorporated new technologies and/or other innovations since its initial deployment? (In 300 words or less)

IREMS was initially deployed in November 2011. Since then, the IREMS team has further developed and enhanced its capabilities. IREMS has focused on three additional capabilities over the past year to maximize the benefit of the system to Soldiers in theater and other agencies, both foreign and domestic, including INTERPOL for the war on drugs and other criminal activities. The first enhancement to IREMS incorporated the ability to upload multiple biometric files simultaneously. This feature is especially useful when multiple individuals have been detained. The initial release required users to upload each individual file for analysis. The second enhancement provided the ability for the end-user to view the Electronic Fingerprint Transmission (EFT), a biometric file, via a thin client interface. This interface allows the user to submit EFT files to DoD's biometric database, Automated Biometric Identification System (ABIS), for matching. ABIS shares these files with the Department of Homeland Security (DHS) and Federal Bureau of Investigation's (FBI's) biometric databases. EFT is the file type required for submission of fingerprints to ABIS for matching. Lastly, the IREMS team is integrating its solution with the Distributed Common Ground System-Army (DCGS-A) Standard Cloud (DSC). DSC provides access to advanced analytical Intelligence, Surveillance, and Reconnaissance capabilities to intelligence analysts. The DSC user can conduct complex analytics of millions of messages, from hundreds of sources and receives a response in less than one second. The integration of IREMS with this established system can provide vital information for security as disaster relief efforts are established in these areas. The quick deployment of such a system, with the ability to identify potential threats through biometric data, can greatly increase the safety of Soldiers, volunteers, and first responders while relief efforts are underway.

Is implementation of the project complete? If no, please describe the project's phases and which phase the project is now in. (In 300 words or less)

While the initial deployment of IREMS was completed and deployed to Africa in 2011, feature development will continue in multiple phases. IREMS is working to incorporate multiple-language support into the system. This feature will allow for IREMS to be deployed supporting other areas around the world where this technology is unavailable. IREMS leverages three databases to run its analytics for biometric data; currently, it

receives three independent reports if a match occurs. IREMS is working to consolidate the responses in order to provide the most accurate and simplified report so users can take necessary action in a more timely fashion. The DoD has an authoritative list of high-value targets called the Biometric Enabled Watch List (BEWL). This list includes known terrorists and drug dealers. REMS is working to allow users to be able to open the watch list through its thin client. This information will be local on the Secure Electronic Enrollment Kit II (SEEKII) device, so connectivity will not be necessary for users to view files, keeping Soldiers and other responders safer. Lastly, IREMS is working to integrate with Iris-on-the-Move (IOM) technology. IOM is a step-through system, such as an airport metal detector, that captures an individual's face and iris on the fly without stopping. If the individual triggers an alert, security agents will capture his/her fingerprints and conduct a biometric match request through IREMS. IREMS will receive push notifications/alerts of matches against the BEWL to the requestor. In addition, IREMS (SEEKII) will display side-by-side BEWL information and images as well as IOM-captured images. SEEK enrollment files will be transmitted to the Biometrics Identity Management Agency (BIMA) for match verification. The use of IREMS and IOM can significantly reduce airport-security wait times.

Please provide at least one example of how the technology project has benefited a specific individual or organization. Feel free to include personal quotes from individuals who have directly benefited from the work. (In 300 words or less)

IREMS is greatly improving the safety and security of foreign nations in the areas of drug- and human-trafficking. For example, an IREMS user who works as security at the embassy in Praia, Cape Verde, was interviewing an individual requesting a visa for travel to the United States. The individual was acting suspiciously, so the IREMS user contacted the Judicial Police and asked them to enroll his fingerprints. Using the SEEKII biometric collection device to enroll his fingerprints and iris, the Judicial Police created pristine biometric snapshots of this individual. The biometric information was submitted through the IREMS biometric submission portal to find a match within minutes in the DoD's database of biometrics. Simultaneously, the police did some research on the individual and discovered he had an international warrant for narcotics trafficking. While not confirmed, it is quite possible he was traveling to the U.S. on behalf of a criminal enterprise to facilitate the movement of illicit drugs. Unfortunately, Cape Verde does not have extradition treaties except in cases of terrorism, so the individual was able to leave. The positive outcome is that his biometrics profile was submitted through the IREMS portal and added to the DoD BEWL. Not only will IREMS provide information to prevent him from entering the U.S. legally, but also other countries that leverage these services can prevent entry into their territories, enabling a safe environment for their citizens. In countries where extradition treaties do not impose strict limitations, this individual would have been identified as a high criminal target and detained immediately as a result of using the IREMS submission service to obtain the critical match report. The success of IREMS lies in its unique ability to conduct biometric matching within minutes, rather than hours or days.

Would this project be considered an innovation, a best practice or other notable advancement that could be adopted by or tailored for other organizations and uses? If yes, please describe that here: (In 300 words or less)

Many organizations can use matching and relating identities in a variety of ways. For example, IREMS has the capability to provide real-time identity awareness in many sectors, including both national/local security and disaster response. Had it taken place in another country, Hurricane Katrina would have illustrated a possible use for this technology. After the storm passed, more than 50 websites were created to host the identities of the missing and those individuals who had been found. In the United States, when family members cannot identify their loved ones, dental records and other forensics are used to make a positive identification. In countries that don't maintain such records, the victims'' biometric identifiers (face capture, fingerprints, etc.) can be submitted to determine their identity. The process of identifying victims of major disasters is rarely possible by visual recognition. IREMS has the capability to speed up the victim recovery and identification process, enabling families to have closure and begin the healing process. Additionally, IREMS can provide an extra measure of security at airports, nuclear plants, shipyards, etc., by activating the biometric enrollment and positively matching the identity of suspicious individuals. Last year, 1,137 people attempted to enter the Dubai International Airport with forged documents. Although passports and identity documents are becoming more difficult to forge, criminals are now attempting to enter other countries by committing "look-alike fraud," or looking like the person in the document. People can change their appearance, passports, almost everything about themselves except their biometrics. If authorities leverage the IREMS solution, they can positively identify a suspect, no matter what information the person provides. Identity-resolution technology provides a growing number of organizations and law enforcement agencies with enterprise awareness to prevent potential destruction of property or loss of life.

If there are any other details that the judges should know about this project, please note them here: (In 300 words or less)

One of the technology partners on the IREMS project is the International Criminal Police Organization (INTERPOL). INTERPOL's purpose is to assist law enforcement agencies at all levels local, state, and federal by alerting officers worldwide, especially at airports and border checkpoints. The criminal activity that INTERPOL investigates is not commonly understood. Recently, this organization has been in the news as a result of several high-profile cases involving child pornography and kidnapping. Crimes against children have been increasing, especially internationally. Offenders can now distribute and access child pornography more easily via the Internet and even have direct contact with children. In March 2012, a Brazilian citizen arrived at the Grand Junction (Colorado) airport. After multiple communications over the Internet with two young girls, he took an international flight for the purpose of having sex with them. He was apprehended in Colorado, charged with traveling internationally to have sex with two minors under the ages of 16 and 12. These charges were announced by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) in Denver. The International Child Exploitation image database, managed by INTERPOL, allows investigators to share data with officials around the world in order to identify victims and perpetrators. At the end of 2011, more than 2,500 victims from 46 countries and approximately 1,400 offenders had been recorded in the database. Child sex offenders are increasingly traveling to other countries to prey on innocent children. Using IREMS biometrics technology, offenders, who previously might have fallen through the cracks of the system, will be apprehended before it's too late for other young victims.

COMPUTERWORLD