Semantic Scenarios for the Intelligent Enterprise

A Kyield Hypothetical Use Case

October, 2009

This is the third paper in a series of hypothetical use cases intended to be helpful in understanding the potential of semantics for different types of organizations, with a focus on the Kyield platform in particular. View our publications for additional scenarios.

SCENARIO 3: Roger the electrician at the hydro dam

An energy industry employee normally unassociated with the term 'knowledge worker' proves essential to his employer, community, and national security.

Roger is a trusted employee at a major hydro electric facility in the western United States. He married his high school sweetheart 15 years ago after his tour of duty in the military. He and his wife Sandy adopted two children within the first few years of marriage; Jennifer is now 11 and Trent is 13. In his spare time, Roger enjoys working around the house and spending time with his family and friends in the great outdoors near their home. Roger comes from a family with a long history of patriotism and military service.

After leaving the military, Roger trained as an apprentice electrician before joining a large electrical contractor in a fast growing metro area near his home town. When the housing crash occurred, Roger's hours were cut back to a few hours per week, so he began searching for a more stable job. He discovered that one of his old co-workers had been hired on at the hydro plant in the mountains a few years ago, becoming foreman of the maintenance crew, so Roger called his old friend Jack at home to catch up and see if he knew of any openings.

Jack informed Roger that nothing was currently available, but encouraged him to apply anyway so that his resume would be on file. They scheduled a time the following week to introduce Roger to the company's human resource manager. Roger was one of the best electricians Jack had worked with; honest, hard working, smart, dependable, and exceptionally skilled. Several months later a job opened up at the facility and Roger received the call, so he relocated his family to the small town near the facility and settled in to their new rural life.

Due to the importance of the facility and potential hazard for downstream communities, Roger was required to pass an extensive background check and receive special training in terrorism; primarily to spot signs of what might be dangerous activity. Security is a constant consideration for all employees and the topic of daily discussion.

Roger's current duties on the maintenance crew varies considerably depending on need. Some weeks he works as a classic electrician on remodeling projects scattered around the large facility, while

other times he maintains the vast network of security gear. On rare occasions Roger installs or repairs special equipment in the control room. His regular duties include a monthly inspection of all electrical rooms as part of a sophisticated preventative maintenance program.

On one particular day no different than any other, as part of his regular inspection loop, Roger drove one of the crew's all terrain vehicles (ATV) to a mechanical room below the dam. He enjoys this particular monthly excursion down a rough dirt road to a concrete bunker perched above the rapids.

On a routine task a key employee in the field notices something odd, which initiates a series of data transactions.

The mechanical room Roger inspects is located behind a large steel door, containing primarily heating and cooling equipment for the network of corridors on the lower side of the dam. Adjacent to the mechanical room is a long tunnel used primarily as an air return serving the massive room housing the hydro electric turbines. The tunnel is further protected by a locked iron gate.

Roger completed his inspection and tests as usual with no surprises, returning his tools to the ATV. Since it was his final task of the day he decided to walk down to the river to enjoy the sounds of the rapids, and hopefully catch a close-up glimpse of one of the giant sturgeons that could often be seen from on top of the dam.

As he hopped over a small pool of water on a granite boulder, Roger spotted something unusual that took him by surprise. Rising just above the pool of water was an outline of a boot print, so he knelt down for a closer look and confirmed his suspicion. Looking across the boulders he could make out a faint trail of prints that led to the backside of the mechanical building, where he found several more boot prints in two different sizes. Roger suspected that the boot prints belonged to the security crew, but couldn't understand why they would be so interested in the backside of the concrete bunker. It then dawned on Roger that he was standing directly above the tunnel.

A 'near miss' between Roger and Jack's personal mobile phones has potentially catastrophic consequences. A brief overnight thunderstorm could have erased the evidence, preventing the photos from match-making functionality with partners.

Roger thought of calling his boss Jack on the radio, which is the normal protocol for anything that looked odd, but Jack had surely gone home for the day by now, so Roger decided to take a few pictures on his new mobile phone and send it to Jack; one of few numbers Roger had bothered to key in to his phone.

Jack was waiting for his wife at the local café when his phone jingled in a tone meaning that someone was sending him a text message or picture; usually junk mail. When he saw that the message was from Roger at work, he was surprised; and more so by the close up photos of boot prints. Jack thought it must have been an accident and was about to erase the message when the second photo arrived of the boot prints behind the old mechanical building, followed by text: “weird find.. on my way home – R”.

Jack recognized the location above the lower tunnel entrance; a place very few people have visited since the facility was built. He was not aware of any reason why two or more people would be in this secure location, so he forwarded the picture to the security manager at the plant with a brief message.

Rita was just getting ready to leave the office after a long day of mundane tasks when she received the incoming message on her hand-held from Jack. As soon as she saw the photos, Rita immediately realized that if Jack didn't send the owners of the boot prints to this location, no one from the facility did. Even if a couple of her people had decided to explore the area without informing her, she could think of no one at the facility who wore boots matching that kind of print.

Rita had been named acting head of security at the facility the previous year so she attended a mandatory Department of Homeland Security (DHS) conference in D.C. for new security supervisors of key facilities. The photos she was now viewing were eerily similar to those in a slide show given by a speaker at the DHS conference who was the nation's premier anti-terrorist specialist. Rita called home and left a message for her husband Jim to not expect her for dinner, then called her manager at home to brief him on the issue, before informing each member of her crew.

The data reaches the appropriate team member in the decision chain, who begins the investigation. The system design empowers members to escalate immediately to appropriate experts and decision makers through automated predetermined parameters set by the Kyield CKO Module. Members also have the option of using personal judgment.

Rita walked to the adjoining office that contained monitors of security cameras throughout the facility. She tested two cameras that covered the area in the photos Jack sent. The coverage wasn't optimum, but she could not understand how these intruders could have made it to this location without detection. Rita quickly scanned the camera files through the previous four days since the last heavy rain, finding the prints appearing for the first time the morning after the rain. Still wondering why the intruders did not trigger an alarm from motion detectors, she scanned back through the digital film until she finally found two dark figures in a very heavy rain; apparently a large male and small female, dressed in black with masks. She realized that she would probably have missed spotting these figures in such conditions even if fresh and watching the monitors closely. Rita quickly copied the clip to a disk and hurried over to a work station across the room.

For the previous three months, Rita had been participating with a select group of major U.S. facilities in a confidential test of a new system under consideration by the DHS. This new system was similar to the semantic web technologies Rita had read about, but this system was more advanced and tailored to the specific needs of the DHS; fully encrypted and under tight security. As part of the test, Rita received a PC on loan from the DHS with a security card, biometric layer, and password protection. The DHS computer was on a separate network from her company LAN and work PC with its

own external high bandwidth circuit that was reported to have additional extra security of some kind. Rita's computer was just one node of a large DHS test network that included a super computer for crunching large data sets.

All Rita knew about the system was that when the computer confirmed her identity as she logged on to the DHS partner network, every information 'transaction' she made was tracked with embedded intelligence on every person, organization, and file created, stored, shared, read, or sent. So far Rita had only conducted the online training and tests that were otherwise very similar to her company's intranet. This custom DHS system was fully automated, using the browser for creating documents and to operate the special communications account. Each member of the network was listed in a topically designed database with simple and fast navigation. This network had three primary purposes; to prevent terrorism acts against major U.S. facilities; to assist in prosecuting anyone conspiring to commit such acts; and to learn as much as quickly as possible about improving those tasks.

Fortunately for downstream residents, the facility was included in a test of the DHS prototype; a highly defined mission-oriented system with precision semantic intelligence embedded in every file entered into the system.

Rita logged on to the DHS network, downloaded the photos from her hand-held device, and opened the browser to the real-time communications program, which Rita considered a hybrid of video conferencing, email, and chat. Rita first selected the nature of her topic from the menu: 'possible terrorist threat', and then selected 'evidence attached', followed by typing a short text message describing the event.

Rita's original message and each one to follow was automatically routed based on embedded intelligence about her individually, her location and facility, the selections she chose for the message, and the text within her message. She then selected the titles of six recipients for the message, fully aware that many others with a need to know and proper clearance would automatically receive an alert, any of whom could then elevate immediately within their own networks to whomever they felt appropriate. Each of those recipients could also select a pre-determined phrase that would automatically alert the appropriate people.

The system designer intended to maintain both opaque and transparent messaging in the system simultaneously to prevent the type of systemic failures that led to crises in recent years. DHS analysts believed that if such a system were in place at the time of the Phoenix memo, the 9/11 attack could have been prevented.

Within seconds of uploading her security cam file, four green lights adjacent to identities on her list confirmed that all but two of Rita's selected recipients had received the files and were viewing, and another larger yellow blinking light appeared on her screen confirming that the 24x7 analyst on duty, a senior anti-terrorism

expert, was live and reviewing her activity. Another red light flashed seconds later confirming that one of her selected recipients had elevated the message to a party restricted from her security level, which automatically committed additional resources to the event, including scheduling a time on calendars for a team of experts to discuss in a video conference the next morning.

What Rita didn't know was that her selection of 'possible terrorist threat', followed by 'evidence attached', automatically launched a powerful algorithm employing a super computer that cross-referenced the photo files with intelligence agencies around the world, the results of which were immediately visible in a small window of the DHS senior anti-terrorism analyst's PC. Encrypted alerts were then sent live with links to the search results arriving within seconds to on-duty analysts in several agencies. Within a few minutes the super computer returned potential matches to the photos along with an estimated mathematical probability. Due to the masks worn by the intruders, distance from the cams, and heavy rain, in this case the probability of a match was below 30%.

The fully automated DHS system embraces interoperable standards, allowing less costly integration with powerful programs, essential allies, and global partners.

The embedded intelligence on Rita, her facility, and the dates on the security cam file also triggered an automatic cross-reference search with transportation and financial databases. The initial search cross-referenced the previous query return, turning up only one suspect on the list who traveled through the region using a credit card under their real name. The second query cross-referenced all known terrorist suspects in the network databases, returning several aliases believed to be used by Al-Qaeda suspects who traveled through the area during the time window.

After quickly reviewing the automated query returns, the DHS analyst on duty forwarded a file link for specialists to run additional queries and follow up on the data. He then clicked on Rita's image adjacent to the message, right click 'video call', and Rita appeared in a two-way video conference. The DHS analyst thanked Rita for fine work, asked several additional questions surrounding the event, and requested that her crew seal off the entire area. He then informed her that his office was already contacting local and regional officials, five of whom had been alerted automatically and were currently reviewing the growing file of evidence on DHS computers identical to Rita's.

After several visits from investigators, Rita received a message on her DHS computer with preliminary results. One expert on security cams reported a little known flaw with the motion detector system in use by the hydro facility. Suspected terrorists had conducted similar reconnaissance at several facilities in North America and Europe that employed the same model of motion detector. Apparently the intruders were able to confirm the make and model of the security devices with high powered scopes, and then coordinated their on-

site reconnaissance with forecasts of heavy rain or snow. They were able to 'fool' the motion detectors with a low tech, home-made deflector, and by avoiding the brightly lit areas were able to prevent detection by security cams with black clothing on very dark nights. Security consultants were able to replicate the intrusion with a live test in similar conditions at a DHS facility. The report outlining the flaw in the motion detectors was 'red flagged' by a DHS analyst to 'facility security managers', automatically alerting Rita's peers who were participating in the prototype test.

The initial consensus by analysts was that the intruders were seeking a path of least resistance into the tunnels at the base of the dam, where others in their cell would return at a later date to place high powered explosives and detonate in a suicide attack. The effectiveness of the attack would depend on the placement of the device, the type and size of explosives, and if the intruders made it that far; a certain amount of luck. If the dam failed, an alarm would be sounded downstream, but within 40 minutes tens of thousands of people would lose their lives unless they could be evacuated in time. Unfortunately, while terrorism experts were confident of the identity of the two intruders, they were not yet in custody, nor were their locations known... at least one major facility was under surveillance by sophisticated terrorists who may be sharing intel with others.

A classic case of well connected dots along a data trail with short cuts made possible only by highly relevant semantic intelligence embedded within a logical, holistic design.

The immediate solution for Rita was to upgrade the security system and begin the process of reinforcing all access points to the dam. After consultations with DHS and private security consultants, the facility agreed to partner with federal and local law enforcement to substantially increase the use of heavily armed guards to thwart a less stealthy attack. A few weeks after the event, some normalcy returned to hydro facility, although at a new higher level of functionality.

Ten months later Rita received a follow-up message through the DHS computer network, which was in the process of being expanded to all high-risk facilities in the U.S. and EU. A law enforcement agency in the EU had recently submitted photos to the network of suspects thought to be conducting surveillance for terrorist attacks, which were automatically matched to two suspected terrorists who rented a car using false IDs at an airport close to Rita's hydro facility; the dates aligned. The super computer then also cross-referenced the photos submitted by Rita. The security cam image of the two dark figures returned a probability match of over 50%, but it was Roger's photo from his mobile phone of the boot prints that convinced both the super computer and the judge who issued an arrest warrant that it was the same individuals. The couple had made the mistake of wearing the same boots in the EU, leaving identical prints that increased the probability of a match to over 90%. Human expert review subsequently concurred with the super computer program.

A hypothetical yet plausible scenario is presented that demonstrates the value of a state-of-the-art knowledge system deployed in a highly tailored, mission-specific environment, resulting in a very high triple bottom line ROI.

When investigators searched the suspects' hotel room, they found a laptop that contained detailed notes on several facilities in the U.S. and EU, as well as clear links to Al Qaeda VIA communications with known members in Pakistan. Fake identification was found that linked the pair to multiple trips to Pakistan and Algeria during the previous two years. Additional evidence found at the scene led to several other members of the same cell in multiple countries, including several in the U.S. believed to be close to executing an attack. The terror alert in the U.S. was elevated as law enforcement in many countries aggressively pursued all leads related to locating the members of this dangerous terrorist cell.

Almost a year to the day from when Roger discovered the boot prints along the river, he was watching the morning news with his family while enjoying a rare breakfast together, when the network interrupted with a breaking news story:

> ".... is reporting that two terrorist suspects have been arrested at an apartment hotel five miles from a nuclear power plant in the southwestern U.S. Officials report that police found large amounts of Semtex and C-4 in the suspects' room, as well as detailed drawings, photos, and notes describing security details at the nuclear plant. A warrant has just been issued for an employee at the plant who is suspected of conspiring to commit a terrorist act.... A few minutes ago a high ranking security official in the administration confirmed that the suspects were linked to a terrorist cell planning multiple attacks in the U.S. and EU. The cell was initially uncovered due to evidence discovered by an unnamed maintenance worker at a U.S. hydro facility last year.... more details to follow."

A few months later Roger received an award from the Secretary of the DHS and a check for $25,000 presented to him by a fire chief from his hometown fifty miles downstream from the dam. The token of appreciation represented 50 cents for every citizen living within the estimated flood zone of a catastrophic dam failure. The funds were raised by first responders in communities located all along the river below the dam who were grateful to be spared.

Kyield

Semantic Scenarios for the Intelligent Enterprise

SCENARIO 3: Roger the electrician at the hydro dam

October 2009
Author: Mark Montgomery
Phone: +1.505.629.5433
Email: markm@kyield.com
www.kyield.com