Enhancing IoT Security with ATTRIBUTES!
The common thread in the fabric of security

Queralt, Inc.
Michael Queralt and John Tolbert

December 16, 2014
Team Profile

- David Cook - CEO
- Michael Queralt - President
- John Tolbert - VP, Cybersecurity; SAML / XACML; OASIS Distinguished Contributor
- Daphne Page - Security Engineer; System Administrator
- Jesse Youngblood – Lead Architect; developer
- Steve Abbagnaro - Lead Architect; developer

Location-based Access Control
http://www.youtube.com/watch?v=SbneUulzvuU

Supported NCCDC
Queralt Evolution

Sensorial Hardware Integrator & Reseller
Resold RFID hardware & end user solutions

DHS SBIR (Phase I)
Science & Tech Directorate
Highly Scalable IdM (Identity & Access Mgt)
Context-aware Physical & Logical Access Control
Proof of Concept

DHS SBIR (Phase II & III)
Science & Tech Directorate
Location-based Service adding Geospatial Coordinates and Sensorial Data as Attributes in Access Control Decision
End-to-end System Pilot @ Advanced Physics Lab at Johns Hopkins

Custom SW Development:
Sensorial Solutions (v0)
(I) RFID (active + passive) asset mgt
(II) people monitoring (eldercare)
(III) location tracking analytics

Platform Redesign (v2)
(I) Linux migration
(II) re-architect (context engine & decision engine based on context)

DHS - S&T Back-End Attribute Exchange
(I) BAE Use Cases
(II) Architecture
(III) Oper. Pilot
(IV) Commercialization

"Data Agnostic Informatics" Program (v1)
(I) standard aggregation of data sources
(II) "simple" decision engine (IFTTT)
(III) Behavioral learning system (prototype)

PaaS for Devs (v3)
(I) scalability & performance
(II) designed as PaaS from ground up (modularized & API driven)
Queralt Funding
The Threat

China could take down America's power grid: US official

Military secrets theft hacking trail leads to Russia

Intel boss' warning on cyber attacks no joke, say experts

Experts Say Russian Website Routinely Watches You Via Your Webcam

Russia is behind cyber attack on banks, says Kevin Mandia
The Threat
The Impact of the Threat
iQ3 turns your information into intelligence

Information without context is meaningless. Our platform takes your data and through thorough real-time analysis, turns it into meaningful, actionable intelligence.
Our Approach - Context

• Injecting Real Time Context into Security Decisions

  – What is context
    • “the interrelated conditions in which something exists or occurs”

- Why is it important

How do we do it
  • Using IoT Platform
  • Using BAE
  • Cyberphysical systems for Real Time Decision Making
  • Standards
User: Rene.Descartes
Group: Philosophers
Citizenship: French
Group: Rationalists
Location: France

USG Clearance: None
NATO Clearance: Secret
EU Clearance: Top Secret
Group: Epistemologists
Approach — Attributes

- Qualities of People, Places, and Things
- XACML: Characteristic of a subject, resource, action or environment that may be referenced in a policy
- Attributes can be the basis of physical and logical access control systems
- Subject attributes can be stored in SQL databases, LDAP databases, XML files, flat files, and PIV(-I) cards
- Resource attributes can be stored as metadata on data objects
- Attributes can also be obtained at run-time from environmental conditions (computers, networks, sensors, etc.)
XACML Attribute Types and examples

- **Subject**: users, devices
- **Resources**: data objects, networks, devices, physical systems, etc.
- **Actions**: CRUD, SMTP send, copy, paste, open, etc.
- **Environment**: Time, date, geolocation, etc.
Approach — BAE

- BAE Operational Pilot follows SAML BAE profile: common set of attributes such as FASC-N and UID from PIV-I certificates, DN from x.509 certificates, etc.
- Serves as “attribute router” between authoritative domains
- Proof-of-concept underway; pilot in 2015
- Providing new capabilities for First Responders
- Integrating Incident and Disaster Response across federal, state, and local jurisdictions
- Creating a Trusted Environment when connecting DHS to their partners across federal, state, local, and private sector entities
Technology

Backend Attribute Exchange

Diagram showing the integration of different enterprises and systems, including DHS Affiliate, DHS S&T R&D General Support System, Partner Enterprise, and various services and protocols such as LDAP and FICAM-BAE.
Benefits —

• Increase security
  – Diverse attribute locations (no single point of attack)
  – Real time Adjustment

• Local attributes are best — most likely to be accurate

• Links Identity Provider organizations to a variety of applications

• Enables Cyber-Physical use cases: digital attribute evaluation for physical access

• Reduces architectural and infrastructure duplication

• Reduces cost and complexity of integrating inter-agency identity providers with computing applications and cyber-physical systems
Early use cases

Customer Solutions:

- **Context aware access control & security application**
- **Context aware eldercare safety & wellness application**
- **Context aware inventory & compliance application for specialty labs**
Context Platform as a Service

Platform modules coded to analyze + process data and apply “context” to it (e.g. pressure normalization; resident wander, etc.)

Evaluators

Platform modules coded to evaluate rules based on context (e.g. pressure out of range; location change, etc.)

Act

Finalize
(Export)

Hosting & Support: Queralt Cloud (Included in subscription)

Monthly subscription fees covers:
(metered by # of entities & type)
1) Processes all data-in-motion, in Real-Time
2) Hosting & support of PaaS modules

End-User: Assisted Living Provider

Contextual Questions:
1) Where are all residents currently?
2) Is resident “John Smith” at risk due to location and/or condition?

1) Customizable components to make for easy software solution development (canned reports, dashboards, etc.)
2) Sensor connection library making it easy to integrate real-world data

Solution:

Hardware Environment

Deployment:

Assisted Living Campus

Entities & Tags

Residents - Bracelet w/ RFID

Readers & Zones

Reader - Impinj w/2 Antennas

End-User Roles & Form factors

Nurses - iPad App, Web Interface
Security - Pager / Mobile

Secure APIs

Platform modules developed using iQ3 API specification; Developed internally or by Queralt Professional Service ($)

Solution components required to display real-time data

Alerts

Solution components required to display alerts/notifications + enforce decisions based on context (e.g. 911 alert, geofence violation alert)

Dashboard

Solution components required to display reports w/processed data

Reports

Solution components required to display processed data

Legacy

Additional Software applications that connect to the iQ3 powered solution (or vice versa)

Admin

Contextual Questions:

1) Where are all residents currently?
2) Is resident “John Smith” at risk due to location and/or condition?

1) Customizable components to make for easy software solution development (canned reports, dashboards, etc.)
2) Sensor connection library making it easy to integrate real-world data

Solution:

Software Solution

Solution developed using iQ3 building blocks as a framework

Developed internally or by Queralt Professional Service ($)

Hosted: Queralt($) Support: Masonicare, Queralt($)

End-User Roles & Form factors

Nurses - iPad App, Web Interface
Security - Pager / Mobile

Secure APIs

Platform modules developed using iQ3 API specification; Developed internally or by Queralt Professional Service ($)

Solution components required to display real-time data

Alerts

Solution components required to display alerts/notifications + enforce decisions based on context (e.g. 911 alert, geofence violation alert)

Dashboard

Solution components required to display reports w/processed data

Reports

Solution components required to display processed data

Legacy

Additional Software applications that connect to the iQ3 powered solution (or vice versa)

Admin

Contextual Questions:

1) Where are all residents currently?
2) Is resident “John Smith” at risk due to location and/or condition?

1) Customizable components to make for easy software solution development (canned reports, dashboards, etc.)
2) Sensor connection library making it easy to integrate real-world data

Solution:

Software Solution

Solution developed using iQ3 building blocks as a framework

Developed internally or by Queralt Professional Service ($)

Hosted: Queralt($) Support: Masonicare, Queralt($)

End-User Roles & Form factors

Nurses - iPad App, Web Interface
Security - Pager / Mobile

Secure APIs

Platform modules developed using iQ3 API specification; Developed internally or by Queralt Professional Service ($)

Solution components required to display real-time data

Alerts

Solution components required to display alerts/notifications + enforce decisions based on context (e.g. 911 alert, geofence violation alert)

Dashboard

Solution components required to display reports w/processed data

Reports

Solution components required to display processed data

Legacy

Additional Software applications that connect to the iQ3 powered solution (or vice versa)

Admin

Contextual Questions:

1) Where are all residents currently?
2) Is resident “John Smith” at risk due to location and/or condition?

1) Customizable components to make for easy software solution development (canned reports, dashboards, etc.)
2) Sensor connection library making it easy to integrate real-world data

Solution:

Software Solution

Solution developed using iQ3 building blocks as a framework

Developed internally or by Queralt Professional Service ($)

Hosted: Queralt($) Support: Masonicare, Queralt($)

End-User Roles & Form factors

Nurses - iPad App, Web Interface
Security - Pager / Mobile

Secure APIs

Platform modules developed using iQ3 API specification; Developed internally or by Queralt Professional Service ($)

Solution components required to display real-time data

Alerts

Solution components required to display alerts/notifications + enforce decisions based on context (e.g. 911 alert, geofence violation alert)

Dashboard

Solution components required to display reports w/processed data

Reports

Solution components required to display processed data

Legacy

Additional Software applications that connect to the iQ3 powered solution (or vice versa)
Our Products

• iQ3 – IoT Platform for Industrial Customers
• Attribute-based access control services
  – BAE Compliant Visitor Log
  – Managed Service Tiers for Backend Attribute Exchange
  – System Integration and Testing
  – GeoXACML and CyberPhysical authorization
  – Strong Authentication and Authorization via Mobile Devices
  – Policy Management, Distribution, and Synchronization
• IoT and Open Source Intelligence Analysis
Roadmap

• 2015
  • BAE Managed Service Provider
  • Onboarding federal, state, local agency identity providers
  • Integrating with TSCP applications
  • Mobile device authorization pilot
  • Geo4NIEM POC development
  • Policy Management system development

• 2016
  • Policy Management Pilot
  • Mobile device authorization system deployment
  • Geo4NIEM pilot
  • IoT & Open Source Intelligence Analysis development
Contact Info

• Michael Queralt
  • michael.queralt@queraltinc.com
  • 914-450-0879

• John Tolbert
  • john.tolbert@queraltinc.com
  • 253-670-5322
THANK YOU