FoxGuard Solutions

The Patch and Update Management Program for Energy Delivery Systems

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

Patch and Update Management Program

Objective

- Simplify Patch Management of Energy Delivery Systems

Schedule

- **Project Start:** October 2014
  - **Phase I** – Plan, Prep & Research (Completed)
  - **Phase II** – Design & Develop (In Process)
  - **Phase III** – Test, Implement & Demo (In Process)
  - **Phase IV** - Commercialization
- **Project End:** September 2017 (Projected)

Performer:	**FoxGuard Solutions**
Development Partner:	**TDi Technologies**
Program Participant:	**NRG Energy**
Federal Cost:	**$3,298,891.00**
Cost Share:	**$995,344.00**
Total Value of Award:	**$4,294,235.00**
Funds Expended to Date:	**38%**

Advancing the State of the Art (SOA)

Current State

- Existing solutions:
  - Are fragmented with limited coverage
  - Do not provide standardized actionable output
  - Have widely varying capability sets

Feasibility of Our Approach

- Fill a gap left by existing solutions
- Minimize performance impact and ensure system stability
- Leverage what has come before us and has been proven in this environment
- Release iteratively, remain flexible and pivot when necessary

Advantages to Our Approach

- Common interface across different equipment types and genres
- Data translation layer promotes uniformity of information to the end user

Advancing the State of the Art (SOA)

End User Benefits

- Centralizes patch and update information
- Supports programmatic equipment querying using automation and a common toolset
- Simplifies association between software and available patches / updates

Cybersecurity Advancements

- Promotes end user awareness around patching, presence of vulnerabilities and change management processes
- Provides common security classification in absence of vendor classification
- Considers named sub-components and libraries to provide more comprehensive security assessment
- Reduces likelihood of incorrect patch application
- Standardizes presentation of patch information to end user

Challenges to Success & Paths to Overcome

Challenge 1: Lack of Vendor Cooperation and Support

- Engage the asset owners – leverage collective voice to drive vendors' attention
- Continued education and discussions with vendors

Challenge 2: Technical Limitations with Equipment Querying

- Usage of native equipment protocols and commands
- Allow flexibility in defining what should be programmatically queried vs. manual

Challenge 3: Patch and Update Data is Compromised

- Implementation of secure development practices and technologies
- Usage of "meaningless keys" to represent sensitive equipment attributes

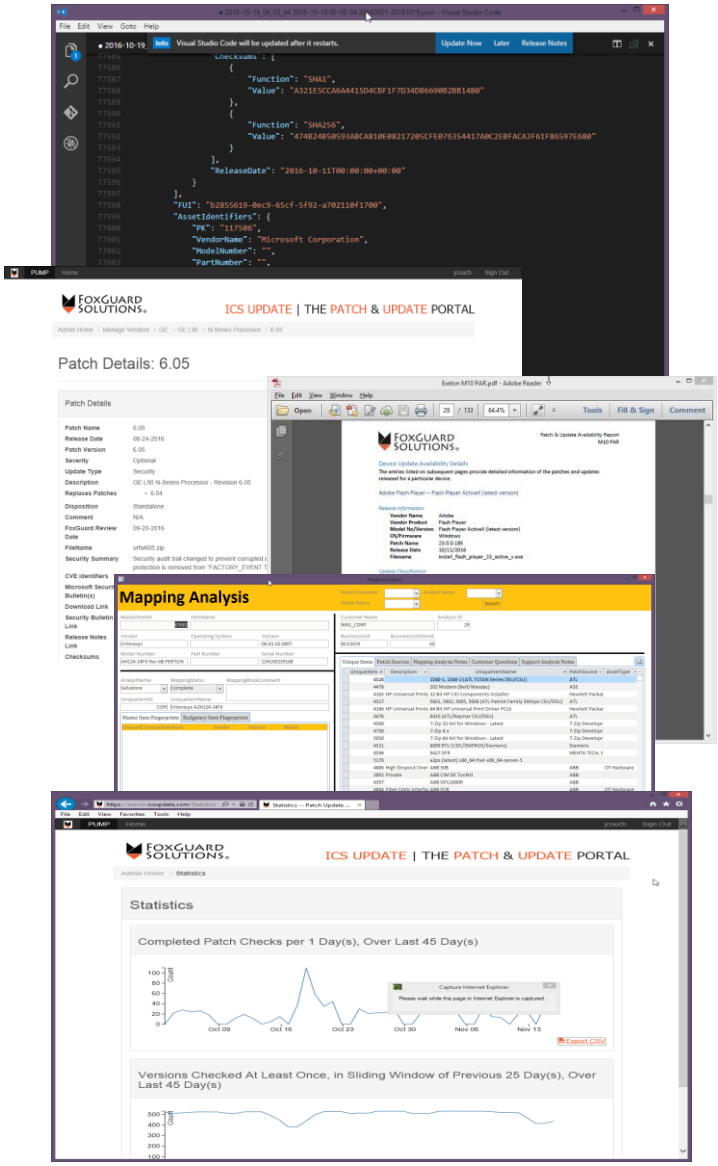
Challenge 4: Standardizing a Highly Diverse Industry

- Usage of a data translation engine to standardize outputs based on diverse inputs
- Usage of automation technologies

Progress to Date

Major Accomplishments

- Patch and Update Portal and Administration Portal (backend) is fully operational for internal use and being tuned based on daily use
- First iteration patch mining automation tools created
- First iteration of the Asset Analysis Tool created, launched and in use
- Patch and Update Portal and Equipment Query Solution integration proof of concept successful
- Patch Availability Reporting capabilities are fully operational for external use and being tuned based on participant and asset owner feedback



Milestones Reached

Milestone #2 – Conduct Project Research & Field Interviews Completed

Collaboration/Technology Transfer

Asset Owner Benefits

- Patch and Update Portal
- Equipment Querying Solution
- Additional Program Elements

End-to-end solution features

Vendors and Equipment Manufacturers Benefits

- Patch and Update Portal
  - Increase accessibility to publically available patch and update information
  - Drive awareness of sub-component and library changes for development teams

Other Industry Member Benefits

- Patch and Update Portal
  - Increase accessibility to publically available patch and update information
  - Awareness of private patch and update information

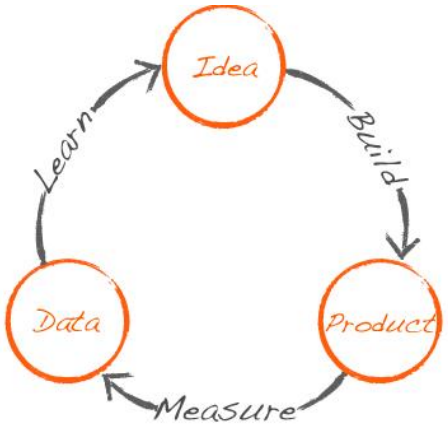
Gaining Industry Acceptance

Do Not Operate in a Vacuum – Inform & Solicit Feedback

- Collaboration with program participant and other asset owners to maintain continuous feedback loop
- Continued education and exposure with vendor, OEMs and other industry members

Utilize MVP Approach, Iterate and Pivot When Necessary

- In-house testing of individual program elements
- In-house testing of partial system integration
- End-to-end dry run testing in our in-house lab environment
- End-to-end field testing with program participant at demonstration site



Support with Factual Data to Quantify Benefit

Next Steps in Our Project

Next Steps

- Completion of Patch Validation, Education and Training efforts
- Refinement of Equipment Querying Solution
- Full integration between program elements
- In-house dry run testing
- In-field testing with on-site demonstration with program participant (NRG Energy)
- Continued commercialization activities
- Go to Market!

Key Milestones to Accomplish

05/31/2017 – Design and Development Complete

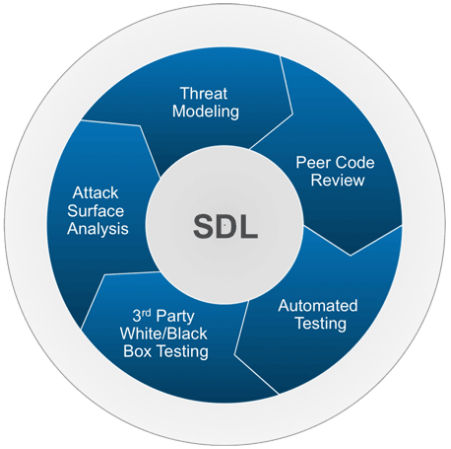
07/31/2017 – In-House Dry Run Testing

09/15/2017 – In-Field Demonstration with Program Participant

Cybersecurity Considerations

Development Approach

- Secure Development Lifecycle (SDL) is standard operating procedure
  - Use of pair programming and peer review prior to commit
  - Automated unit, integration and system testing to ensure code promises are met
  - Strict use of version control and code merge practices
  - Protections in place against insider threat
  - Continuous learning / awareness of latest threat vectors



- Where possible, approach is to simply avoid development methods that have insecure implementation possibilities – reduce attack surface

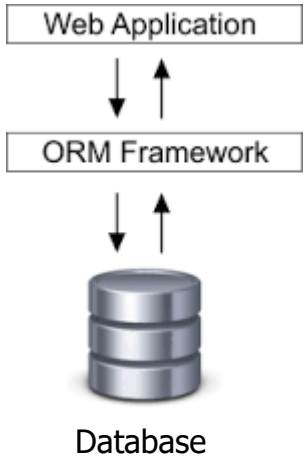
How are We Protecting Sensitive Information

- **Data in Transit:** Delivered via secure site-to-site file transfer technologies with automated removal from externally accessible system upon receipt
- **Data at Rest:** Stored in encrypted storage requiring multi-factor authentication over physical and logically restricted network segment

Cybersecurity Considerations

How are We Securing the Patch and Update Portal

- Hosted entirely in cloud
  - Provides strong physical security, high availability and stringently managed environments
- Running on Service Oriented Architecture (SOA)
- Uses Object Relational Mapping (ORM) and Model View Controller (MVC) frameworks to abstract direct database access
  - ORM framework protects database (mitigates ability to execute SQL injection and other common web/database attacks)
  - Code is not executed directly against the database, but rather against the ORM framework (which handles the backend database communication)
  - MVC helps protect against XSS and other similar attacks



- Minimum application layer / component interdependence
- No shared code between the various application layers and functions means that a compromise of code in one component does not mean a compromise elsewhere

Conclusion

Follow-On Discussion

Q&A