

Information Sharing Issues with Control System Security Incident Reports

Paul Thompson
Dartmouth College

I3P Process Control System Security Project

- Objective
 - Develop and demonstrate a concept for next generation PCS incident reporting that addresses some important obstacles (technical and cultural) to information sharing
 - Team
 - MITRE Corporation
 - Dartmouth College
 - Sandia National Labs

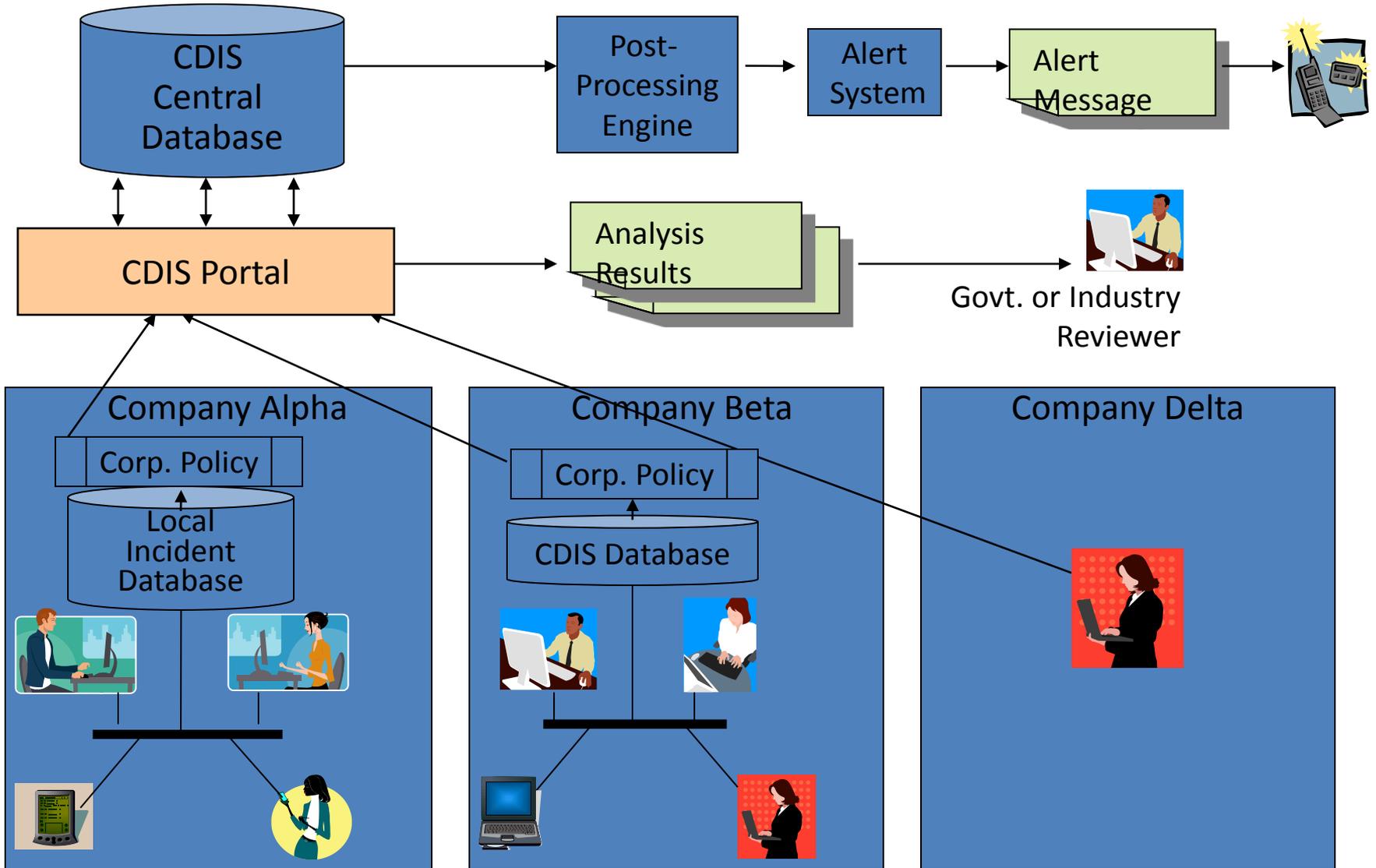
Focus Areas

- Collect and document information sharing requirements
 - Cyber incidents and warnings
 - Suspicious behavior/events (physical, social engineering)
 - System status (steady state, crisis)
 - Taxonomy for classifying information

Focus Areas (cont.)

- Identify and document gaps in technology
 - Controlled information sharing
 - Anonymity in reporting
 - Automated and interactive analysis capability
 - Searchable database of PCS incident information
- Develop an incident taxonomy as a means of categorizing effects and mitigations
- Develop and demonstrate a proof-of-concept prototype

3-Tiered Information Sharing Model

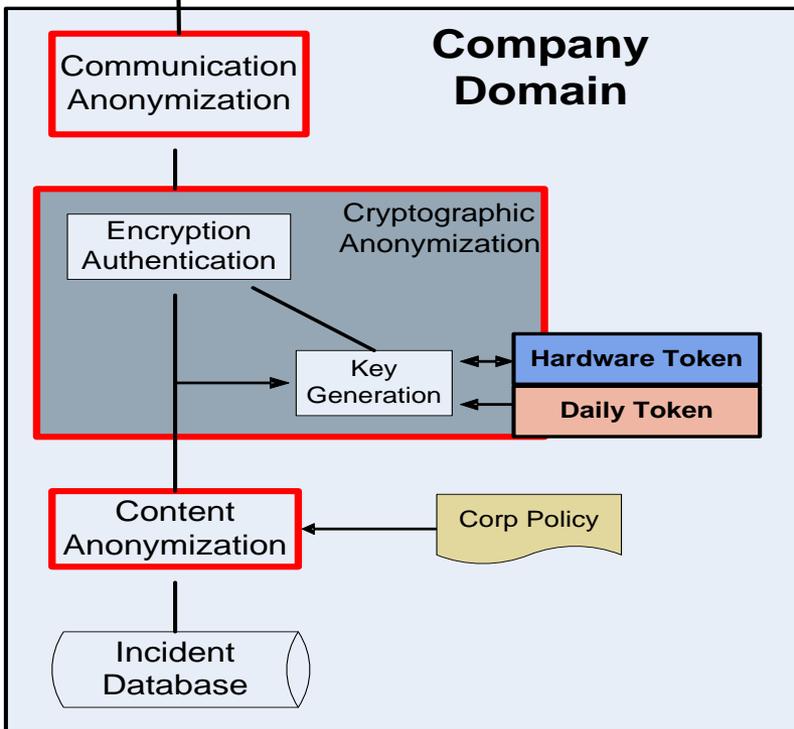
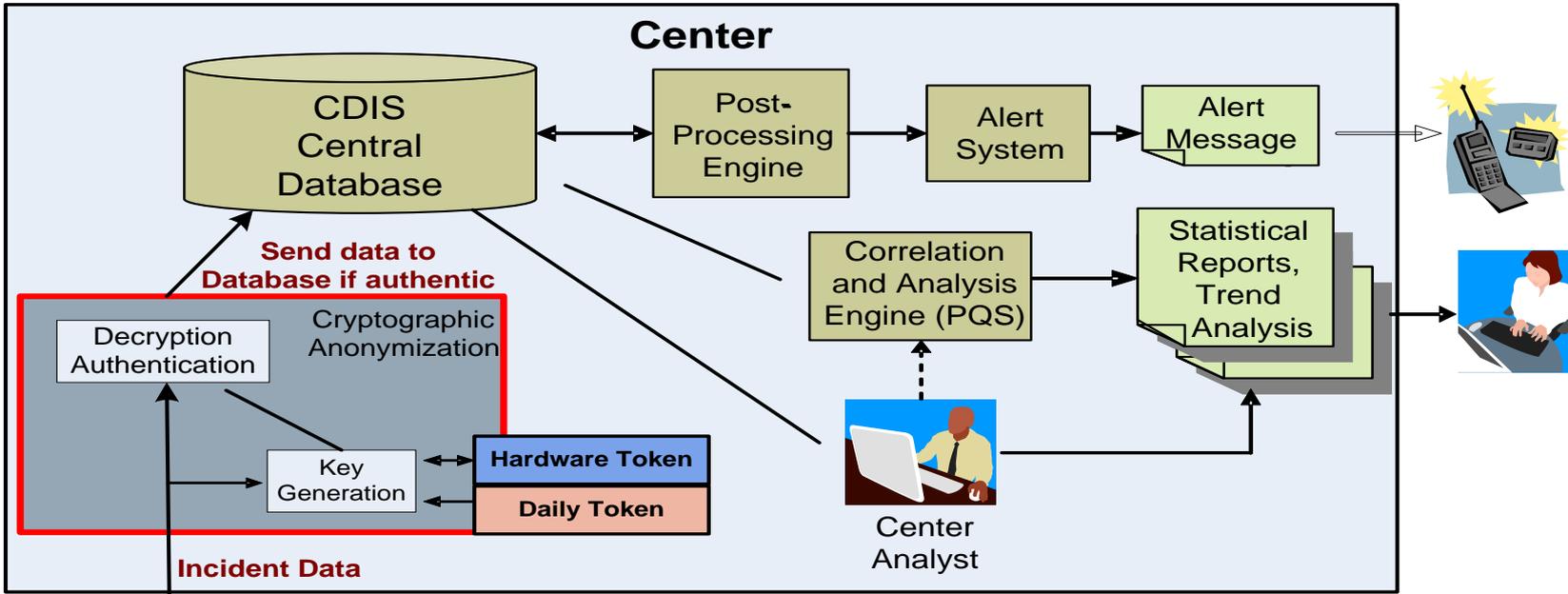


Anonymity in Incident Reporting

- Premise: The community maybe more motivated to share if security and anonymity protections were in place
- Application of Sandia National Labs research in anonymous, authenticated communications
- Key attributes of an anonymity solution
 - Anonymity of the information provider
 - Anonymous network communication paths
 - Authentication of the source
 - Anonymity, confidentiality and integrity of the data
 - Protection against system abuse by insiders

Anonymity (cont.)

- Key technical elements
 - Crypto-based protocols for anonymity
 - Anonymous network communication
 - Anonymizing message content



Anonymous, Authenticated
Communication in a CDIS
Application

Industry Information Sharing

- Technology alone will not motivate information sharing
- Culture shift is needed
- Standard nomenclature for incident artifacts will improve consistency and quality of reporting and analysis
- Anonymity is important, but will affect quality of analysis

Correlation Analysis in the CDIS

- Analyses of incident types and effects
 - Statistical trend analysis
 - Correlation analyses, e.g.,
 - Incidents at this site compared to the sector
 - Incidents at this sector compared to industry wide
 - This site, or sector, is being targeted
 - Momentum analysis
 - Attacks are increasing, or decreasing
 - Analysis of alarm data and incident reports
- Visualization and summarization of data

Next Steps

- Make CDIS proof-of-concept demonstration available on the internet
- Follow-up with interested parties
 - Concept for PCS incident information sharing
 - Contributing CDIS technologies
 - Discussions with US CERT

Acknowledgements

- Sandia: Tim Draelos, William Neumann,
Richard Schroepfel
- MITRE: Christine Eliopoulos
- Dartmouth: George Bakos, George Cybenko,
Marion Bates