U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

Gordon H. Rueff

Idaho National Laboratory (INL)

Sophia Proof of Concept

INL/CON-10-19389

INL Idaho National Laboratory

Summary Slide: Sophia Proof of Concept

- **Major Successes:**
  - Deployed at 2 utilities.
  - Additional use cases found during development/deployment.
  - Deployed at 1 vender.
  - Saved 1 man-month of time.
- **Roadmap Goals:**
  - **Measure and Assess Security Posture**
    - **(long) Real-time security state monitoring for new and legacy systems commercially available**
    - **(end) Energy asset owners are able to perform fully automated security state monitoring of their control system networks with real-time remediation**

- **Schedule:**
  - 2009.12.10 - Deployed
  - 2010.05.25 - Final Report
- **Level of Effort:** $200K
- **Funds Remaining:** $0K
- **Performers:** INL
- **Partners:** Idaho Falls Power, Austin Energy, ABB

Idaho National Laboratory

Summary Slide: Sophia Proof of Concept

- **Consistent training materials on cyber and physical security for control systems widely available within the energy sector**
  - **(mid) Secure connectivity between business systems and control systems with corporate network**
- **Sustain Security Improvements**
  - **(near) Major info protection and sharing issues resolved between the U.S. government and industry**
  - **(mid) Compelling, evidence-based business case for investment in control system security**
  - **(end) Energy asset owners and operators are working collaboratively with government and sector stakeholders to accelerate security advances**

- **Schedule:**
  - 2009.12.10 - Deployed
  - 2010.05.25 - Final Report
- **Level of Effort:** $200K
- **Funds Remaining:** $0K
- **Performers:** INL
- **Partners:** Idaho Falls Power, Austin Energy, ABB

Summary Slide: Sophia Proof of Concept

- **Roadmap Challenges:**
  - Limited ability to measure and assess cyber security posture
  - Growing risks from increasingly interconnected systems
  - Poorly designed connections of control systems and business networks
  - Performance may degrade from security upgrades to legacy systems
  - Increasingly sophisticated hacker tools
  - Poor industry-government coordination
  - Poor understanding of cyber risks
  - Weak business case for cyber security investments

- **Schedule:**
  - 2009.12.10 - Deployed
  - 2010.05.25 - Final Report
- **Level of Effort:** $200K
- **Funds Remaining:** $0K
- **Performers:** INL
- **Partners:** Idaho Falls Power, Austin Energy, ABB

Technical Approach and Feasibility

- **Approach**
  - – Develop “best guess” using “tribal knowledge”
  - – Vet “best guess” against target audience
  - – Plan finished tool based on tool success and feedback from audience
- **Metrics for Success**
  - – As a proof of concept, success is defined by whether the concept is proved useful. The metric for this is the response from industry.

Technical Approach and Feasibility

- **Challenges to Success**
  - Refine Sophia
    - Choose features wisely
    - Keep it simple

- **Technical Achievements to Date**
  - Deployed at 2 asset owners
  - Deployed at 1 vendor
  - Feedback and lessons learned

Collaboration/Technology Transfer

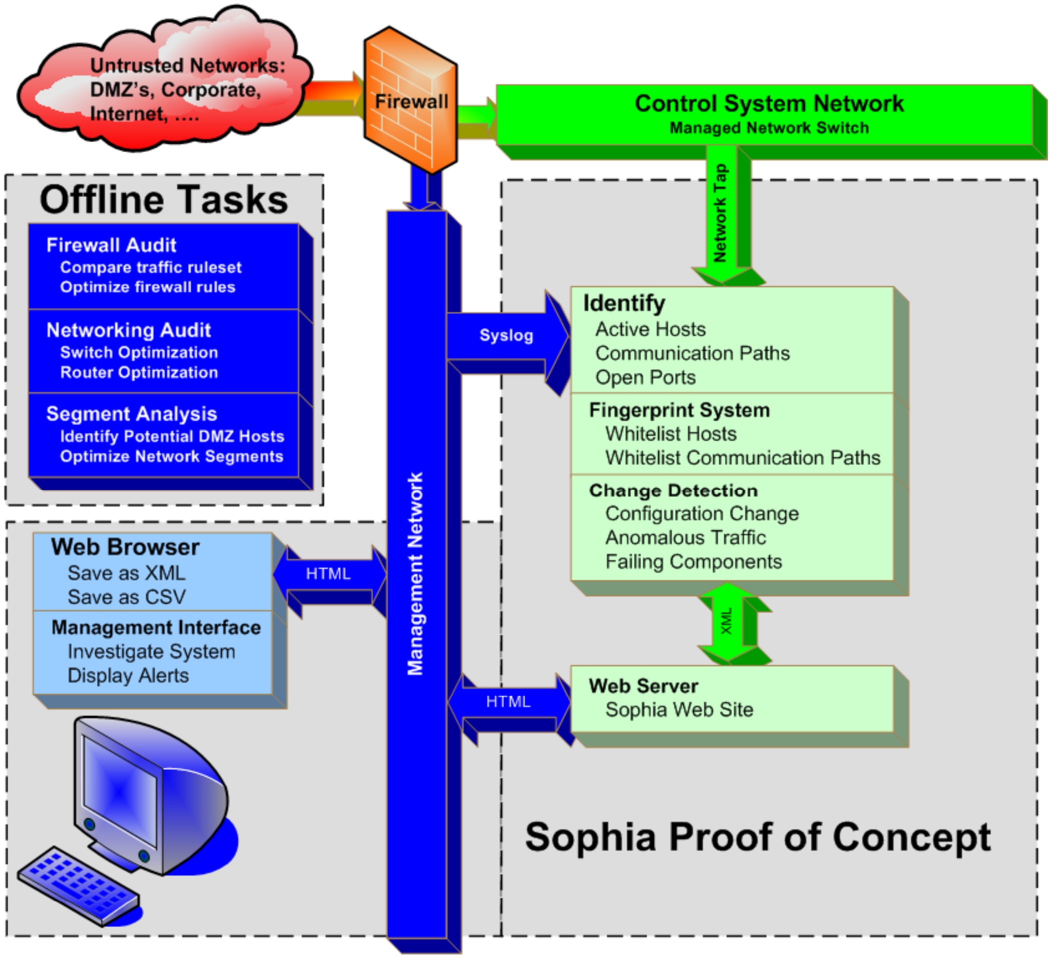
- **Plans to gain industry input**
  - Industry needs to direct the path of Sophia into a useful tool.
  - Industry involvement was planned into the proof of concept by seeking industry concept testers before the proof of concept was developed.
  - Industry network environments are very different between sites. Finding representative networks is not easy.
- **Plans to transfer technology/knowledge to end user**
  - Asset owner networks are the targeted use case for Sophia.
  - INL plans to continually respond to feedback from Sophia industry partners until the end of development.
  - Sophia will be licensed through third party support companies that will provide end user support.

Next Steps

- **Current State**
  - The proof of concept is finished.

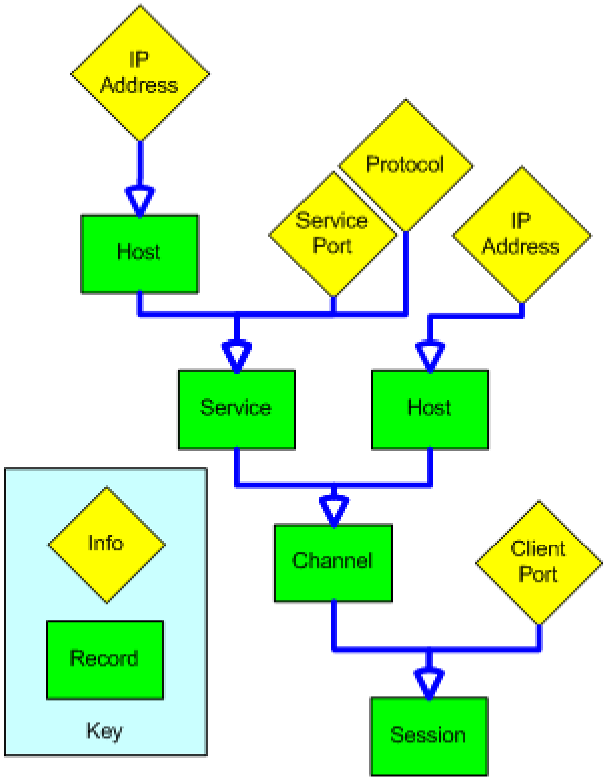
- **Future Work**
  - Develop Beta Sophia Tool
  - Continual Beta Testing During Development
  - License Beta Software Through Third Party

Concept Design

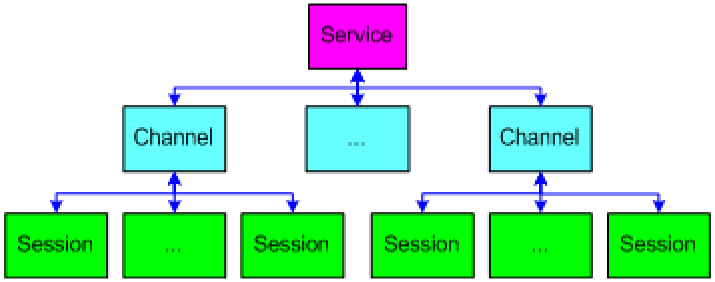


Sophia Records

Sophia Records Defined



Record Multiplicity

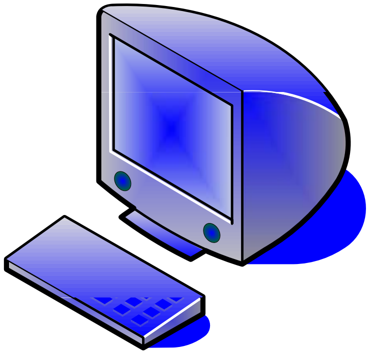


Idaho National Laboratory

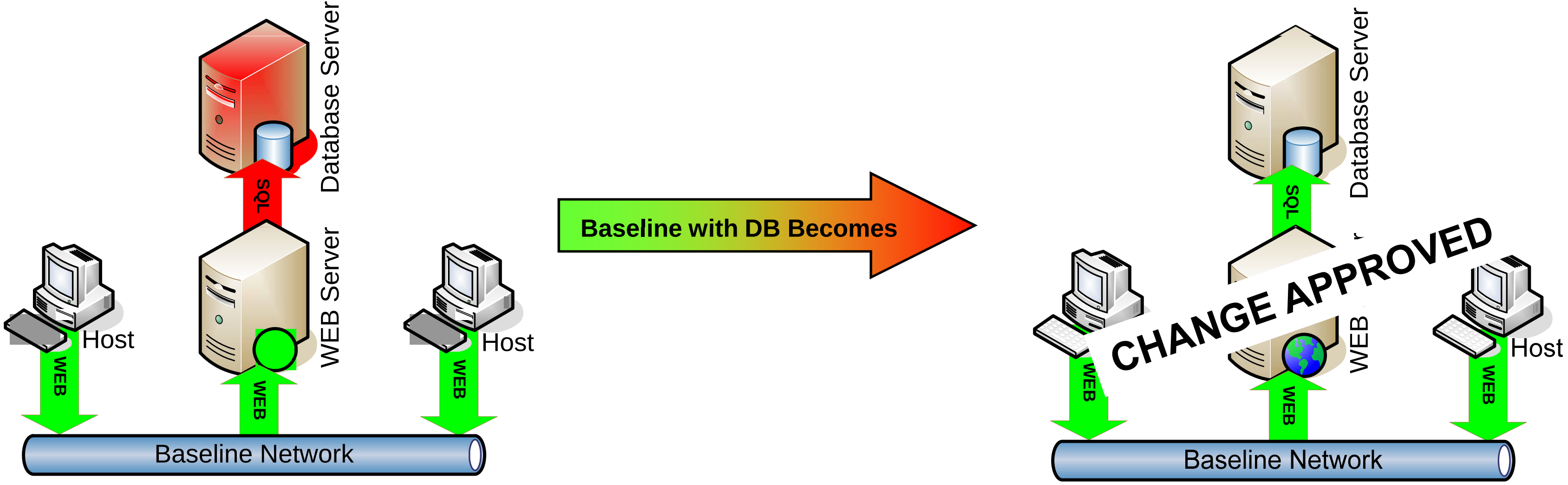
Change Detection

- Pulls key Information from other tools
  - Monitors Network Changes
  - New Hosts
  - New Communication Paths
- Alerts on deviation from base fingerprint
- Management Interface to alter base fingerprint

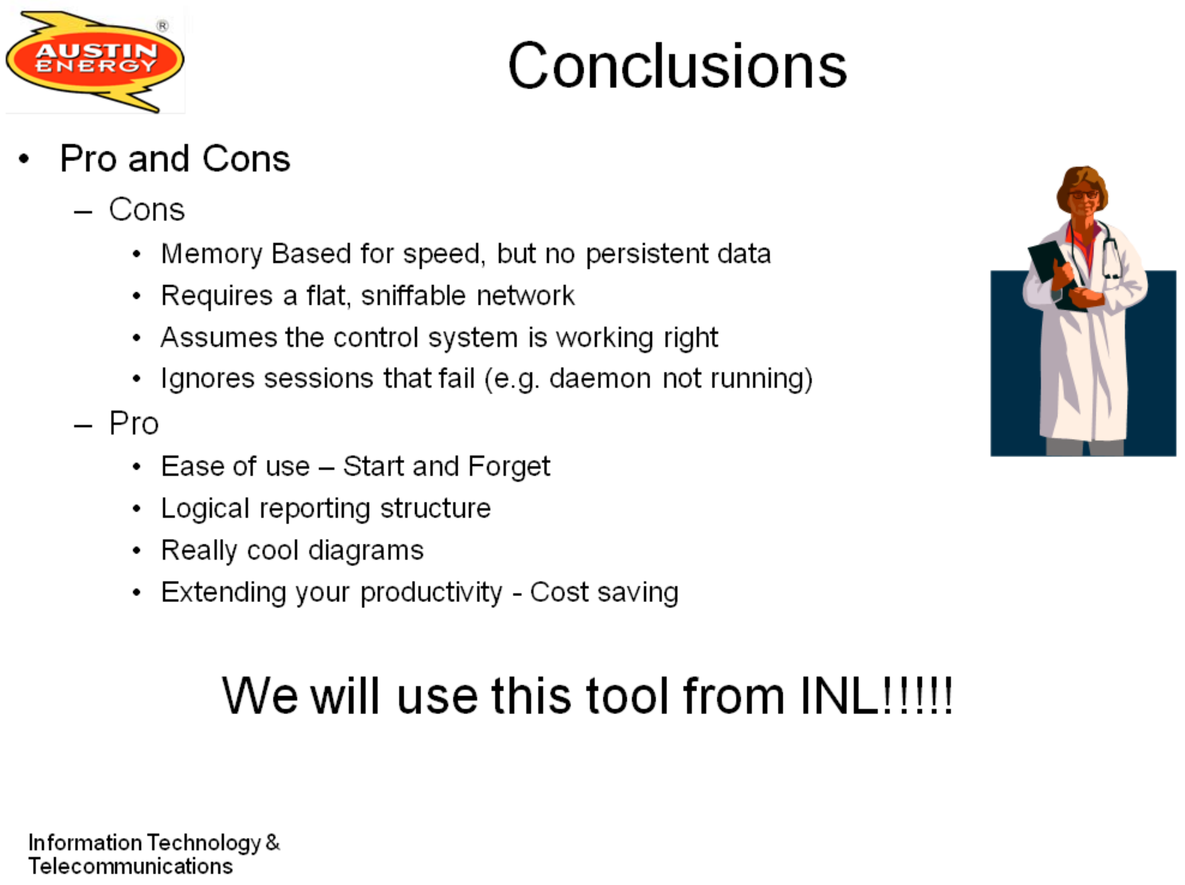
- Example: Adding a simple backend database



Tool Management Console



Feedback



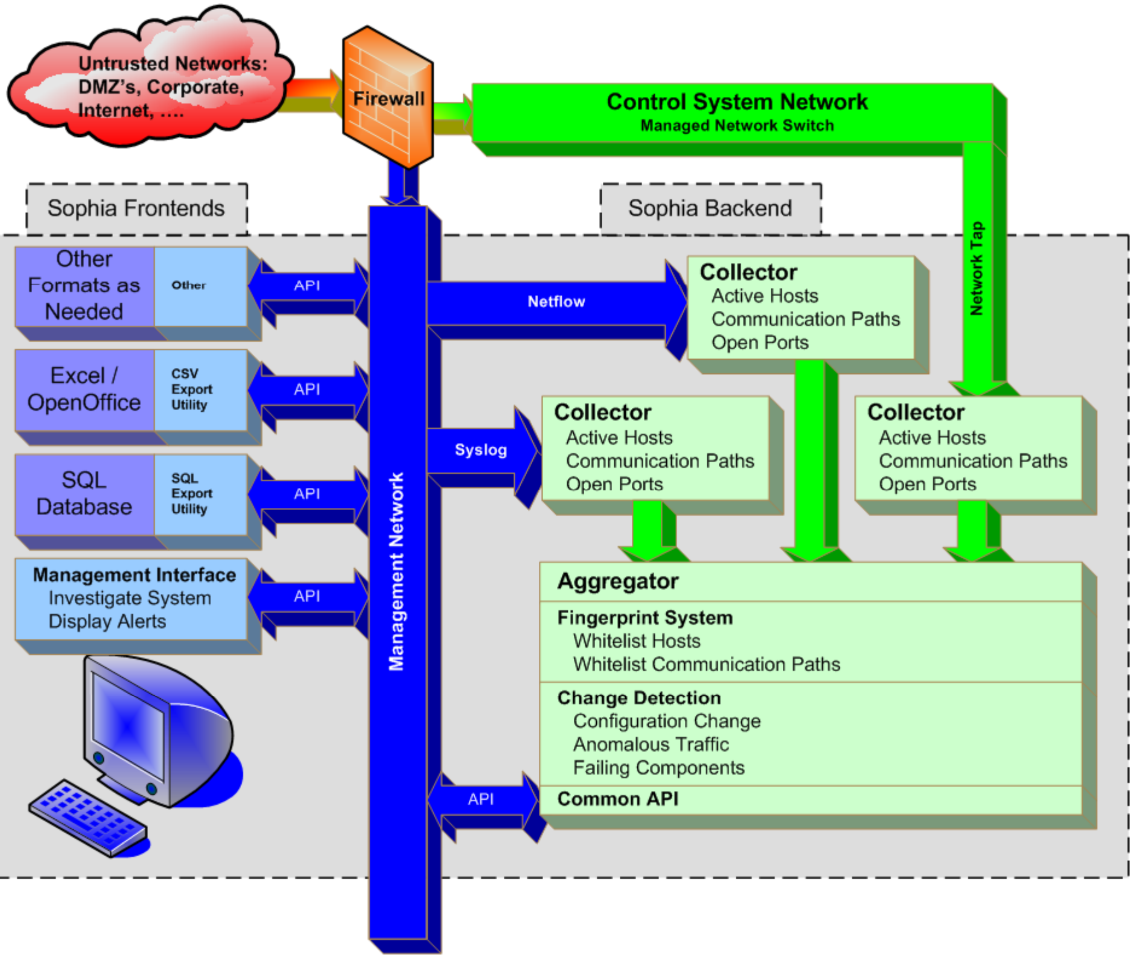
Conclusions

- Pro and Cons
  - Cons
    - Memory Based for speed, but no persistent data
    - Requires a flat, sniffable network
    - Assumes the control system is working right
    - Ignores sessions that fail (e.g. daemon not running)
  - Pro
    - Ease of use – Start and Forget
    - Logical reporting structure
    - Really cool diagrams
    - Extending your productivity - Cost saving

We will use this tool from INL!!!!!

Information Technology &
Telecommunications

Beta Design


Untrusted Networks:
DMZ's, Corporate,
Internet, ...
Firewall
Control System Network
Managed Network Switch
Sophia Frontends
Sophia Backend
Other Formats as Needed
Other
API
Excel / OpenOffice
CSV Export Utility
API
SQL Database
SQL Export Utility
API
Management Interface
Investigate System
Display Alerts
API
Management Network
Netflow
Syslog
Network Tap
Collector
Active Hosts
Communication Paths
Open Ports
Collector
Active Hosts
Communication Paths
Open Ports
Collector
Active Hosts
Communication Paths
Open Ports
Aggregator
Fingerprint System
Whitelist Hosts
Whitelist Communication Paths
Change Detection
Configuration Change
Anomalous Traffic
Failing Components
API
Common API

Questions?

- Gordon H. Rueff
  - Gordon.Rueff@inl.gov
  - Office: (208) 526-0311
  - Cell: (208) 360-7440
- Jared Verba
  - Jared.Verba@inl.gov
  - Office: (208) 526-6120
  - Cell: (208) 521-9939
- Dave Kuipers
  - David.Kuipers@inl.gov
  - Office: (208) 526-4038
  - Cell: (208) 360-6456
- Jim Davidson
  - James.Davidson@inl.gov
  - Office: (208) 526-0422
  - Cell: (208) 520-2806

Idaho National Laboratory