



Argonne
NATIONAL
LABORATORY

... for a brighter future



U.S. Department
of Energy



THE UNIVERSITY OF
CHICAGO



**Office of
Science**

U.S. DEPARTMENT OF ENERGY

A U.S. Department of Energy laboratory
managed by The University of Chicago

Federations for Cyber Defense

Scott Pinkerton

Argonne National Laboratory

25 October, 2006

Background

- Cyber Defense continues to be a challenging problem for Federal agencies and R&E communities alike
- Security challenges
 - Threat landscape evolving rapidly - our defensive strategies and methodologies need to as well
 - Technology paradigm evolving rapidly - national networks; dynamic provisioning
- Risk based approach to cyber defense still needs to:
 - Keep the “bad guys” out
 - Let the “good guys” in, and
 - “Keep the wheels on” maintain effective operations & perform mission
- Investment in information security today is largely a cost of doing business - particularly when trust and security are expected (esp for PII)
- Propose that there is an opportunity for all of us to work smarter using Federations for Cyber Defense

Motivation behind a Federated Approach

- Lots of energy (\$\$) going into analysis, monitoring, tracking, and possibly blocking packets on the wire
 - Each agency/site is doing this every day (in their own unique way)
 - However, there is no convenient way to interact with the each other in a near real-time automated manner, E.g.
 - *Announce - this IP was hostile to us for ssh brute force attack*
 - *Announce - this IP was a resource site for a root kit used here*
 - *Query - what traffic have you seen to/from this IP ?*
 - *Query - is this a valid/routed IP at your site ?*
 - *Action Request - Suggest you add this IP to your watch list*
 - *Action Request - Suggest you block this IP*

- (Today) We don't have an infrastructure that enable us to adapt and evolve rapidly with our threats - unacceptable risk position
- Goal is to create a future state that enables action - more than just sending e-mails

The Vision - Framework

- Create an infrastructure (tools) that let agencies interact efficiently
 - Close to real-time (< 10 minutes)
 - Autonomously (without human intervention)
 - Using simple underlying technology

- Encourage the development of Federations
 - Multiple federations, not just one
 - Join the *ones* that make sense
 - Share appropriate info to each federation

- Define some formats for information sharing
 - XML based
 - IETF standards based
 - Defined well enough to support autonomous operations
 - Flexible enough to adapt over time

What would we do with this Framework/Infrastructure ?

- Share information with each other
 - Announce malicious network behavior detected at one agency/site in an attempt to deter or prevent the spread of this behavior
 - Include history of an IP's behavior, severity, and local actions taken

- Implement a query/response mechanism that would allow a trusted agent at one site to solicit information from other sites
 - Are you seeing in-bound scanning from this IP ?
 - Are you seeing out-bound activity to this IP:port ?
 - Ideally this should be an automated lookup - each site controls what info sources they will share from

- Implement an action request mechanism for a site to *advise* that other agencies/sites block or watch an IP address

The Strategy

- Create an infrastructure for passing data between federation members
 - Based on limited function web service (upload and download of files)
 - RSS used to signal new data available

- Develop standards/templates on what information we should share

- Encourage the formation of federations
 - Encourage groups to think about automation points

- Develop vendor partners

- Stir well and see what happens

Our Federated Model Features

- Grass Roots Concept
 - Provide an open list of participants and official POC
 - Allow multiple communities to leverage the infrastructure (based on a limited function web server)
- Sites directly participate
 - Sites maintain local control of what information they share
- Sites control/decide who they want to interact with
 - One federation for sharing info, one for queries, one for action
 - Via pgp key management (out of band)
- Implemented through a limited function web site
 - Goal is to implement as a near real-time automated system
 - Allows upload from registered participants only
 - Supports download to registered participants only
 - Supports RSS to allow sites to determine when new data is available

Reasons for Participating

- To be successful in the future - need to speed up our OODA loop for cyber defense !!!
- Improve the data glut, information famine problem
- Assumption: malicious attackers prey on related sites (government, defense, financial, research & education, etc)
- Creating an IP profile enables better suited response actions
 - Know what to watch for
 - Quicker and possibly more severe response to known “bad guys”
- Valuable resource for incident response
 - We saw “x”, wonder if anyone else did ?
- Valuable resource for US CERT, CIAC, or other trusted agencies
 - Automated method for CIAC to push an IP address to all the sites with the suggestion of blocking it (fully automated)
- Valuable tool for interacting with “Internet Service Providers”
 - DISA, ESnet, etc

Information being Disseminated Falls into 3 Categories

- Announcements from a site
 - This IP was bad for the following reasons ...
 - *Extends the “corporate memory” of anti-host (bad guy) knowledge*
 - *Maintains situational awareness, recidivism*
- Query to a site
 - We are interested in the following IP address
 - *Can you send us flow data from your site over time range ... ?*
 - *Have your IDS logs seen this IP before ... ?*
 - Is this a valid IP address at your site
 - *Network currently being routed at the site ?*
 - *Is that IP address in use ?*
 - *Did that IP address send e-mail over time range ... ?*
- Action Request (strongly suggested)
 - The following IP address is actively involved in an exploit at our site, suggest you block it
 - US CERT/CIAC advisory that we block (or watch list) an IP address

What Information is Shared ?

- Strictly unclassified information

- Information on (usually external) IP addresses that was malicious enough to warrant a site response (blocking or other)
 - IP address:tcp/udp port #
 - Time of attack
 - Type of attack
 - Exploit attempted
 - Severity of attack
 - Previous history of offending IP at that site (corporate memory)

 - We could periodically share watch lists

- Information presented in a standardized exchange format
 - XML file
 - Using IETF standards for cyber data exchange

What can be Queried for ?

- Query would be in a standardized exchange format
 - XML file
 - Extensible to add capabilities over time
- Common queries would be:
 - Have you seen traffic to or from this IP ?
 - Have you seen outbound traffic to IP:port ?
 - Is this a valid/routed IP address at your site ?
 - Do you have any {netflow|IDS} data/records for this IP ?
- Queries would be followed up with an acknowledgment message
 - acknowledge *pending*
 - acknowledge *no data coming*
 - acknowledge *results uploaded*

What Action Requests can Occur ?

- Action requests would be in a standardized exchange format
 - XML file
 - Extensible to add capabilities over time
- Common action requests would be:
 - Add this IP to your watch lists - ref “case #”
 - Add this IP to your watch lists & can you notify us when you see traffic ?
 - Suggest you block outbound traffic to this IP
 - Suggest you block all traffic (in & out) to this IP
- Action requests would be followed up with an acknowledgment message
 - acknowledge *action taken*
 - acknowledge *action NOT taken*

Case Study

- Phishing scam at our site

Vendor Support

- Sharing information within a federation based on a template
- IF, I can query my local systems (IDS, MARS, etc) and get answers formatted per my template
 - All the easier to share data
- The challenge - find ways to utilize user defined templates to tailor the information given back to the users
 - Pull all IDS signature fires associated with an IP address, and present info to me based on a template

What can you do ?

- Think about how you would like to speed up your OODA loop
- Create a federation - even if it is with just a single organization
- Think about what you have automated to date
 - What can you/should you automate in the future
- Get involved
- For additional info:
 - <https://www.anl.gov/it/federated>