CSI2 Working Group

Computer Security Incident

Internet2

April 2006

Draft Charter

- How to consistently identify security incidents
- How information about the incidents can be shared
  - To improve the overall security of the network and the parties connected to the network.
- Publish a report identifying tools, tool output and existing information sharing frameworks Preparation and background for future systems and tools.

Three primary activity areas

- Tools
  - Shared darknets
  - Distributed IDS
- Data
  - retention, anonymization, related policies
- Sharing
  - formats such as IODEF and tools to implement

Tools

- Survey existing tool sets
  - What tools are in use by campuses that could be shared?
- Future tools
  - Can we improve the security posture of the community by supporting development of these tools?
- Assess the value and difficulty of "extending" the tools with an inter-realm dimension
  - REN-ISAC

Tools: Darknets

- A darknet collector listens to one or more blocks of routed, allocated, but unused IP address space.
- Because the IP space is unused (hence "dark") there should be very little if any legitimate traffic entering the darknet
- ***Team Cymru Darknet Project***
  - http://www.cymru.com/Darknet/index.html

Darknets

- Complex campus networks need an IGP
- We use hold-down (nailed-up) routes anyways
  - Static routes at the border to minimize route flapping
  - Pointing our address space to Null0 with a high metric
  - Fail safe

Darknets

- Why not inject hold-down routes for unused space to a stub router?
  - And generate netflow records in one place
- Doesn’t need a lot of horsepower
- Unused space dynamically falls in to the Darknet

Shared Darknet

- Develop a wide-aperture, powerful network security sensor
  - directly serve higher-education and research institutions
  - indirectly serve Internet users at large.
- Institutions who run local darknets send their collector data to REN-ISAC
  - Only hits from remote sources

Shared Darknet

- The data is analyzed to identify compromised machines by IP address, destination ports
- The REN-ISAC compiles the darknet data contributions
  - Distributes notifications and reports.
- Limited policy overhead
  - Low privacy requirements for this data

Data: Policy Issues

- Sharing data beyond campus may require different policies to ensure data privacy
- Many campuses have or are developing data release/retention policies for network data
- Can campus policies be mapped to share data beyond the campus?
- Not attempting to draft new policies, but survey what can be done now and where we need improvement.

Data: Sharing

- Value of this data improves with the number of sources
- Do campuses currently have policies that allow sharing of data?
  - With REN-ISAC, others?
- Is there more sensitivity with incident data than standard diagnostics
  - EDDY, e2epi?

Data: Policy Questions

- Do we need to anonymize this data if REN-ISAC is a trusted party?
  - How is this related to outputs from REN-ISAC?
  - Do campuses maintain some control of data disclosure?
- How can existing trust fabrics be leveraged?

Sharing data

- Can we broadly support sharing of incident data?
  - Within policy constraints
  - Incident Reports, Netflow
- What standardization currently exists?
  - IODEF
  - http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-05.txt

Sharing data: RENOIR

- What to use for transport?
  - Scp?
  - EDDY? (http://www.cmu.edu/eddy)
- How do we authentication/authorize sharing this rich data
  - Shibboleth?
- Can we leverage existing federations?
  - InCommon
  - REN-ISAC Registry?

RENOIR Design

- Research and Education Networking Operational Information Repository
- Design around the concept of ticket system handling security data
  - vast array of sources
- Organizing the data into high-level cases
  - use for reporting on daily operational incidents.
- Rely on a trusted third-party to facilitate communication

RENOIR Design

- Accept human input and structured data to form tickets
  - using IODEF in an appropriate format.
- Allow input from users from a variety of roles
  - Reporting party, affected site, administrators
  - *Researchers?*

RENOIR Design

- Use, widely-accepted, encrypted transport mechanisms
  - In the transport layer
  - Encrypting message content.
- Use a repository of contact information
  - Facilitate automated notifications of affected sites
  - REN-ISAC contacts?

RENOIR Design

- Extendable to include new security problems and reported incident types as they occur.
  - Accommodate dynamic threat environment
- Interaction with campus-scoped ticketing
- Incremental development of capabilities
  - Due to system and transaction complexity

www.internet2.edu