From Local to Global Awareness: A Distributed Incident Management System (DIMS)

University of Washington
David Dittrich

September 17, 2013
Team Profile

Applied Physics
Laboratory UW
PI: David Dittrich

Next Century
Corporation
Lead: Todd Hughes

RCES LLC
Lead: Mickey Ross

TrustGroup$_1$
(ops-trust)

TrustGroup$_2$
(Beadwindow, etc.)

TrustGroup$_N$
(PRISEM re-implementation)

Public Regional
Information Security Event
Monitoring

9/14/2013
Customer Need

Indicators from multiple sources (e.g. Alienvault, Shadowserver, Malwarebytes, Mandiant, etc.)

http://botnets.org

http://ops-trust.net

http://code.google.com/p/collective-intelligence-framework/

Customer Need

Each trusted group can have their own DIMS backend & Dashboard UI

Data shared as groups allow

US-CERT

IOC_{src1}

IOC_{src2}

IOC_{srcN}

Indicators from multiple sources (e.g. Alienvault, Shadowserver, Malwarebytes, Mandiant, etc.)
Approach

Develop a system for collaborative response detection and mitigation mechanisms to counter target and advanced threats

- Web Application Service front end (dashboard) for data mining, analysis, reporting, and data ingest/export
- Role based access controls, account management, and data anonymization/filtering
- Integrate alerting from protective and detective systems with contextual information and cross-organizational situational awareness
- Integration with host-based forensic tools to facilitate triage, implementing “course of action” steps
- Vertical (US-CERT) and horizontal information sharing with trusted groups (e.g., ops-trust, Beadwindow, etc.)
Benefits

• **Improved Performance**
  – Platform for collaborative situational awareness and response, integrating Indicators of Compromise (IOCs) from multiple sources
  – Security-assessed ops-trust portal for increased collaboration across trust groups
  – Improve operator effectiveness in mitigating targeted and advanced threats
  – Provide actionable intelligence and course of action options

• **Lower Cost of Ownership**
  – Prototypes developed as open source for rapid innovation & diffusion
  – Use combined strength of UW, Next Century, to support technology transfer

• **Better situational awareness (at scale)**
  – Integrated approach to monitoring, analysis, visualization, and data sharing
  – Enhance existing Security Event Information Management (SEIM) systems with vendor-neutral dashboard
Contact Information

• David Dittrich (Principal Investigator)
  dittrich at uw dot edu
  http://staff.washington.edu/dittrich/