

Camus: Mapping Cyber Assets to Missions and Users

Systems administrators in large data centers often do not know the mission of the machines they manage; their strategy is, *Let's pull the plug and see who calls* (*The Economist*, 2008). The problem is similar for computer security analysts – they do not know the **cyber capabilities, mission, or users** that depend on a machine that is attacked. To assess the impact of a compromised or degraded cyber asset, analysts need to know:

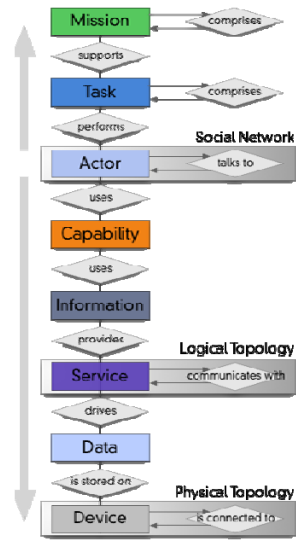
- Who relies on an attacked asset for their job?
- What social network will be disrupted if an asset is compromised?
- What organizational mission is impacted by the loss of an asset?
- What other assets or cyber capabilities depend on an attacked asset?
- Where is the attacked asset located in the physical or logical network?

This lack of contextual information makes it impossible to effectively prioritize cyber events or assess the impact of attacks.

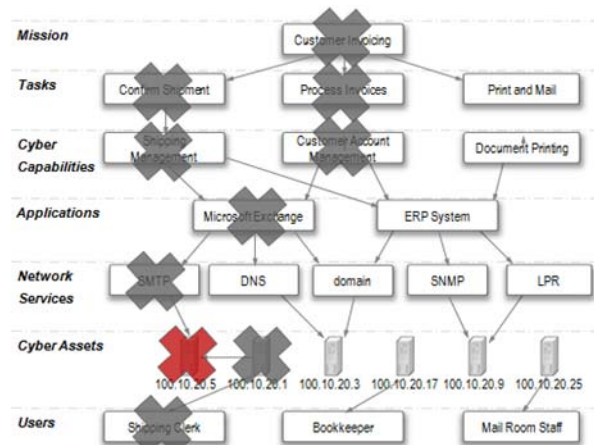
Applied Visions Inc. Secure Decisions division is developing **Camus**, a framework for modeling and a system for automatically collecting data to map **Cyber Assets to Mission and Users**. Underlying the Camus technology is a cyber asset-to-mission ontology, which is being developed with a multidisciplinary group of leading subject matter experts (SMEs) and operational practitioners. Using semantic web technologies, Camus defines the critical relationships between cyber assets, network services, capabilities, users, and missions.

The Camus system contains a sophisticated and flexible data fusion engine. Instead of using traditional databases, Camus uses a high-performance, scalable ontology-based structure for storage and querying. Disparate data sources, such as traffic captures and people directories, are fused into a comprehensive model that reveals relationships between cyber assets and the users and missions that rely on them.

We are also developing web-based visualization tools for comprehension and exploration of resource dependencies and potential mission impacts when failures occur. Security analysts can quickly locate the portions of the enterprise that are affected by outages, using rich graphical displays, and easily incorporate them into reports for documentation and dissemination. This capability provides analysts with a clear picture of critical systems as well as the organizational missions they support.



Camus Candidate Conceptual Ontology developed by SMEs



Example of how a failed cyber asset has cascading effects to users, services, applications, capabilities, tasks and missions.

Camus will improve the effectiveness and efficiency of the decision-making process of security analysts and mission commanders by providing visibility into dependencies and insight into the context required to accurately assess the mission impact of a cyber attack. Beyond security, system and network administrators will also find the dependency mapping useful in performing routine maintenance tasks, disaster planning, and upgrades of applications and systems.

Camus is funded by the Office of the Secretary of Defense, and managed by the Air Force Research Laboratory through a two-year Phase II Small Business Innovative Research contract that commenced in May 2008. For more information, please contact the Principal Investigator: Dr. John Goodall, at johnhg@securedecisions.com.