Air Force Institute of Technology

Integrity - Service - Excellence

An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment (CIMIA)

Michael R. Grimaila, PhD, CIV / USAF
Robert F. Mills, PhD, CIV / USAF
Larry W. Fortson, Capt / USAF

13th International Command and Control Research and Technology Symposia (ICCRTS)
Bellevue, WA
June 17-19, 2008

Research Sponsors:
Air Force Research Laboratory (AFRL/RHX)

UNCLASSIFIED

Disclaimer

The views expressed in this presentation are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government…

Overview

- Research Motivation
- Background
- Information is an Asset
- Tracking Information Assets
- Conclusions

Research Motivation

Consider the following hypothetical scenario:

- In Iraq, coalition partners are provided connectivity to a US Secret level network for information sharing purposes
- A breach of a coalition partners system occurs
- The breach is detected and stopped
- The breach enabled the adversary to access a server which contains multiple databases
- One of the DBs contains convoy routes and schedules
- The Incident Response Team begins their investigation
- IRT works with the system custodians to identify and notify all information owners / consumers
- The process takes days to complete...

Meanwhile, the Next Day

Background

- Virtually every organization is dependent upon information accessed/stored/processed in cyberspace
- Despite our best efforts at developing defensive capabilities, cyber incidents are inevitable
- Cyber dependence introduces <u>significant</u> risk to both cyber-assets and real-world operations
- Commanders need accurate and timely damage assessment <u>in terms of their Mission</u>
- This is not a new development (RAND Report, 1995)
- We have failed to account for the value of <u>information</u>
- We don't collect, document, and refine knowledge of mission-to-information dependencies effectively!

Prior Research

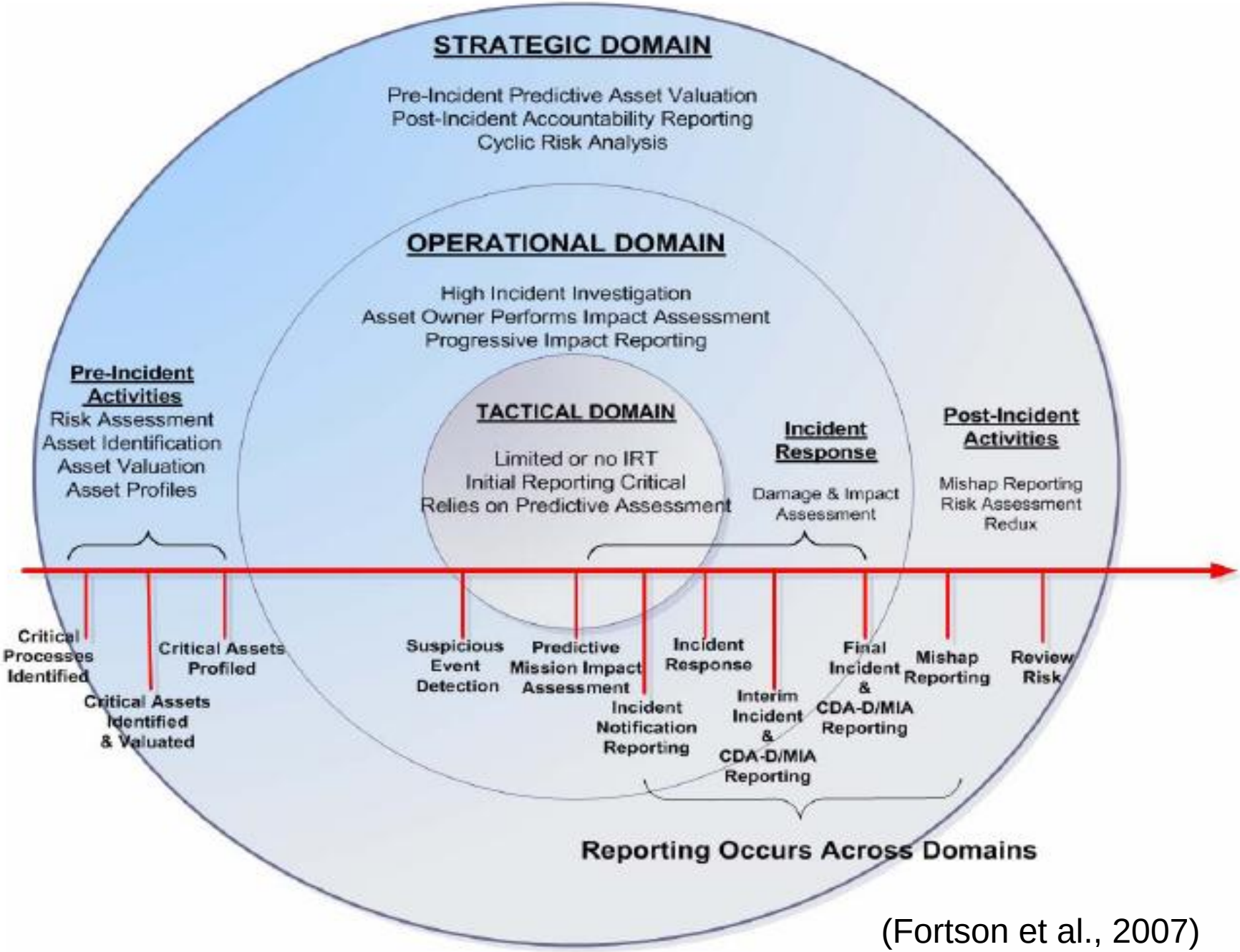
- RAND Report (1995) – The Day After Exercises
- Lala and Panda (2001) – Database damage assessment
- Thiem (2005) – Lack of standardized AF damage assessment methodologies
- Stanley (2005) – Mission impact analysis of communication link state availability
- Wong-Jiru (2006) – Net centric operations model for holistic view of mission dependencies between entities
- Shaw (2007) – Model of network outages in CAOC
- Fortson (2007) – Proposed defensive Cyber Damage Assessment (CDA-D) methodology
- Hellesen (2008) – Proposed an information valuation schema
- Sorrels (2008) – Proposed a system architecture for Cyber Incident Mission Impact Assessment

Key Problems Identified

- Focus on infrastructure protection
- Lack of a formal, standardized risk assessment
- Lack of documentation explicitly identifying:
  - Information Assets
  - Information Valuation
  - Mission / Information Dependencies
- Dynamic nature of missions and organizations
- Lack of timely notification of information consumers following cyber incidents
- Lack of an appreciation for potential impacts
- Lack of accountability
- Lack of after action follow-up

Risk Assessment

- Risk Assessment provides the information required for accurate and timely mission impact assessment
- Risk Assessment requires the identification and documentation of critical organizational resources
- Criticality is determined by how a given resource supports the organizational mission
- The valuation of any resource is:
  - Frame of reference dependent
  - Temporally dependent upon the mission(s)
  - Inherently subjective
- Risk = (Threats ∩ Vulnerabilities)*Probability*Loss
- Allows for a racking and stacking of the risks



(Fortson et al., 2007)

Impediments to Risk Assessment

- Conducting a documented risk assessment is:
  - Labor intensive
  - Time consuming
  - Must periodically be revisited (maintenance)
- Organizations and resources are dynamic entities
- Several different organizations may access and depend upon a resource (hard to estimate value)
- Buy-in from commander is needed to insure compliance and accountability
- Knowledgeable personnel must value resources
- Security aspects of critical asset identification
- Social barriers

Cyber Incident Mission Impact Assessment (CIMIA) Project

Provide decision makers near real-time situational awareness of mission impact following cyber incidents

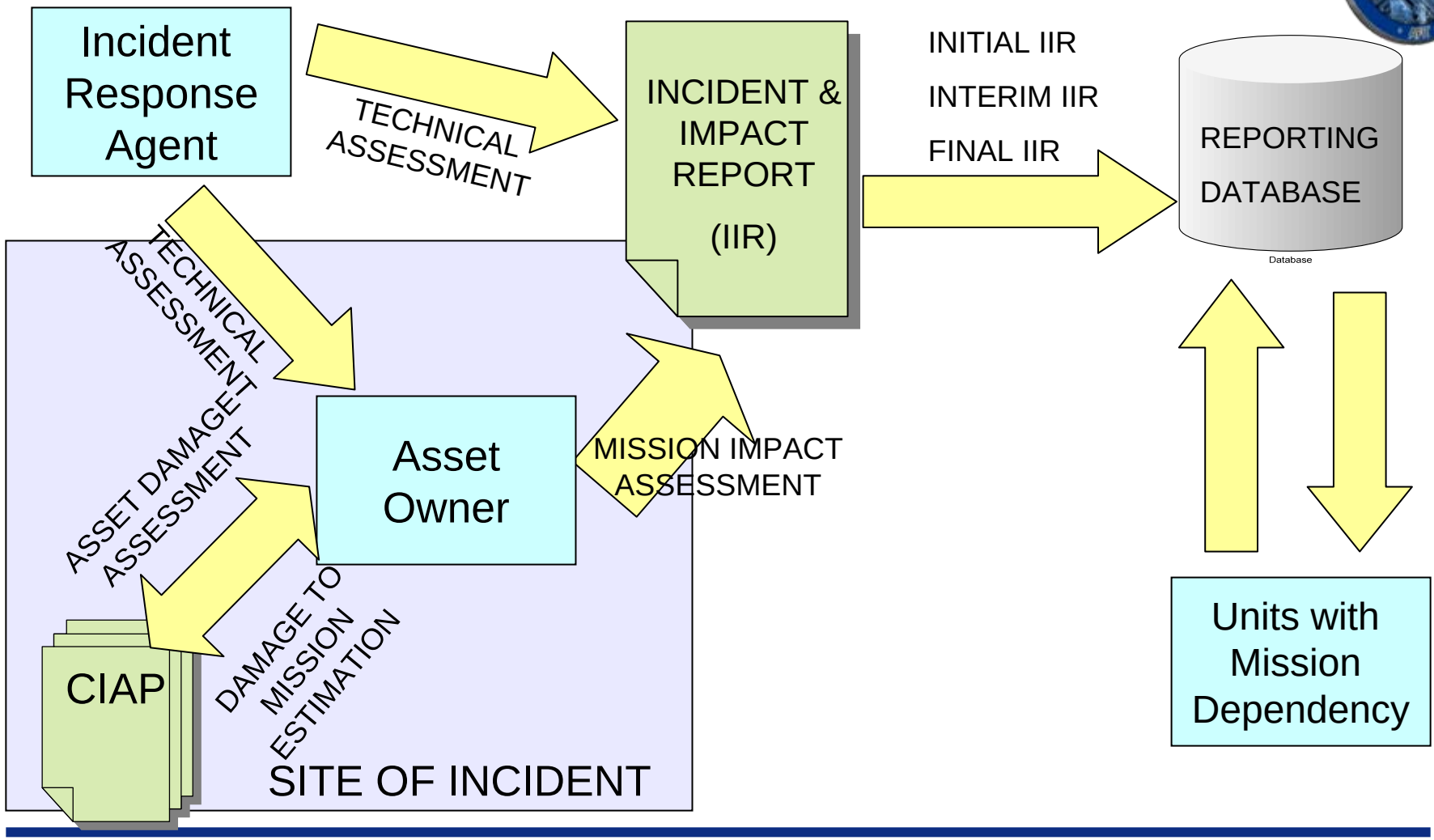
<u>Foundations:</u>

- **Mission operations focus**
- **Holistic approach to mission impact assessment**
  - **Confidentiality, integrity, and availability**
- **Requires a chain of interdependent activities:**
  - **Information asset identification**
  - **Information asset valuation**
  - **Technical (IRT) damage assessment**
  - **Damage-to-mission impact mapping**
  - **Mission impact reporting**

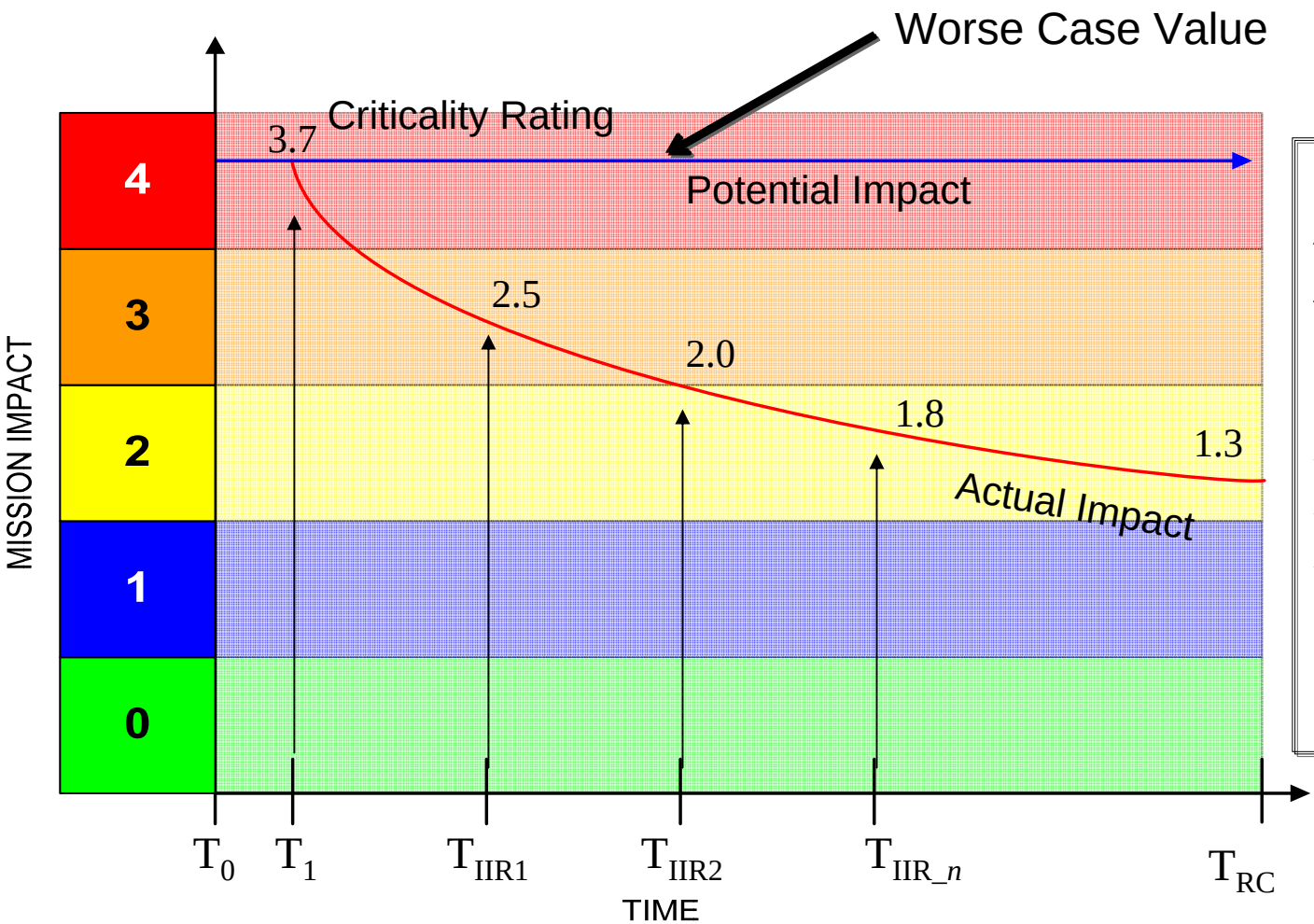
CIMIA Goals

- Notification of all downstream information consumers when an incident occurs
- Mission impact assessment from incident declaration (estimated) through remediation (actual)
- Mapping of mission processes to information assets
- Temporal mission information valuation models
  - Learn historical mission patterns
- Enforce:
  - Accountability / Documentation / Secrecy
- Exploit:
  - Automation to the extent possible
- Explore non-traditional mechanisms

Conceptual CIMIA Reporting



Mission Impact Estimation as a Function of Time



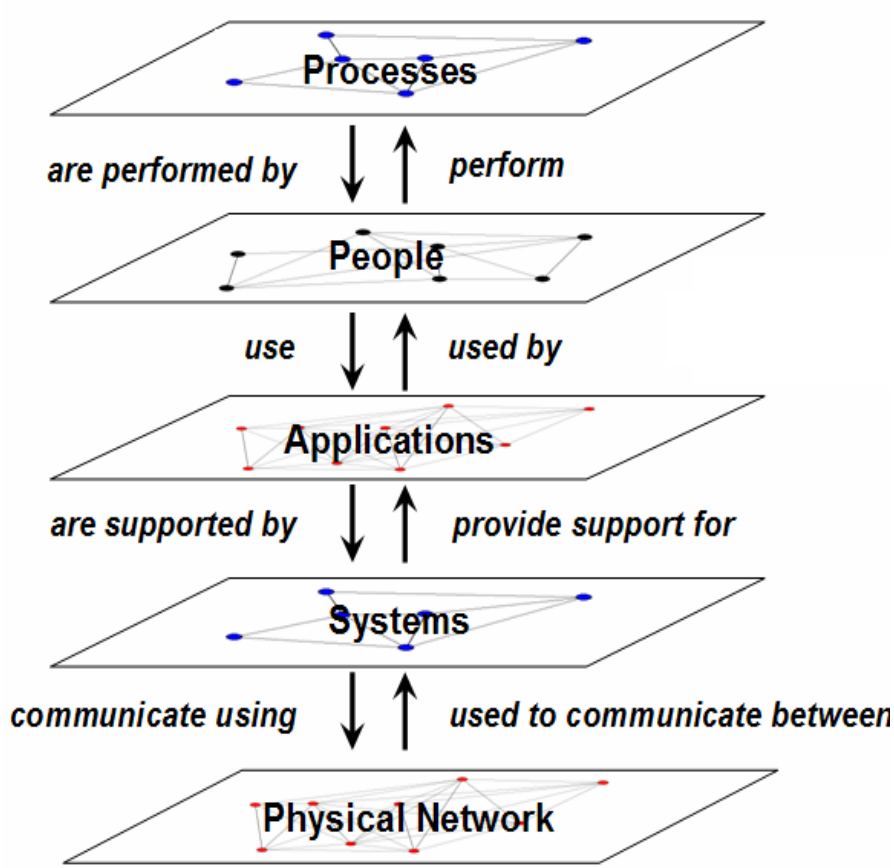
Impact Summary:

A confirmed data spill at Mosul NCC has resulted in the following compromised mission supporting systems:

System	Est	Mission
XXXX1	4	UAV Feed
XXXX3	4	Convoy Mvmnt
XXXX11	3	Personnel Data
…	…	…
…	…	…

Mission Mapping Abstractions

- How to best map mission to underlying resource dependencies?
- How to represent the "value" provided by each intermediate resource?
- What is necessary and feasible to collect and maintain in a mapping?
- How to insure an adversary cannot access and exploit this information?



A Paradigm Shift

- Information is THE asset in cyberspace
- Each organization has a different valuation “lens” through which they view information assets
- The true value of an information asset can only be determined by summation of each consumers valuation using a common measurement scheme
- System focused methods (e.g., DIACAP) do not:
  - Account for all the value consumers derive from accessing information on the system
  - Dynamically update as information assets are added/removed

Information Asset

- A specific grouping of data which provides value
- The granularity is user definable
  - Coarse: All information contained in a system
  - Fine: A specific field within a specific database within a system
- Multiple information assets may reside within the same information container
- The information asset must be uniquely identifiable across the enterprise
- Multiple information assets may be repackaged with other information, creating a new information asset (e.g., intelligence reports)
- How can we manage our information assets?

Information Sources (Providers)

- Any network addressable node that sources (provides) information assets upon request
- Information sources are uniquely identified by the triple containing at least:
  - <IP address , Port number , Resource number>
- Resource number is a locally assigned system resource identifier
- An information source can contain multiple information assets
- Information sources “know” the entities who make requests for information assets
- Example: Weather reports provided by a web server

Information Sinks (Consumers)

- Any network addressable node that receives an information asset and sinks (consumes) it
- Information consumers are uniquely identified by the triple containing at least:
  - <IP address, Port number, Consumer number>
- Consumer number is a local organizational entity identifier (e.g., individual, agent, process)
- There can be multiple consumers present simultaneously on a system
- Information sinks know from whom they received information assets
- Example: A web browser application being run by the weather officer in a Air Operations Center

Information Asset Tag

- Each information asset has an enterprise-wide key ("tag") which is used to uniquely identify it
- The "tag" is a pointer into a database which contains metadata about the information asset
- When an information asset is moved, the tag moves
- Tagging of information assets enables the tracking of the assets from the source (provider), through the infrastructure elements, to the sink (consumer)
  - Accountability can be enforced
  - Network traffic can be prioritized
  - Mission specific patterns can be identified

Information Asset Database

- **A database containing information about the given information asset from the owners perspective:**

  - Key “Tag”
  - Owner
  - Producer
  - Provider
  - Pedigree
  - Age
  - Comments
  - Composite elements
  - Confidentiality Sensitivity
  - Integrity Sensitivity
  - Availability Sensitivity
  - Rated Criticality
  - Derived Criticality
  - Last update

- **Maintained by a central authority (e.g., JTF-GNO)**
- **Global database located in a higher classification network only accessible by authorized entities**

Fictional Information Asset Database

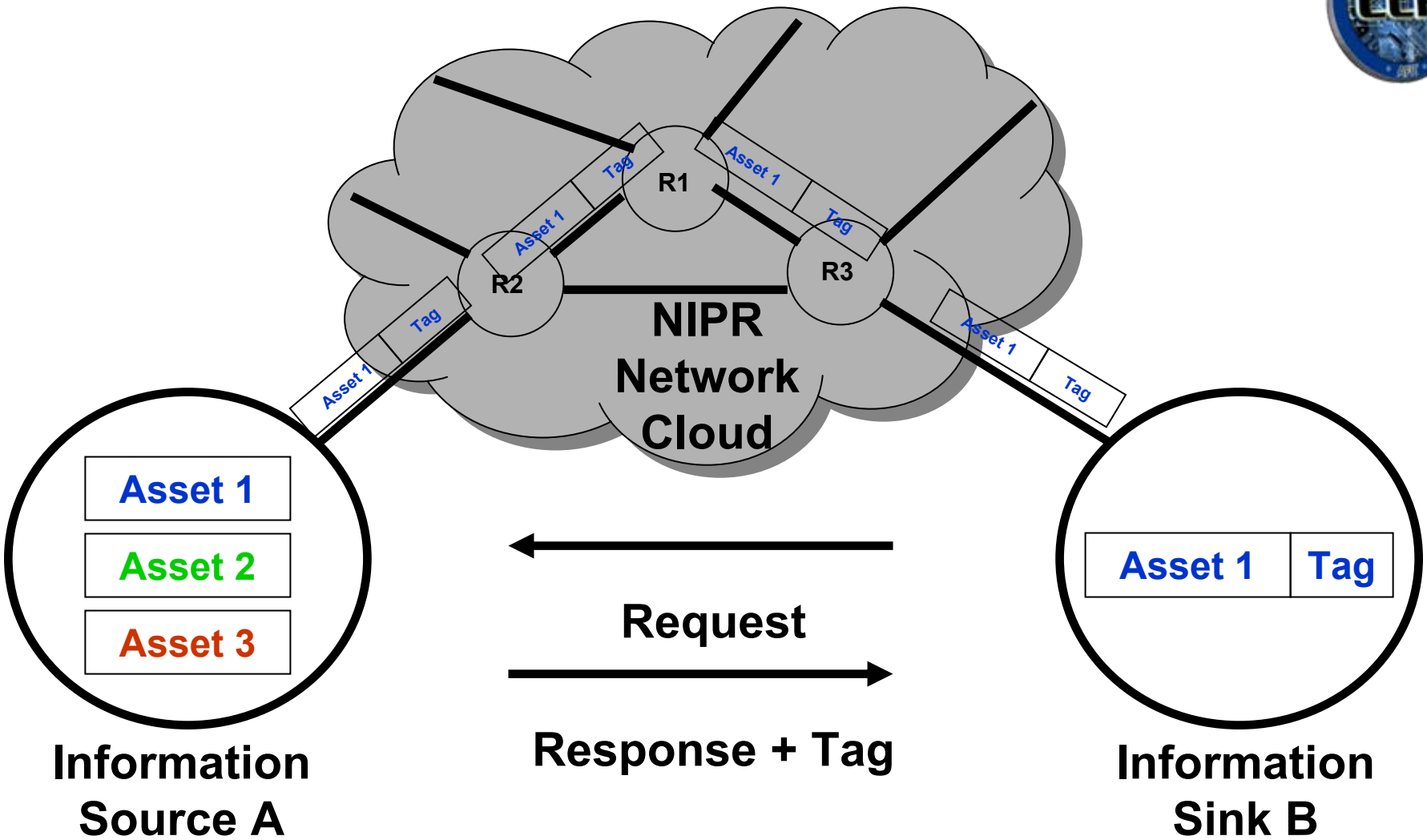
Tag	Owner	Producer	Age	Rated Criticality	Contains	SA_LABEL
7FD3BA30	AFIOC	33rd IOS	Daily	Very High	23A9D3D7, DD3100AC	TS-SCI/HCS
B723AA29	67th NWW	GREEN	10 June 2008	High	<NULL>	S/BELL
23A9D3D7	NASIC	SMAI	Daily	Very High	<NULL>	TS-SCI/TK
DD3100AC	NSA	GROUP 4	Weekly	High	<NULL>	TS-SCI/G

Note: Not all fields are shown for brevity

Tagging Information Assets

- Tags are “intelligently” inserted into the network data stream at the source:
  - One time for a given requestor
  - After a defined time interval has passed
  - When a change in the asset occurs
- Very low overhead impact
- Tag may be inserted in multiple ways (e.g., unused bits, IPV6 Flow Label, encoded into data)
- The tag itself does NOT contain any information about the information asset
- The tag is an encrypted using symmetric encryption
- The tag encryption changes daily using an automated process that is seeded monthly

Information Asset Source / Sink Architecture



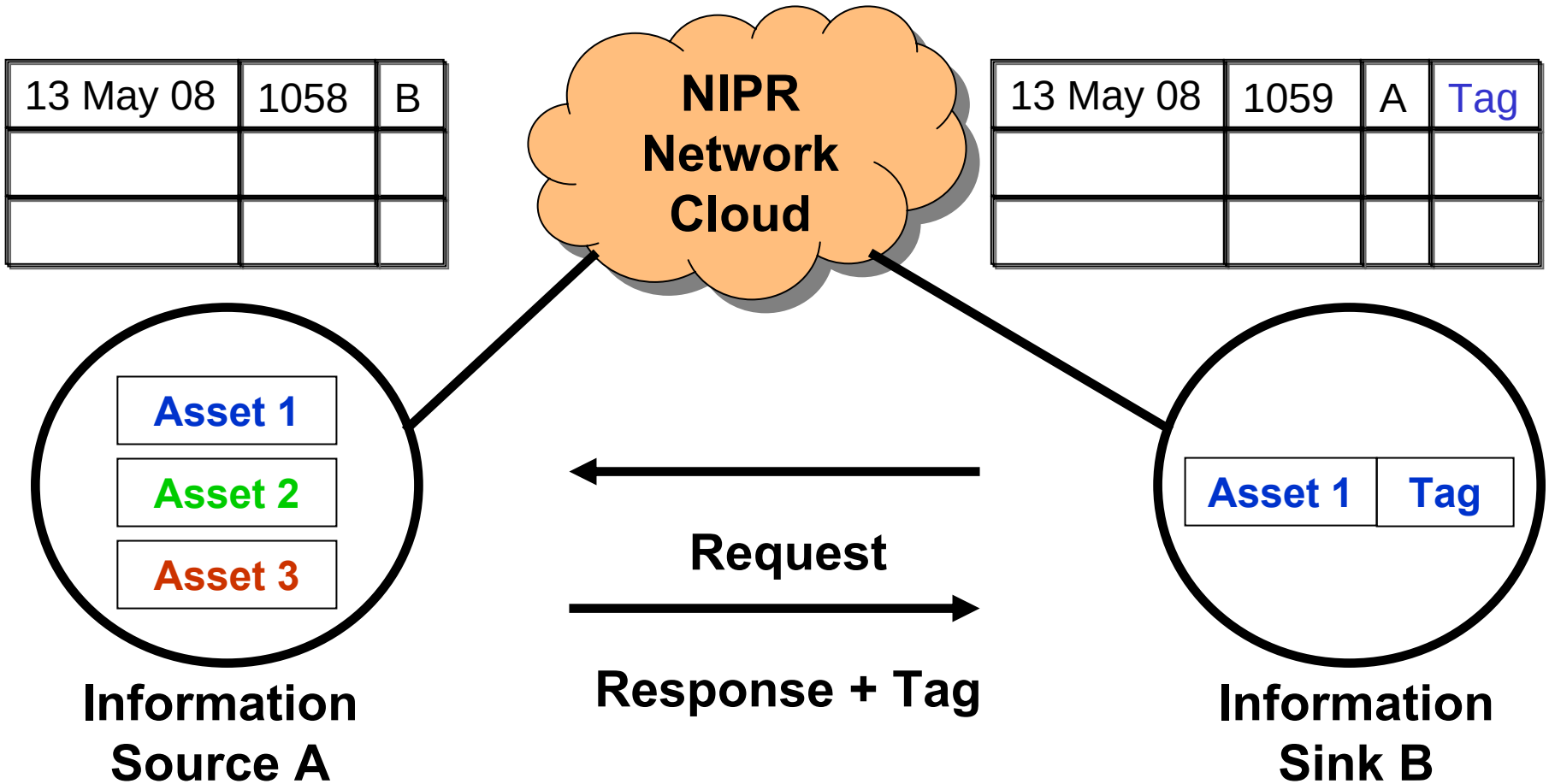
Source (Provider) Lightweight Database

- A lightweight database which keeps a record of all consumers who request an information asset
  - Collects summary statistics for each consumer including information asset tag, last access, frequency of access, amount of data transferred
- The source periodically transfers this information to a single local high side database (Tier III) which collects all requests made within the organization
- The information is periodically passed to Tier II, and then on to the Tier I systems
- Communication is passed through a one-way trusted guard

Sink (Consumer) Lightweight Database

- A lightweight database which keeps a record of all requests made to information sources
  - Collects summary statistics for each information asset received including the information asset tag, last access, frequency of access
- The consumer (or organizational representative) must explicitly link each requested information asset to the mission process(es) is supports and assign a “value” in terms of criticality of C/I/A
- The database is periodically transferred to a single local high side database (Tier III) which collects all information dependencies within the organization
- Similarly, this is transmitted securely up the chain

Source / Sink Lightweight Databases



Central Authority Process

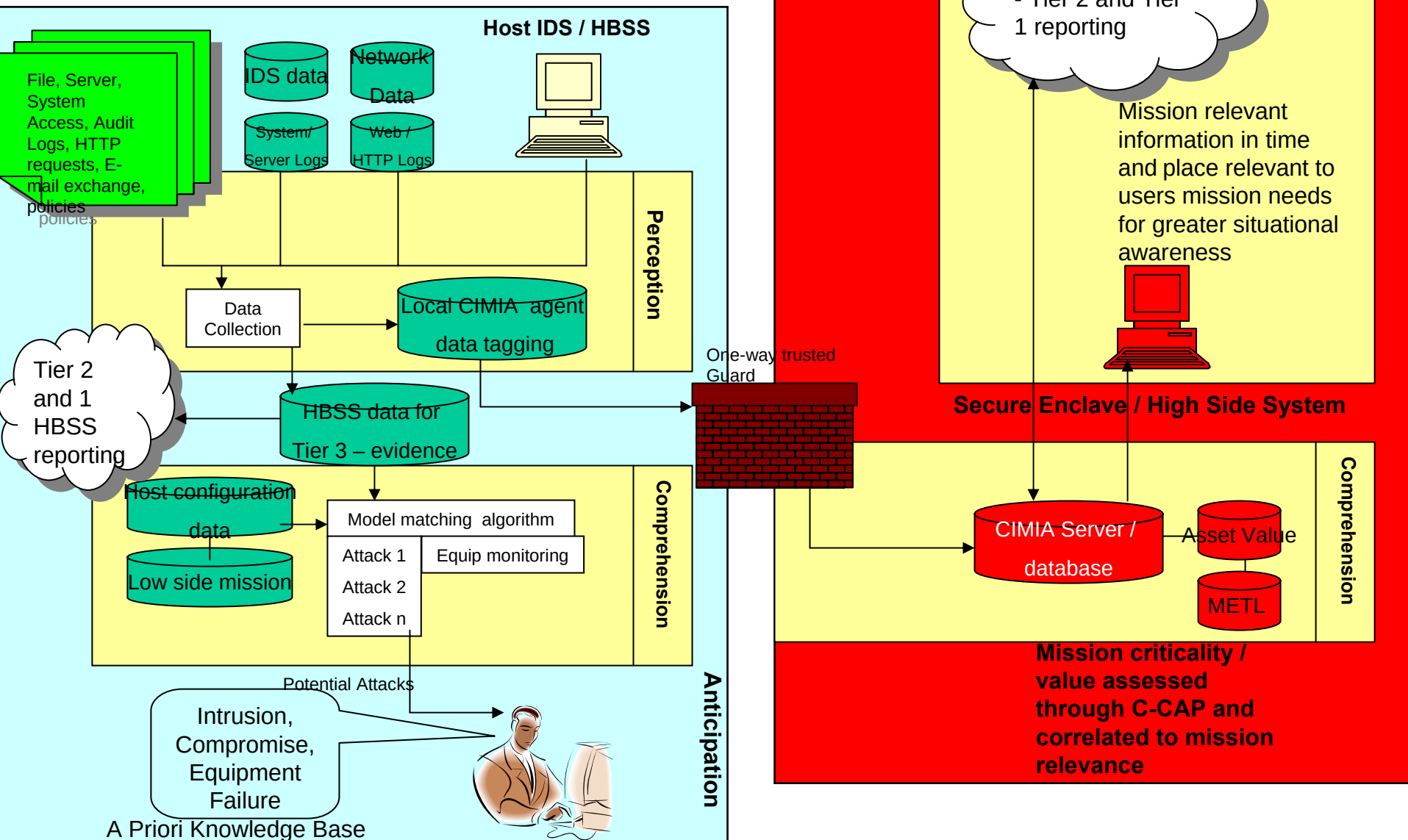
- Links information asset sources and sinks
- Determine all information dependencies
- Provides the capability to immediately notify downstream information consumers when an incident occurs
- Consuming organizations periodically download an encrypted message from the central authority
- Possible to calculate an aggregate enterprise-wide valuation for each information asset
- Consuming organizations are now accountable for identifying critical information resources
- Lesson learned can be shared

Host Based System Security (HBSS)

- An HIDS for workstations and servers
- Mandated to be installed on all DoD nodes
- Collects
  - Authentication information
  - Utilization of applications
  - File/System level access
- Does
  - Virus checking
  - Firewall monitoring
  - Malicious Traffic monitoring
  - Standard configuration enforcement
- Multi-tier level reporting
- Enables tag insertion and collection

(Gregory & Hensley 2007)

Proposed CIMIA System Architecture



Conclusions

- The research highlights the importance of documenting a formal risk assessment
- CIMIA can significantly improve the accuracy and timeliness of impact assessment
- Information asset identification is the first step in the CIMIA process
- Information asset tagging provides a mechanism to automate a portion of the task
- HBSS provides a vehicle for information tagging
- Prototype underway to show proof of concept

Questions

Michael R. Grimaila, PhD, CISM, CISSP, NSA IAM/IEM
Center for Cyberspace Research
Air Force Institute of Technology
Wright-Patterson AFB, OH 45433-7765
Michael.Grimaila@afit.af.mil