

PFIC



Paraben's Forensic Innovations Conference

Park City, Utah

November 8th-11th 2009



Incident Response Lab

Using P2 Enterprise Shuttle

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Post-Incident

* NIST SP 800-61

Six Step Incident Response Procedures



- Preparation → • Write Policies, Procedures, etc
- Detection • Secure network design
- Containment • Patches
- Eradication • Firewall, IDS, etc deployments
- Recovery • Custom rule sets
- Post-Incident • Training
- Rehearsals

Six Step Incident Response Procedures



- Preparation
- Detection →
 - Event Correlation
- Containment
 - NTP
- Eradication
- Recovery
- Post-Incident
 - False Positive
 - Verification

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment →
 - Filters
- Eradication
 - Email, network traffic, etc
- Recovery
 - Pull the plug
- Post-Incident
 - On the box?
 - On the whole network?

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication →
 - Remove the evil
- Recovery
 - Virus Cleaners
- Post-Incident
 - Spyware Removers
- Remove everything

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication
- Recovery →
 - Recover from backups
- Post-Incident
 - Rebuild systems

Six Step Incident Response Procedures



- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Post-Incident →
 - After Action Review
 - Policy, Procedure, etc rewrite?
 - Firewall, IDS, etc rules rewrite?

Four Step Forensic Procedures



- Collection
- Examination
- Analysis
- Reporting

* NIST SP 800-86

Four Step Forensic Procedures



- Collection →
 - Define scope of case
- Examination
 - Decide what to image
- Analysis
 - Protect evidence integrity
- Reporting
 - Maintain chain of custody

Four Step Forensic Procedures



- Collection
- Examination →
 - Find potential evidence
- Analysis
 - Data recovery
- Reporting
 - Password cracking

Four Step Forensic Procedures



- Collection
- Examination
- Analysis →
 - Is it evidentiary?
 - Does it pertain to the case?
 - How?
 - Expert opinion
- Reporting

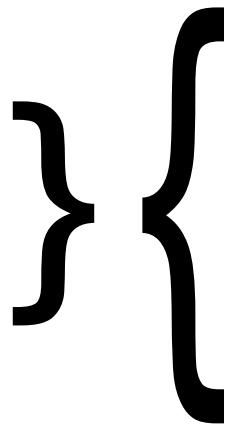
Four Step Forensic Procedures



- Collection
- Examination
- Analysis
- Reporting →
 - Report writing
 - Exhibit preparation
 - Longest part of the process

How Do We Do Both?

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Post-Incident



- Collection
- Examination
- Analysis
- Reporting

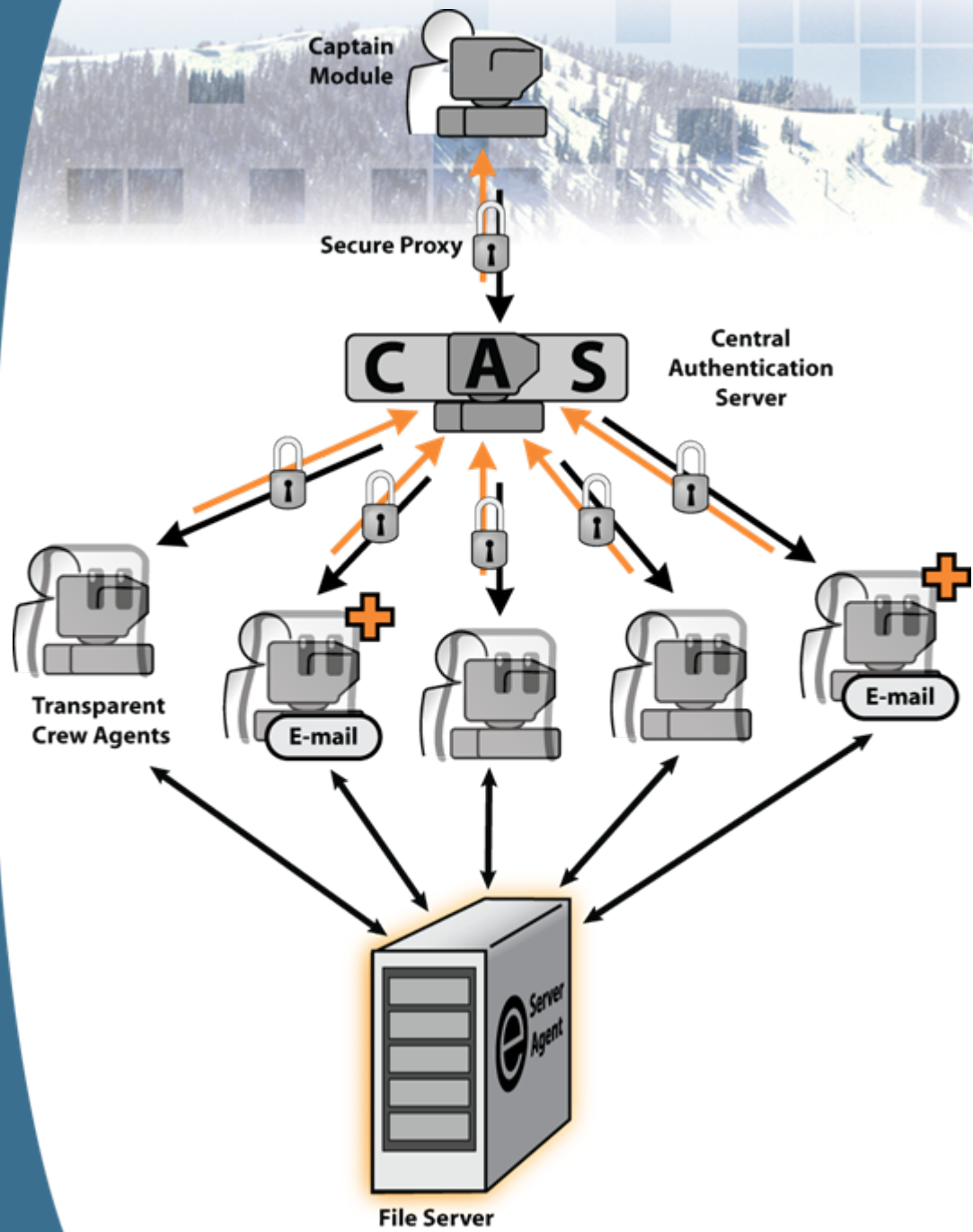
P2 Enterprise System



Shuttle Edition



Full Edition



P2 Enterprise System

General Structure



P2 Enterprise Agents



- Three Agent Types
 - Standard Agent
 - Plus Agent
 - Server Agent

- Common Features (Shuttle/Full)
 - Stealth
 - Acquisitions (File/Drive)
 - Memory Acquisitions
 - Cross Agent Searching

PRACTICAL

