Arca Systems, Inc.
an Exodus Communications Company

Incident Response Fundamentals Class

Instructor
Eric Winterton
eric.winterton@exodus.net

Creators
Klayton Monroe
Eric Winterton

Problem Statement:

- The successfulness of a given incident response depends on several factors:
  - knowing where to begin,
  - being able to clearly evaluate the situation,
  - gathering information and evidence properly and in the correct order, and
  - knowing when to request outside assistance
- Therefore, people involved in responding to incidents need to be educated in the basic procedures of incident response.

Course objectives

- To introduce the student to the basic definitions, concepts, and procedures of or relating to incident response.
- To answer the following questions:
  - Who can help me respond to an incident?
  - What are the main elements of an incident response team?
  - How do I REACT to a perceived incident (anomaly)?
  - How does the Incident Response Team RESPOND to a reported anomaly?
  - How do I RECOVER in the wake of an incident?

What is not covered

- How to develop and write policy
- How to develop and write procedures
- How to conduct a risk assessment
- Law enforcement issues
- Detailed forensic analysis of gathered data
- Setting up Intrusion Detection Systems
- How to harden systems against attack

Fundamental Concepts

- An *Anomaly* is something different, abnormal, or peculiar (e.g. event or system state).
- An *Incident* is any anomaly that violates an organization's security policy.
- *Incident Response* is the timely marshalling of appropriate resources in response to a reported incident or anomaly.
- *Forensics* is the application of scientific knowledge to legal problems.
- *Computer Forensics* is the application of scientific knowledge to legal problems involving computer-related evidence.

Fundamental Concepts (*continued*)

- **REACT**
  - **Review policy and procedures**
  - **Evaluate the situation**
  - **Avoid panic**
  - **Collect information**
  - **Take appropriate action**

Fundamental Concepts (*continued)*

- RESPOND
  - Request information
  - Evaluate the situation
  - Stop the "attack" and Secure the "crime scene"
  - Preserve evidence
  - Organize forensic examination
  - Note findings
  - Determine cause(s)

Fundamental Concepts (continued)

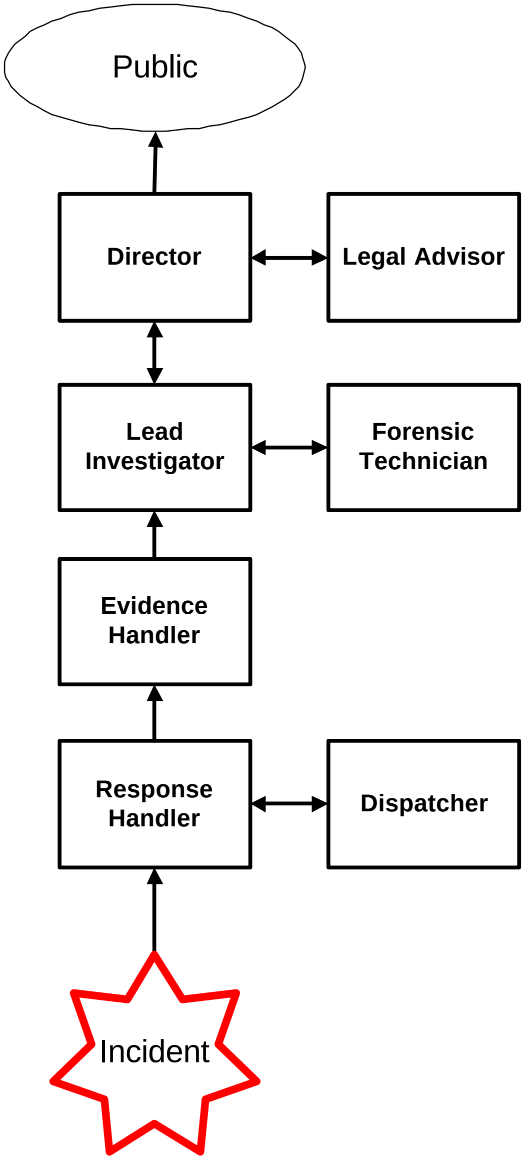
- RECOVER
  - Raise security expectations
  - Evaluate current security posture
  - Create implementation plan
  - Order it to be done
  - Validate the implementation
  - Expect the unexpected
  - RECOVER on a regular basis

Who can help me respond to an incident?

- Arca/Exodus Incident Response Team (IRT)
- Law enforcement
  - State
  - Federal
- CERTs
- Refer to handouts for detailed contact information

What are the main elements of an incident response team?

- Director
- Lead Investigator
- Forensic Technician(s)
- Response Handler
- Evidence Handle
- Legal Advisor



Public

Director

Legal Advisor

Lead Investigator

Forensic Technician

Evidence Handler

Response Handler

Dispatcher

Incident

Director

- The *Director* is a person from senior management who has the authority to carry out incident response activities. The Director answers directly to top management (e.g. CEO).

Lead Investigator

- The *Lead Investigator* is in charge of making sure that incident response activities are executed in the right order and at the right time. The Lead Investigator reports to the Director, and ensures that the technicians and the Evidence and Response Handler have the resources necessary to carry out their duties. The Lead Investigator is responsible for preparing an incident report and briefing any findings and/or determinations to senior management. The Lead Investigator is also responsible for interfacing with law enforcement and other IRTs.

Forensic Technician

- *Forensic Technicians* carry out incident response tasks at the direction of the Lead Investigator. Forensic Technicians must be experts at what they do. It is likely that more than one technician will be required because different systems and configurations require different skills and knowledge. At a minimum there should be a collective expertise available to the IRT to address all distinct system components involved in the incident. Forensic Technicians are responsible for analyzing that evidence, and reporting on their findings.

Response Handler

- The *Response Handler* is usually the first one on the scene and must react quickly. The responsibilities of the response handler is to secure the crime scene and collect evidence.

Evidence Handler

- The *Evidence Handler's* function is to protect all evidence gathered during the course of the incident. This person will receive any evidence that is collected by technicians, ensure that it is properly tagged, check it into and out of protective custody, and maintain a strict chain of custody.

Legal Advisor

- The *Legal Adviser's* job is to provide guidance consistent with all applicable state and federal laws. The Legal Adviser is responsible for helping the company decide whether to pursue any kind of legal action.

Dispatcher

- *Dispatchers* man the Incident Response hotline. Their responsibilities are to receive distress calls from clients, provide general information about the various incident response services, fill out incident reports, assign tracking numbers to new cases, and connect clients with the appropriate IRT personnel for further assistance. Typically, the dispatch function will be staffed around the clock.

So your being attacked...

- Question: What do you do?
- Answer: You REACT
  - Review policy and procedures
  - Evaluate the situation
  - Avoid panic
  - Collect information
  - Take appropriate action

REACT: Review policy and procedures

- Locate the policy that addresses IR
- Locate the IR procedures
- Locate policy on what is and is not allowed
- What if I don’t have any

REACT: Locate the policy that addresses IR

- It should define roles and responsibilities
  - Director
  - Lead Investigator
  - Forensic Technicians
  - Response Handler
  - Evidence Handler
  - Legal Adviser
  - Dispatcher
- It should name a plan of action
  - IR procedures

REACT: Locate the IR procedures

- They should state what to do, when, and by whom.
- They should already be prioritized according to your company’s goals.
- Ideally, they should “do the thinking for you.”
  - They should highlight course details while still providing fine details.
    - 911
    - ABCs
    - Stop, Drop, and Roll
    - REACT, RESPOND, and RECOVER

REACT: Locate policy on what is and not allowed

- Remember, its not technically an incident unless it violates your security policy.
- It should address the following:
  - Network traffic (protocol matrix)
  - Host applications/services (services matrix)
    - Web, Email, FTP
  - User account activity
  - Administrator account activity
  - Guest/other account activity
  - etc.

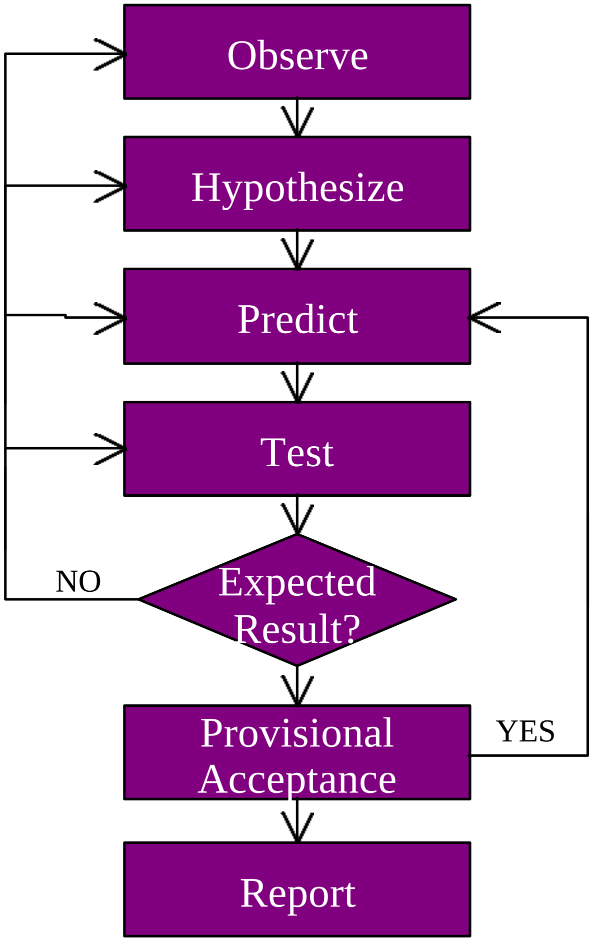
REACT: What if I don’t have any?

- Notify senior management.
- Form an ad hoc IRT.
  - Director (required)
  - Lead investigator (required)
  - Staff other roles if able
- Follow the REACT procedures.
- Get help.

REACT: Evaluate the Situation

- Is the incident over? (urgency)
- What major assets are involved? (criticality)
- What is the damage? (criticality)
- Is continued operation possible/required?
- Re-evaluate any/all recent changes to your site's configuration
  - Try to rule out the following:
    - bad configuration
    - bad assumptions
    - operator error

REACT: Scientific Methodology



REACT: Exercise: Problem solving

- Observation: “My machine is slow.”
- What hypotheses can you think of?
- What predictions can you develop for each hypothesis?
- What tests can be applied to either prove or disprove each hypothesis?
- Is your test environment controlled?

REACT: Avoid Panic

- Don’t trash the “crime scene”
- Practice good OPSEC
- Know your limitations
- A panic example

REACT: Don’t trash the “crime scene”

- Unless otherwise directed by the IRT don’t do the following:
  - Log in and poke around
  - Let other people do the same
  - Run attack probes to determine if your site is vulnerable to some particular attack
  - Halt the machine via an unapproved or abnormal procedure
  - Engage the attacker
  - Probe the involved networks

REACT: Practice good Operations Security

- *Operations Security (OPSEC)* is a collection of processes by which an organization denies to potential adversaries gratuitous information about its structure, intentions, and activities.
- Will your actions indicate that something's up?
  - Flurry of email or other in-band communications
  - Buzz in the air
  - A change in the established daily routines
- Maintain a strict need to know
  - The attacker may be among you or monitoring you.
  - "Loose lips sink ships."

REACT: Know your limitations

- Don’t hesitate to bring in expert help
  - Incident Response Team
  - Forensics Team
  - Subject matter experts
  - Auditors
- Call on your Director and Lead Investigator
  - for decision making support
  - for response priorities
  - questions concerning state and federal law (e.g. ECPA)
    - Monitoring (Court order, self-defense, consent)
  - questions concerning liability

REACT: A panic example

- The case of the disturbing note...

REACT: Collect Information

- Start a log book
- Safeguard evidence
- Gather latest configuration details
  - Do this without modifying the target system(s)

REACT: Start a log book

- Record everything you do
  - Observations
  - Hypothesis
  - Ideas
  - Assumptions
  - Date and Time
  - Actions taken
  - People spoken to
- Use an engineer’s notebook and ink

REACT: Safeguard Evidence

- Establish and maintain a chain of custody
  - Make it verifiable
  - Employ witnesses
- Assign an Evidence Handler
- Tag and seal ALL evidence taken into custody
  - Date,
  - Unique evidence number,
  - Item name,
  - Description of suspected contents,
  - Signature of technician, and
  - Signature of witness (if available)

REACT: Gather Configuration Details *

- Start with the basics
  - Network topology diagram
  - Host names and addresses
  - Machine and OS types
- Then fill in the details (use worksheets)
  - Firewalls
  - Gateways
  - Hosts

REACT: Take Appropriate Action

- Decide what kind of response is appropriate
  - Protect and proceed
  - Pursue and prosecute
    - Criminal
    - Civil
  - Not sure?
    - Get expert advise
- Estimate the level of effort
  - Do you need external support?
  - Not sure?
    - Get expert advise

REACT: Take Appropriate Action *(continued)*

- Consider legal ramifications
  - State Law and Federal Law
    - ECPA: Monitoring requires one of following conditions:
      - Court order
      - Self-defense
      - Consent
  - Employee rights
    - Have they signed consent forms?
    - Do you have warning banners?
  - Customer rights
    - Do you have warning banners?

How does the Incident Response Team RESPOND to a reported anomaly?

- Request information
- Evaluate the situation
- Stop the “attack” and Secure the “crime scene”
- Preserve evidence
- Organize forensic examination
- Note finding(s)
- Determine cause(s)

RESPOND: Request Information

- Contact information
- Law enforcement status
- Problem description
- Determine the client’s desired level of support

RESPOND: Contact information

- Company vitals
  - Name
  - Address
  - Customer ID
  - Service subscription details
- Incident Handler and Technical POCs
  - Name
  - Address
  - Phone, fax, pager, email, etc.

RESPOND: Law enforcement status

- Has law enforcement been called?
- Have they opened a case?
  - Who is the POC?
  - What is the current status?
- Note: Investigations are controlled by law enforcement

RESPOND: Problem description

- How critical is this event?
- Who observed the problem/event/anomaly?
- Has any evidence already been collected?
- What machines are involved?

RESPOND: Support needs

- What kind of support is being requested?
  - Consultation, Evidence collection, forensics, the works, etc.
- How much support will be needed?
- What are the client’s response priorities?
  - Protect and proceed
  - Pursue and prosecute
  - Private investigation
  - other

RESPOND: Evaluate the Situation

- Determine the source of the problem
- Estimate the level of effort that will be required
- Identify if and when there may be a need for subject matter experts
- Construct a basic plan of action

RESPOND: Determining the problem

- Passive techniques
  - Interviews
  - Monitoring
    - Network traffic
    - Host activity
    - Video surveillance
  - Phone records
  - Timecards
  - Building entry/exit logs
  - Honey pot

RESPOND: Determining the problem

- Active techniques
  - Scan the network/host for known vulnerabilities
  - Engage the suspected attacker
    - This can be both good and bad
    - Email, talk, IRC, phone, etc.
  - Retrieve log files and other critical data
  - Call neighboring ISPs
  - Traceroute
  - Load generation direction finding
- Apply scientific methodology

RESPOND: Stop the “attack”

- Temporary measures
  - Change network address
  - Pull the plug (network, power)
  - Firewall rules
  - Higher bandwidth
  - System patches
- Long term measures: Identify the root cause and eliminate it
  - Bug (hardware/software)
  - Configuration error (network/host)
  - Locate the attacker(s)
  - Don’t just patch and play

RESPOND: Secure the "crime scene"

- Coordinate with a "trusted" technical contact from the local firm who is knowledgeable about the system in question.
- Look before you leap.
- Document all actions taken in your log book.
- Carry an emergency kit with you.
  - Important contact information
  - Tools (software, hardware)
  - Assorted accessories
- Maintain client confidentiality, and practice good OPSEC.
- Enforce the moral equivalent of yellow police tape.

RESPOND: Preserve Evidence

- A proverb
- Objectives
- Goal
- Issues
- Types
- Chain of custody

RESPOND: A Proverb

- The criminal always takes something from the scene and always leaves something behind
- The question is “Can you collect what’s available while it’s available?”

RESPOND: Objectives

- Preserve the scene
- Preserve data integrity
- Preserve legal integrity
- Establish a chain of custody

RESPOND: Goal

- Collect all relevant evidence

RESPOND: Issues

- Diligence & Patience vs. Speed & Accuracy
- Heisenberg Principle
  - By trying to collect or observe evidence:
    - You could be destroying/modifying it
    - You could be creating it
- Booby traps
- Volume
  - How much evidence is there?
  - Can you handle that much?
  - Can you afford not to handle this much?
- Symptom vs. Cause
- Superficial vs. Deep

RESPOND: Evidence types

- Volatile evidence
  - Memory
  - Active Processes
  - Active network connections
  - Contents of the computer screen
  - Finger prints
- Non-volatile evidence
  - Physical equipment
  - Persistent storage
  - Printouts from various audit and monitoring logs
  - Recorded video surveillance

RESPOND: Chain of Custody

- The objective is provenance
  - Paper trail
  - No gaps
  - Immutability
- Ways to get it done
  - Engineer’s notebook and ink
  - Evidence labels and transmittals
    - Refer to REACT
    - Need a transmittal sample
  - Digital signatures and checksums
  - Two Person Integrity (TPI) and witnesses
  - Assign an Evidence Handler

RESPOND: Organize Forensic Examination

- Evidence pre-processing
- Analysis

RESPOND: Evidence Pre-Processing

- Objective
  - Transition evidence into the analysis environment without affecting its integrity
- Issues
  - Production of analyzable image
  - Platform dependencies
  - Volume
  - Medium
  - Format
  - Distribution to analysts

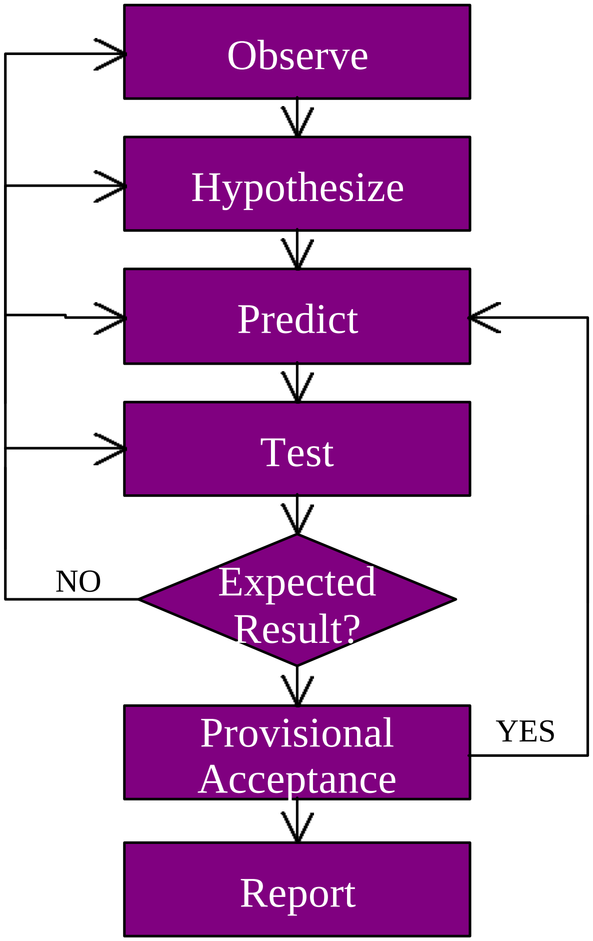
RESPOND: Analysis

- The analysis product will be a combination of:
  - Postmortem
  - Deductive reasoning
  - Inductive reasoning
  - Scientific method
- *Postmortem* is an analysis or discussion of an event after it is over.
- *Deductive reasoning* flows from general to specific.
- *Inductive reasoning* goes from a set of specific observations to general conclusions.

RESPOND: Analysis: Requirements

- Non-destructive process
- Logically compelling story
- Certifiable tools and techniques
  - Widely used in the field by practitioners
  - Independently verifiable
    - Repeatable results
    - By hand equivalents
    - Well known error rate
  - Documented algorithms
  - Can withstand cross examination

RESPOND: Analysis: Methodology



RESPOND: Analysis: Advice

- Always question the validity of information
- Don’t eliminate a hypothesis just because it doesn’t have any supporting evidence
- Use an engineer’s notebook and ink
- Employ multi-disciplinary teams
- Visualization techniques can elucidate patterns

RESPOND: Note Findings and Determine Causes

- Build timelines
- Logical process of elimination
  - Apply scientific method
    - Generate a list of all possible causes
    - Does/could action lead to the observed state
    - Determine what evidence would be needed to support each cause
  - Rule out accidental causes
    - Operator error
    - Configuration error
- Generate a report
- Brief the client

How do I RECOVER in the Wake of an Incident

- Raise your security expectations
- Evaluate your current security posture
- Create implementation plan
- Order it to be done
- Validate the implementation
- Expect the unexpected
- Recover

RECOVER: Raise your Security Expectations

- It’s not good enough to say “we need security.”
  - You have to commit resources.
  - Management must support the cause.
- Is there a security budget?
  - Does it address the following:
    - Security tools and patches
    - Training classes and resources
    - 3rd party consulting
      - Tiger teams
      - Security auditors
    - Long term staffing requirements

RECOVER: Raise your Security Expectations

- Is there a security training program?
  - Does it address the following:
    - User awareness
      - Policy and procedures
      - Security
    - System security configuration
    - Incident response
    - Security tools
    - Network/Host audit
- Are there security personnel?
  - Who is responsible for getting it done?
  - Do they have resources and authority?

RECOVER: Evaluate your Current Security Posture

- Determine and document your current configuration
  - Use the worksheets
- Conduct a risk assessment
  - What is your security budget?
  - Where is that mission critical data?
  - How much risk are you willing to take?
  - What are the threats to your system(s)?
    - Audits, penetration testing, Internet postings

RECOVER: Create Implementation Plan

- Revise policy and procedures
    - Address corporate goals
    - Add definitions about what is and is not allowed
    - Add procedures to address
        - Deficiencies that occurred during this response
        - Baselining
        - Basic system installation and configuration
        - Security configuration
        - Backups
        - Security audits
        - Incident response
        - others...

RECOVER: Create Implementation Plan

- Reload system from trusted media
  - Why can’t we just fix the problem?
  - Why can’t we user our last backup?
- Apply known approved patches
  - Some patches may introduce new vulnerabilities
- Tighten system/network configurations
  - Per host service matrix
  - Per host protocol matrix
  - Enable auditing
  - Boundary controls
  - Disable unused and unnecessary accounts
  - Enforce strict password controls

RECOVER: Create Implementation Plan

- Baseline it
  - Disk image
  - Backups
  - Create a system profile
- Consider installing intrusion detection sensors and network monitors
  - Do you have someone who has the responsibility of reviewing audit logs?

RECOVER: Order it to be done and Validate the implementation

- Require a status report
- Hold individuals accountable for doing their job
- Employ 3rd party security audits as an independent verification tool

RECOVER: Expect the Unexpected

- **Configurations change**
- **People move in and out of jobs**
- **Company policies and goals may change**
- **Your systems will become vulnerable to new attacks**
- **20/20 … no ... X-ray vision is required**

RECOVER: Recover on a Regular Basis

- **Whenever anything changes**
- **At least yearly**

Closing remarks

- Go back to your office and locate your company’s security policy and IR procedures.
  - If you have none or they are woefully inadequate, start creating them immediately.
- Use the worksheets.
- Start RECOVERing now!
  - Prevention is a good investment
- Start developing your X-ray vision
  - Detection is key
- REACT to perceived incidents.
- Call on the Arca IRT to RESPOND to your incidents.

Questions...