Security Talk
Incident Response

Brian Epstein <bepstein@ias.edu>

What is Incident Response?

- Response by person or team to an attack
- Organized reaction
- Pre-planned as much as possible

AIC Triad with Incident Response

- Availability
  - How long of an outage is this going to create?
- Integrity
  - Can we trust the recovery of a compromised system?
- Confidentiality
  - Was our private information compromised?

What to do During an Incident

- Preparation
- Identification
- Communication
- Containment
- Recovery and Analysis

Preparation

- 90% of Incident Response is in preparation
- Identification of System and Data owners
- Categorization of Systems and Data
- Communication Plans and Lists
- Backups and Patches

Identification

- Intrusion Detection System (IDS)
  - Network Based
  - Host Based
- Logs – make sure they are time sync'ed
- Event Correlation
- Confirmation

Communication

- Immediately deploy SIRT (explained below)
- Audit Trail
  - Log all communication
  - Follow communication path policy
- Sign communications
- Communicate soon and often

Containment

- Intrusion Prevention System (IPS)
- Firewall
- Service Interruption
- High Availability
- Cost of Downtime

Recovery

- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- System and Data Recovery
- Mitigation of risks to avoid re-contamination

Analysis

- Root Cause Analysis (RCA)
- Cost of Incident
- Speed and Cost Effectiveness of Response
- Update Plan

Examples

- Virus
- System Compromise
- Network Device Compromise
- Compromise of Confidential Data

Virus

- Identification
  - Mass mailing, communication with C&C
  - Bootable virus scanner
- Containment
  - Remove computer from network, physical or logical
  - Containment practices should be known by user

Virus

- Recovery
  - Full Cleansing of machine
  - Possible rebuild and scan of all data files
- Analysis
  - How did the virus infect the system?
  - How can we mitigate this risk in the future?

System Compromise

- Identification
  - HIDS, NIDS
  - System trending
- Containment
  - Can this system be removed from the network?
  - How can we best preserve the current system state?

System Compromise

- Recovery
  - Fix the system
  - Re-image system – or fix and re-image system
- Analysis
  - What was the cost of compromise (resources, time)?
  - How can we mitigate this risk in the future?

Network Device Compromise

- Similar to System Compromise
- Could cause outage to a number of services
- May be easier to physically replace the device

Compromise of Confidential Data

- Communication to data owner and customer
- Issue new data if possible (credit card number)
- Trace data usage to find thief
  - Credit record
  - honeypots

Security Incident Response Team (SIRT)

aka. CIRT, CERT, SERT

- Three types of team members
  - Managers
  - Fixers/Solvers
  - Communicators
- Dynamic Team on as-needed basis (HR & PR)

SIRT Charter

- Identify team members (permanent/transient)
- Formalize scope and responsibility
- Describe organizational structure
- Plan communication
  - Between members and Human Resources
  - Public Relations and Law Enforcement

SIRT Recovery Goals

- Protect and Proceed
  - Get back online as soon as possible
- Pursue and Prosecute
  - Balance compromising sensitive data versus catching the perpetrator

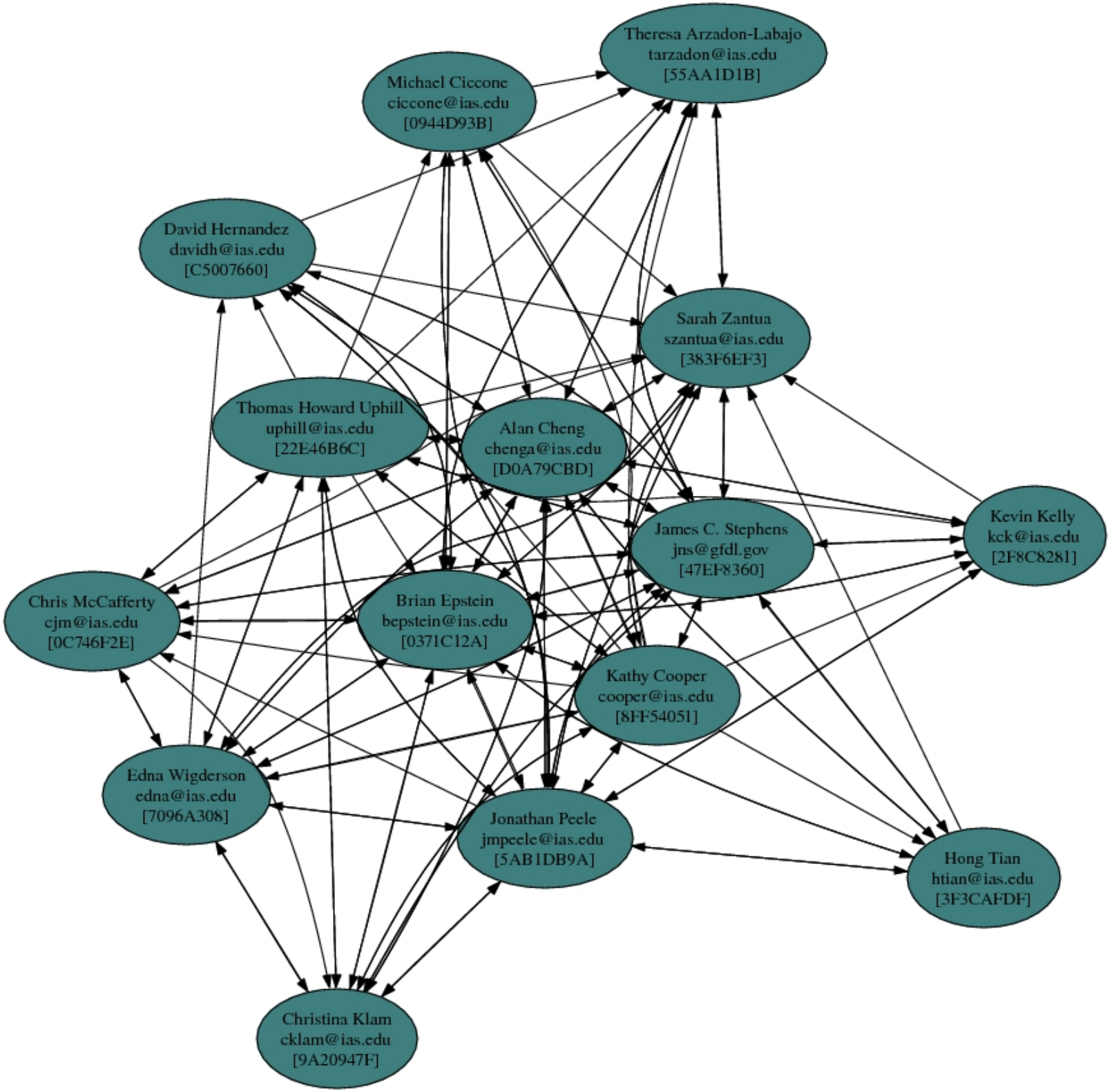
SIRT Response

- SIRT determines false alarms
- May include environmental incidents
- SIRT authorizes investigation
  - Heisenberg Uncertainty Principle
  - Pristine crime scene investigation

Questions?

References

- http://www.securityfocus.com/infocus/1184
- http://www.sans.org/rr/incident/IRCF.php
- http://labmice.techtarget.com/security/incidentresponse.htm
- Avolio, F. (2002). Practical IR. Columns. Retrieved November 27, 2006 from http://infosecuritymag.techtarget.com/2002/oct/justthebasics.shtml
- Cook, C. (2000). An Introduction to Incident Handling. Retrieved November 27, 2006 from http://www.securityfocus.com/infocus/1184


Theresa Arzadon-Labajo
tarzadon@ias.edu
[55AA1D1B]
Michael Ciccone
ciccone@ias.edu
[0944D93B]
David Hernandez
davidh@ias.edu
[C5007660]
Sarah Zantua
szantua@ias.edu
[383F6EF3]
Thomas Howard Uphill
uphill@ias.edu
[22E46B6C]
Alan Cheng
chenga@ias.edu
[D0A79CBD]
Kevin Kelly
kck@ias.edu
[2F8C8281]
James C. Stephens
jns@gfdl.gov
[47EF8360]
Chris McCafferty
cjm@ias.edu
[0C746F2E]
Brian Epstein
bepstein@ias.edu
[0371C12A]
Kathy Cooper
cooper@ias.edu
[8FF54051]
Edna Wigderson
edna@ias.edu
[7096A308]
Jonathan Peele
jmpeele@ias.edu
[5AB1DB9A]
Hong Tian
htian@ias.edu
[3F3CAFDF]
Christina Klam
cklam@ias.edu
[9A20947F]

Security Talk
Incident Response

Brian Epstein <bepstein@ias.edu>

What is Incident Response?

- Response by person or team to an attack
- Organized reaction
- Pre-planned as much as possible

AIC Triad with Incident Response

- Availability
  - How long of an outage is this going to create?
- Integrity
  - Can we trust the recovery of a compromised system?
- Confidentiality
  - Was our private information compromised?

What to do During an Incident

- Preparation
- Identification
- Communication
- Containment
- Recovery and Analysis

Preparation

- 90% of Incident Response is in preparation
- Identification of System and Data owners
- Categorization of Systems and Data
- Communication Plans and Lists
- Backups and Patches

Identification

- Intrusion Detection System (IDS)
  - Network Based
  - Host Based
- Logs – make sure they are time sync'ed
- Event Correlation
- Confirmation

Communication

- Immediately deploy SIRT (explained below)
- Audit Trail
  - Log all communication
  - Follow communication path policy
- Sign communications
- Communicate soon and often

Containment

- Intrusion Prevention System (IPS)
- Firewall
- Service Interruption
- High Availability
- Cost of Downtime

Recovery

- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- System and Data Recovery
- Mitigation of risks to avoid re-contamination

Analysis

- Root Cause Analysis (RCA)
- Cost of Incident
- Speed and Cost Effectiveness of Response
- Update Plan

Examples

- Virus
- System Compromise
- Network Device Compromise
- Compromise of Confidential Data

Virus

- Identification
  - Mass mailing, communication with C&C
  - Bootable virus scanner
- Containment
  - Remove computer from network, physical or logical
  - Containment practices should be known by user

Virus

- Recovery
  - Full Cleansing of machine
  - Possible rebuild and scan of all data files
- Analysis
  - How did the virus infect the system?
  - How can we mitigate this risk in the future?

System Compromise

- Identification
  - HIDS, NIDS
  - System trending
- Containment
  - Can this system be removed from the network?
  - How can we best preserve the current system state?

System Compromise

- Recovery
  - Fix the system
  - Re-image system – or fix and re-image system
- Analysis
  - What was the cost of compromise (resources, time)?
  - How can we mitigate this risk in the future?

Network Device Compromise

- Similar to System Compromise
- Could cause outage to a number of services
- May be easier to physically replace the device

Compromise of Confidential Data

- Communication to data owner and customer
- Issue new data if possible (credit card number)
- Trace data usage to find thief
  - Credit record
  - honeypots

Security Incident Response Team (SIRT)

aka. CIRT, CERT, SERT

- Three types of team members
  - Managers
  - Fixers/Solvers
  - Communicators
- Dynamic Team on as-needed basis (HR & PR)

SIRT Charter

- Identify team members (permanent/transient)
- Formalize scope and responsibility
- Describe organizational structure
- Plan communication
  - Between members and Human Resources
  - Public Relations and Law Enforcement

SIRT Recovery Goals

- Protect and Proceed
  - Get back online as soon as possible
- Pursue and Prosecute
  - Balance compromising sensitive data versus catching the perpetrator

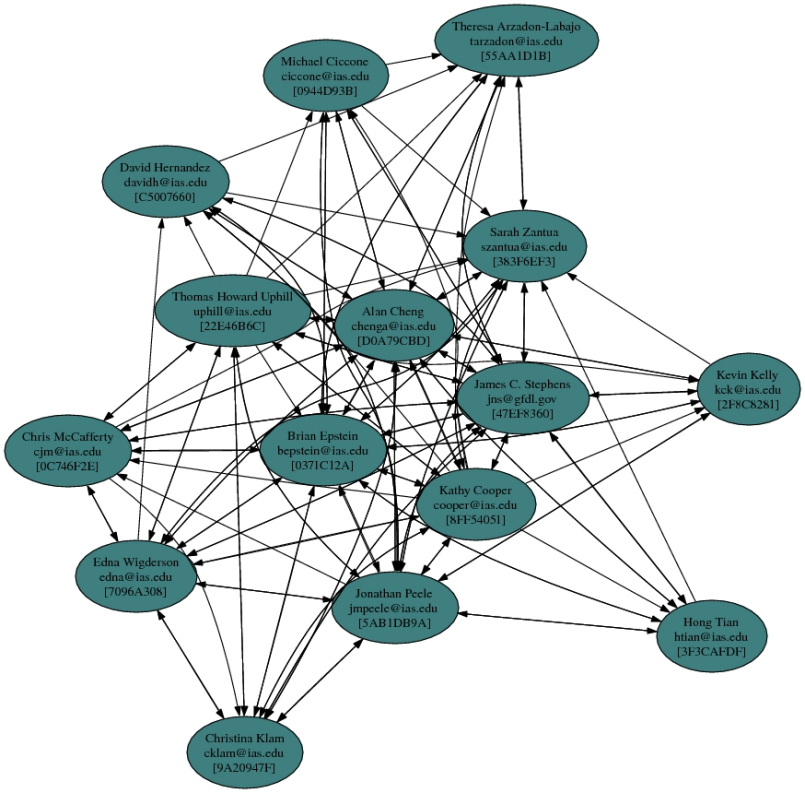
SIRT Response

- SIRT determines false alarms
- May include environmental incidents
- SIRT authorizes investigation
  - Heisenberg Uncertainty Principle
  - Pristine crime scene investigation

Questions?

References

- http://www.securityfocus.com/infocus/1184
- http://www.sans.org/rr/incident/IRCF.php
- http://labmice.techtarget.com/security/incidentresponse.htm
- Avolio, F. (2002). Practical IR. Columns. Retrieved November 27, 2006 from http://infosecuritymag.techtarget.com/2002/oct/justthebasics.shtml
- Cook, C. (2000). An Introduction to Incident Handling. Retrieved November 27, 2006 from http://www.securityfocus.com/infocus/1184


Theresa Arzadon-Labajo
tarzadon@ias.edu
[55AA1D1B]
Michael Ciccone
ciccone@ias.edu
[0944D93B]
David Hernandez
davidh@ias.edu
[C5007660]
Sarah Zantua
szantua@ias.edu
[383F6EF3]
Thomas Howard Uphill
uphill@ias.edu
[22E46B6C]
Alan Cheng
chenga@ias.edu
[D0A79CBD]
Kevin Kelly
kck@ias.edu
[2F8C8281]
James C. Stephens
jns@gfdl.gov
[47EF8360]
Chris McCafferty
cjm@ias.edu
[0C746F2E]
Brian Epstein
bepstein@ias.edu
[0371C12A]
Kathy Cooper
cooper@ias.edu
[8FF54051]
Edna Wigderson
edna@ias.edu
[7096A308]
Jonathan Peele
jmpeele@ias.edu
[5AB1DB9A]
Hong Tian
htian@ias.edu
[3F3CAFDF]
Christina Klam
cklam@ias.edu
[9A20947F]