ECE 443/518 – Computer Cyber Security
Lecture 23 Digital Forensics and Incident Response

Professor Jia Wang
Department of Electrical and Computer Engineering
Illinois Institute of Technology

November 11, 2024

Outline

Reading Assignment

- Please refer to the books below for more details
  - "File System Forensic Analysis", Brian Carrier
  - "Digital Forensics and Incident Response", Gerard Johansen

Outline

Incident Response

- How should we address security risks on a day-to-day basis?
- "By failing to prepare, you are preparing to fail."
  – Benjamin Franklin
- The incident response process
- The incident response framework
- The incident response plan
- The incident response playbook
- Testing the incident response framework

The Incident Response Process

- Preparation: create and staff a plan, acquire forensics hardware and software, training.
- Detection: identify malicious activity from events, possibly with the help from users or external entities.
- Analysis: collect evidence, ascertain what happened and what it affected, determine root cause and reconstruct actions.
- Containment: limit/prevent further actions by threat actors.
- Eradication and recovery: wipe infected machines, remove/change affected users, update software and hardware, restore backups, audit other users and systems.
- Post-incident activity: review all actions to determine what worked and what did not work, documentation, incorporate "lessons learned" into the process itself.

The Incident Response Framework

- A framework to put the incident response process to work.
- Computer Security Incident Response Team (CSIRT)
  - A.k.a., Computer Emergency Response Team (CERT)
  - Sponsored by senior leadership: cost vs. benefit
  - Proactive services: training, testing and deploying, etc.
  - Reactive services: responding to incidents at they occur.
- CSIRT core team
  - Incident response coordinator, e.g. Chief Security Officer
  - CSIRT analysts and senior analysts
  - Security operations center analyst: provide almost immediate response to potential security incident via 24/7 monitoring
  - IT security engineer/analysts
- Technical support personnel, e.g. sysadmin and help desk
- Organizational support personnel, e.g. legal and HR
- External resources, e.g. software/harware vendors

The Incident Response Plan

- A documentation outlines the high-level structure of the organization's incident response capability.
- The mission statement and constituency to establish CSIRT.
- Expanded services catalog as offered by CSIRT, e.g. forenstic services to recover evidences from a hard drive (but not to recover accidentally deleted files).
- Identify CSIRT personnel and their roles and responsibilities.
- Contact list 24/7
- Internal communication plan: between senior leadership and the CSIRT, as well as between CSIRT core and support personnel, avoid potentially conflicting instructions.
- Training and maintenance

The Incident Response Playbook

- Each incident response playbook contains a set of instructions and actions to be performed at every step in the incident response process for a set of threats.
- For example, consider phishing attacks
  - Preparation: employee awareness of potential phishing emails
  - Detection: via employee alerts or email security controls
  - Analysis: review logs and network traffic
  - Containment: isolate the affected host from the network
  - Eradication and recovery: reimage with a known good image
  - Post-incident activity: standard procedures to follow

Testing the Incident Response Framework

- Table-top exercises before deployment.
  - Involve the entire CSIRT team for a specific playbook.
  - Document the results and any updates for senior leadership to approve.
- Penetration test after deployment.
  - Red/Blue or Purple Team exercises.
  - Test the plan and the playbooks against a live adversary.
  - Provide more value than a penetration test that only detect security issues.

Outline

Digital Forensics

- A branch of forensic science.
  - To support or refute a hypothesis before criminal or civil courts.
  - For other investigations in private sectors.
- Digital
  - Recover and investigate material found in digital devices.
  - Often in relation to computer and cyber crime.
- A critical component of incident response to support the overall incident response process, e.g.
  - Understand the technical aspects of the incident
  - Potentially identifying the root cause
  - Discover unidentified access or other malicious activity
- We will leave legal aspects of digital forensics to other courses.

Digital Forensic Process

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation

Identification

- Trace evidence like fingerprints and DNA in traditional forensics.
- When hardware and software systems interact with each other
  - Username
  - Network addresses
  - CPU serial numbers
  - Special hardware/software features that can be tied to certain people or group.
  - Watermarks and other identification mechanisms leaving by certain software.
  - Private keys.
- Can any of these evidences be forged?

Preservation and Collection

- Preservation: protect identified evidence against any modification or deletion, e.g.
  - Enable controls to protect log files
  - Isolate a host system
  - Snapshot a virtual machine
- Collection: process to acquire digital evidence
  - Be careful with volatile evidences that are gone when a system is powered down. Refer to RFC 3227 for more details.
  - Some tasks may potentially alter the original evidence and proper documentation is nedded.
  - Document the life cycle of an evidence as chain of custody including information like date/time acquired, device model, serial number, and manufacturer, hash of individual files.

Examination, Analysis, and Presentation

- Examination
  - Discover and extract additional data from the acquired evidence using specific tools and techniques.
  - Need to continue to preserve the evidence.
- Analysis
  - Make connections between evidences to correlate them, e.g. using host IP address to isolate particular traffic from captured network packets.
- Presentation
  - Reporting of facts needs to be clear, concise, and unbiased.
  - Often part of a larger incident investigation that helps to determine the root cause of an incident.
  - May need to testify in court to present facts and conclusion without bias, and may additionally offer opinions as an expert witness with necessary skills.

Summary

- Incident responses need to be well-planned ahead of actual incidents.
- Digital forensics serve as a critical component of incident response processes.