Security Through Examples

Exploring Cyber Security in Critical Infrastructure

Tim Yardley, University of Illinois Urbana-Champaign
yardley@illinios.edu

Introduction Material
September 30, 2016

CYBER RESILIENT ENERGY
DELIVERY CONSORTIUM

Setting The Stage

Categories, properties, and constraints

1

Categories of Information System Adversaries

Adversary	Description
Nation States	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, which is normally not well organized or financed. Normally consists of few individuals, or of one individual acting alone.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or Poorly Trained Employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another example of an insider threat or adversary.

Properties of Interest/Goals

- Keep the lights on
- Protect equipment/infrastructure from damage
  - Very expensive and difficult to replace
- Ensure safety of employees/people
- Make money
- Cyber Security

- Availability
- systems, data
- Integrity
- Data, control commands, systems
- Confidentiality
  - Data (especially market influencing data)
- Privacy
  - On consumer side

Limitations/Constraints

- **Time Scale**
  - Milliseconds to Minutes
    - 4ms for protection messages (LAN)
    - PMU data – a sample every 33ms
- **Application of Existing IT Security Principles**
  - Not always suitable

- Resource Constrained
  - Embedded systems
    - CPU and Memory constraints
  - Low bandwidth
    - Serial links common
- Legacy Integration
  - Backwards compatibility
  - 8-bit systems out there
  - No security features

Ethical Assessment

The basics of how to approach a security assessment

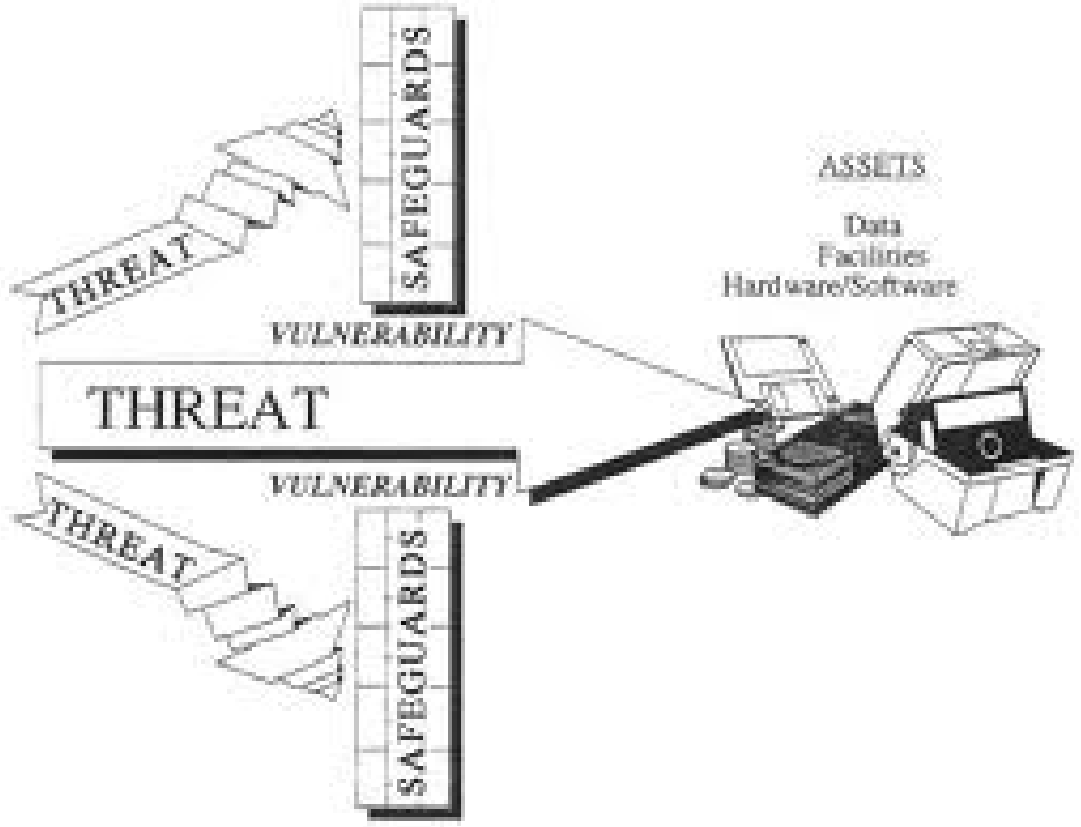
2

Introduction to Ethical Assessment

- Based on the approaches used by Certified Ethical Hacking (CEH) training.
- Focus on the skills for doing professional security work.
- This is not complete training; think of it as being like a beginner- to intermediate-level boot camp.

Terminology

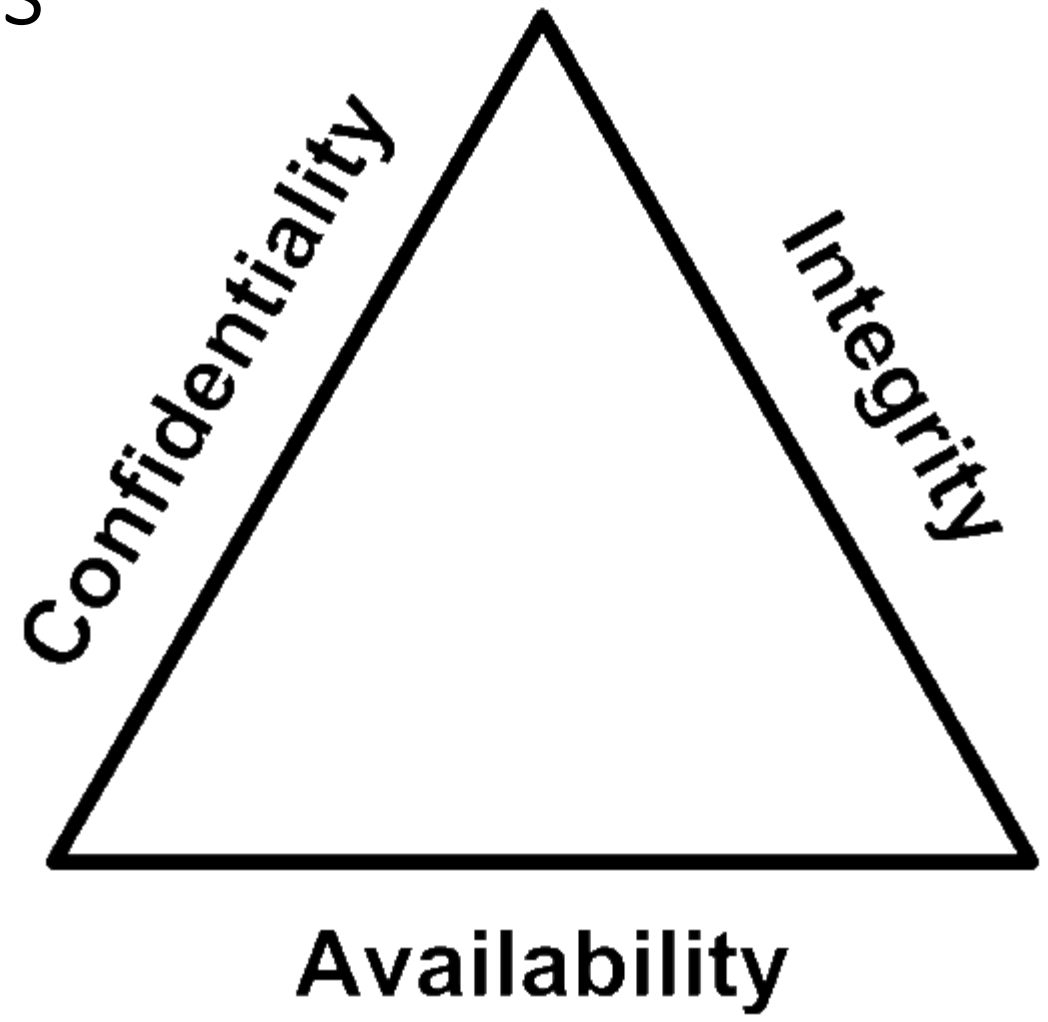
- Asset
- Network resource
- Threats
- Vulnerabilities
- Exploits
- Target of Evaluation (TOE)



http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter7.html

Security Concepts

- Confidentiality
- Integrity
- Availability

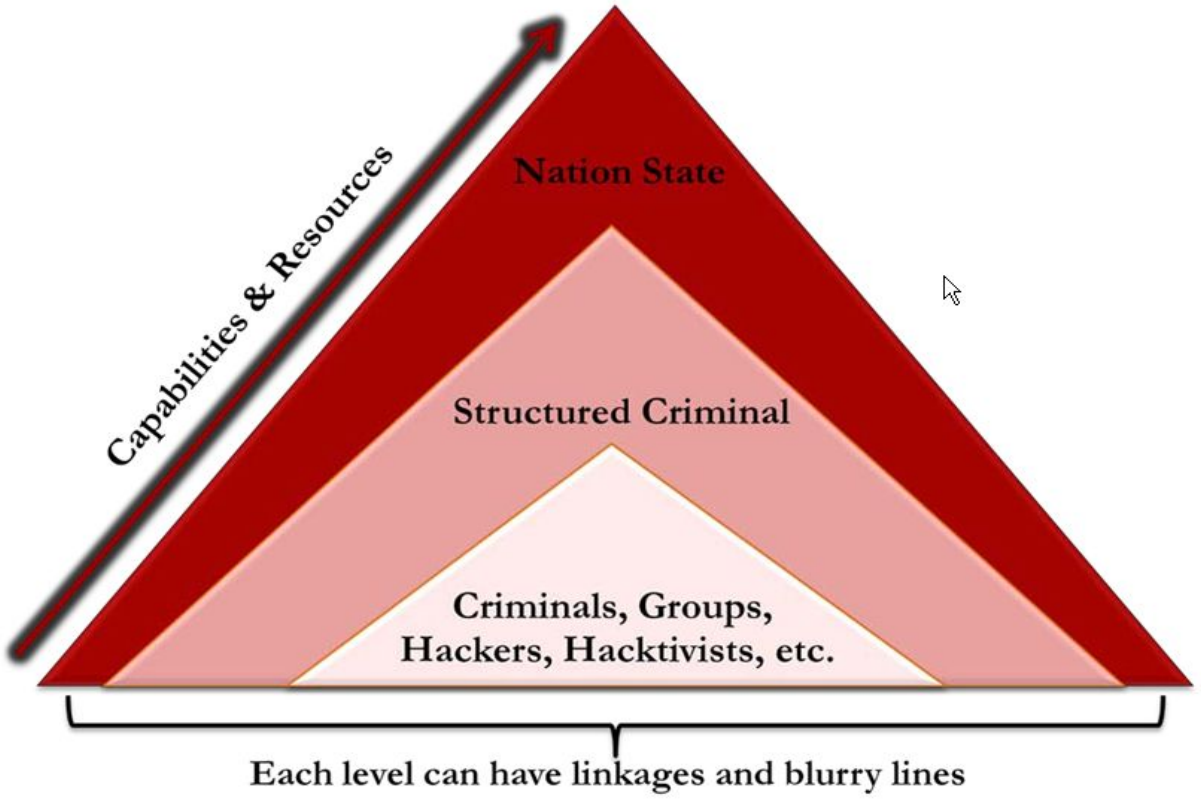


Classes of “Hackers”

- Blackhat
- Greyhat
- Whitehat

Categories of “Hackers”

- Script kiddies
- Disgruntled employees
- Whackers
- Phreakers
- Software crackers
- System crackers
- Cyber terrorists
- Nation-state attackers



Activities Involved in an Assessment

- Discovering networks
  - Using tools
  - Utilizing insiders
- Penetrating networks
  - Determining network resources
  - Leveraging vulnerabilities
- Providing mitigations for assessment observations
  - Observations have little value if there are no mitigations for them.

Steps of an Assessment

- Preparation
  - Define scope.
- Evaluation/conduct
  - Respect system operators.
  - Understand consequences of downtime.
- Conclusion
  - Clearly define and explain any noteworthy items.
  - Suggest mitigations.

Legal Approach

- Determine needs.
- Get permission.
- Schedule assessment.
- Perform assessment.
- Analyze results.
- Create report.
- Present report.

Legality

- Dept. of Justice Title 18 (http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf)
  - Section 1029 (Access Device Fraud) and Section 1030 (Computer Fraud and Abuse)
    - **"Protected Computer"** Section 1030(e)(2) defines protected computer as
      - (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
      - (B) which is used in or affecting interstate or foreign commerce or communication…
    - **"Without Authorization" or "Exceeds Access"**
      - The term "without authorization" is not defined by the CFAA. The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).
      - The legislative history of the CFAA reflects an expectation that persons who "exceed authorized access" will be insiders (e.g., employees using a victim's corporate computer network), while persons who access computers "without authorization" will typically be outsiders (e.g., hackers).

Phases of an Assessment

- Passive and active reconnaissance
- Define scope
- Scanning
- Refine scope
- Gain access
- Determine mitigations
- Maintain access
- Draft report
- Final report

Different Approaches to Assessment

- Black box
- White box
- Grey box

Assessments Entry Vectors

- Remote networks
- Local networks
- Dial-up
- Stolen equipment
- Social engineering
- Physical entry

Details in Your Report

- Results of activities
- Types of tasks performed
- Actual successful tasks with details of techniques
- Disclosure of all security issues discovered
- Mitigations for security issues

Discussion

What makes assessing a control system different?