

Taxonomy of Computer Security Breaches

CSH5 Chapter 8

“Using a Common Language for Computer Security Incident Information”

John D. Howard

1

Copyright © 2011 M. E. Kabay. All rights reserved.

Topics

- What is a Common Descriptive Language?
- What is a Taxonomy?
- Why a Language/Taxonomy for Computer Crime?
- The Model as a Whole
- Actions
- Targets
- Events
- Vulnerability
- Tool
- Unauthorized Result
- Objectives
- Attackers

CSH5 Chapter 8:
“Using a Common Language for
Computer Security Incident Information”

2

Copyright © 2011 M. E. Kabay. All rights reserved.

What is a Common Descriptive Language?

- Set of terms that experts agree on in a field
- Clear definitions to the extent possible
 - ❑ Precise
 - ❑ Unambiguous
 - ❑ Easy to determine in the field
- A common language does not necessarily imply a causal or structural *model*
- Provides means of communication among experts
- Supports analysis

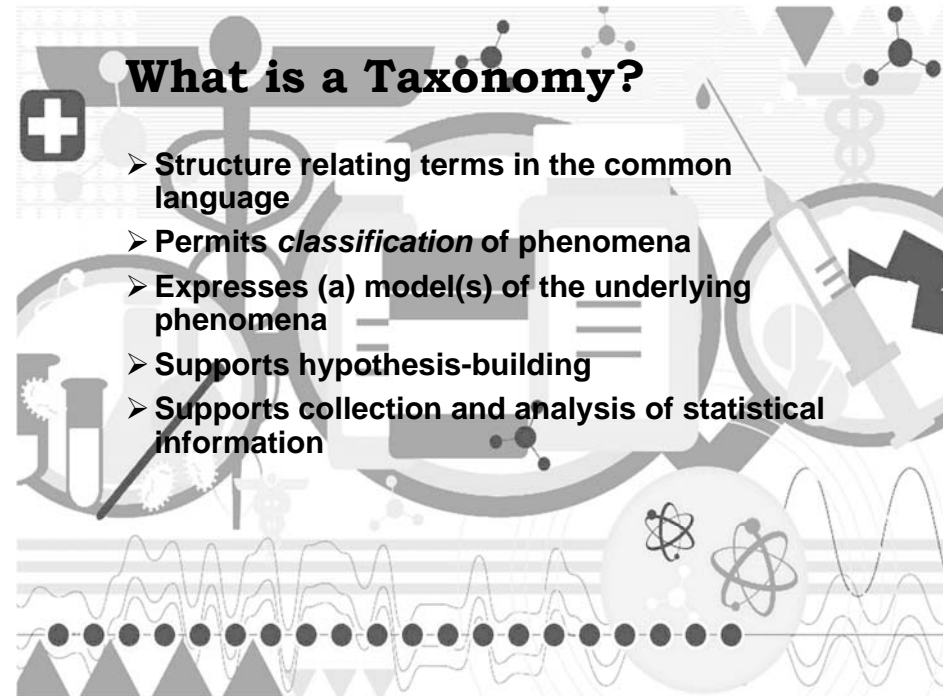


3

Copyright © 2011 M. E. Kabay. All rights reserved.

What is a Taxonomy?

- Structure relating terms in the common language
- Permits *classification* of phenomena
- Expresses (a) model(s) of the underlying phenomena
- Supports hypothesis-building
- Supports collection and analysis of statistical information

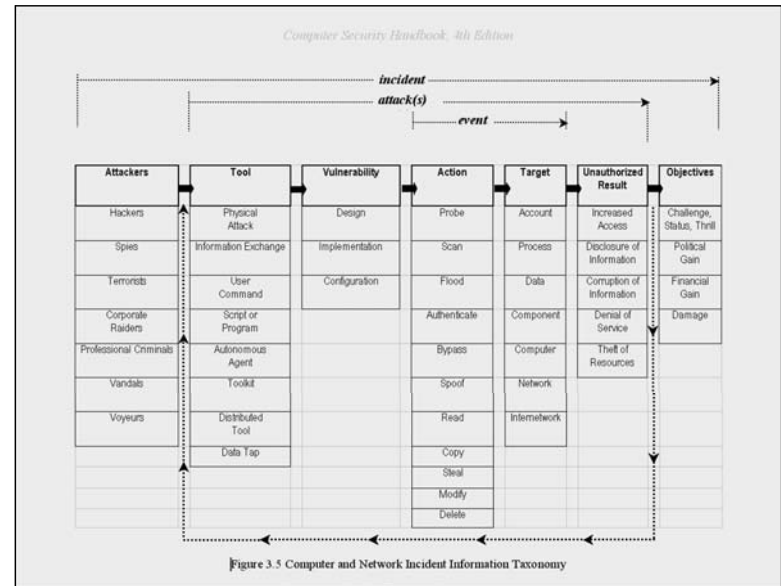


Why a Language/Taxonomy for Computer Crime?



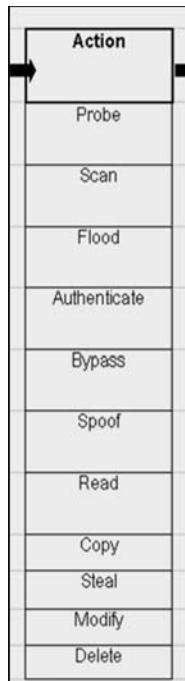
- Field of information assurance growing
 - ❑ More people
 - ❑ Less common experience
 - ❑ Growing variability in meaning of terms
- What's wrong with ambiguous terminology?
 - ❑ Can cause confusion – talking at cross-purposes
 - ❑ Can mislead investigators and others
 - ❑ Wastes time in clarification time after time
 - ❑ Interferes with data-gathering
 - ❑ Makes comparisons and tests difficult or impossible

The Model as a Whole



Actions

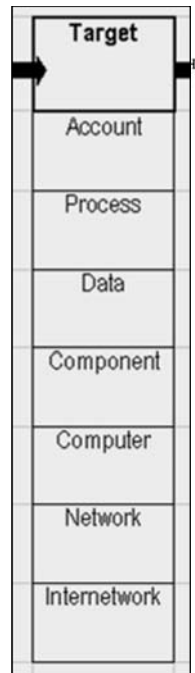
- Probe / scan
- Flood
- Authenticate / Bypass / Spoof
- Read / Copy / Steal
- Modify / Delete



Targets

Analyze the following real cases and identify the target(s) in the events:

- A criminal inserts a Trojan Horse into a production system; it logs keystrokes
- A criminal hacker defaces a Web page
- An attacker launches millions of spurious packets addressed to a particular e-commerce server
- The Morris Worm of November 1988 takes down 9,000 computers on the Internet



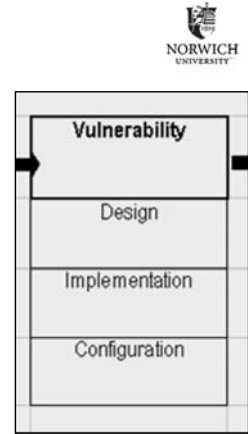
Events

- An event consists of an action taken against a target
- Analyze the following events in these terms:
 - An 8-year-old kid examines all the ports on a Web server to see if any are unprotected
 - A dishonest employee makes copies on a Zip disk of secret formulas for a new product
 - A saboteur cuts the cables linking a company network to the Internet

Action	Target
Probe	Account
Scan	Process
Flood	Data
Authenticate	Component
Bypass	Computer
Spoof	Network
Read	Internetwork
Copy	
Steal	
Modify	
Delete	

Vulnerability

- Vulnerability = a weakness
- Distinguish among vulnerabilities due to
 - Design
 - Implementation
 - Configuration



Common Vulnerabilities and Exposures Dictionary



Sponsored by DHS National Cyber Security Division/US-CERT

<http://web.nvd.nist.gov/view/vuln/search>

NIST National Institute Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview Search CVE and CCE Vulnerability Database ([Advanced Search](#))

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 43542 [CVE Vulnerabilities](#)
- 166 [Checklists](#)
- 203 [US-CERT Alerts](#)
- 2416 [US-CERT Vuln Notes](#)

Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

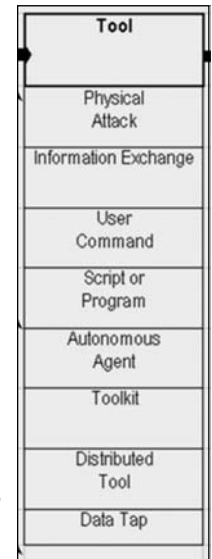
Show only vulnerabilities that have the following associated resources:

- Software Flaws (CVE)
- Misconfigurations (CCE), under development
- US-CERT Technical Alerts
- US-CERT Vulnerability Notes
- OVAL Queries

NVD now maps to CWE! See [NVD CWE](#) for more details.

Tool

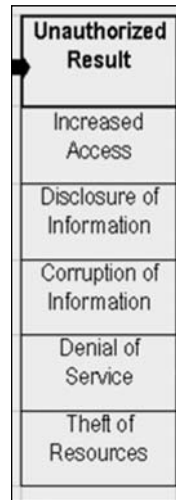
- Means of *exploiting* a vulnerability
- Widely available on Internet
- Exchanged at hacker meetings
 - 2600
 - L0pht (defunct)
- Discussed and demonstrated at black-hat and gray-hat conferences
 - DEFCON – Las Vegas
 - HACTIC – Netherlands
- Many exploits usable by script kiddies and other poorly-trained hackers



Unauthorized Result

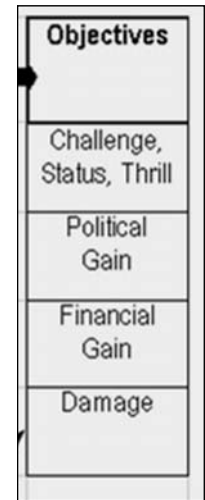
Analyze the results of the following attacks:

- Someone installs a Remote Access Trojan called BO2K on a target system
- An e-mail-enabled worm (e.g., KLEZ) sends a copy of a confidential document to 592 strangers
- The Stacheldraht DDoS tool completely interdicts access to an e-commerce site
- A secret program installed by an employee uses all the "excess" CPU cycles in a corporate network for prime-number calculations



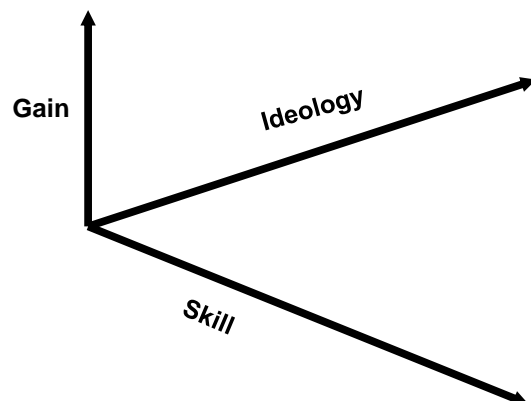
Objectives

- Characteristics of the human beings involved in the attack
- Different objectives and define different labels
 - Criminal hacking
 - Industrial espionage
 - Industrial sabotage
 - Information warfare

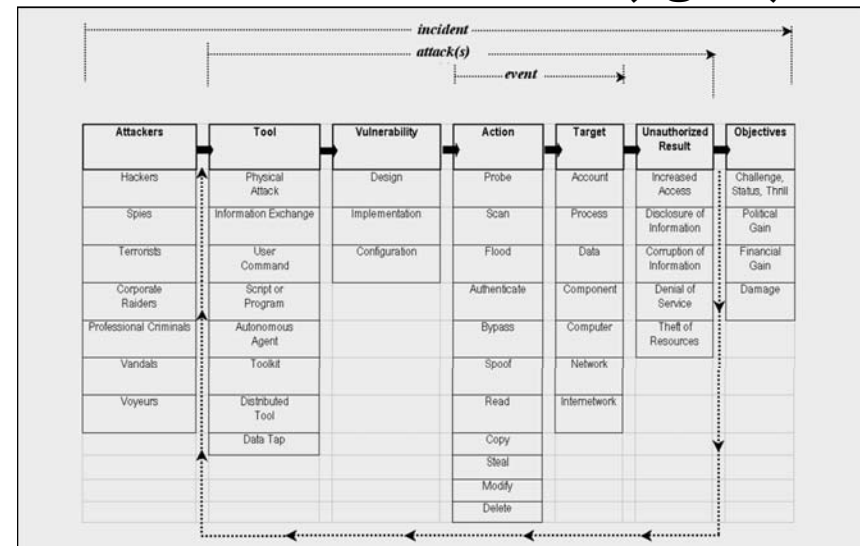


Attackers

- Wide range of attributes
- Subject of later chapter (6)



The Model as a Whole (again)



DISCUSSION