



Taxonomy of Computer Security Breaches

CSH6 Chapter 8

“Using a Common Language
for Computer Security
Incident Information”

John D. Howard

1

Copyright ©2014 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

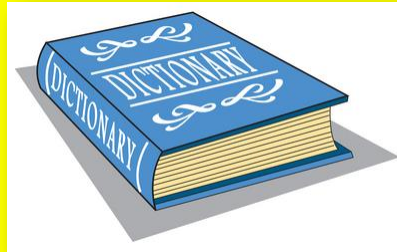
CSH6 Chapter 8:
“Using a Common Language for
Computer Security Incident Information”

2

Copyright ©2014 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



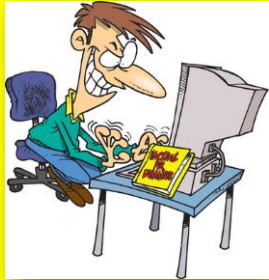
3

Copyright © 2014 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

5

Copyright © 2014 M. E. Kabay. All rights reserved.

The Model as a Whole

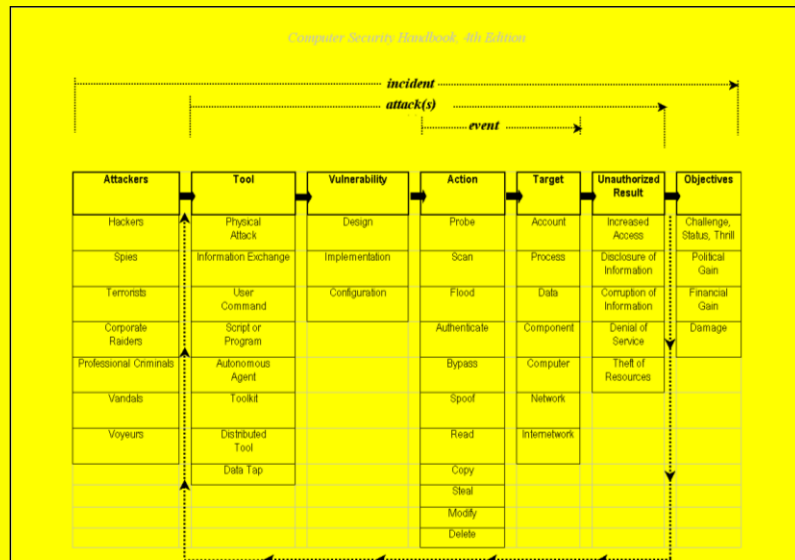


Figure 3.5 Computer and Network Incident Information Taxonomy

6

Actions

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

Action
Probe
Scan
Flood
Authenticate
Bypass
Spoof
Read
Copy
Steal
Modify
Delete

7

Copyright © 2014 M. E. Kabay. All rights reserved.

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

Target
Account
Process
Data
Component
Computer
Network
Internetwork

8

Copyright © 2014 M. E. Kabay. All rights reserved.

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

The diagram shows a table with two columns: 'Action' and 'Target'. A dashed arrow labeled 'event' points from the left to the table. An arrow points from the 'Action' column to the 'Target' column. The table contains the following data:

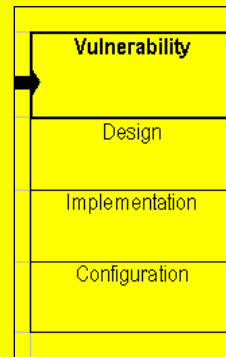
Action	Target
Probe	Account
Scan	Process
Flood	Data
Authenticate	Component
Bypass	Computer
Spoof	Network
Read	Internetwork
Copy	
Steal	
Modify	
Delete	

9

Copyright © 2014 M. E. Kabay. All rights reserved.

Vulnerability

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



10

Copyright © 2014 M. E. Kabay. All rights reserved.

The screenshot shows the NVD website interface. At the top, it is sponsored by DHS National Cyber Security Division/US-CERT and NIST. The main heading is "National Vulnerability Database" with the subtitle "automating vulnerability management, security measurement, and compliance checking". Navigation links include Vulnerabilities, Checklists, 800-53/800-53A, Product Dictionary, and Impact Metrics. A search section titled "Search CVE and CCE Vulnerability Database (Advanced Search)" features a keyword search box and radio buttons for "Search All", "Search Last 3 Months", and "Search Last 3 Years". Below this, there are checkboxes for "Software Flaws (CVE)", "Misconfigurations (CCE), under development", "US-CERT Technical Alerts", "US-CERT Vulnerability Notes", and "OVAL Queries". A red banner states "NVD now maps to CWE! See NVD CWE for more details." On the left, a "Resource Status" sidebar lists counts for CVE Vulnerabilities (57721), Checklists (223), US-CERT Alerts (248), US-CERT Vuln. Notes (2746), OVAL Queries (8140), and CPE Names (77373). It also shows the last update date as Mon Sep 02 13:28:42 EDT 2013 and a CVE Publication rate of 11.8. The footer includes the number "11" and a copyright notice for 2014 M. E. Kabay.

The slide is titled "Tool" in a large, bold, red font. It defines a tool as a "Means of exploiting a vulnerability" and lists several characteristics: widely available on the Internet, exchanged at hacker meetings, discussed and demonstrated at black-hat and gray-hat conferences, and many exploits usable by script kiddies and other poorly-trained hackers. A checklist includes 2600, L0pht (defunct), DEFCON – Las Vegas, and HACTIC – Netherlands. On the right, a vertical stack of boxes lists various tool types: Physical Attack, Information Exchange, User Command, Script or Program, Autonomous Agent, Toolkit, Distributed Tool, and Data Tap. The slide footer includes the number "12" and a copyright notice for 2014 M. E. Kabay.

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

Unauthorized Result
Increased Access
Disclosure of Information
Corruption of Information
Denial of Service
Theft of Resources

13

Copyright © 2014 M. E. Kabay. All rights reserved.


Objectives

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

Objectives
Challenge, Status, Thrill
Political Gain
Financial Gain
Damage

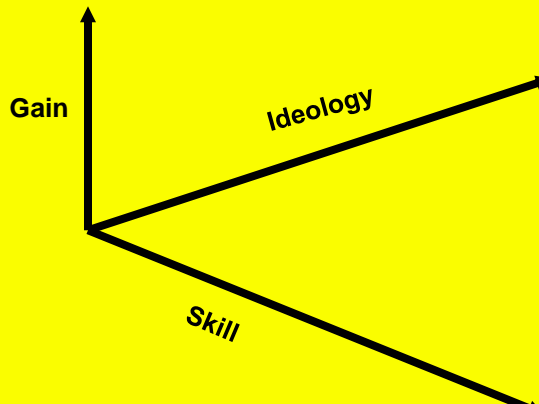
14

Copyright © 2014 M. E. Kabay. All rights reserved.



Attackers

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



Attackers

Hackers

Spies

Terrorists


Corporate Raiders

Professional Criminals


Vandals

Voyeurs

15 Copyright © 2014 M. E. Kabay. All rights reserved.



The Model as a Whole (again)



Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge, Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

16 Copyright © 2014 M. E. Kabay. All rights reserved.



**Now go and
study**