Cyber Investigation

CSH5 Chapter 55

Peter R. Stephenson

Copyright© 2013M. E. Kabay. All rights reserved.

Topics

- Introduction
- End-to-End Digital Investigation
- Applying Framework & EEDI
- Using EEDI & Framework
- Motive, Means, & Opportunity: Profiling Attackers
- Some Useful Tools
- Concluding Remarks

Copyright© 2013M. E. Kabay. All rights reserved.

INTRODUCTION

- Cyber Investigation Evolves
- Defining Cyber Investigation
- Distinguishing Between Cyber Forensics & Cyber Investigation
- DFRWS Framework Classes

Copyright© 2013M. E. Kabay. All rights reserved.

Cyber Investigation Evolves

- *Cyber investigation* aka *digital investigation*
- Early phases (before 2000) used term as equivalent to *computer forensics*
  - "The investigation of a computer system believed to be involved in cybercrime." – *Computer Desktop Encyclopedia*
  - But cyber investigation now distinct discipline, not just a set of techniques
  - American Academy of Forensic Science recognizes forensic computer-related crime investigator

Copyright© 2013M. E. Kabay. All rights reserved.

A Note on Etymology (added by Kabay)

fo·ren·sic [fə rénssik, fə rénzik] adjective

1. crime-solving: relating to application of science to decide questions arising from crime or litigation; forensic evidence
2. of debating: relating to debate & formal argumentation; forensic oratory

[Mid-17th century. < Latin forensis "of legal proceedings" < forum "forum" (as a place for discussion)]

Microsoft® Encarta® 2008. © 1993-2007 Microsoft Corporation. All rights reserved.

Copyright© 2013M. E. Kabay. All rights reserved.

Defining Cyber Investigation (1)

- Rogers, Brinson & Robinson establish *cyber forensics* as an *ontology* [on tólləjee] (plural on·tol·o·gies). noun
  - 1. study of existence: most general branch of metaphysics, concerned with nature of being
  - 2. theory of existence: a particular theory of being

[Early 18th century. < modern Latin, "study of being" < Greek ont- "being" (see onto-)]

Microsoft® Encarta® 2008. © 1993-2007 Microsoft Corporation. All rights reserved.

- Stephenson's *ontology* focuses on defining unique *aspects* of computer-related crime that can be studied

Copyright© 2013M. E. Kabay. All rights reserved.

Copyright © 2013 M. E. Kabay *All rights reserved.*

Defining Cyber Investigation (2)

- Cyber investigation relies on *taxonomy* (tax·on·o·my) [tak sónnəmee] (plural tax·on·o·mies) noun
  1. grouping of organisms: science of classifying plants, animals, & microorganisms into increasingly broader categories based on shared features. Traditionally, organisms were grouped by physical resemblances, but in recent times other criteria such as genetic matching have also been used.
  2. principles of classification: practice or principles of classification
  3. study of classification: study of rules & practice of classifying living organisms

[Early 19th century. < French taxonomie < Greek taxis (see taxis)]

Microsoft® Encarta® 2008. © 1993-2007 Microsoft Corporation. All rights reserved.

Copyright© 2013M. E. Kabay. All rights reserved.

Rogers' Taxonomy (1)

- Two major classes
  - Profession – structure of human endeavors
  - Technology – subjects of investigation
- Benefits
  - Supports understanding of concepts
  - Each additional sub-category supports more detail in analysis
  - Framework encourages thorough attention to details
  - Can serve as a checklist to avoid overlooking evidence
  - Supports analysis of cyber crime

Copyright© 2013M. E. Kabay. All rights reserved.

Rogers' Taxonomy (2):

Profession	Law	Enforcement	Evidence	Technology	Software	Analysis tools	Proprietary
			Collection/Analysis				Open-source tools
		Courts	Laws			Operating systems	Proprietary OS
			People				Open-source OS
	Academia	Research	Discipline definition			File systems	Windows
			Problem solving				UNIX/Linux
		Education	Contributions				Mac
			Professional outcome		Hardware	Large-scale digital devices	Clusters
	Military	Offensive	Passive				Grids
			Active			Small-scale digital devices	Cell phones
		Defensive	Proactive				PDAs
			Reactive				Solid-state drive OS
	Private sector	Industry	System admins			Computers	Desktops
			Legal contact				Laptops
		Consulting	Data recovery				Servers
			Forensic analysis				Tablets
			Expert witness consultant			Storage devices	Thumb drives
							Digital music players
							External music players
							External hard drives
						Obscure devices	Gaming devices
							Recording devices

Exhibit 55.1 (revised)

Distinguishing Between Cyber Forensics & Cyber Investigation

Clarification:

"Cyber *investigation* uses tools of cyber *forensics* as part of investigative procedures."

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Framework Classes

- *D*igital *F*orensics *R*esearch *W*ork*S*hop (2001)
- Framework for digital investigation
- Supports *end-to-end digital investigation* (EEDI)
- Each *class* comprises *elements*

EXHIBIT 55.2 DFRWS Digital Investigation Framework

Identification	Preservation	Collection	Examination	Analysis	Presentation
Event/Crime detection	Case management	Preservation	Preservation	Preservation	Documentation
Resolve signature	Imaging technologies	Approved methods	Traceability	Traceability	Expert testimony
Profile detection	Chain of custody	Approved software	Validation techniques	Statistical	Clarification
Anomalous detection	Time synchronization	Approved hardware	Filtering techniques	Protocols	Mission impact statement
Complaints		Legal authority	Pattern matching	Data mining	Recommended countermeasure
System monitoring		Lossless compression	Hidden data discovery	Timeline	Statistical interpretation
Audit analysis		Sampling	Hidden data extraction	Link	
		Data reduction		Spatial	
		Recovery techniques			

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Class: Identification

- How investigator is notified of potential incident
  - ~half of reports of possible security breaches turn out not to be crimes
- Framework classes in Identification
  - Event/crime detection: direct evidence (e.g., discovery of unauthorized access)
  - Resolve signature: intrusion detection/prevention systems, gateway security devices using pattern recognition
  - Profile detection: heuristic pattern recognition; attack scenarios, attack profiles
  - Anomalous detection: deviation from observed norms
  - Complaints: person reports event or results of event
  - System monitoring: situational awareness processes
  - Audit analysis: analysis of log files

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Class: Preservation

- Management of evidence ensuring integrity
- Case mgmt: notes, process controls, quality controls, procedural issues
- Imaging tech: making bit-for-bit image copies of evidence
- Chain of custody: preventing unauthorized access to & modification of evidence – preservers evidentiary value
- Time synchronization (normalization):
  - Ensuring that all time records use a common base time
  - No evidence modified
  - Determine offsets from a baseline (e.g., "- 0:00:07.6 GMT-5" for 7.6 seconds behind GMT-5)

13

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Class: Collection (1)

- Approved methods:
  - General acceptance by courts
  - E.g., qualifying under *Daubert* rule for admission of technical information – see CSH5 Ch 73
  - Or qualified under current case law
- Approved software: source code identical to that of tool that has qualified in courts (see above)
- Approved hardware: same principles as above
- Legal authority: policy (e.g., for owner of equipment), subpoena, warrant
- Lossless compression: provable fidelity

14

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Class: Collection (2)

- Sampling: demonstrated validity & safety for data
- Data reduction:
  - Valid, repeatable, provable results
  - Applied only to *copies* of evidence
- Recovery techniques
  - Extraction of useful data from data repositories
  - Comply with all court-permitted techniques
  - Forensic investigators must keep up to date with current case law

15

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Class: Examination (1)

- Traceability or *chain of evidence*
  - Clear documentation of reasoning linking *evidence to other evidence* (not *conclusions*)
  - Traceability & continuity of chain of evidence crucial to credibility of conclusions
  - Distinct from chain of custody!
- Validation techniques
  - Corroboration
  - May involve demonstration of internal consistency
  - Resistance to claims that evidence has been modified or fabricated

16

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Class: Examination (2)

- Filtering techniques
  - Sometimes source filtering (e.g., IDS) eliminates some data in stream
    - ✓Must supply courts with evidence of techniques used
    - ✓Demonstrate validity of remaining records
  - Also refers to extraction of relevant data types (e.g., images) from data
    - ✓May include comparison using hashes
    - ✓All such tools & techniques must be *understood* by investigator / examiner
    - ✓Understanding includes clear grasp of appropriate usage & a reasonable grasp of underlying principles (see Daubert Rule)

17

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS Class: Examination (3)

- Pattern matching
  - Finding potential events by matching *signatures* & other patterns
  - E.g., Intrusion-detection & anti-malware systems
- Hidden data discovery
  - Deleted but recoverable
  - Stored outside a file system's control (e.g., slack space)
  - Encryption
  - Steganography
- Hidden data extraction
  - Getting reliable data from sources described above

18

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS: Analysis

- "Fusion, correlation & assimilation of material for reasoned conclusions."
- Tying together evidence into coherent & probably correct scenario of events
- Ideally use accepted standards for processes of deduction & induction
  - Deduction: reaching a conclusion by applying rules of logic
  - Induction: forming a generalization based on observed evidence

19

Copyright© 2013M. E. Kabay. All rights reserved.

DFRWS: Presentation

- Reporting facts with organization, clarity, conciseness, & objectivity
  - Organization: using a comprehensible structure
  - Clarity: unambiguous, easily understood communication
  - Conciseness: using fewest words possible to supply necessary information
  - Objectivity: free from bias, not trying to convince anyone of a particular interpretation
- See CSH5 Ch 73 for recommendations on being an expert witness in court

20

Copyright© 2013M. E. Kabay. All rights reserved.

END-TO-END DIGITAL INVESTIGATION

1. Collecting Evidence
2. Analysis of Individual Events
3. Preliminary Correlation
4. Event Normalizing
5. Event Deconfliction
6. Second-Level Correlation
7. Timeline Analysis
8. Chain of Evidence Construction
9. Corroboration

21

Copyright© 2013M. E. Kabay. All rights reserved.

Collecting Evidence

- Approved tools & techniques
- Trained technicians
- Time sensitive
- *Incidents* must be considered in context of prior, concurrent & following *events*
  - Events are most granular element of incident
  - Incidents are collection of events that lead or could lead to a compromise
  - Incident becomes a *crime* when laws are broken
- Critical data collection includes
  - Images of affected computers
  - Logs of intermediate devices (esp. Internet)
  - Logs of affected computers
  - Logs & data from intrusion detection systems, firewalls etc.

22

Copyright© 2013M. E. Kabay. All rights reserved.

Analysis of Individual Events

- Events may leave records in multiple places
- Analysis assesses value of events to investigation
- Tie events into each other
- Aim to understand incident
  - Put events into coherent narrative

23

Copyright© 2013M. E. Kabay. All rights reserved.

Preliminary Correlation

- Correlation distinguishes among
  - Evidence that stands alone (unique events)
  - Evidence recorded in different ways & located in different places
  - Evidence that supports other information located elsewhere
- Corroboration supports formulation of *chain of evidence*
  - Consistent description of incident
  - Time sequences are called *timelines*
  - *Causal sequences* impute causes & effects

24

Copyright© 2013M. E. Kabay. All rights reserved.

Event Normalizing

- Combine evidentiary data from multiple sources
- Eliminate duplications to ensure each unique event is correctly represented once in timeline & causal sequence

Copyright© 2013M. E. Kabay. All rights reserved.

Event Deconfliction

- Some events have multiple repetitions of identical or near-identical steps
  - E.g., denial-of-service attacks may have 1000s of similar or identical packets flooding perimeter
  - These may be defined as *subevents*
- If reasonable, may define multiple subevents
  - ✓e.g., probes
  - that occur in a defined time period
    - ✓e.g., 48 seconds
  - as a single event
    - ✓e.g., "Denial-of-service"

Copyright© 2013M. E. Kabay. All rights reserved.

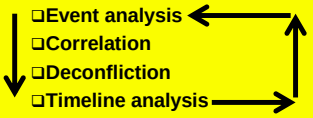
Second-Level Correlation

- Normalization & deconfliction should support creation of a coherent picture of events
- Second-level correlation of remaining data establishes a basis for building chains of evidence

Copyright© 2013M. E. Kabay. All rights reserved.

Timeline Analysis

- Use normalized, deconflicted data to create a sequence (timeline) of events
- Expect to update constantly
- Iterative process
  - Event analysis
  - Correlation
  - Deconfliction
  - Timeline analysis



Copyright© 2013M. E. Kabay. All rights reserved.

Chain of Evidence Construction

- Ideally
  - Each link in chain supported by evidence
  - Leads to next link
- In reality
  - Often gaps in chain
  - Must *infer* links
    - ✓Not evidence: a *lead*
    - ✓May point to legitimate evidence
  - May also *corroborate* missing or dubious link
    - ✓If all corroboration points to same link, may be acceptable

Copyright© 2013M. E. Kabay. All rights reserved.

Corroboration

- Match every element of chain of evidence
  - With other, independent evidence
  - Using correlated & uncorrelated data
- Best evidence
  - Developed using digital methods
  - Corroborated using traditional investigative methods
- Final evidence chain
  - Digital & traditional evidence
- Similar process in *investigation* vs *postmortem analysis*

Copyright© 2013M. E. Kabay. All rights reserved.

APPLYING THE FRAMEWORK & EEDI

- Overview
- Supporting EEDI Process
- Investigative Narrative
- Intrusion Process
- Describing Attacks
- Strategic Campaigns

Copyright© 2013M. E. Kabay. All rights reserved.

Overview

- Evidence management is paramount
- DFRWS Framework & EEDI
  - Help manage evidence
  - Not substitute for good investigation
- Incident may be crime – or not
  - Even if crime, might not be prosecuted
  - E.g., corporation may decide not to pursue civil complaint

Copyright© 2013M. E. Kabay. All rights reserved.

Supporting EEDI Process

- Traditional investigators often resist process
- Prof Stephenson's research finds practice conforms to his recommendations
- Thus DFRWS Framework & EEDI can serve traditional investigators entering world of cyber investigation
- Provide guidance on sequence of actions in investigation

Copyright© 2013M. E. Kabay. All rights reserved.

Investigative Narrative

- Investigator's detailed notes
- EEDI supports construction of investigation using framework(s)
- DFRWS Framework helps focus attention on all elements of situation
- E.g., DFRWS Collection class refers to authorized/approved methods
  - Therefore must be careful to use accepted, standard software, hardware & methods
  - Basis is case law – acceptance by courts

Copyright© 2013M. E. Kabay. All rights reserved.

Intrusion Process

- Details of specific attacks vary – increasingly *blended*
- But in general, attacks include
  - *Information gathering*: research, locating IP addresses, superficial scans
  - *Footprinting*: scanning IP addresses for visible devices
  - *Enumerating*: probes/scans to document operating systems & other details of exposed systems
  - *Probing for weaknesses*: vulnerability scans or social-engineering attacks
  - *Penetration*: obtaining unauthorized access
  - *Backdoors, Trojans, rootkits*: payload deposited for immediate or later exploitation
  - *Cleanup*: wiping tools, altering logs, generally covering tracks

Copyright© 2013M. E. Kabay. All rights reserved.

Describing Attacks (1)

- Various attack taxonomies available
  - But no generally accepted language
- Howard's Taxonomy (CSH5 Ch 8)
  - Simple, concise
  - Good starting point

Copyright© 2013M. E. Kabay. All rights reserved.

Describing Attacks (2)

- *Description of attack*: events, targets, vulnerabilities
- *Type of attack*: exploit, denial-of-service, reconnaissance
- *Attack mechanism*: how accomplished
- *Correlations*: comparison with other attacks, current attacks
- *Evidence of active targeting*: generic or specific
- *Severity* = Target Criticality + Attack Lethality – System countermeasures – Network Countermeasures
  - Rough guesses
  - Usually lowest 1 to 5 highest
  - Heuristic purposes only – not analytical or rigorous

Copyright© 2013M. E. Kabay. All rights reserved.

Describing Attacks (3)

Informal template for early interviews

1. Nature of incident?
2. How to be sure there really was an incident?
3. What was/were entry point(s) to system?
4. What kind of evidence are we looking for in this context?
5. What monitoring systems may have collected evidence?
6. What legal issues are relevant?
7. Who could have caused or allowed incident?
8. What security was in place at time?
9. What nontechnical (business) issues may have affected attack?
10. Who knew about attack – & when?

Copyright© 2013M. E. Kabay. All rights reserved.

Strategic Campaigns (1)

- Attack may be isolated
- But may be a tactic in a larger strategy; e.g.,
  - Spam
  - Identity theft
  - Hacktivism
  - Cyber war
- Differences between tactical attack & strategic campaign
  1. Single objective vs ongoing objectives
  2. Low-hanging fruit vs sustained efforts
  3. Trivial vs complicated targets & objectives

Copyright© 2013M. E. Kabay. All rights reserved.

Strategic Campaigns (2)

Distinct phases

1. Mapping & battle space preparation
2. Offensive & defensive planning
3. Initial execution
4. Probes & skirmishes
5. Adjustment & sustainment
6. Success & termination

Copyright© 2013M. E. Kabay. All rights reserved.

MOTIVE, MEANS, & OPPORTUNITY: PROFILING ATTACKERS (1)

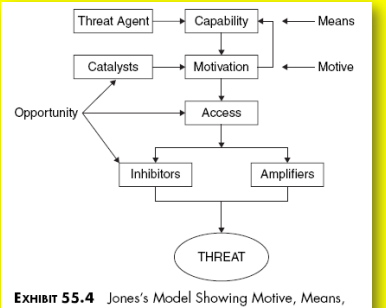


Exhibit 55.4 Jones's Model Showing Motive, Means, and Opportunity

Copyright© 2013M. E. Kabay. All rights reserved.

MOTIVE, MEANS, & OPPORTUNITY: PROFILING ATTACKERS (2)

Threat agents deliver a threat

- What are benefits of attack? (motive)
- Does agent have capability for attack? (means)
  - Access
  - Inhibitors vs amplifiers affect planning
- When is best time to attack? (opportunity)
  - Catalysts are variable factors that affect decision

Copyright© 2013M. E. Kabay. All rights reserved.

Motive (1)

- Understanding motive may help
  - Understand/analyze attack
  - Narrow down field of possible attackers
  - Identical attacks may have different motives
- Outcomes may differ significantly
  - Seeking revenge: embarrass victim
  - Seeking profit: extort money from victim
- Groups may behave differently from individuals

43

Copyright© 2013M. E. Kabay. All rights reserved.

Motive (2)

Adversarial matrix can help refine picture of motives

- States
  - Theft of intellectual property
  - Disruption
- Organized crime and terrorists
  - Money laundering
  - Theft of trade secrets for resale
  - Disruption
- Competitors
  - Competitive advantage
- Cyber mercenaries
  - Personal gain
- Gangs, new-age gangs
  - Financial gain
- Lone hackers and hacker "clubs"
  - Peer respect and power
  - Occasionally knowledge
- Disgruntled employee
  - Revenge
  - Personal gain

EXHIBIT 55.5 Types of Threat Agents and Their Motivations

44

Copyright© 2013M. E. Kabay. All rights reserved.

Motive (3)

Jones' motivation taxonomy:

- Political
- Secular
- Crime
- Personal gain
- Revenge
- Financial
- Knowledge / information

45

Copyright© 2013M. E. Kabay. All rights reserved.

Means (1)

- Tools & techniques used in attack
- Relate means to skill of attacker
  - Potential divergence between sophistication of attack tools & competence of attacker
  - Script-kiddies classic example
- More productive to exclude suspects who cannot be attacker

46

Copyright© 2013M. E. Kabay. All rights reserved.

Means (2)

EXHIBIT 55.6 Adversarial Matrix Behavioral Characteristics

Category of Offenders	Motivation	Personal Characteristics	Potential Weaknesses
		Crackers	
Groups	Intellectual challenge; peer group fun; in support of a cause	Highly intelligent individuals, counterculture orientation	Do not consider offenses crimes, talk freely about actions
Individuals	Intellectual challenge; problem solving; power; money; in support of a cause	Moderately to highly intelligent	May keep notes and other documents of actions
		Criminals	
Espionage	Money and a chance to attact the system	May be crackers operating in groups or as individuals	Become greedy for more information and then become careless
Fraud/Abuse	Money or other personal gain; power	Same personal characteristics as other fraud offenders	Become greedy and make mistakes
		Vandals	
Strangers	Intellectual challenge; power; money	Same characteristics as crackers	May become too brazen and make mistakes
Users	Revenge against organization; problem solving; money	Usually have some computer expertise	May leave audit trail in computer logs

47

Copyright© 2013M. E. Kabay. All rights reserved.

Means (3)

EXHIBIT 55.8 FBI Adversarial Matrix Resource Characteristics

Category of Offenders	Training Skills	Minimum Equipment Needed	Support Structure
		Crackers	
Groups	High level of informal training	Basic computer equipment with modem	Peer group support
Individuals	Expertise gained through experience	Basic computer equipment with modem	BBS, information exchanges
		Criminals	
Espionage	Various level of expertise	Basic computer equipment with modem, in some cases, uses more sophisticated devices	Support may come from sponsoring intelligence agency
Fraud/Abuse	Some programming experience	Computer with modem or access to target computer	Peer group support, possible organized crime enterprise
		Vandals	
Strangers	Range from basis to highly skilled	Basic computer equipment with modem	Peer group support
Users	Some computer expertise, knowledge of programming ranges from basic to advanced	Access to targeted computer	None

48

Opportunity

- Opportunity helps determine if suspect is credible perpetrator
- Includes knowledge of victim system
- Insiders or confederates of insiders should be examined
- External groups may be involved
  - E.g., Anonymous or LulzSec

Copyright© 2013M. E. Kabay. All rights reserved.

SOME USEFUL TOOLS

- The Usual Toolkit
- Link Analysis
- Attack-Tree Analysis
- Modeling
- Statistical Analysis

Copyright© 2013M. E. Kabay. All rights reserved.

The Usual Toolkit

- Computer forensic imaging and analysis
- Network forensic/log aggregation and analysis
- Malware discovery
- Media imaging (without analysis)
- Network discovery
- Remote (over-the-network) computer forensic analysis and imaging

CSH5 p 55.20

- Well known & accepted
- See product evaluations; e.g., in *SC Magazine*
  - May 2011 edition in particular
  - http://www.scmagazine.com/lets-go-analyze-something/article/200541/ or http://tinyurl.com/6unu4ab

Copyright© 2013M. E. Kabay. All rights reserved.

Link Analysis (1)

- Link analysis immensely useful
  - Analyze large data sets
  - Find non-obvious relationships
  - Applied to fraud, drugs, terrorism, organized crime
- Core theory
  - Pairs of related items; e.g.,
    - ✓People/address
    - ✓Source/destination IP addresses
    - ✓Alias/realname
  - Pairs can lead to further linkage

Copyright© 2013M. E. Kabay. All rights reserved.

Link Analysis (2)

- Example: linking data about cyber attacks
  - Hacker alias / realname
  - Alias / group
  - Alias / attack
  - Group / attack
- Clusters
  - Group of entities bound more closely to each other by links than to surrounding entities
  - Cluster analysis simplifies link maps

Copyright© 2013M. E. Kabay. All rights reserved.

Link Analysis (3)

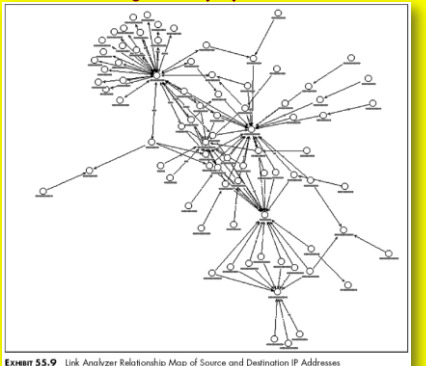


EXHIBIT 55.9 Link Analyzer Relationship Map of Source and Destination IP Addresses

Copyright© 2013M. E. Kabay. All rights reserved.

Link Analysis (4)

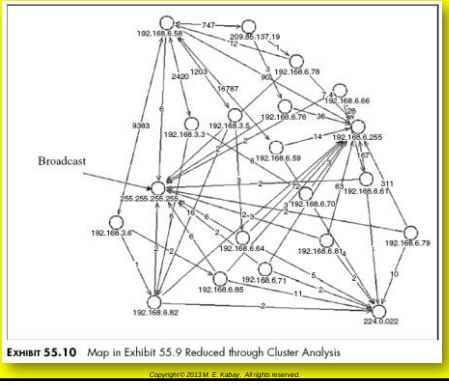


EXHIBIT 55.10 Map in Exhibit 55.9 Reduced through Cluster Analysis

Copyright© 2013 M. E. Kabay. All rights reserved.

Attack-Tree Analysis (1)

- Method for analyzing possible attack scenarios
  - Define goal as root
  - Hypothesize attack method as leaves
  - Look at probabilities of scenarios
  - Eliminate impossible sequences

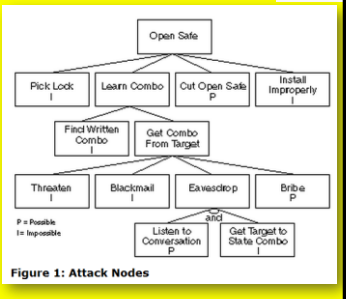


Figure 1: Attack Nodes

See Schneier, B. (1999). "Attack trees." *Dr Dobb's Journal.* < http://www.schneier.com/paper-attacktrees-ddj-ft.html >

Attack-Tree Analysis (2)

- Can assign any Boolean (logical) value to nodes; e.g.,
  - Easy/difficult
  - Legal/illegal
  - Special equipment req'd/not-req'd
- Even quantitative variables can be assigned; e.g., cost

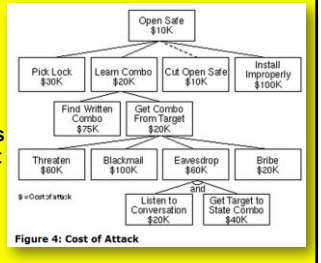
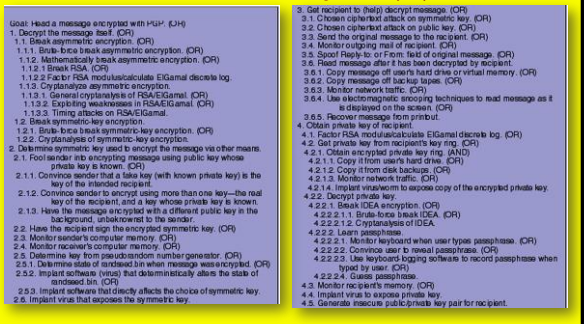


Figure 4: Cost of Attack

Copyright© 2013 M. E. Kabay. All rights reserved.

Attack-Tree Analysis (3)



Schneier's Figure 7: Attack Tree Against PGP

Copyright© 2013 M. E. Kabay. All rights reserved.

Attack-Tree Analysis (4)

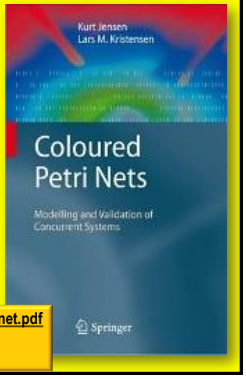
- "Attack trees provide a formal methodology for analyzing security of systems & subsystems. They provide a way to think about security, to capture & reuse expertise about security, & to respond to changes in security. Security is not a product -- it's a process. Attack trees form basis of understanding that process."

Schneier's Conclusion to Attack-Tree article

Modeling: CPN (1)

- Simulating attack behavior
- *Coloured Petri Nets* (CPN) useful language
  - Invented by K. Jensen at Aarhus University in Denmark
  - Transferred to Eindhoven University of Technology, The Netherlands (2010)
  - Good overview at < http://cs.au.dk/CPnets/ >
  - See brief paper by Jensen:

http://www.gsic.uva.es/wikis/yannis/images/c/c4/CP-net.pdf
or
http://tinyurl.com/8352ehy



Modeling: CPN (2)

- Graphical language -- constructing models of concurrent systems & analyzing properties
- Foundation of graphical notation & basic primitives for modeling concurrency, communication, & synchronization
- Standard ML -- definition data types, describing data manipulation, & creating compact models
- Typical application domains: communication protocols, data networks, distributed algorithms, embedded systems, business processes, workflows, manufacturing systems, & multi-agent systems
- Simulation-based performance analysis – delays, throughput, & queue lengths in system are investigated

http://cs.au.dk/CPnets/

61

Copyright© 2013 M. E. Kabay. All rights reserved.

Modeling: CPN (3)

http://www.gsic.uva.es/wikis/yannis/images/c/c4/CP-net.pdf
or
http://tinyurl.com/8352ehy

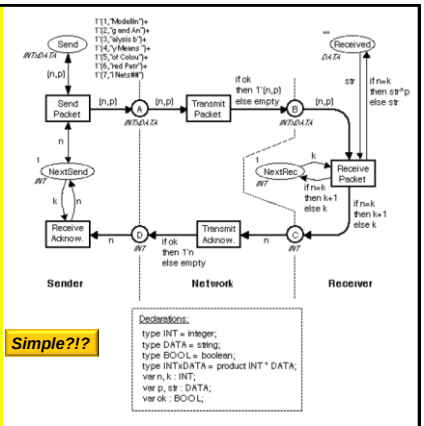


Fig. 1. Simple example of Coloured Petri Net

Simple?!?

62

Statistical Analysis

- Statistical methods & probability analysis of great value
- Look for anomalies – events with low probability if not related to crime & high probability if related
- Calculate probabilities of sequences of events; e.g., if faced with n events, each with probability p_i,
  - ✓Probability that all events would occur simultaneously or in sequence by chance alone: P{all} = $\Pi p_i \rightarrow p^n$ for identical p_i
  - ✓Probability that at none of events would occur simultaneously or in sequence by chance alone: P{none} = $\Pi(1 - p_i) \rightarrow (1 - p)^n$ for identical p_i
  - ✓Probability that at least one of events would occur simultaneously or in sequence by chance alone: P{>=1} = $1 - \Pi(1 - p_i) \rightarrow 1 - (1 - p)^n$ for identical p_i

63

Copyright© 2013 M. E. Kabay. All rights reserved.

DISCUSSION

64

Copyright© 2013 M. E. Kabay. All rights reserved.