Developing Standardized Processes for Incident Response: Opportunities and Challenges

DoD Cyber Crime Conference 2012

Jim Yuill, PhD
Advanced Technologies Laboratories
Lockheed Martin Corp.
james.yuill@lmco.com

Martin Nystrom
Computer Security Incident Response Team
Cisco Systems

1

- Copyright info:
  - (C) 2012 by the authors, under the terms of the Creative Commons Attribution-ShareAlike 2.0 license:
    - http://creativecommons.org/licenses/by-sa/2.0/deed.en
  - Some slides contain pictures and figures that are copyrighted by others. Copyright information is contained in the notes section of those slides. These figures are used in accordance with US copyright laws.

- Citation:
  - Yuill, J., M. Nystrom. "Developing Standardized Processes for Incident Response: Challenges and Opportunities", *Department of Defense Cyber Crime Conference 2012*, Atlanta, GA, January 2012.

Abstract

This talk presents principles and guidelines for developing standardized processes for incident response (IR). These principles can also be used for evaluating and using existing IR processes, e.g., those developed by others.

Developing standardized processes is one of the key steps for successful small organizations to grow into large organizations. However, everyone who has worked in a large organization knows how standardized processes often create obstacles and make work unpleasant.

In general, creating effective standardized processes is difficult. It is a job skill that requires understanding and experience. With IR, it is substantially more difficult due to the nature of investigation and the adversarial relationship with hackers.

This talk explores the underlying nature of standardized IR processes, and the challenges and opportunities for developing such processes.

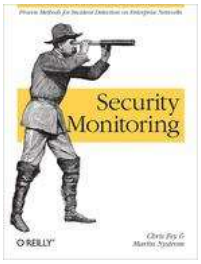
3

- From my experience, in any field (not just IR and computer security) efforts to create standardized processes often turn out badly, and standardized processes that work typically have significant problems
- IR deals with an intelligent adversary. This makes IR process development fundamentally more difficult than process development in other fields where relationships are cooperative or benign, e.g., software engineering
- We've pulled together a set of principles and guidelines for process development
- Process-development skill comes with experience
- Those who are relatively new to process work are likely to run into significant problems
- Relaying principles for creating effective standardized processes, with a focus on IR, and its unique requirements and challenges
- Also, relaying common mistakes and problems, to help to avoid them

Authors

Jim Yuill works at Lockheed Martin's Advanced Technologies Laboratory where he is a Senior Research Scientist. He has a PhD from North Carolina State University, with a thesis on designing deception-operations for computer security. Much of his research has been for the U.S. Department of Defense (OSD, USSTRATCOM, DARPA, and NSA), and he has presented at IEEE, ACM, and DoD conferences. (james.yuill@lmco.com)

Martin Nystrom works at Cisco Systems, where he's the manager for the CSIRT global architecture. He is a co-author of the O'Reilly book *Security Monitoring*.



4

Jim Yuill's process-development experience includes:

a) Applying the Army's battlefield-intelligence process to IR

b) Developing processes and techniques for IR data-management, based on jurisprudence research in evidence-collection

c) Research in computer-security development processes, including an extensive survey of industry and government processes, and developing criteria for evaluating process effectiveness

d) Deploying codified software-engineering processes at IBM, for operating system development, and

e) Teaching software-engineering at NCSU, in collaboration with IBM

Picture:

- Cover of a book published by O'Reilly. © 2009 by Fry and Nystrom. Reprinted by "fair use"

Disclaimer

- Presentation focuses on principles for IR process development
- The presentation is **NOT** intended to represent specific IR policies or processes where we work:
  - Lockheed Martin
  - Cisco Systems
- Jim co-developed this presentation before joining Lockheed

5

Presentation Outline

- **Chapter 1:** Introduction
- **Chapter 2:** Process types
- **Chapter 3:** Principles of process development
- **Chapter 4:** The IR investigation process
- **Chapter 5:** Creating Effective Processes

6

- Underlying principles of process development AND how they apply to IR
- The IR investigation process AND the challenges and opportunities for standardizing the IR investigation process

Chapter 1: Introduction

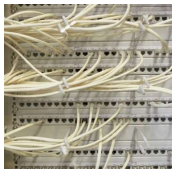
Chapter 1 Outline

- What is incident response (IR)?
- What are standardized processes, and why use them?
- Difficulties of developing effective processes
- Presentation objectives
  - Principles for developing standardized IR processes
  - Principles for evaluating and using existing processes

8

What Is Incident Response (IR)?

- Incident response: handling computer-security-related incidents
  - e.g., “attacks”, “security breaches”, etc.
- Response can be for known or suspected computer-security problems
  - For many IR teams, most of the reported incidents have benign causes (do not involve hacking)
- Two realms of IR:
  - IT systems
    - e.g., corporate IT systems



  - Software products
    - e.g., Windows
    - Concerned with vulnerability discoveries, exploits, and fixes
    - IR is part of vulnerability management

- This presentation focuses on IR for IT systems

9

Typical IR Activities

- Incident Handling
  - Investigation
  - Attack containment
  - System repair
  - Monitoring for recurrence

10

Figure from Microsoft clip art. © Microsoft, used by permission

Typical IR Activities (cont'd)

- Prosecution

- Incident reporting
- Incident management
  - e.g., tasking and tracking

11

Typical IR Activities (cont'd)

- IR leadership and support activities
  - Developing IR strategy and policies
  - Developing IR capabilities and systems (e.g., tools)
  - Analysis of protected networks and systems
  - Intelligence analysis
  - Coordination between the IR team and other groups

12

What Are Standardized Processes, and Why Use Them?

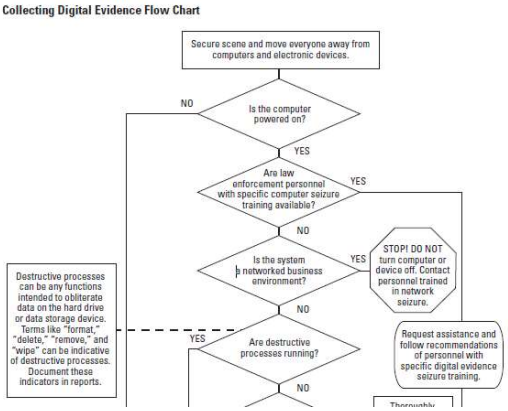
- All business units and workers have a "process"
- Processes can vary between:
  - being *ad hoc*,
  - or being well-defined and well-practiced
- Standardized processes are:
  - codified, and
  - made standard practice

13

- For the process principles presented here, most apply to any type of production, not just to IR
- Hereafter, when the context is clear, we'll refer to *standardized processes* as just *processes,* and *standardized IR processes* as just *IR processes*

IR Process Examples

- Processes for collecting digital evidence:
- Ad hoc: each investigator collects evidence however he thinks is best
- Well-defined standardized process: DOJ's recommended procedure



14

Figure from US Federal Government publication:

"Electronic Crime Scene Investigation: A Guide for First Responders", Second Edition

National Institute of Justice

http://www.nij.gov/nij/publications/ecrime-guide-219941/welcome.htm

It does not appear to be copyrighted.

Having a Process is Unavoidable

- It is not a matter of "***if***" you will have a process, but how good your process will be
- Also, how well is the process understood?
  - Just implicitly, without reflection and analysis, or
  - Well enough to standardize the process
    - To the extent it can be standardized

Why Use Standardized Processes?

- Standardization often needed for effective operations
  - e.g., rapid response
- Standardization needed for process improvement
  - Often, when a process is to be improved,
  - a new standardized process is developed

16

- Process understanding and improvement comes at a cost

The Need for Standardized Processes (cont'd)

- Essential for small organizations to grow into large organizations
- It's how organizations repeat their success
  - e.g., fast-food franchises, Toyota factories, IT consulting
- Inability to standardize processes limits growth

17

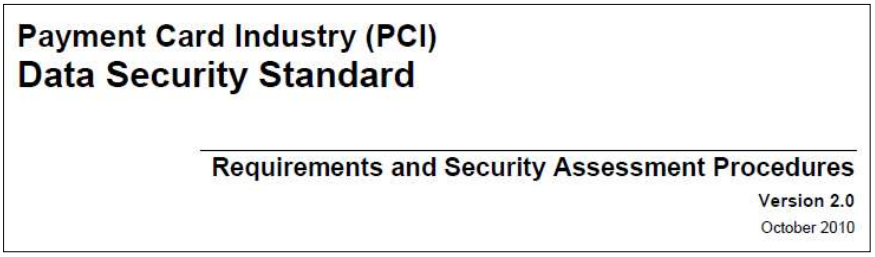
- The inability to standardize processes can prevent a small company from growing into a big company.
- Examples of standardization:
  - Franchise fast-food restaurants, such as McDonalds and Papa Johns, have created standard procedures for successfully running a small business
  - Toyota has factories in many countries, spread throughout the world
  - IBM's consulting services are based on standardized processes, e.g., for providing computer-security outsourcing

- Picture sources
  - http://commons.wikimedia.org/wiki/File:McDonald%27s_Tampa_1979_05_02.JPG
    - Stated copyright: "Wahkeenah grants anyone the right to use this work for any purpose, without any conditions,"
  - http://www.flickr.com/photos/avatarr8/3588954352/
    - Copyright: http://creativecommons.org/licenses/by/2.0/deed.en
    - Attribution: alex_and_stacy's Photostream (no real name given)
  - http://www.flickr.com/photos/alui0000/1982097127/
    - Copyright: http://creativecommons.org/licenses/by-sa/2.0/deed.en

- Attribution: Alfred Lui

The Need for Standardized Processes (cont'd)

- Can be needed due to external requirements, e.g.,
  - From laws (e.g., ISO 27002)
  - From business partners (e.g., PCI DSS)
  - To show due diligence (e.g., to avoid law suits)



18

Figure is from the cover of:
PCI DSS Requirements and Security Assessment Procedures, Version 2.0

Difficult to Develop Effective Standardized Processes

- "Process" is Hard to Do Well
- Most small companies do not become big companies
  - and many for this reason
- Everyone who works in a large organization has to deal with ineffective processes, to some extent
- A common theme in Dilbert comics

19

- Ineffective standardized processes can hamper or prevent growth

Photo:

- Source: http://www.dilbert.com/
- This image is from a comic strip, webcomic or from the cover or interior of a comic book. The copyright for this image is most likely owned by either the publisher of the comic or the writer(s) and/or artist(s) which produced the comic in question. It is believed that the use of low-resolution images of a single panel from a comic strip to illustrate the scene or storyline depicted qualifies as fair use under United States copyright law.

Difficult to Develop Effective Standardized Processes

- Employees tend to be leery of, and resistant to, standardized processes
  - People resist changing the way they do things
  - People don't like being told what to do
  - People want to use their own style and approach

20

- Ineffective standardized processes can hamper or prevent growth

Photo:

- http://commons.wikimedia.org/wiki/File:Ford_assembly_line_-_1913.jpg
  - "This media file is in the public domain in the United States. This applies to U.S. works where the copyright has expired, often because its first publication occurred prior to January 1, 1923."
  - Date: 1913

Presentation Objectives

- Provide principles and techniques for:
  - Developing your own standardized IR-processes
  - Evaluating and using standardized IR-processes created by others, e.g., published in books
- Understand some of the common causes of ineffective processes
- Understand why some IR processes are not amenable to standardization

21

Evaluating and Using IR Processes Created by Others

- Publicly available IR processes, e.g., in books
  - Evaluate those IR processes, for your own use
  - How well will the process work for you?
  - What modifications are needed, to use it on your system?
- IR processes used by business partners that have access to your internal network
  - Evaluate the business partner's IR processes, to assess their IR capabilities

22

What the Presentation Does **NOT** Cover

- **NOT** focusing on particular IR processes
  - Developing particular IR processes is a project itself
  - There are a number of books on specific IR processes

CHAPTER 2:

Types of Standardized Processes

Types of Standardized Processes

- There are many types of standardized processes
  - Not just cookbook-like procedures
- Some typical types of standardized processes:
  - Process frameworks
  - Procedures
  - Techniques
  - Methods
  - Process principles
  - etc.
- Examples follow…

Ad Hoc Processes: an Example

- The early days of software development are characterized by "hacking"
- Hacking is an *ad hoc* software development process
  - Tends to focus on programming, and neglect planning and design
- Synonyms for hacking
  - *cowboy coding:* name based on the image of a frontier life without rules
  - *chaos software development:* name based on typical outcome from hacking
- Hacking is similar to aviation's early days, when there were no rules

26

- Hacking here refers to software development, not compromising computer security

Picture sources:

- http://commons.wikimedia.org/wiki/File:Aerial_Acrobatics.JPG

This media file is in the public domain in the United States. This applies to U.S. works where the copyright has expired, often because its first publication occurred prior to January 1, 1923.

Original source: http://www.nytstore.com/ProdDetail.aspx?prodId=2801

- http://commons.wikimedia.org/wiki/File:Cattle_branding_(Grabill_1888).jpg

This media file is in the public domain in the United States. This applies to U.S. works where the copyright has expired, often because its first publication occurred prior to January 1, 1923.

Typical Problems from Ad Hoc Processes

- Ad hoc processes are the opposite of standardized processes
  - An ad hoc process is not defined nor documented
- Ad hoc processes may be OK for small operations, but
- They become increasingly problematic as an organization grows, e.g., as:
  - The volume of work increases
  - The complexity of work increases
  - The number of workers increases
  - Interactions among workers increases

27

Example from a company I did systems analysis for:

- It was an industrial service-company with about a dozen employees and 800 customers. In doing systems analysis I learned the company was experiencing a high number of errors in servicing customer accounts. I also learned that the company relied heavily on ad hoc processes, and they had done little to standardize operations. The company started in the owner's basement, and ad hoc processes were sufficient there, when the company was small. However, as the company grew, the ad hoc processes became increasingly problematic.

- A friend of mine works on the support team for an open-source operating system. This support team has done relatively little to standardize its processes. A major reason appears to be the open-source-development culture, which values personal autonomy and is accustomed to using ad hoc processes. My friend had described how these ad hoc processes make support work very unpredictable, and how that can burn-out employees and cause high turn-over.

Typical Problems from Ad Hoc Processes (cont'd)

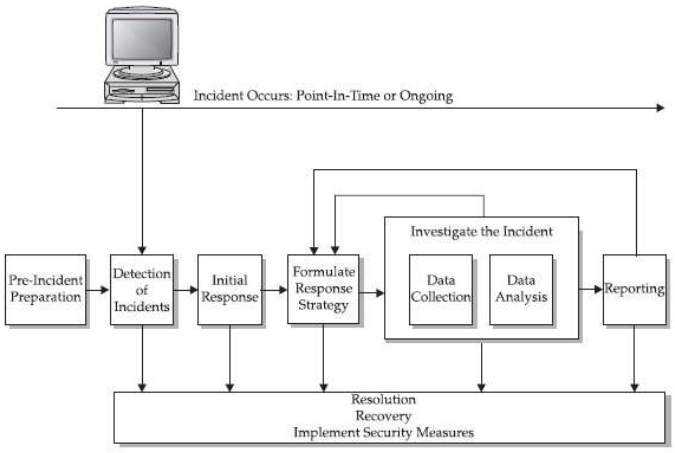
- Often, ad hoc processes are not sufficiently reliable
  - e.g., problems with quantity, quality, and schedules
- For employees, ad hoc processes can make work frustrating and overly-complex
- Ad hoc processes can make management difficult
  - e.g., in evaluating workers' progress, or
  - in evaluating a worker's productivity

28

- Quality problem: Ad hoc processes may not be sufficiently thorough
- Burn-out due to: work being unpredictable, e.g., don't know what you'll be expected to do next
- Management: if workers are not doing the same type of thing (e.g., each incident can be different), and they are not doing things in the same way, it can be hard for a manger to:
  - Evaluate a worker's progress (difficult to know how far along the worker is)
  - Evaluate a worker's productivity (difficult to know if the worker is fast or slow)

Example: IR Process Framework and Detailed Processes

- Figure: IR process framework, from IR book
- Book provides this overall framework, and also, detailed processes and techniques

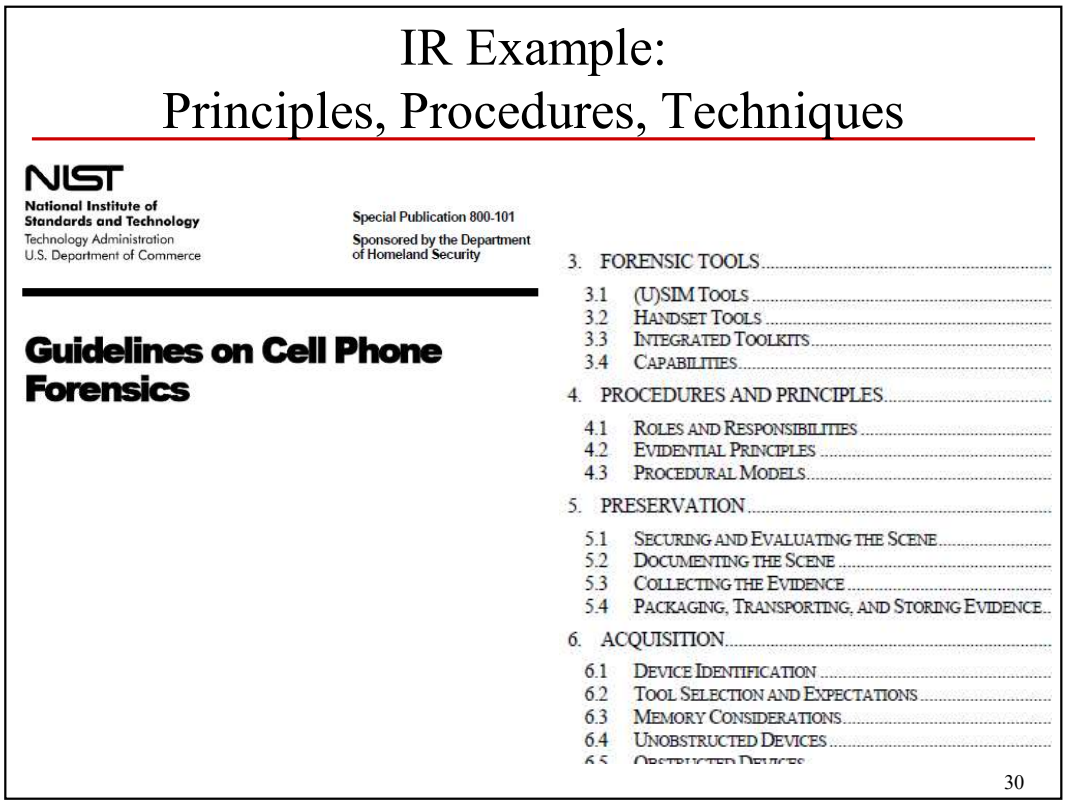


29

Figure from: *Incident Response: Investigating Computer Crime*, by Prosise and Mandia, (c) 2001 McGraw Hill

Used by fair-use.

IR Example: Principles, Procedures, Techniques



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-101
Sponsored by the Department of Homeland Security

Guidelines on Cell Phone Forensics

30

Figures: Guidelines on Cell Phone Forensics, by Jansen and Ayers, NIST publication, no copyright information available

Used by fair-use

Hacker Processes

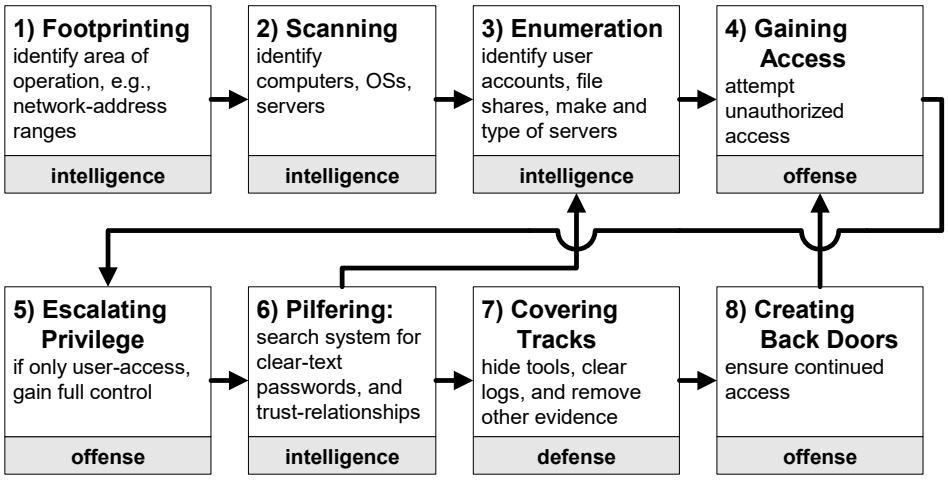
- ***Hacker***:
  - Someone who seeks to compromise computer security
  - (earlier reference was to software-development *hacking*)
- Principles for developing standardized processes
  - Can be useful for describing and understanding hackers' processes

31

- Earlier reference to hacking was to ad hoc programming.
- This reference to hackers is to those who intentionally compromise computer security.

Example: Hacking Process

- A model of the hacking process (adapted from *Hacking Exposed)*



32

This model is adapted from the book *Hacking Exposed : Network Security Secrets and Solutions*, by McClure, S., J. Scambray, and G. Kurtz., Osborne/McGraw-Hill, © 1999

Each of these hacking steps is described in a chapter in the book.

CHAPTER 3

Principles of Process Development:

Viewing Codified Processes as Models

33

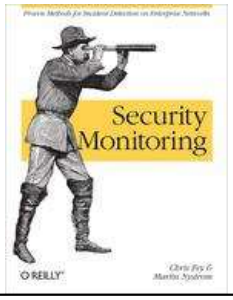
Chapter 3 Outline:

- Inherent limitations of published IR processes
- Understanding codified processes as models
- Practical applications of viewing processes as models
- Reading published IR processes critically

34

Challenges in Using Published IR Processes

- Process development often involves finding and using the best IR books and papers
  - To build on existing best-practices
- Since Cisco is a leader in networking, their IR books would be appealing:



35

Picture from: *Computer Incident Response and Product Security*, by Damir Rajnovic, © 2011 Cisco Systems, Inc

Used by fair-use.

Limitations in Using Cisco's Published IR Processes

- However, Cisco's IR environment is a-typical, in many ways
- Presumably (Jim's presumptions, not Martin's):
  - Cisco's network engineers have exceptionally high skill
  - Cisco has top-of-the line networking equipment
  - Cisco has a relatively huge budget for security and IR
- When using Cisco's IR processes in another organization:
  - Incompatibilities are very likely
  - The Cisco IR process will likely require modification

36

Challenges in Using Another Organization's IR Processes

- In general, IR processes from one organization are likely to have significant incompatibilities for use in another organization
- e.g., expect differences in IR processes for:
  - Cisco, banking, government agencies, military



37

Photos:

- Capitol

http://commons.wikimedia.org/wiki/File:US_capitol_building.jpg

This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.

Attribution: Raul654

- Cisco

http://commons.wikimedia.org/wiki/File:Ciscosystemsheadquarters.jpg

This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.

Attribution: Original uploader was Coolcaesar at en.wikipedia

- ATM:

http://commons.wikimedia.org/wiki/File:Fr%C3%BCher_Bankautomat_von_Nixdorf.jpg

This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.

Attribution: de:User:Stahlkocher

- Pentagon

http://commons.wikimedia.org/wiki/File:Pentagon_Aerial_on_September_11,_2002_by_Angela_Stafford,_U.S._Air_Force_%28DOD_020911-F-3968S-001%29_%28290165442%29.jpg

Attribution: David Shapinsky from Washington, D.C., United States

Understanding Codified Processes as Models

- Viewing codified processes as models
- Helpful in understanding:
  - Limitations of codified processes
  - How to develop new processes
  - How to adopt existing published processes
- Explained on the following slides…

38

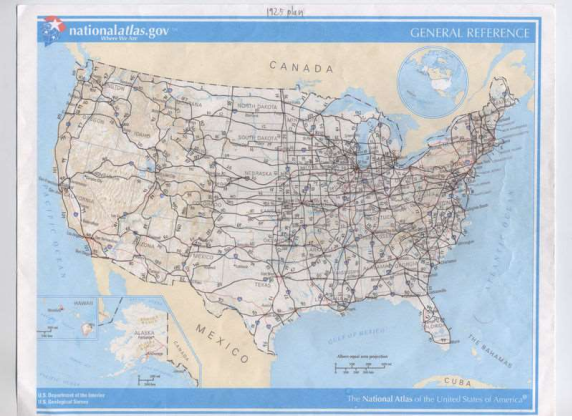
Codified Processes are Models

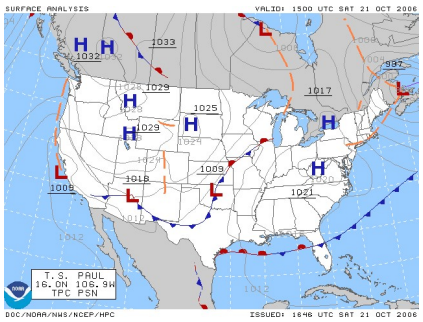
- A codified process is a **model** of how the process is actually carried-out in practice
- ***Model***: a simplified description of a highly complex thing or process
- A model must **omit information**
- Typically, a model is an **approximation**
- A model is always built to serve a particular **purpose (use)**
  - ***A model cannot be understood apart from its purpose***

39

Illustration of a Model

- A map is a model
- The map's purpose determines what it shows
  - e.g., a highway map vs. a weather map
- The purpose also determines what is omitted and the accuracy





40

- accuracy: how much approximation there is in the model

Pics are public domain:

http://commons.wikimedia.org/wiki/File:Surface_analysis.gif

http://commons.wikimedia.org/wiki/File:1925us.jpg

Purpose Includes Objectives & Context

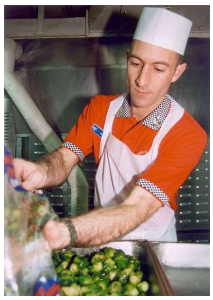
- A model's purpose includes both:
  - **Objectives** for using it
  - **Context** for using it
    - Who is using it—where, when and how?
- For a map: what it shows is also determined by the context for using it
  - Who is using the map:
    - Weather map for a meteorologist vs. TV news
    - A highway map for a trucker vs. a holiday traveler
  - Where the map is being used:
    - A map for use on a dashboard GPS vs. on a PC

41

Process Example: Cooking

- A recipe is a standardized process, and thus a model of cooking
- Different types of recipes are needed, depending on
  - Objectives: meal quality and quantity
  - Context: cook's skill-level, cooking facilities, etc.

Gourmet Chef



U.S. Navy Mess Hall Cook

Boy Scout

42

- Cooking instructions (e.g., recipes, cookbooks) are codified process
- The type of instruction (what is described, amount of detail, etc.) varies depending on purpose (including attributes listed above)
- Cooking is described quite differently when comparing:
  - A cookbook for professional chefs, a manual for military cooking, and a Boy Scout handbook
- Resources: time, quality of ingredients, cooking facilities

Sources:

- Campfire:

http://commons.wikimedia.org/wiki/File:Cooking_snags_over_campfire.jpg

Attribution: "Fir0002/Flagstaffotos"

- Chef:

http://commons.wikimedia.org/wiki/File:Chef_Lorenzo.jpg

Attribution: Jesus Guillermo Lorenzo

This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.

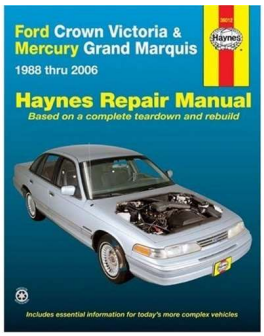
- Cook:

http://commons.wikimedia.org/wiki/File:US_Navy_020213-N-7741S-004_Midnight_food_preparation_aboard_JFK.jpg

As a work of the U.S. federal government, the image is in the public domain.

Process Example: Auto Repair

- Auto repair-manuals contain car-repair procedures
  - They are a model of car-repair
- Auto repair-manuals are different for different contexts:
  - Factory manuals: for professional mechanics at a car dealership
  - Haynes manuals: for amateur mechanics in their home garage



43

Auto-repair manuals written differently, depending on skill-level of intended audience

Pictures: Used by fair-use

- *Ford Crown Victoria & Mercury Marquis, 1988 THRU 2006*, Delmar Cengage Learning, 2008, © 2008

http://www.amazon.com/Crown-Victoria-Automotive-Repair-Manual/dp/1563926393

- CD image from: http://www.davegrahamautoliterature.com/shop/home.php, © 1997-2012 GearHead Old Car Books

Wide Variations in IR-Processes' Purposes

- Recall: a model's purpose includes both:
  - Objectives for using it
  - Context for using it
    - Who is using it—where, when and how?
- Developing codified IR processes can be challenging due to
  - Wide variations in IR objectives
  - Wide variations in IR contexts
- These variations occur:
  - Within an organization's network
  - Among different organization's networks
- Examples follow

44

Example: How IR Objectives Can Vary

- IR processes are very different for objectives of:
  - containment and repair vs. prosecution

- IR processes from law-enforcement and e-discovery
  - Likely to be excessive if only containment and repair are needed

45

Sources:

- http://commons.wikimedia.org/wiki/File:Detenido.JPG

Attribution: GatoDesing

This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported, 2.5 Generic, 2.0 Generic and 1.0 Generic license.

- http://commons.wikimedia.org/wiki/File:FEMA_-_34684_-_Residents_of_all_ages_help_protect_homes_from_flooding_with_sandbags_in_Arkansas.jpg

This image is a work of a Federal Emergency Management Agency employee, taken or made during the course of an employee's official duties. As works of the U.S. federal government, all FEMA images are in the public domain.

Example: How IR Objectives Can Vary (cont'd)

- IR processes are influenced by risk-management objectives:
  - e.g., determines how much certainty and thoroughness is required
- Risk-management objectives vary within a network
- e.g., IR processes are different for critical production servers than for workstations

46

Example: How IR Objectives Can Vary (cont'd)

- Differing risk-management objectives are primary cause of differences in IR processes for:
  - Cisco, banking, government agencies, military

47

Example: How IR Contexts Vary

- IR processes will vary, depending on the resources available:
  - Personnel, skill-levels, budgets, time available
  - IR tools and network-management resources
  - Security and monitoring resources, etc.

48

Example: How IR Contexts Vary

- Responders vary in skill-level
- IR processes for rookies vs. experienced responders

- Responders also vary in aptitude and native ability

49

Sources:

- http://www.flickr.com/photos/enigmachck/2591355896/sizes/m/in/photostream/

This file is licensed under the Creative Commons Attribution 2.0 Generic license.
Attribution: Bri Lehman

- http://www.flickr.com/photos/familymwr/5335454714/sizes/z/in/photostream/

This file is licensed under the Creative Commons Attribution 2.0 Generic license.
Attribution: familymwr
Photographer not specified.

Example: How IR Contexts Vary

- Networks vary in how they are built and used
  - Variation within an organization
  - Variation between organizations
- How a network is built and used influences the IR processes
- IR processes for a DMZ vs. a LAN with desktop workstations

50

Sources:

• Fence:

http://commons.wikimedia.org/wiki/File:Concertina_wire_on_the_FAA_airplane_station.jpg

Attribution: darinmarshall

Practical Application of Models: Developing New Processes

- When developing new standardized IR processes:
  - Need to **accurately** identify the IR process's purpose:
  - both its objectives and context
- IR objectives and contexts can vary widely within a large network
- Parts of the network my have different objectives and context than what the process-developer is familiar with
  - e.g., different risk-requirements, skill-levels
  - Easy to make wrong assumptions

51

Practical Application of Models: Using Published IR Processes

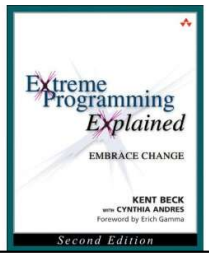
- Viewing standardized IR processes as models
  - is most useful when using a published IR process
  - e.g., from a book

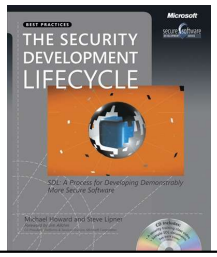
- For IR processes developed by someone else, it can be difficult to accurately know:
  - What their objectives and contexts were
  - How their objectives and contexts differ from yours

52

Personal-Experience Biases

- It's easy for process developers to be biased by their own experience
- It's easy for process developers to:
  - Wrongly assume a network's IR objectives and contexts are the same as those they have worked with
  - Not realize there are other IR objectives and contexts which are different
- This is a common problem in software engineering books





53

** Easy to make assumptions about purpose and context, without realizing it

Book: *Extreme Programming Explained: Embrace Change*, by Beck and Andres, Addison-Wesley Professional, © 2004

Used by fair-use

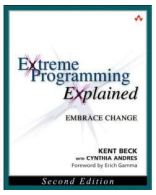
Book: *The Security Development Lifecycle*, by Howard and Lipner, (c) 2006 by Howard and Lipner

Used by fair-use

Skill-Level Biases

- Tendency to assume others are like us, e.g.,
  - Have similar skill-levels
  - Assume that processes which worked well for us should work well for others

- An example from two popular software-engineering books:
  - Authors report tremendous successes using their development processes
  - However, they are genius "super-programmers"
  - Some of their techniques are not well-suited for typical programmers



Skill-Level Biases (cont'd)

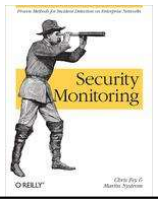
- For process development, wrong assumptions about users' skill can be ruinous
- An related example from teaching computer-science:
  - Student skill-levels vary widely among colleges
  - Teaching must be adjusted accordingly

Practical Application of Models: Approximation

- A codified process is a model:
  - It is a simplified description
  - Often, models are approximations of the real world
- Processes models might just cover typical cases,
  - and not all cases,

Approximation (cont'd)

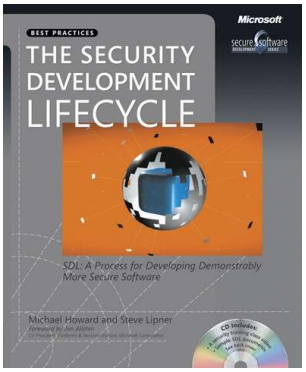
- Published processes often describe ideal processes,
  - and not those typically used in practice
- Martin's confession, from his security monitoring book:
  - "...the authors have a confession to make.
  - We rarely follow the details of our own advice.
  - Something always goes wrong, and we find ourselves speeding through the setup so that we can meet a deadline..."



57

Practical Application of Models: Contexts Change

- IR contexts (environments) change over time
  - e.g., technology, threats, vulnerabilities, assets, etc.
- If standardized IR processes are developed,
  - there must also be an on-going process for updating them



Number	Date	Title
SP 800-101	May 2007	Guidelines on Cell Phone Forensics SP800-101.pdf
SP 800-94	Feb 2007	Guide to Intrusion Detection and Prevention Systems (IDPS) SP800-94.pdf
SP 800-86	Aug 2006	Guide to Integrating Forensic Techniques into Incident Response SP800-86.pdf SP800-86-pdf.zip
SP 800-84	Sep 2006	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities SP800-84.pdf
SP 800-83	Nov 2005	Guide to Malware Incident Prevention and Handling

58

Table is from the beginning of NIST's list of its IR technical guides. Note how dated they are.

- Table:

http://csrc.nist.gov/publications/PubsTC.html#Incident%20Response

US Government web-site

Used under fair-use

Practical Application of Models: Omitting Info

- A codified process is a model
  - It is a simplified description
  - It necessarily omits information
- Typically, codified processes cannot, and should not, attempt to:
  - Specify everything that has to be done
  - Cover every possible case
- Omission is part of the nature of modeling
  - A model that omits stuff is not necessarily flawed
- Another reason to omit stuff:
  - Users have limited reading time

59

Reading Published Processes Critically

- Essential to read published-processes critically
- To figure-out how it applies to your network, objectives and context
- Expect that the process will need to be modified to work in your environment
  - Focus on understanding the underlying principles
- Expect that parts of the process will not be applicable to your environment

60

Reading Critically (cont'd)

- Typically, authors of published processes want as large of a following as possible
- Typically, process authors are not very clear about:
  - The specific objectives and contexts in which the process can be used
  - The process's limitations and weaknesses
- Typically, critical reading and investigation is needed to figure this out

61

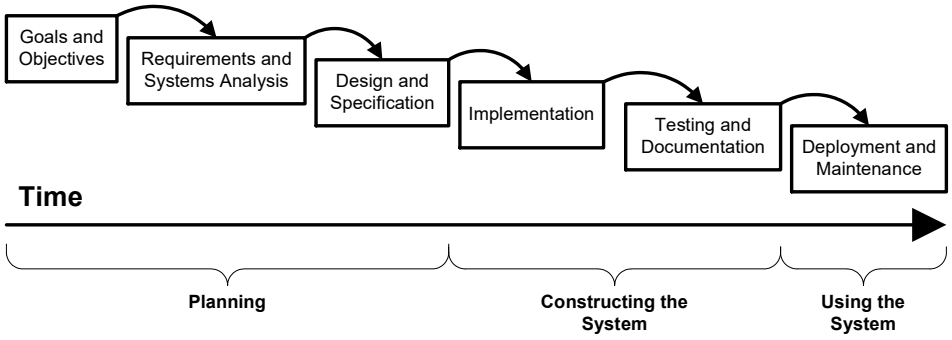
Reading Critically (cont'd)

- What is the author's background and experience?
  - Some investigation may be needed
  - He is probably writing from that perspective
  - How is it different than your environment?
- What is the author's motive in writing and publishing the process?
  - Company PR,
  - Consultant's advertising
  - Academic researcher
  - Government process-development
- How was the work funded?
- Are there plans to update the work?

62

Reading Critically (cont'd)

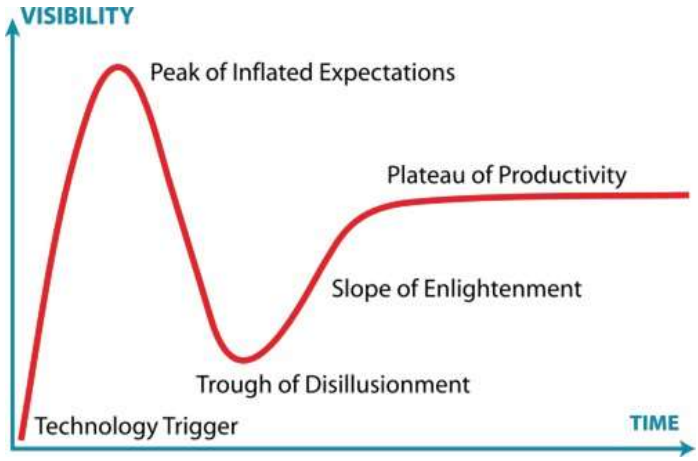
- A popular process is not necessarily sound
- Waterfall development-process example



63

Reading Critically (cont'd)

- The technology "hype-cycle" can also apply to processes



64

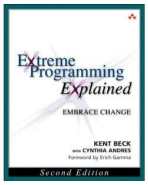
Picture source:

http://en.wikipedia.org/wiki/File:Gartner_Hype_Cycle.svg

Attribution: Jeremykemp at en.wikipedia

Reading Critically (cont'd)

- Process may not be actually used in practice, as they are described
  - e.g., describes an ideal case



- Extreme Programming (XP) is a set of 12 software development practices and techniques.
  - Most XP users do not use all 12 practices.
  - It appears that many enthusiasts use less than 6 to 8

65

Survey circa 2005: A Survey of Empirical Studies of Extreme Programming

Survey circa 2009: http://www.ambysoft.com/surveys/practices2009.html

Reading Critically (cont'd)

- Misleading and false info not uncommon
  - Fabricated data
  - Author promoting a process he hasn't actually used

CHAPTER 4:

The IR Investigation Process

Introduction:
The IR Investigation Process

- Much of IR is a process of investigation.
- Presenting a general model of investigation:
  - It describes how investigation works, in general
  - (From Dr. Schumm's jurisprudence research)
- It reveals limitations and opportunities for standardizing the investigation process

68

This section presents a general model of how the investigation process works

The purpose of the model is to show opportunities and limitations for standardizing the IR investigation process

Model is from: Schum, D. "Marshaling Thoughts and Evidence During Fact Investigation", South Texas Law Review, 40(2): 401-454, Summer 1999.

Hypotheses and Evidence

A conceptual model of investigation:

- The investigator creates hypotheses:
  - Possible explanations of the thing being investigated
- The investigator works with hypotheses and evidence:
  - He has evidence for which he is seeking hypotheses
  - He has hypotheses for which he is seeking additional evidence

69

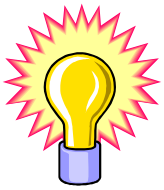
- Typically, the investigator has partial information about what happened
- He forms possible explanations of what happened, based on the evidence
- These explanations are hypotheses

Conceptual Model of Investigation (cont'd)

- At any point, the investigator can do one of two things:

1) Search for new evidence

2) Develop new hypotheses based upon the available evidence

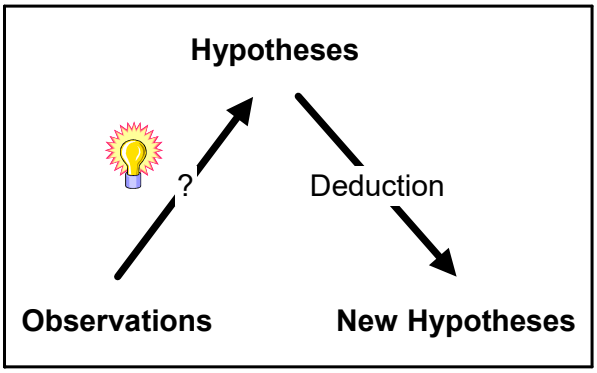


70

Figures from Microsoft clip art. © Microsoft, used by permission

The Process of Hypothesis Creation

- The investigator **creates** hypotheses
  - Based on observations (of evidence)
- The mental process of **creativity** is not understood
  - Limits proceduralization of hypothesis creation



71

- Observations are of evidence
  - The evidence itself is just data
  - Hypotheses put meaning to the data; they explain the data
- Creativity
  - Since we don't understand how creativity works in the brain, we cannot proceduralize that function itself.
  - However, there are things we can do to aid creativity.
- Deduction (skip this if not enough time)
  - Hypotheses explain what happened
  - Observations are just data
  - When deductions are based on observations, the deduction itself is a hypotheses

Uncertainty in Investigation

- Adversarial relationship with hackers
  - Uncertainty due to hackers' efforts to hide and deceive
- Uncertainty in human action
  - By nature, not entirely predictable
- The nature of evidence:
  - Temporary, so some may have vanished
  - Evidence can be overlooked
  - Uncertainties about known evidence

72

- Even when investigating someone who is not an adversary, there can be uncertainty due to free will
- Uncertainties regarding evidence itself, e.g., a witness's memory of what happened

- Figure:

http://commons.wikimedia.org/wiki/File:Fingerprint_%28PSF%29.png

This figure was donated to the Wikimedia Foundation and released into the public domain by Pearson Scott Foresman.

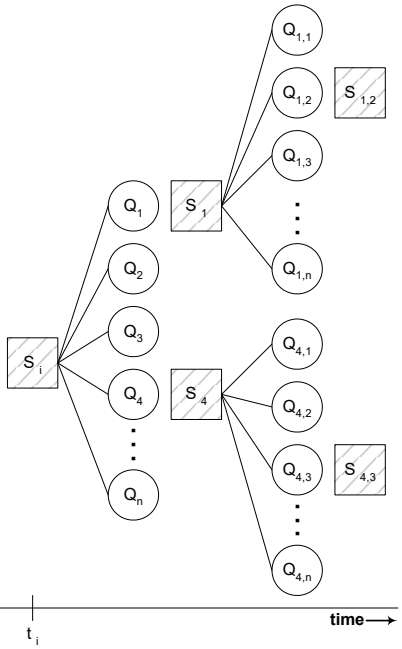
Uncertainty in Investigation (cont'd)

- Uncertainty is an inherent part of investigation.
- It reduces predictability in the investigation process,
- and thus limits the amount of proceduralization possible.

73

Photo: http://commons.wikimedia.org/wiki/File:Fingerprint_%28PSF%29.png

Investigation's Decision-Making Process



- **S_i**: current set of hypotheses and evidence
- **Q_i**: current set of questions the investigator has
- The investigator must choose which question he will investigate next

74

- The investigator has limited resources for investigation
  - He can't investigate every question
- He'd like to choose the best question to investigate next, but which question is best can be hard, or impossible, to know
  - The investigator's understanding of the case is usually uncertain and incomplete, and it might even be incorrect
  - Also, the investigator may have several hypotheses that explain the evidence, and all of them are quite possible
  - In addition, often, the investigator cannot know exactly what he will find when investigating a particular question
- So, it is not uncommon to pursue false leads or leads that are not very fruitful
  - It is an inherent part of investigation,
  - due to decision-making with incomplete and uncertain information

- One practical application of this model is evaluating investigation effectiveness, for a an individual investigator, or even a department of investigators
- When the investigator chooses a question to purse (i.e., a lead to pursue)
  - The test of competence is not, "did he purse the lead that would most quickly solve the case?"
  - but, "did he make a wise choice based on what is currently known?"

- Much of the after-the-fact analysis of 9/11 seemed to not understand the nature of investigation
    - For example, prior to 9/11, the hijackers had attended flight school, and their teacher reported them to the FBI because they were only interested in learning to fly planes, and not land them or take-off.
    - However, the FBI did not investigate those flight-school students
    - After 9/11, the FBI was faulted by the press for not pursuing that lead.
    - However, not pursuing that lead could have been reasonable given the FBI's resources, and their knowledge and experience up to that point

- ** Martin's experience: early in his career he overestimated the incidence of malicious incidents. Now he first looks for a benign explanation
- ** Due to uncertainty and temporal nature of evidence, it is often useful to collect as much evidence as possible at the beginning of the investigation
- ** Decision making cannot be a checklist or flowchart, as there are too many possible paths

Figure: adapted from the paper:

[Sch99] Schum, D. "Marshaling Thoughts and Evidence During Fact Investigation", South Texas Law Review, 40(2): 401-454, Summer 1999.

Investigations: IR vs. Scientific Method

- Two broad categories of investigation
  - Investigation of the natural world
  - Investigation of purposeful human action
- Natural world:
  - Governed by natural laws, e.g., gravity
  - Fixed relationships between things
  - Predictable outcomes, and amenable to math modeling
- Purposeful human action:
  - Governed by human nature
  - Relationship with people not as fixed
  - Less predictable, and math models not nearly as useful
- IR investigates adversarial human action
  - Limits opportunities for using math models in IR

Routine vs. Non-Routine Investigations

- Routine investigations:
  - Are the same as, or similar to, prior investigation
  - There is a known solution
  - Can be routinely solved by using a codified procedure
    - e.g., a flowchart
- Non-routine investigations:
  - The difficult new cases

Non-Routine Investigations

- What characterizes non-routine investigations?
- Novel incidents, from the investigator's view:
  - New types of attacks
  - New type of environment, e.g., a new technology
- A high degree of variation among cases
  - Variation in who conducts the attack, and how and where
  - Variation in how the investigation is carried out
- Work with uncertain and incomplete information

77

Limitations for Standardizing Non-Routine Investigations

Limitations Due to the Nature of Investigation:

- Developing new hypotheses is an act of creativity
  - Limited opportunity for proceduralizing creativity
- Decision-making based on uncertain and incomplete information
  - Often requires subjective judgment,
  - Based on experience and wisdom

78

Limitations for Standardizing Non-Routine Investigations

Limitations Due to the Types of Cases:

- Often a high degree of variation among new cases
  - Highly variable tasks not amenable to standardization
- May involve novel technology or a novel environment
  - That must be learned and new skills developed

79

easy cases can be standardized and done by junior people

Opportunities for Standardization

- Although creativity can't be proceduralized
  - There are parts the investigation process that are amenable to standardization
- It is possible to document what an investigator typically needs to know
  - Rather than how he learns (investigates) those things

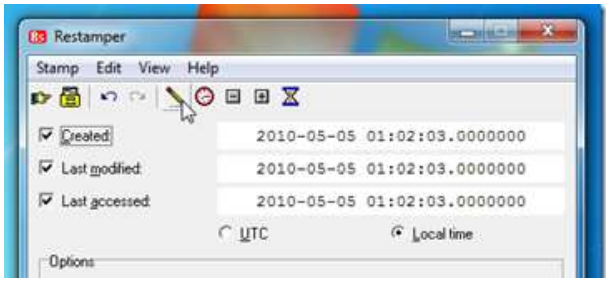
80

This is what the Army and USMC do in standardizing the battlefield intelligence process:

- They document the types of things one typically wants to know about the battlespace and the enemy
- They do not document how to go about getting that information—it's not amenable to standardization

Opportunities for Standardization

- Although creativity can't be proceduralized
  - There are techniques for aiding hypothesis creation
- How evidence is organized affects discovery
  - The juxtaposition of evidence can inspire hypotheses



81

Example of juxtaposition:

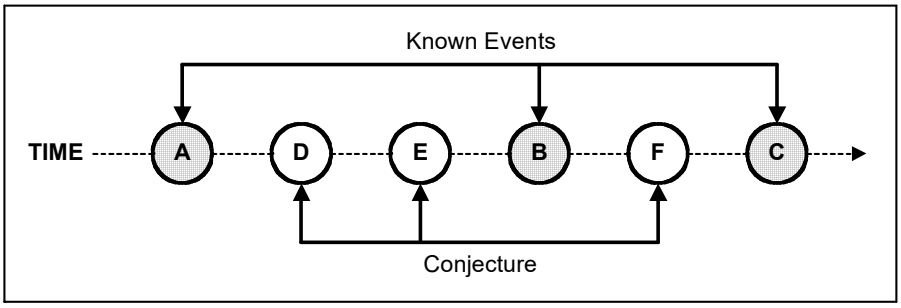
- Considering file MAC times together vs. separately:
  - If a file was accessed before it was created, then the system clock may have been changed

Photo:

http://www.addictivetips.com/windows-tips/restamper-change-date-and-time-stamps-of-filesfolders/

Opportunities for Standardization

- Conceptual frameworks for inspiring hypothesis creation
  - Scenarios: time-ordering of events



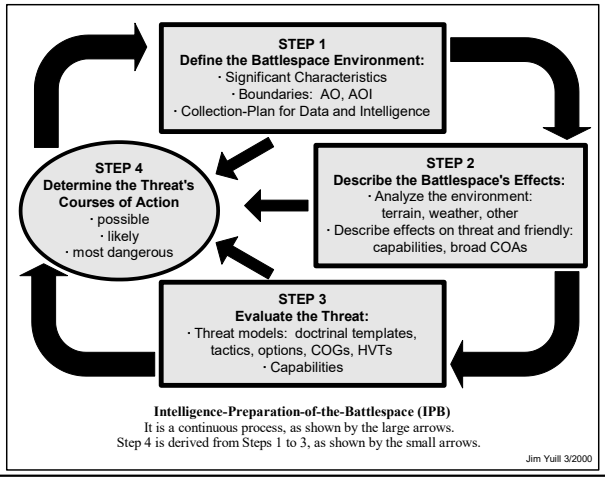
82

Figure: adapted from the paper:

[Sch99] Schum, D. "Marshaling Thoughts and Evidence During Fact Investigation", South Texas Law Review, 40(2): 401-454, Summer 1999.

Opportunities for Standardization

- Models for understanding an adversary's actions
  - Battlefield-intelligence model
  - Economics-of-crime model



83

Distinctive Attributes of IR Processes

- How IR is unlike manufacturing
- Tactical considerations for IR processes

IR vs. Manufacturing

- Process-development books are often based on manufacturing
- There are fundamental differences between manufacturing and IR:
  - **Manufacturing is a process of replication**
  - **Much of IR is a process of investigation, of an adversary**

85

- Process-development is a job skill and career field
  - There are a number of well-known and influential books on process development, such as those by Dr. Deming
  - Many process-development books are based largely on manufacturing
  - In reading process-development books, it's important to keep in mind that there are fundamental differences between manufacturing and IR
- Manufacturing replicates an existing thing
- IR investigation is a process of discovery and learning, about something that is new to you

Photos:

- Cars:

http://commons.wikimedia.org/wiki/File:12_%28236012210%29.jpg

This file is licensed under the Creative Commons Attribution 2.0 Generic license.

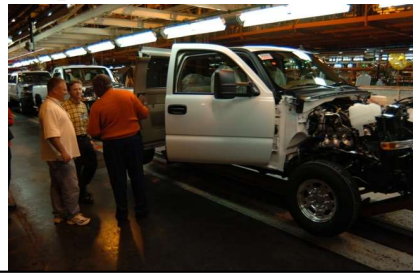
Attribution: SteelCityHobbies

- Police:

http://commons.wikimedia.org/wiki/File:US_Army_CID_agents_at_crime_scene.jpg

Manuf. Processes Easier to Standardize

- Manufacturing is a process of replication
- It works with things that are tangible and measurable
- The environment is highly controlled:
  - Designed to have repeatable processes
  - Variation is minimized in processes, and in parts and materials
- Social relationships are relatively cooperative:
  - Employees
  - Suppliers



86

- IR is very different, and in some ways, the opposite of this
- Contrasting manufacturing with incident response. In IR:
  - There is a lot of variability among cases, especially difficult cases
  - Much of what you work with is intangible and not amenable to measurement—information and software
  - There are primary aspects of the IR process that the investigator has little control over
    - Hackers
    - System design, administration, and use
  - Relationship with hackers is adversarial—the opposite of co-operative

Tactical Considerations

- IR involves battle with an intelligent and adaptive adversary
- Standardized processes are necessary,
  - but we must be willing, able, and ready to do things differently
- Ways standardized IR processes can create vulnerabilities
  - There can be weaknesses in the processes themselves
  - The processes can make the responder predictable
    - Hacker exploits that, e.g., to hide or attack
  - Outsourced security:
    - Security provider's processes could be revealed via another customer

87

Chapter 5:
Creating Effective Processes

88

Creating Effective Processes

- ***Reading a book on brain surgery does not make you a brain surgeon***
  - Standardized processes are useful for training and operations, but they also have limitations.
- ***Painting by the numbers does not produce a masterpiece***
  - In some cases, proceduralization can lower quality, so care is needed to preserve core competencies.
- ***All models are wrong, but some models are useful***
  - Standardized processes will inevitably have problems, so on-going revision is not optional.

89

Topics (cont'd)

- ***Herding cats, prima donnas, and smart people***
  - Creating effective standardized processes requires leadership and co-operation
- ***Everyone can cook, but not everyone is a chef***
  - Creating IR processes that are effective requires an unusual set of skills, and also, the desire to serve rather than prescribe.
- ***Writing a book on brain surgery does not make everyone else a brain surgeon***
  - The challenges in creating codified IR-processes that other companies can use, e.g., publishing IR processes for marketing purposes.

Reading a book on brain surgery does not make you a brain surgeon

- Codified IR processes are useful
  - For training and operations, but there are limitations.
- Often, standardized processes can
  - Speed the training of apprentices and journeymen,
  - But they can't make you an expert
- For some jobs, becoming an expert requires:
  - Experience, e.g., over many years
  - Skills that can't be proceduralized, e.g., creativity

91

By following a cookbook recipe, anyone can make a decent meal.

Professional gourmet chefs have skills and abilities that can't be codified in a cookbook recipe.

Painting by the numbers does not produce a masterpiece

- When some processes are proceduralized,
  - The quality of the output will be lessened
- Gourmet cooking vs. McDonalds

92

- Proceduralization may “dumb down” the process
- May produce journey-man level work, but not master-level work

Need to Preserve Core Competencies

- What things does your organization do well,
  - That are essential to "stay in business"
- For example, what things are necessary to
  - Maintain funding
  - Or, to provide competitive advantage?
- Need to ensure that proceduralization
  - Does not cause loss of core competencies

93

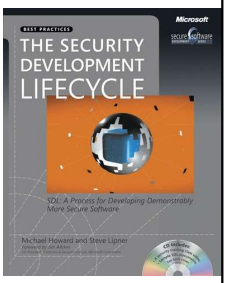
Example:

- A restaurant's market niche is gourmet meals
- If standardization lowers the meals' quality, they will no longer be serving the same market
- There is a market for their high quality food, but there may not be a market for the lower quality food

- Don't remove needed creativity and flexibility
- Don't replace good subjective processes with mediocre cookbook processes

All models are wrong, but some models are useful

- Difficult to get standardized processes right
- Helpful to start on a small scale
  - Get processes working well with a small group,
  - Before deploying them with a large group
- On-going feedback and correction is essential
  - To identify and fix problems
- On-going adaptation is needed
  - The objectives and context will change over time
  - e.g., business and technology changes
  - Need to budget for this



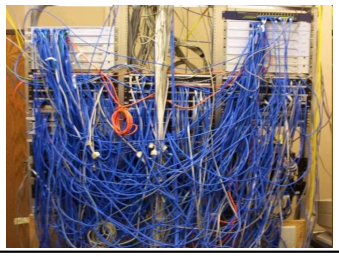
94

This quote is from Einstein. I think he's referring to the limitations of models, e.g., omitting information, and providing approximations

However, in my experience, almost all standardized processes I've worked with or researched have significant problems. The more detailed they are, the more problems they have.

Herding cats, prima donnas, and smart people

- Difficulties of effectively deploying standardized processes
- Acquiring new skills is difficult
  - It can be hard work, take a long time, and problems will likely arise
  - Old habits and expectations can be hard to change
- Process changes can have negative effects for some people
  - New job skills may be required
  - Current job skills may diminish in value



95

- Make compliance easy and non-compliance hard
  - Tool support
  - Training
  - Enforceable

Photos:

- Messy cables

http://commons.wikimedia.org/wiki/File:Cable_closet_bh.jpg

This work has been released into the public domain by its author, Bhankins.

- Neat cables

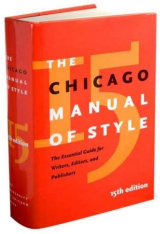
http://commons.wikimedia.org/wiki/File:Switches_in_rack.jpg

This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.

Attribution: Parkis

Herding cats, prima donnas, and smart people

- Developing and deploying standardized processes is a form of **leadership**
- Management owns the development processes
- Technical leadership needed:
  - Need process vision
  - Draw on expertise of individual team members



- Need to inspire acceptance of the spirit of a process
  - Perfunctory compliance can result in huge waste

96

Management owns the development processes

- Provides funding
- Only management has the authority to prescribe how things are done

Technical leadership needed

- No one is good at everything, or the best at everything
- Need to draw on team's expertise: a collection of skills
- On the other hand, the way most people currently do things, or like to do things, may not be the best
- If you want to improve the team's writing skills, you don't survey the team to see how they currently write, you get leadership and direction from a highly skilled technical writer

Book:

The Chicago Manual of Style: The Essential Guide for Writers, Editors, and Publishers, by Chicago Editorial Staff, University Of Chicago Press, © 1993

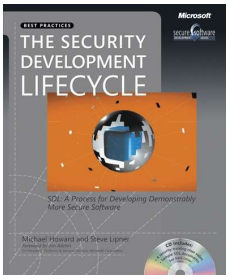
Used by fair-use

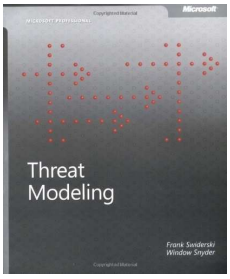
Everyone can cook, but not everyone is a chef

- Creating effective standardized processes requires:
  - Technical expertise and vision
  - Leadership skills
  - Experience and skills with process development
- Dr. Deming: revolutionized manufacturing
  - Through his work in process development

Writing a book on brain surgery does not make everyone else a brain surgeon

- The challenges in creating standardized IR-processes that other organizations can use,
  - e.g., publishing IR processes for marketing purposes
- Microsoft's experience
  - Publicizing its security development processes





98