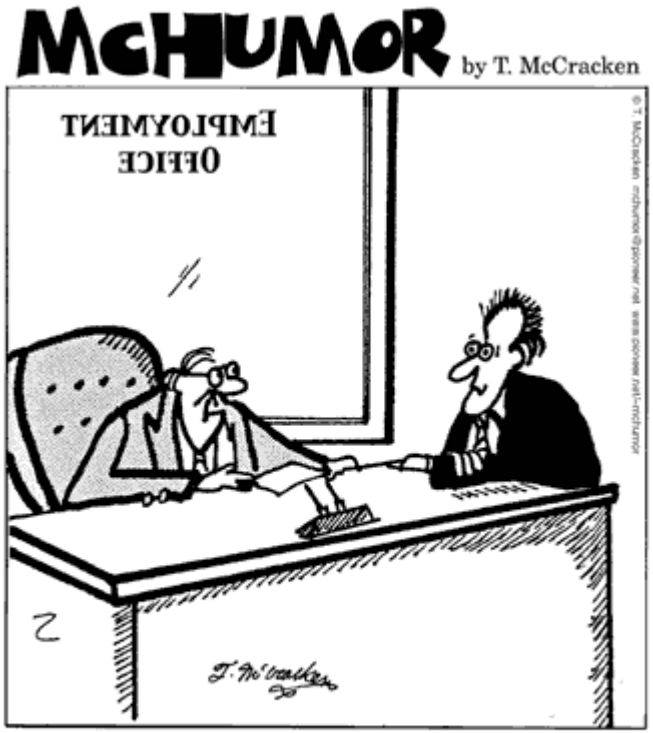
Transforming into Security Testers

Marc René

Road Map

- Basic awareness
  - Data privacy; Attacks
- Risks
  - Financial; Legal; Reputation
- Testers perspective
  - Application domain; Testing skills; Technology
- Techniques
  - Misuse cases; Identifying injection flaws; Test planning checklists
- Handling test data
- Balance

Security



"You've certainly got some unique career goals: to break into the computer systems of the CIA, the Department of Defense, Bank of America..."

Attributes of software that bear on its ability to prevent unauthorized access, whether accidental or deliberate, to programs or data

ISO 9126

Security Properties (CIAN)

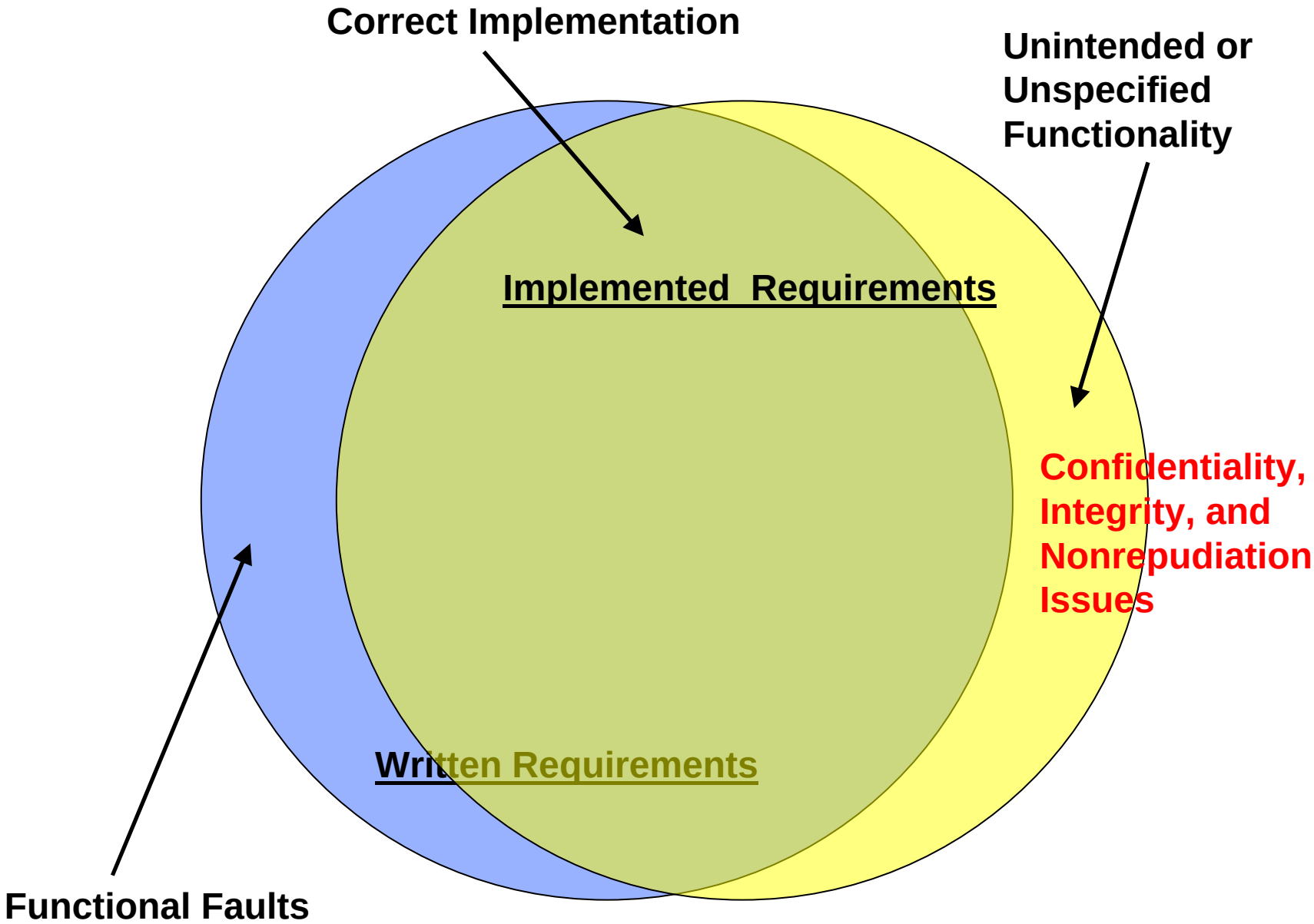
- **Confidentiality**
  - The property that information is **not** made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity**
  - The property that data has **not** been changed, destroyed, or lost in an unauthorized or accidental manner
- **Availability**
  - The property of a system or a system resource being accessible and usable on demand by an authorized system entity, according to performance specifications for the system
- **Nonrepudiation**
  - A security service that provides protection against false denial of involvement in a communication or action

RFC 2828 Internet Security Glossary

Personal Information

- An individual's name *(address?)* in combination with one or more of the following, when either are not encrypted
  - Social security number
  - Driver's license number
  - Financial information including bank account or credit card numbers
  - Medical information
  - …more fields being added

- Does not include publicly available information that is made available to the general public from federal, state, or local government records



02-Oct	The Nature Conservancy	A hacker illegally gained access to a computer of The Nature Conservancy containing personal information…	14,000
04-Oct	MA Division of Prof. Licensure	Social Security numbers of about 4[illegible]0 licensed professionals were inadvertently released…	450,000
10-Oct	Wheels Inc./Pfizer	The spouses and domestic partners of about 1,800 Pfizer employees, including 23 from Connecticut, learned last month about a data breach at Wheels Inc…	1,800 + 23
10-Oct	Commerce Bank	A hacker gained access to a database with about 3,000 customer records and accessed data belonging to 20 of them…	20
12-Oct	King County Trans. Department	A laptop computer containing personal information about current and former employees has been stolen...	1,400
13-Oct	Montana State University	An unknown hacker remotely accessed a computer server that housed records containing credit card numbers and Social Security numbers.	1,400
23-Oct	Blockbuster	A Saras[illegible]nt was fishing in a trash container for boxes when he found 400 documents...	Unknown
23-Oct	Dixie State College	An unauthorized person reportedly gained access to a computer system and confidential files, including Social Security numbers.	11,000
28-Oct	Art.com	Cyberspace criminals gained system's entry despite "multiple security layers" and accessed some credit card transactions...	Unknown
29-Oct	ABC Phones	[illegible]men found a box in a dumpster...	Unknown
30-Oct	University of NV, Reno	A University of Nevada, Reno a administrative employee has lost a flash drive that contained names and Social Security numbers of 16,000 current and former students…	16,000
05-Nov	Alabama Department of Public Health	The personal information, including the names, ages and Social Security numbers of families enrolled in the state's [illegible] health care coverage program, were accidentally sent to the wrong families last week…	1,554
16-Nov	U.S. Department of Veteran Affairs	Investigation from a man's home discovered a computer that held about 1.8 million Social Security numbers from the U.S. Department of Veteran Affairs, where he had been employed as an auditor...	185,000
21-Nov	University of Florida	More than 400 former UF students might have been put at risk for identity theft after their Social Security numbers were posted on UF's Computing & Networking Services Web site.	415

Legislation

- Gramm Leach Bliley Act (GLB, effective May 02)
- California Legislation, most states follow this in some form (effective July 03)
  - State legislation requiring consumer notification of data security breaches has been approved in at least 25 states
  - Federal Bill is being proposed
- HIPAA
- Payment Card Industry (PCI) data security standard

Security Breach Notification

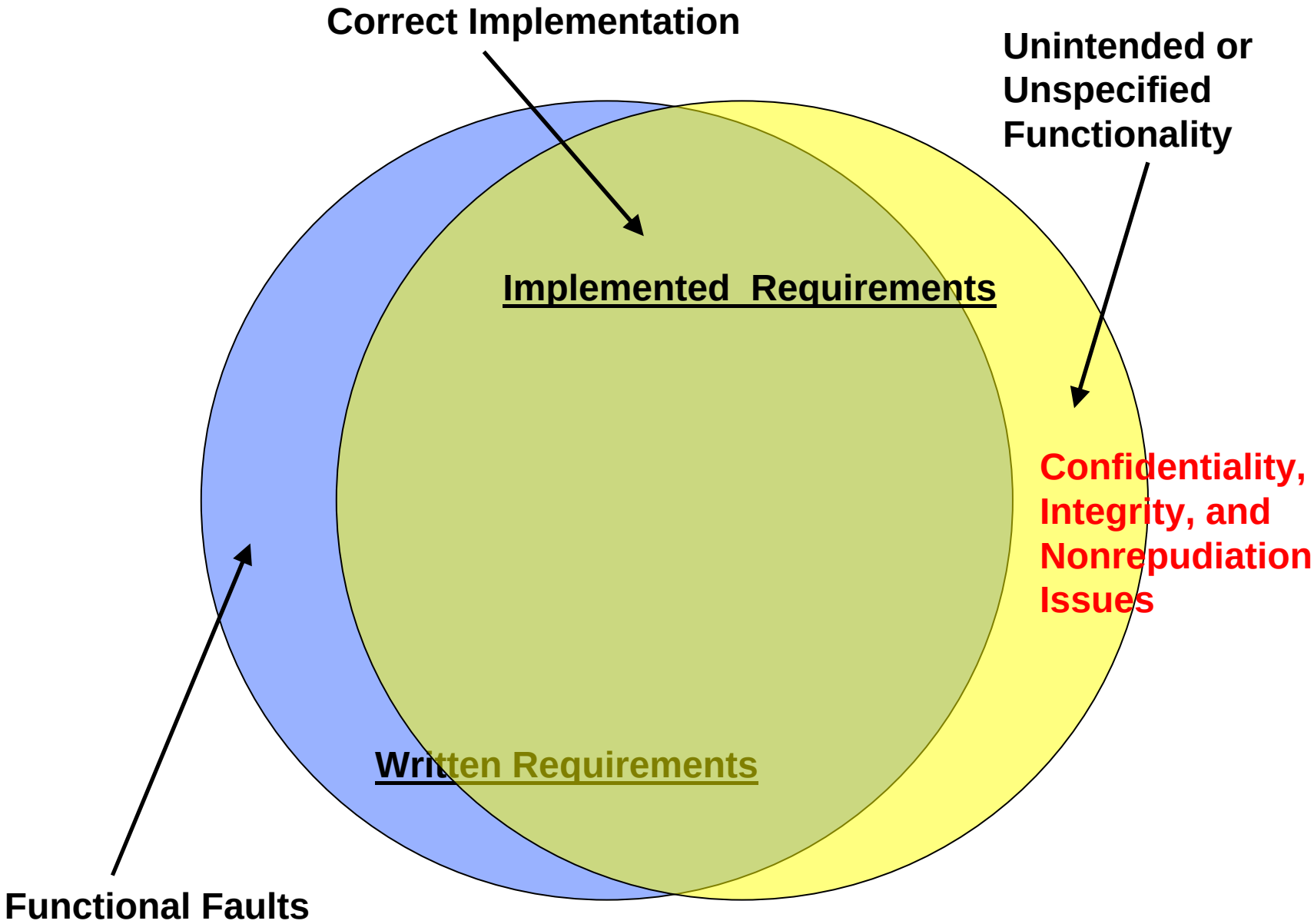
- What is a Breach of Security?
  - The unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by an organization
- Security Breach Notification
  - Most state laws modeled on California's security breach notification law
  - Requires a company to provide notice to affected individuals if it discovers that personal information has been obtained by someone without authorization

What Makes a Good Tester?

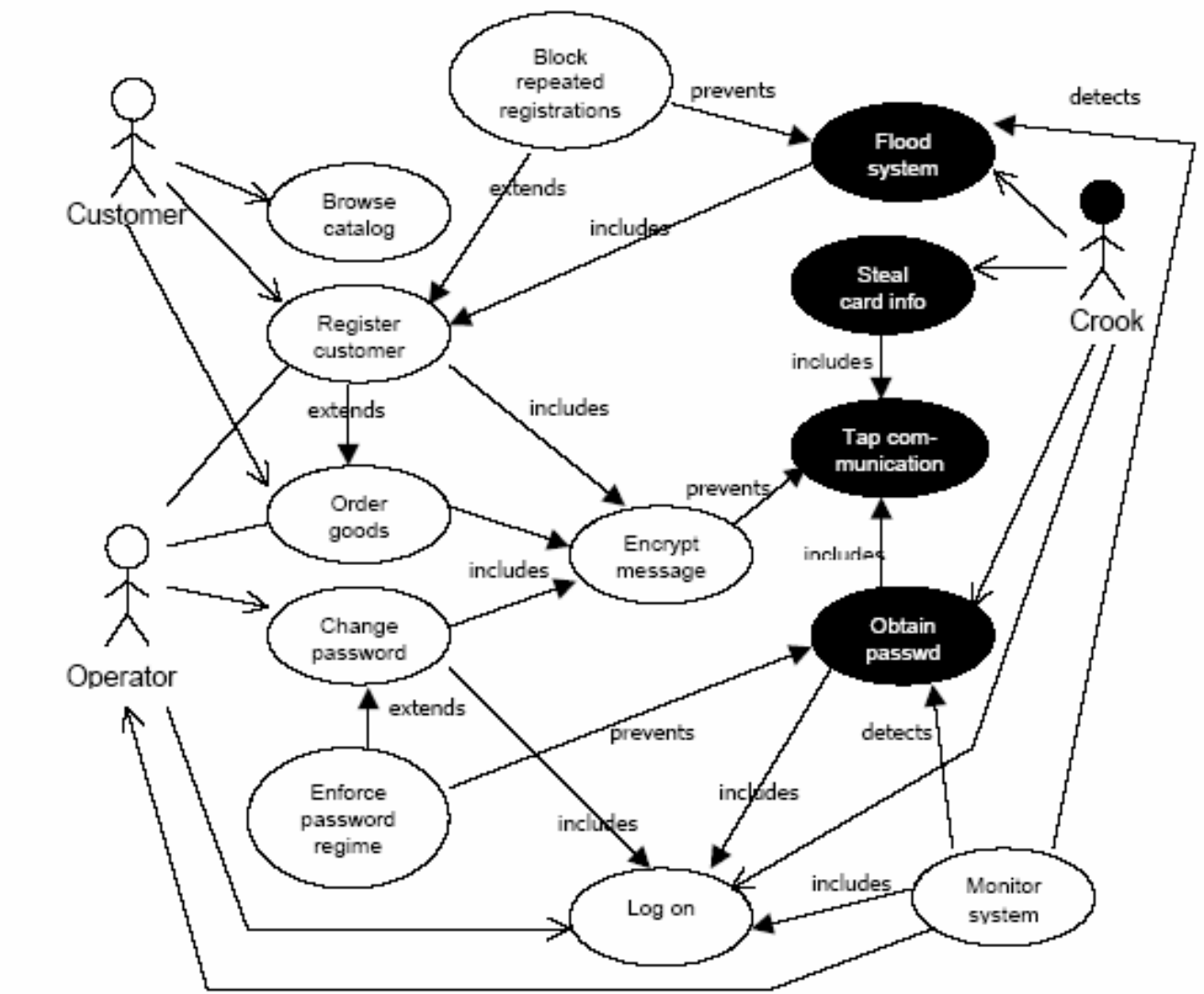
- Knowledge of
  - Application Domain
  - Testing Tools and Techniques
  - Implementation Technologies

- *How Does Security Fit?*

Perspective



Misuse Cases



http://www.nik.no/2001/21-sindre.pdf

OWASP Top Ten

- Cross Site Scripting (XSS)
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access

http://www.owasp.org/index.php/Top_10_2007

Identifying Injection Flaws

- Buffer Overflow Vulnerabilities
  - Programming errors involving improper input array bounds in memory that enable invalid input leading to the execution of the attacker's code at a high level of privilege
- Structured Query Language (SQL) Injection Vulnerabilities
  - Arise when SQL statements are cleverly embedded in user input, allowing an attacker to perform operations on a backend SQL database (e.g., change the administrator password or delete rows)
- Many other examples
  - Allowing a user to input a filename
  - Programs that permit filenames with directory traversal
  - Universal Naming Convention (UNC) for shared storage resources are prone to attack

Injection Flaws - Considerations

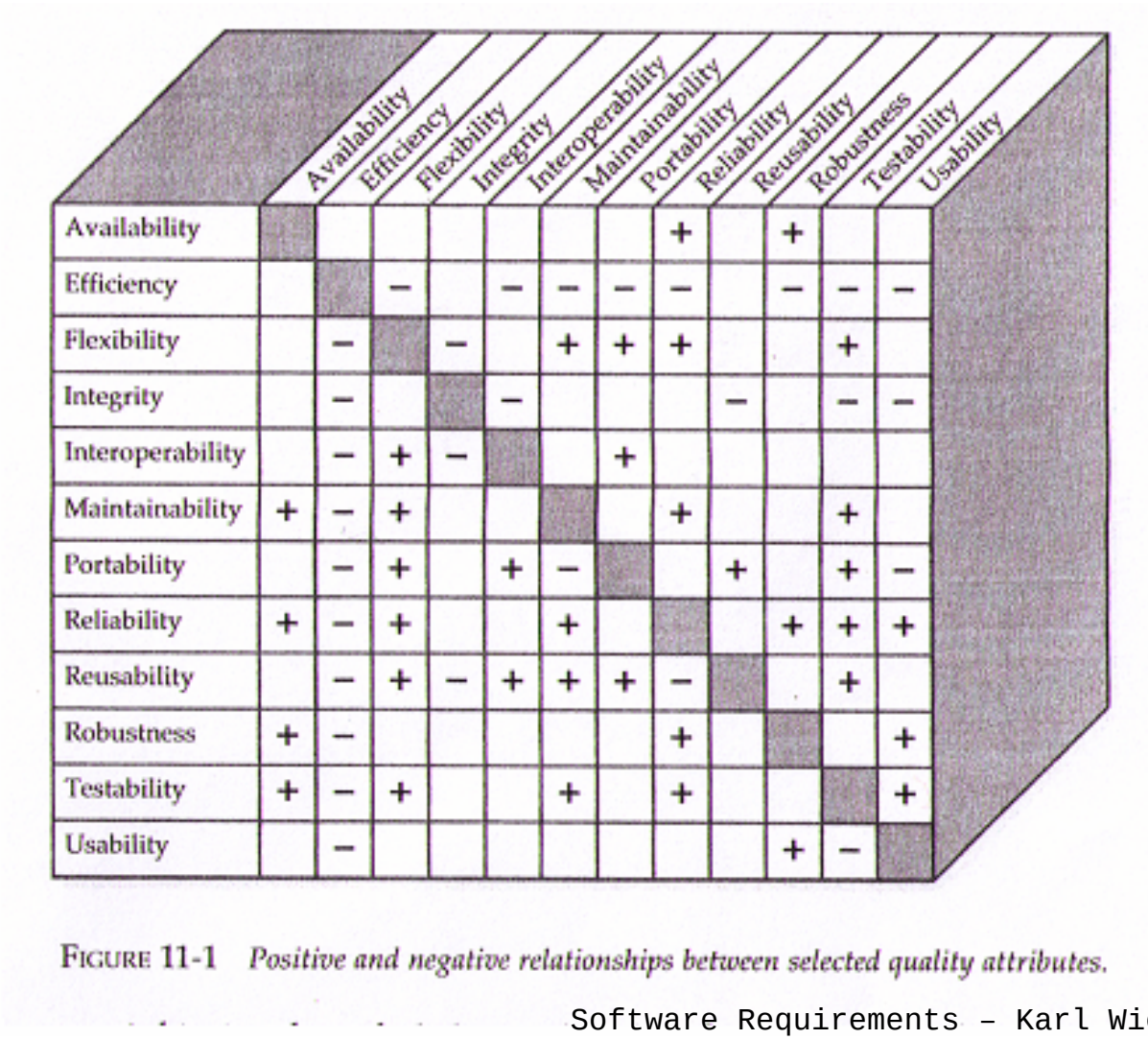
- Does your system accept input from untrusted sources?
  - What if your trusted sources turn out to be untrustworthy?
  - If the trusted sources turn out to be untrustworthy, have you examined the potential security vulnerabilities thoroughly?
- Do you have a data validation strategy that you have communicated to all software engineers?
- Are you confident that the system is not vulnerable to attacks stemming from inadequate data validation (e.g., buffer overflow or cross-site scripting)?

Test Planning Checklists

Handling Test Data

- Do you use “production data” to test?
- Do you create plans to:
  - Limit amount of data used?
  - Limit access to that data?
  - Remove data when complete?
  - Correctly handle any output?

Balance



	Availability	Efficiency	Flexibility	Integrity	Interoperability	Maintainability	Portability	Reliability	Reusability	Robustness	Testability	Usability
Availability							+		+			
Efficiency			−		−	−	−	−		−	−	−
Flexibility		−		−		+	+	+			+	
Integrity		−			−				−		−	−
Interoperability		−	+	−			+					
Maintainability	+	−	+					+			+	
Portability		−	+		+	−			+		+	−
Reliability	+	−	+			+				+	+	+
Reusability		−	+	−	+	+	+	−			+	
Robustness	+	−						+				+
Testability	+	−	+			+		+				+
Usability		−								+	−	

FIGURE 11-1 *Positive and negative relationships between selected quality attributes.*

Software Requirements – Karl Wiegers

Road Map - Revisited

- Basic awareness
  - Data privacy; Attacks
- Risks
  - Financial; Legal; Reputation
- Testers perspective
  - Application domain; Testing skills; Technology
- Techniques
  - Misuse cases; Identifying injection flaws; Test planning checklists
- Handling test data
- Balance