Classification, Facets, and Conceptual Space in Security Analysis and the Use of Patterns

Dr. Michael Van Hilst
Farquhar College of Arts and Sciences
Nova Southeastern University

Security Challenges

- Gaps in knowledge
- Gaps in coverage
- Risks that are complicated and subtle
- Broad range of issues
- Different kinds of expert knowledge

- *One exploit is one too many*

Goal of Work at NSU & FAU

1. Easier ways to apply solutions
   - – disseminate knowledge and expertise
2. Better ways to see the big picture
   - – comprehensive coverage (no gaps)
3. Simpler solutions with better protection
   - – system level approach

- *Not unlike OWASP's lists & tools*

Two security topics for today

1. Patterns
2. Classification & Coverage

Work with

Eduardo Fernandez (FAU)

Saeed Rajput (Nova)

1. Patterns

- Patterns capture the experience of experts about good or best practices and document these nuggets of wisdom in a format that is easy to understand.

- The use of patterns raises the level of awareness and discourse in a discipline.

A Brief History of Patterns

- 1977 Christopher Alexander – A Pattern Language
  timeless wisdom in architecture & town design
- 1978 Trygve Reenskaug – Model View Controller
- 1987 Cunningham & Beck – OOPSLA paper
- 1994 Gamma, Helm, Johnson, Vlissides - GoF
- 1997 Yoder & Barclaw – security patterns
- 2006 Eduardo B. Fernandez – book(s)

estimated 400 security related patterns exist today

A pattern is self-contained

- Synopsis
- Context where applies
- Example problem
- Problem
- Forces
- Solution
- Solution structure
- Solution dynamics
- Example solution
- Variations
- Known uses
- Consequences

Different kinds of patterns

Traditional patterns

- Design
- Architecture
- Analysis
- Organizational
- Management
- Anti-patterns

Less traditional patterns

- Attacks
- Domains
  - EHR, banking
- Standards
  - HIPPA, SSL, WiMax
- Forensics
  - VOIP

Signed configuration mgmt.

A developer with bad intent could install trap doors or malicious code in the system.

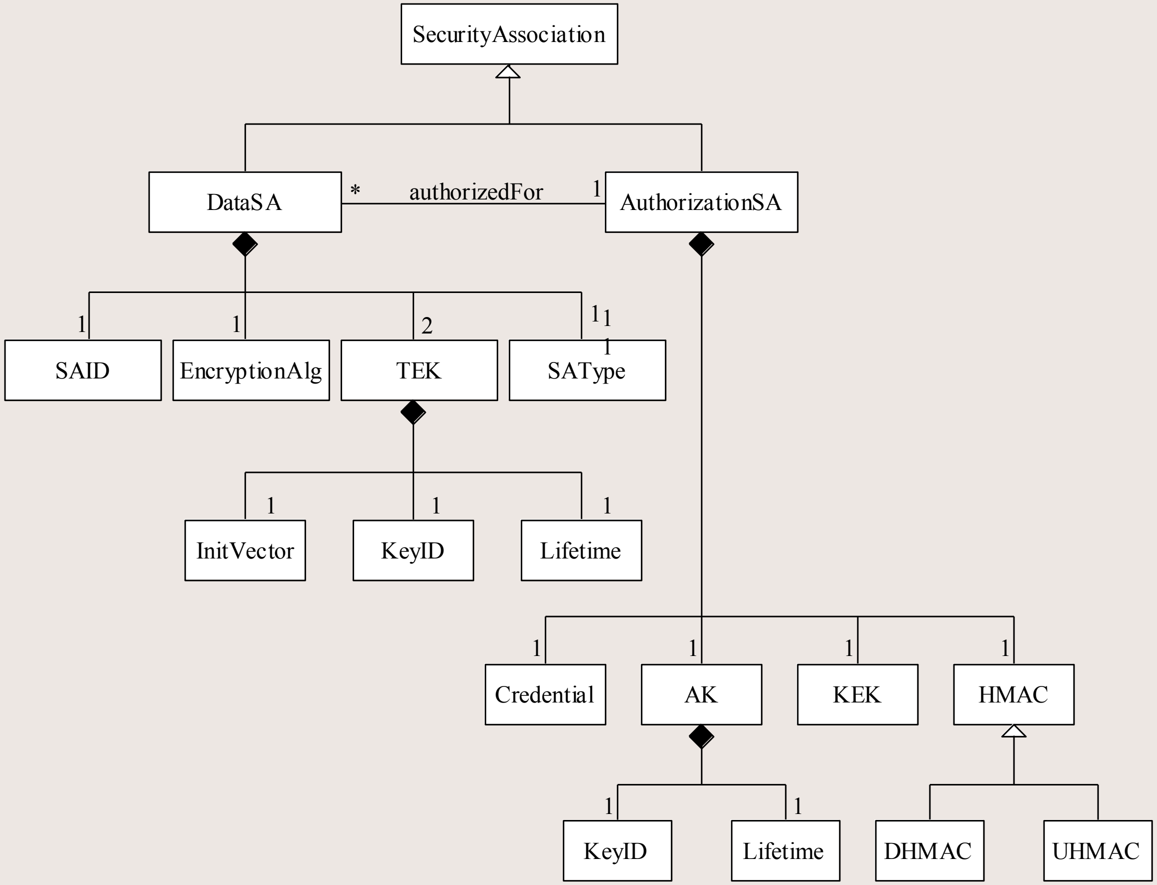
Ensure only validated code is used and create accountability by signing artifacts.

…

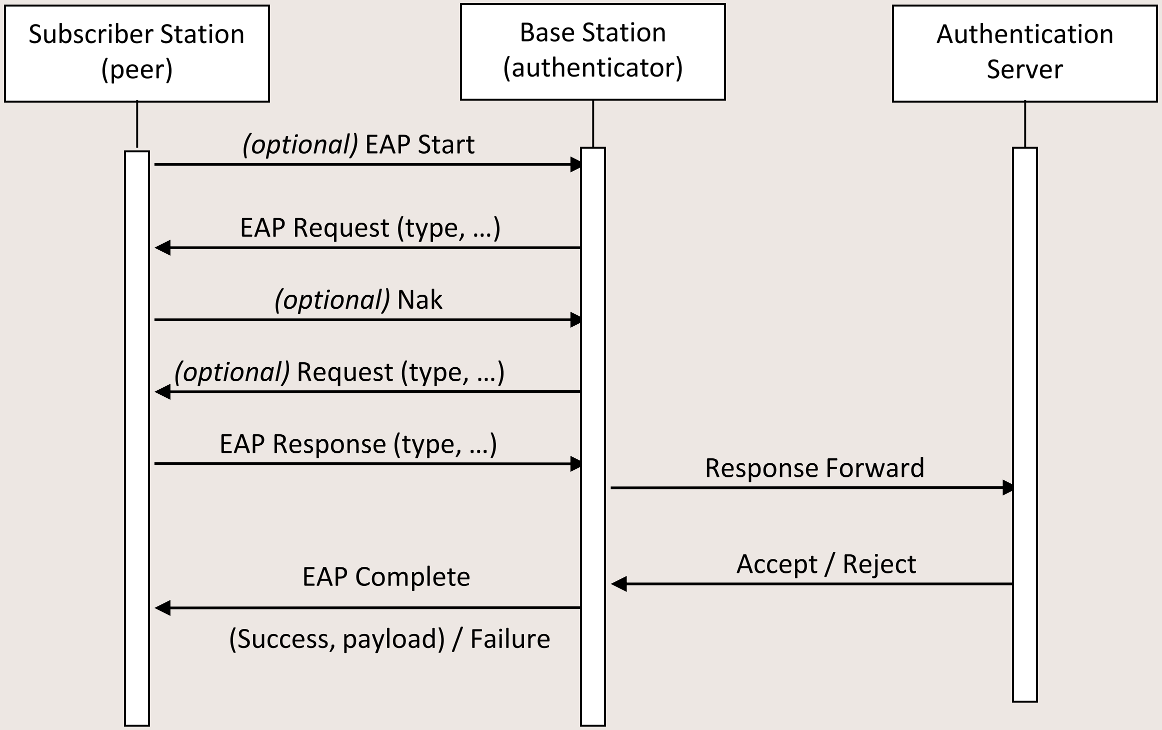
Consequences: code cannot be changed after check and must be signed by the developer.

Known Uses: GIT, Bit Keeper, …

WiMax key mgmt structure



WiMax authenticate dynamic



Patterns make a difference

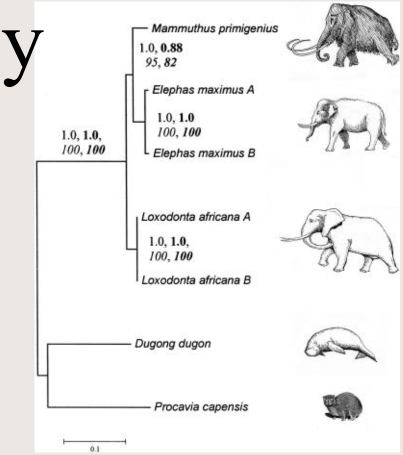
- Patterns deliver targeted knowledge
  - Assume minimal prior knowledge
  - Useable in arbitrary groups and ordering
  - Searchable, downloadable, write your own
- Patterns raise the level of discourse
  - Each pattern represents a higher level solution
  - Each pattern becomes a term in the vocabulary

Classification of patterns?

- With 400+ security patterns, how do we know which ones to look at?
- With patterns, or checklists, how do we know what isn't covered?
- Classification is needed both for search and for coverage analysis
- *OWASP has same problem for its lists*

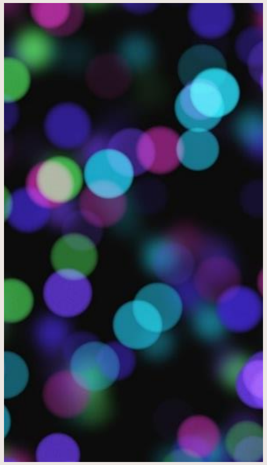
Hierarchy

- The first classifications of patterns used hierarchy (i.e. Yoder and others)
- Good for pattern writers (is it new?)
- Same model as used in biology
- Allows only one label
- Not so good for pattern users



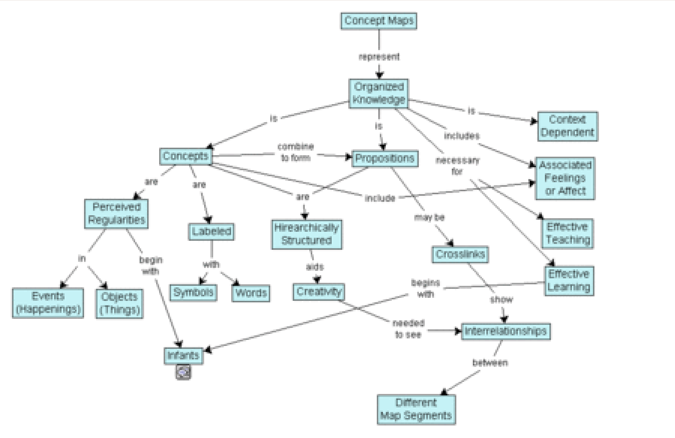
Facets

- The software reuse community uses facets or tags (i.e. Prieto Diaz)
- Gmail and tweets (hashtags)
- Good for grouping and search
- Arbitrary number of labels
- Without relationships among labels, they are just points (doesn’t solve coverage)



Ontology / Concept Map

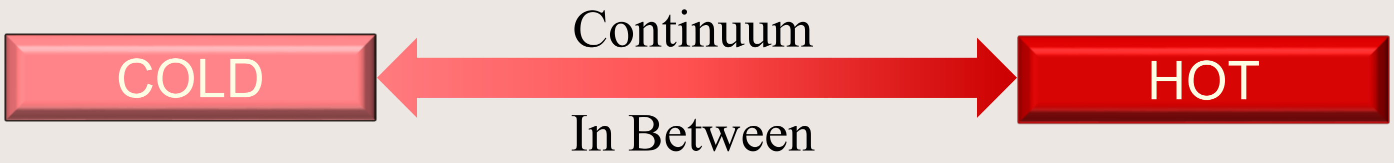
- Network (map) of relationships
- Good for meaning (i.e. semantic Web)
- Does not address coverage (what’s missing)



George Kelly's Concept Grid

Psychological space divided on bi-polar axes is based on psychologist George Kelly's *Personal Construct Theory* (1955).

- Conceptual categories fit along an axis
- Categories can be disjoint and/or overlap



COLD

Continuum

In Between

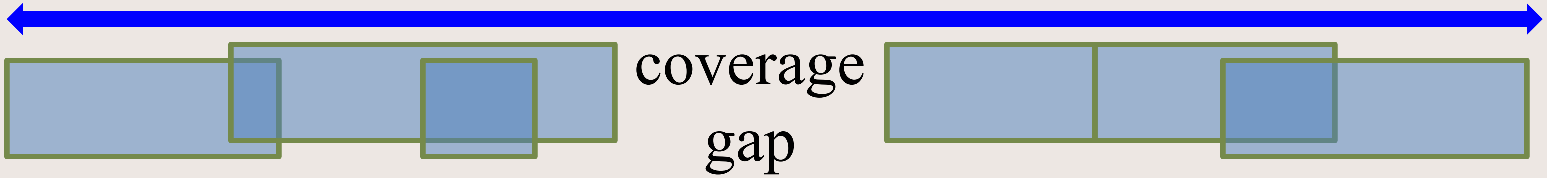
HOT

- Note about conversation with Paul Black, NIST

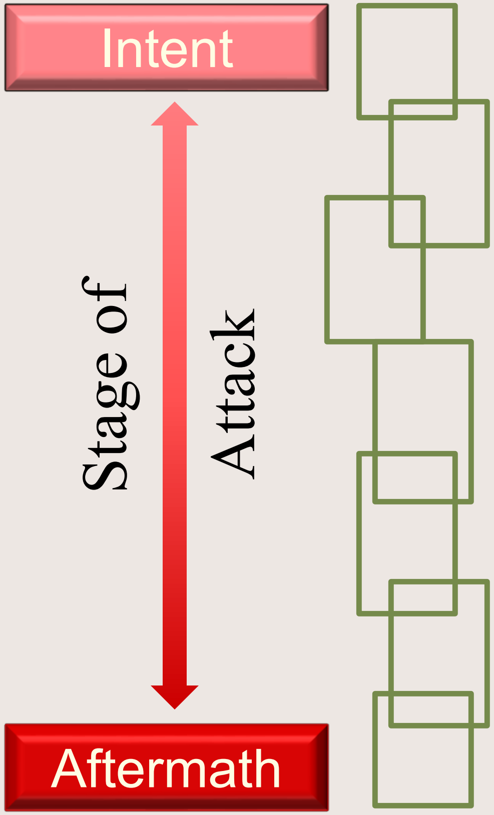
Regions on continua

- Assume a single problem space
- Slice along separate dimensions
- Each dimension is a bi-polar continuum
- Mapping on a continuum reveals the gaps

The challenge is to choose the poles

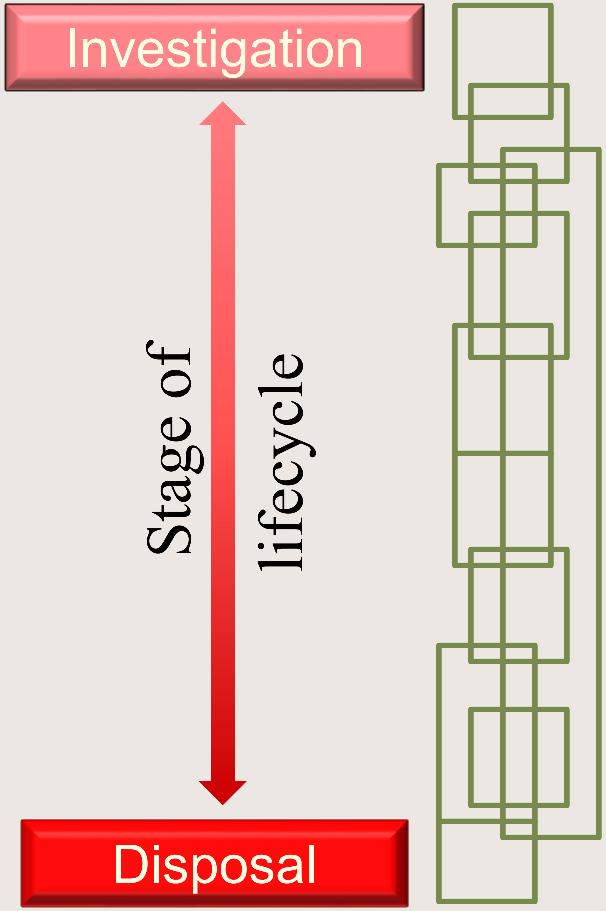


Attack stage responses



- Avoidance
- Deterrence
- Prevention
- Detection
- Mitigation
- Recovery
- Forensics

Stages in lifecycle



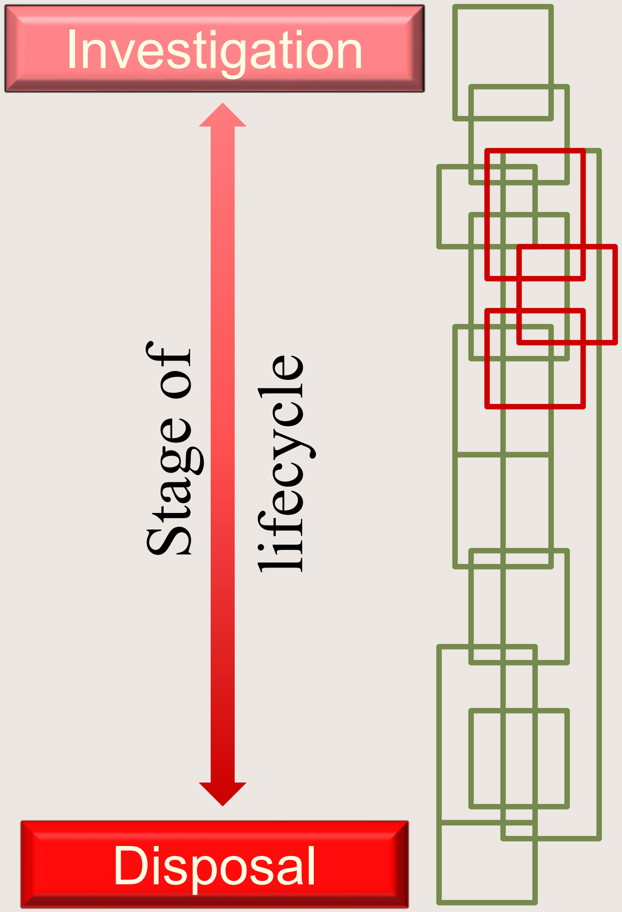
Investigation

Stage of lifecycle

Disposal

- Domain Analysis
- Requirements
- Architectural Analysis
- Design
- Implementation
- Verification/Testing
- Integration
- Deployment/Configuration
- Operation
- Maintenance
- Disposal

Stages in lifecycle (IS)



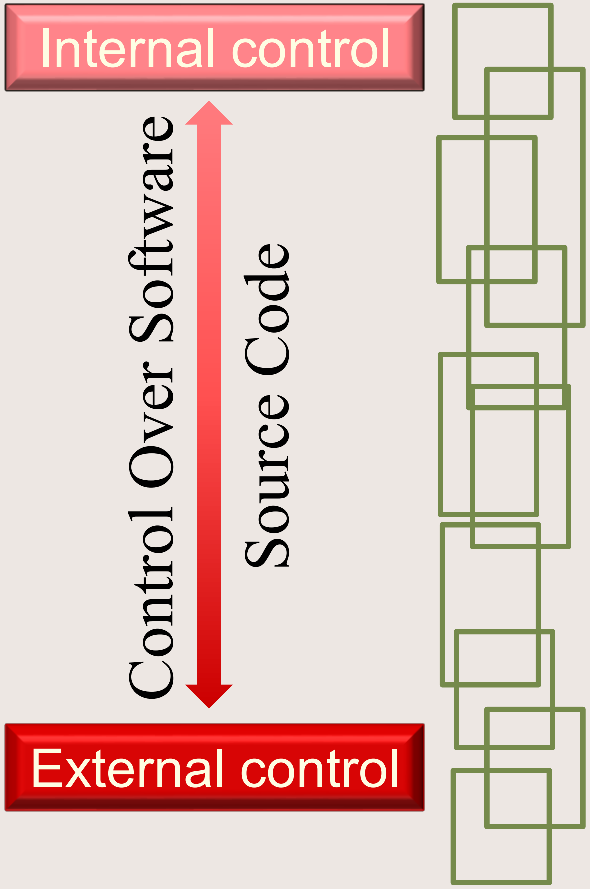
Investigation

Stage of lifecycle

Disposal

- Domain Analysis
- Requirements
- Systems Analysis
- Acquisition
- Installation
- Verification/Testing
- Integration
- Deployment/Configuration
- Operation
- Maintenance
- Disposal

Code source (apropos control)



Internal control

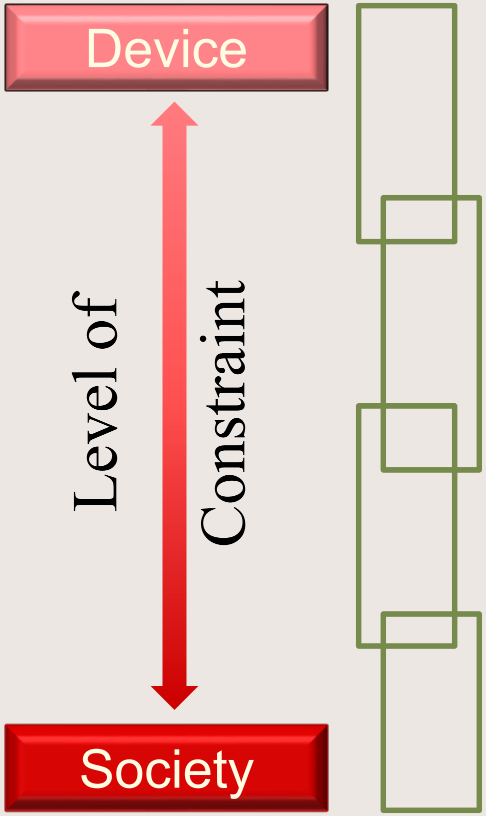
Control Over Software

Source Code

External control

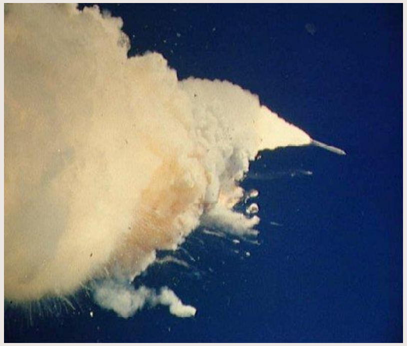
- New code
- Open-source
- Runtime script
- Model transformation
- Wizard forms
- Reuse Library
- Outsourced
- Legacy
- Off-the-shelf
- Remote web service

Level of constraint



- Technical
- Human
- Organizational
- Regulatory

Leveson’s levels of constraint



- Technical
- Human
- Organizational
- Regulatory

http://www.nytimes.com/2014/03/14/nyregion/safety-is-lacking-at-metro-north-us-review-finds-after-a-fatal-crash.html

Other matrix/grid properties

- Supports topic navigation and learning
  - Meaningful adjacency and generality relations
- New axes can be added any time
  - Their use is complementary, not intermingled
  - Axes can also be removed/hidden
- Can have no distinctions on some axes
- Bi-polar concepts don’t fit all issues …

Some dimensions not bipolar

- **Solution type**
  - Encryption, access control, hash digest, … ?
- **Problem type**
  - Authentication, authorization, availability, integrity, non-repudiation, … ?
- **Problem domain**
  - Cellphone, smart grid, e-commerce, … ?

What do/don’t these cover?

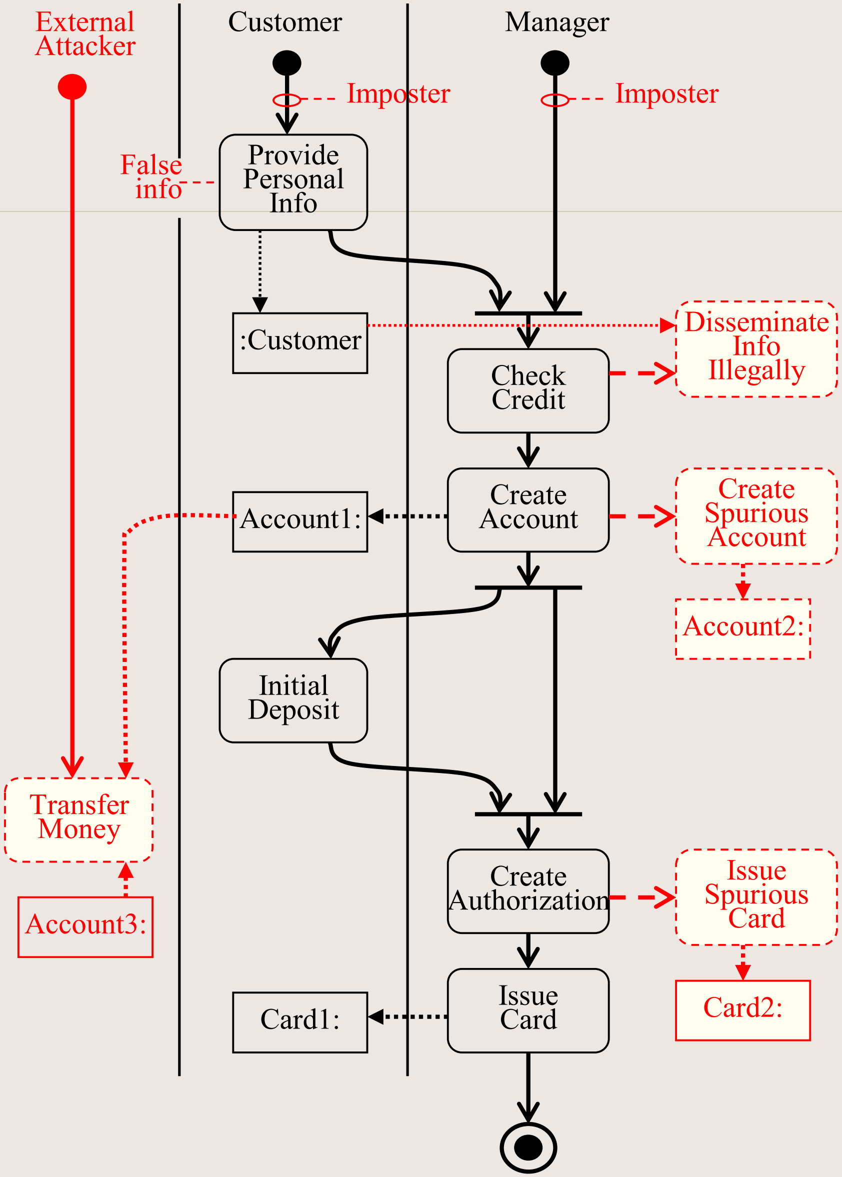
- Common Criteria
- National Training Standard for Information Systems Security Professionals (INFOSEC)
- Sarbanes-Oxley
- Systems Security Engineering Capability Maturity Model
- Viega and McGraw’s 10 principles
- OWASP 15 principles, 10 coding principles
- OWASP 20 weaknesses or vulnerabilities
- OWASP 12 countermeasures

Conclusion

1. Patterns are good for teaching
   - for students
   - for practitioners
   - for experts
2. Coverage classification gives perspective
   - for big picture
   - for consequences of details

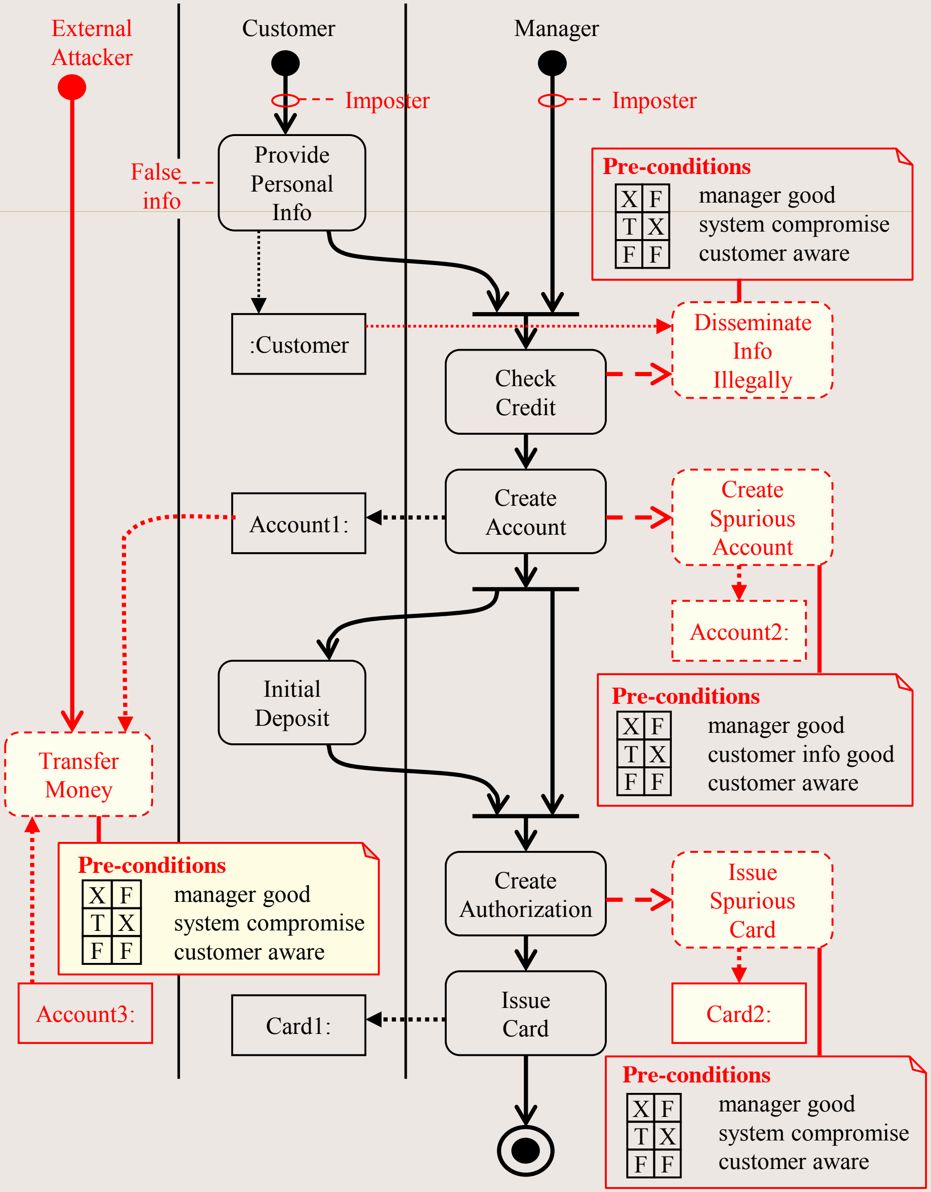
Misuse case

- For each action
  - Who could do harm?
  - What could go wrong?



Misuse case

- For each action
  - Who could do harm?
  - What could go wrong?
- Add checkable conditions



External Attacker

Customer

Manager

Imposter

Imposter

False info

Provide Personal Info

:Customer

Check Credit

Disseminate Info Illegally

Pre-conditions

X	F	manager good
T	X	system compromise
F	F	customer aware

Account1:

Create Account

Create Spurious Account

Account2:

Pre-conditions

X	F	manager good
T	X	customer info good
F	F	customer aware

Initial Deposit

Transfer Money

Pre-conditions

X	F	manager good
T	X	system compromise
F	F	customer aware

Account3:

Create Authorization

Issue Spurious Card

Card2:

Issue Card

Card1:

Pre-conditions

X	F	manager good
T	X	system compromise
F	F	customer aware