Systems Analysis and Threat Modeling in Security Development Lifecycle (SDL)

A tale in two parts

Keith W. Beatty

October 15, 2008

SAIC
From Science to Solutions

Objectives

- **Overview of Systems Analysis[1]**
  - Discuss Systems Analysis as it pertains to a former project
  - Discuss steps used to implement the project analysis
  - Discuss resulting matrix that was produced
    - To support the decision process
- **Detailed examination of Threat Modeling**
  - Stage 4 of Security Development Lifecycle[2]
  - Portion of risk analysis
  - Illustrate the steps involved in producing a TM result
- **Additional observations and conclusions**

[1] Dennis, Wixom, and Roth. Systems Analysis & Design, 3rd edition. Danvers: John Wiley & Sons, 2006. Chs 4&9.
[2] Howard, Michael and Lipner, Steve. The Security Development Lifecycle. Redmond, WA: Microsoft Press, 2006. Chapter 9.

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Systems Analysis

- **Project Objectives**
  - Provide differentiation among a set of competing alternatives
  - Identify strengths/weaknesses of proposed solutions
  - By creating an alternatives matrix
- **Design Theory**
  - Feasibility analysis identifies important project risks (issues) that must be addressed
    - Technical, economic, organizational
  - Non-functional requirements (NFRs) refer to behavioral properties that a system must have
    - Affect design (architectural) decisions
    - Operational, performance, security, and cultural/political
- **Implementation**
  - Built a matrix to organize pros and cons of competing alternatives
    - Listed strengths and weaknesses from each proposal
    - Identified a list of general issues
    - Placed general issues into feasibility categories
    - Provided NFR sub-categories for greater granularity
  - Created a matrix derived from feasibility issues

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Design Implementation Steps

- **Project issues aligned with non-functional requirements (NFRs)**
- **Feasibility issues embedded in NFR sub-categories**
  - Used in calculations of relative importance (weight)
  - Used in scoring cells
- **NFRs served as a general evaluation criteria for matrix**
  - Pros and cons of each proposal mapped to NFR sub-categories
  - Tallied for alternatives
  - Used in scoring cells

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Feasibility issues to NFRs

Feasibility Issues: I. Technical Issues	Maps to NFRs
a. Network Vulnerabilities	IIIA
b. Policy Enforcing Tools	IA
c.	IVA
d.	IIID
e. Diverse Zone Requirements	IC
f. Firewall Compatibility	IB
g.	IIID
h. IPv4/6	IA
i. ANYCAST	IA
j. Bind	IA
k.	IIIC
l. Time to Stability	IVB
m. Timeouts	IIIC
n.	IIIA
o.	IVA
p. New Technology	IA
q. Supports Response Re-writing	IA
r. Business Rules Change	IC
s. Dependencies	IIID

Feasibility Issues: II. Economic Issues	Maps to NFRs
a. Large # of Authorized Servers	IIB
b. Outsourcing	IVA
c. Cost (Make/Buy)	IVA

Feasibility Issues: III. Organizational Issues	Maps to NFRs
a.	IIA
b.	IVA
c. Schedule sensitivity	IVB
d. Risk sensitivity	IVB
e. Cost sensitivity	IVB
f. 1.5 FTEs	IC
g.	IC
h.	IIIC
i. Buy-in	IVB

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Map NFRs to Feasibility Weighted

Weighted NFRs

NFRs		Map to Feasibility issues	Feasibility to NFRs	(+5=) Relative Weight
I. Operational Requirements		**Feasibility Issues**	**Occurrences**	
	a. Technical Requirements	IB, IH, II, IJ, IP, IQ	6	11
	b. System Integration	IF, IIIA	2	7
	c. Maintenance	IE, IIF, IIIG, IR	4	9
II. Performance Requirements		**Feasibility Issues**		
	a. Speed		0	5
	b. Capacity	IIA	1	6
	c. Availability/Reliability		0	5
III. Security Requirements		**Feasibility Issues**		
	a. Outside Threats	IA	1	6
	b. System Value		0	5
	c. Access Control	IK, IM, IIH	3	8
	d. Encryption and Authentication	ID, IG, IS	3	8
	e. Virus Control		0	5
	e. Availability/Reliability		0	5
IV. Organizational Requirements (Political/Cultural)		**Feasibility Issues**		
	a. Customization	IC, IO, IIB, IIC, IIIB	5	10
	b. Unstated Norms	IL, IIIC, IIID, IIIE, IIII	5	10

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Matrix Design

- **% Relative Importance (Weight)**
  - Totals represented relative importance (weight) of requirements categories
  - Scaled to 100 percent
  - Each subcategory assigned a value
    - Reflect relative importance of feasibilities mapped to requirements
  - % Relative Importance = Σ sub-categories within a requirement category
- **Scoring**
  - Scoring calculated per alternative
  - Each requirement sub-category assigned a score value based on identified Pros/Cons
  - Score multiplied by associated Weight value produces weighted score (Wtd Score)
    - Wtd Score = Score x Weight
  - Wtd Scores summed per requirement category
    - Subtotal (Wtd Score) = Σ (sub-category) Scores
  - Each alternative receives a Total Score
    - Total score = Σ Sub Total weighted scores
  - Total score produced a Rank position
- **Stakeholder negotiations revise priorities and weight to create final matrix**

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Final Alternatives Matrix

Requirements	Rel wgt	Score (1-5)	Wtd	Score (1-5)	Wtd	Score (1-5)	Wtd	Score (1-5)	Wtd	Score (1-5)	Wtd	Score (1-5)	Wtd	Score (1-5)	Wtd
Operational Reqs	**33**														
Technical Implementation	**11**	4	**44**	3	**33**	3	**33**	5	**55**	5	**55**	3	33	4	**44**
System Integration	**6**	4	**24**	3	**18**	3	**18**	2	**12**	2	**12**	3	18	4	**24**
Maintenance	**9**	1	**9**	1	**9**	1	**9**	1	**9**	2	**18**	3	27	4	**36**
Customization/Unstated Norms	**7**	2.5	**17.5**	3	**21**	2	**14**	2	**14**	3	**21**	3	21		**21**
Sub total (Wtd Score)			**94.5**		**81**		**74**		**90**		**106**		**99**	**3**	**125**
Performance Reqs	**34**														
Speed	**11**	1	**11**	3	**33**	4	**44**	3	**33**	3	**33**	4	44	4	**44**
Capacity	**11**	3	**33**	3	**33**	3	**33**	3	**33**	3	**33**	4	44	5	**55**
Availability & Reliability	**12**	1	**12**	2	**24**	2	**24**	2	**24**	2	**24**	3	36	4	**48**
Sub total (Wtd Score)			**56**		**90**		**101**		**90**		**90**		**124**		**147**
Security Reqs	**33**														
Threat Resilience	**12**	3	**36**	3	**36**	2	**24**	2	**24**	2	**24**	3	36	4	**48**
System Value	**5**	2	**10**	2	**10**	2	**10**	3	**15**	3	**15**	2	10	2	**10**
Access Control	**8**	3	**24**	4	**32**	2	**16**	3	**24**	3	**24**	3	24	3	**24**
Encryption & Authentication	**8**	5	**40**	5	**40**	2	**16**	5	**40**	2	**16**	3	24	2	**16**
Sub total (Wtd Score)			**110**		**118**		**66**		**103**		**79**		**94**		**98**
Total Score			**260.5**		**289**		**241**		**283**		**275**		**317**		**370**
Rank			**6**		**3**		**7**		**4**		**5**		**2**		**1**

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Threat Modeling

- **Risk Analysis is Stage 4 of the SDL**
  - Principal feature is threat modeling
- **Threat modeling contributes to the risk management process**
  - Main output is documentation
  - Describes background information about the application
- **Modeling defines the high-level application model**
  - Often using data flow diagrams
  - A list of assets requiring protection
  - Threats to the system ranked by risk
  - An optional list of mitigations
- **Relevant background information**
  - Use scenarios
  - External dependencies
  - Security assumptions
  - External security notes

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Threat Modeling

- **Considers the trust boundaries of the application**
- **It is an outside-in (adversary's) view**
- **Models all components inside the trust boundary**
- **Modeling process owned by one person on design team**
- **At high level, follows these steps**
  - Prepare
  - Analyze
  - Determine mitigations

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Steps in Threat Modeling

1. Define use scenarios
2. Gather list of external dependencies
3. Define security assumptions
4. Create external security notes
5. Create one or more data flow diagrams of the application being modeled
6. Determine threat types
7. Identify the threats to the system
8. Determine risk
9. Plan mitigations

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Steps 1:4: Threat Modeling

1. **Define use scenarios**
   - Determine which key threat scenarios are within scope
   - Many may not have security implications
   - Use scenarios are not the same as UML use cases
2. **Gather list of external dependencies**
   - Document all code upon which application is dependent
   - Default system-hardening configurations considered here
3. **Define security assumptions**
   - How to maintain security when using application
4. **Create external security notes**
   - Understanding of application security boundaries

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 5: Data Flow Diagrams

- **Create one or more data flow diagrams for the application**
  - Visual representation of how a system processes data
- **Highest-level DFD is the context *diagram***
  - System under development at the center
    - **Complex process** (multiprocess)
      - » Performs many distinct operations
    - **Process**
      - » Performs one discrete task
  - External entities (entry points)
    - These drive the application
    - Cannot be controlled by the application
  - Data representation
    - **Data stores**: persistent storage
    - **Data flows**: how data moves around system (coms, memory, functions)
  - Privilege boundary
    - Concept that is specific to threat modeling
    - Delineate data moving from low to high (and high to low) trust
- **Data flows are associated with a verb or verb/noun**
- **Components are numbered**

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 5: Data Flow Diagrams

- **Decompose the context diagram**
- **Complex processes become processes**
  - Drill down creates Level-0 data flow diagram (DFD)
  - May become more complex, again
    - Identify/uncover additional complex processes
    - Must drill down into these
    - Until no more complex processes exist
- **Generally from 3 to 7-9 processes per DFD**
- **Generally two levels is sufficient depth**

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 6: STRIDE

- **Microsoft uses a threat taxonomy called STRIDE®**
  - **S**poofing Identity
    - Attacker poses as something or somebody else
  - **T**ampering
    - Threats involve malicious modification of data or code
  - **R**epudiation
    - Denial of having performed the action
  - **I**nformation Disclosure
    - Exposure of information to individuals lacking proper access
  - **D**enial of Service
    - Denial or degrading of service to valid users
  - **E**levation of Privilege
    - Gaining access to increased capability
- **Claims to be more complete than CIA**

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 7: Identify Threats to the System

- **After completing the DFD, list all DFD elements in a table**
  - Cross reference DFD element type to DFD item numbers
  - This does not include complex processes
  - Includes processes, data stores and data flows inside the complex process
    - Must also model data flows in and out of a complex process
    - Most data flows are bi-directional
- **Apply a Reduction process**
  - Combine the number of (similar) entities needing analysis
  - Look for multiple DFD elements of the same type
- **Multiple elements existing behind the same trust boundary can be modeled as one entity if:**
  - Elements written in or using the same technology
  - Elements handle similar data
- **Analysis of threats to one element can be applied to the other**
  - Finds its biggest benefit in reduction of data flows

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 7: Reduced DFD elements

Table 1 – Reduced DFD elements	
DFD Element Type	**DFD Item Number**
External Entities	Customer (1.0) Anonymous User (2.0) Administrator (3.0)
Processes	Web app (4.2) User profile (4.5), order processor (4.7.1) Sync/async order processing (4.7.2 &4.7.3) Auditing engine (4.7.9)
Data Stores	Web app configuration data (4.1) Web pages (4.3), Audit log data (4.7.10) Order and async orders data (4.7.6 & 4.7.8)
Data Flows	Web app reading config data (4.1→ 4.2) Anonymous user req/resp (2.0 →4.2 → 2.0)

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 7: STRIDE to DFD element types

- **Once table of reduced DFD elements is complete, apply STRIDE**
  - To each element in table
  - Nature of attack is determined by DFD element type
- **Map STRIDE to DFD Element Types**

Table 2 – STRIDE mapping

DFD Element Type	S	T	R	I	D	E
External Entity	x		x			
Data Flow		x		x	x	
Data Store		x	†	x	x	
Process	x	x	x	x	x	x

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 7: Combine DFD and STRIDE

- **Combine DFD elements and STRIDE mappings**
  - Gather elements from Table 1
  - Determine the threats to which each is susceptible by using Table 2
- **Map Threat Types to DFD item numbers**

Table 3 – Combine DFD elements and STRIDE mappings

DFD Element Type	Threat Types (STRIDE)	DFD Item Numbers
External Entities	SR	(1.0), (2.0), (3.0)
Processes	STRIDE	(4.2), (4.5), (4.7.2 and 4.7.3), (4.7.9), (4.7.1)
Data Stores	T(R)ID	(4.1), (4.3), (4.7.6 and 4.7.8), (4.7.10 – repudiation)
Data Flows	TID	(4.1→ 4.2), (2.0 →4.2 → 2.0)

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 7: Threats to System

- **Reorder Table 3 by Threat Type for potential threats to system**

Table 4 – Threats to System	
Threat Type (STRIDE)	**DFD Item Numbers**
Spoofing	External entities: (1.0), (2.0), (3.0) Processes: (4.2), (4.5), (and 4.7.3), (4.7.9), (4.7.1)
Tampering	Processes: (4.2), (4.5), (4.7.2 and 4.7.3), (4.7.9), (4.7.1) Data stores: (4.1), (4.3), (4.7.6 and 4.7.8), (4.7.10) Data flows: (4.1→ 4.2), (2.0 →4.2 → 2.0)
Repudiation	External entities: (1.0), (2.0), (3.0) Data store: (4.7.10)
Information disclosure	Processes: (4.2), (4.5), (4.7.2 and 4.7.3), (4.7.9), (4.7.1) Data stores: (4.1), (4.3), (4.7.6 and 4.7.8), (4.7.10) Data flows: (4.1→ 4.2), (2.0 →4.2 → 2.0)
Denial of Service (DoS)	Processes: (4.2), (4.5), (4.7.2 and 4.7.3), (4.7.9), (4.7.1) Data stores: (4.1), (4.3), (4.7.6 and 4.7.8), (4.7.10) Data flows: (4.1→ 4.2), (2.0 →4.2 → 2.0)
Elevation of Privilege (EoP)	Processes: (4.2), (4.5), (4.7.2 & 4.7.3), (4.7.9), (4.7.1)

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Steps 8: Determine Risk

- **Historically, DREAD ratings…**
  - **D**amage potential
  - **R**eproducibility
  - **E**xploitability
  - **A**ffected users
  - **D**iscoverability
- **…and risk as a calculation…**
  - Risk = Chance of Attack x Damage Potential
- **…alternately created a bug bar**
  - Defines the characteristics of a threat and level of risk
  - “Risk level” 1 is highest; level 4 is lowest risk using threat tree pattern/analysis

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 9: Plan Mitigations

- **Countering threat with technology is most common strategy**

Table 5 – Mitigation techniques based on STRIDE threat types	
Threat type	**Mitigation Technique**
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation Services
Information Disclosure	Confidentiality
DoS	Availability
EoP	Authorization

- **Determine appropriate mitigation technology**

Table 6 - Abbreviated list of Threats			
Example Asset	**Asset Type**	**Threat Type Susceptibility**	**Example Threat**
4.7.10	Audit log data store	T(R)ID	T
4.7.1	Order processor process	(S)TRIDE	TE

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Step 9: Plan Mitigations

- **Mitigations can then be built into design**
- **Take threat and map it to a mitigation**

Table 7 – Defenses Used in Portions of Example

Asset	Asset Type	Example Threat	Example Mitigation
4.7.10	Audit log data store	T	Access Control List (ACL) and Mandatory Access Control (MAC)
4.7.1	Order processor process	T and E	ACL, MAC, and reduced process privilege

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

Summary

- **Two methodologies with intersections in implementation**
  - Gather and analyze data
  - Define assumptions and map requirements to model potential solutions
- **Used to solve different problems but employ similar techniques**
- **Raises the potential for applying experience gained in one area to the other**
- **At the architectural level**
  - Software systems design and analysis ←→ Software security analysis (threat modeling)
  - Useful in projects that have overlapping requirements in both analysis and security

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.

POCs

- **Julie Taylor, VP/Division Manager**
  - julie.y.taylor@saic.com
  - 410-953-6877
- **Bob Williamson, VP/Business Development**
  - robert.l.williamson.jr@saic.com
  - 410-953-6219 or 703-450-4198
- **Mark Braga, Director of Communications**
  - john.m.braga@saic.com
  - 410-953-6812
- **Keith Beatty, Principal Systems Security Engineer**
  - keith.w.beatty@saic.com
  - 410-953-6858

© 2008 Science Applications International Corporation. All rights reserved. SAIC and the SAIC logo are registered trademarks of Science Applications International Corporation in the U.S. and/or other countries.