Eliciting Software Security Requirements through Misuse Actions

Fabricio Braz

03/07/08

Intro

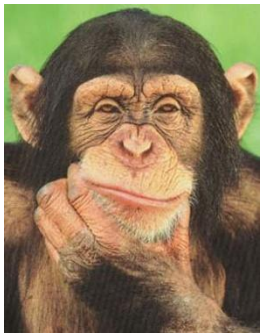
- Software Systems
  - World wide dependency
- Failures consequences
  - Embarrassment
    - “Illegal” affair uncovered
  - Infrastructure harm
    - CIA Confirms Cyber Attack Caused Multi-City Power Outage (01/18/08)
- CERT-CC statistics show hopeless tendency

Security from the beginning

- Experiences' shown about ~~added on security~~ [McGraw06]
- Security as an integral part of lifecycle
  - No single software engineering meth. [Mouratidis06]
  - Software security requirements claim more comprehensive approach [Redwine06]

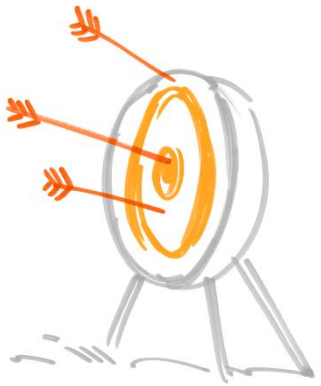
Software Security Requirements (1)

- Wide range from software to software
  - Each system has its particular security goals
    - Authentication, authorization, transaction integrity, logging & auditing …
- Systems fails
  - wrong things are protected correctly
  - right things are protected in the wrong way
- What's important to be protected, and what protection is needed



Software Security Requirements (2)

- Higher system perspective analysis
- What's the attacker goal
  - theft of identity, money …
- Security requirements should define the sec needs without mechanisms commitment
  - Uncovering the potential attack (threat)



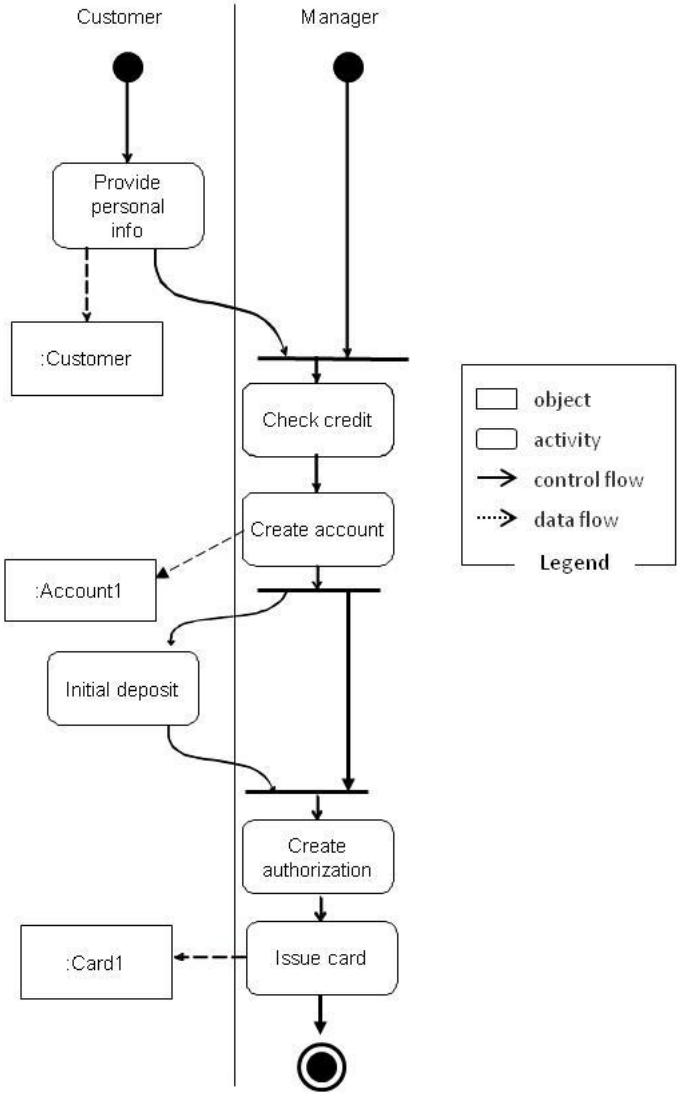
Objective

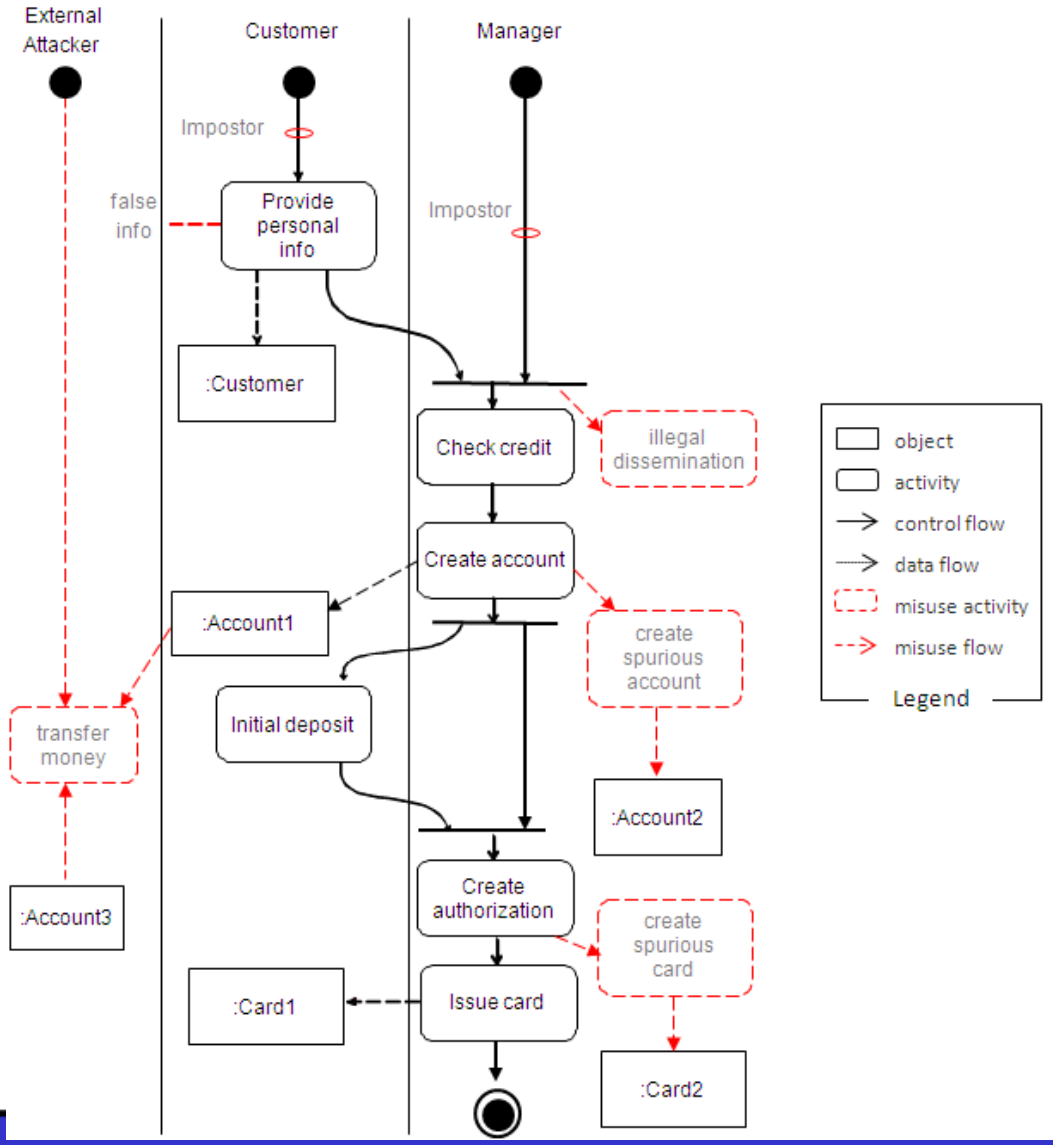
- Evolve the misuse approach in order to
  - give a more systematic way to elicit software security requirements by
    - detailing its dynamics so that analysts can easily uncover threats and select the suitable security policies to mitigate and/or stop them.

Misuse approach (1)

- Systematic way to:
  - identify system threats
    - use case flow of events depicted by activity diagram
    - analysis of each activity in a way to find misuse
  - determining policies to stop/mitigate their effects
    - authentication, logging, separation of duties, closed system, etc. [Fernandez06]

Misuse approach (2)





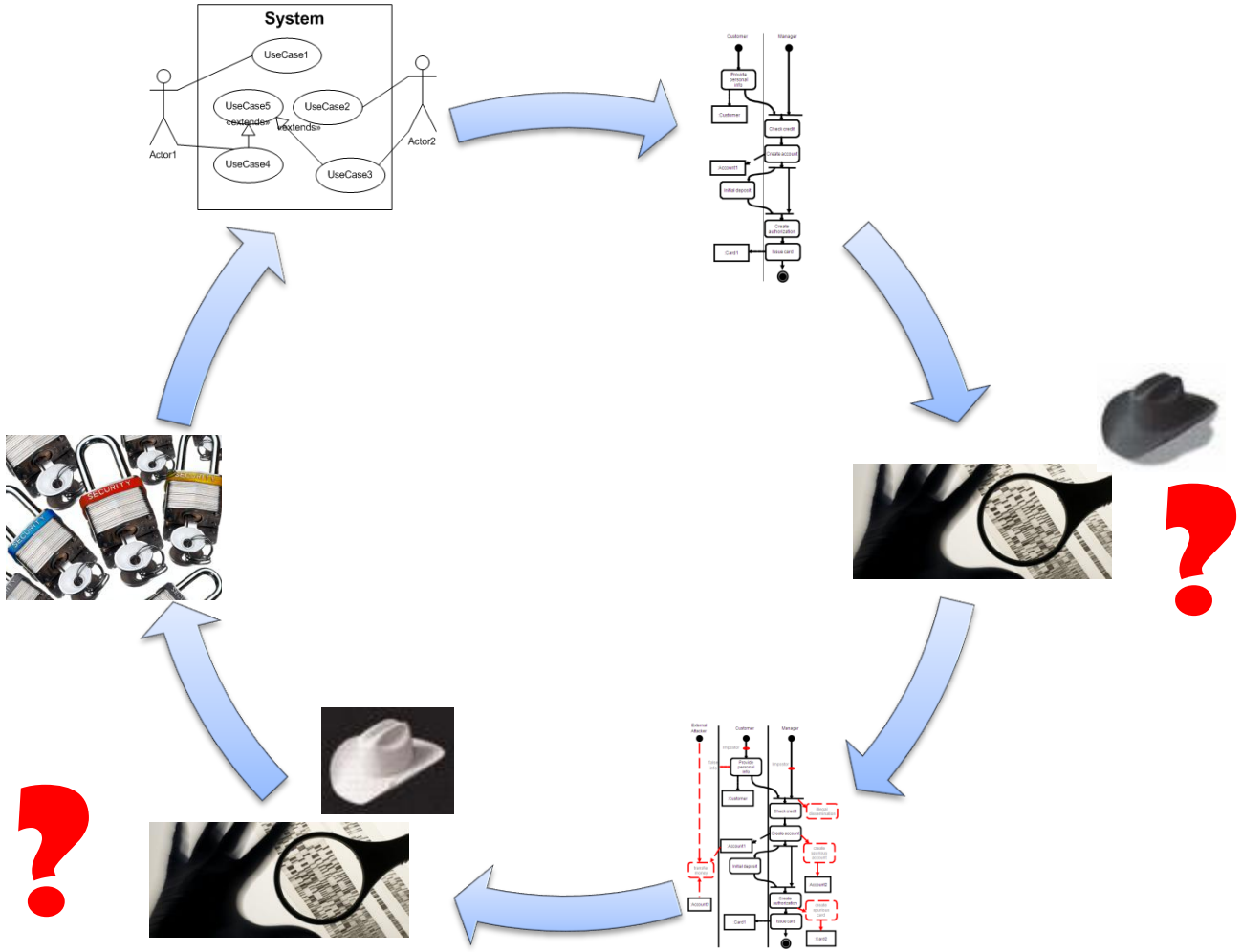
Misuse approach (3)

Threats	Policies
The customer provides false information and opens spurious account	Mutual authentication. Every interaction across system nodes is authenticated
The manager creates a spurious account with the customer's information	Logging. Since the manager is using his legitimate rights we can only log his actions for auditing at a later time
The manager creates a spurious authorization card to access the account.	Separation of administration from use of data. For example, a manager can create accounts but should have no rights to withdraw or deposit money in the account.
An attacker tries to prevent the customers access to their accounts	Protection against denial of service. We need some redundancy in the system to increase its availability.

Misuse approach (4)

- How should the analysis of the activity be employed?
- What is the path between the misuse action and the related system policy or policies?
- What role do high level security policies play?

Misuse Actions Dynamics



System Activities Analysis (1)

- Three levels of systematic
  - Use case
    - Entails all system interactions
  - Source of threat [Cole2005]
    - External
      - Any person without access to org. system
    - Internal authorized
      - Has access to org. system, but not the system/action in consideration
    - Internal unauthorized
      - Has access to org. system, the system/action in consideration included
  - Security concern [Pfleeger2002]
    - Confidentiality, Integrity, Availability, Accountability

System Activities Analysis (2)

- What misuse could be done in <activity> by <source> which compromise <sec propriety>
  - <activity> : find out in the activity diagram
  - <source> : external, internal authorized, internal unauthorized
  - <sec prop.>
    - Conf: snooping, disclosure, eavesdropping
    - Integrity: deception, masquerading, spoofing, usurp
    - Availability: denial of service, disruption
    - Accountability: repudiation

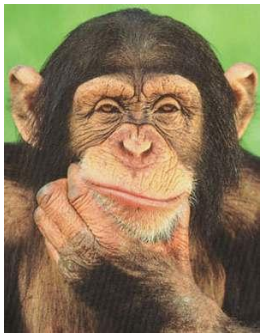
System Activities Analysis (3)

		Misuse			
Actor	Action	Sec. Prop. CO/IN/AV/AC	Source InA/InU/Out	Description	Asset
Customer	Provide Personal Info	AC	InA	Claims did not authorize the account openning	Log
		AV	Out	Overwhelm application	N/A
		CO	Out	Eavesdropping	Customer
		CO	Out	Uncover customer relationship with inst. by trying to create new account in his/her na	Customer
		IN	InA	Invalid financial info provided	Customer
		IN	InA	Personal spurious info provided	Customer
Manager	Check credit	AC	InA	Refuses modification in customer credit info	Log
		AV	InU	Overwhelm application	N/A
		CO	InU	Eavesdropping	Customer
		CO	InA	Collects customer personal info to disseminate illegally	Customer
		IN	InA	Changes the cust. credit info to get more clients	Customer
Manager	Create account	CO	InU	Eavesdropping	Account
		CO	InA	Collects customer personal info to disseminate illegally	Account
		IN	InA	Creates spurious account	Account
		AC	InA	Refuses creating spurious account	Log
Customer	Initial deposit	-	-	-	-
Manager	Create authorization	CO	InA	Create a spurious authorization / card	Card
Manager	Issue card	AV	InA	Do not issue card	Card

Legenda: CO - Confidentiality; IN - Integrity; AV - Availability; AC - Accountability; Out - Outsider; InA - Insider Authorized; InUThreat; H - High; M: Medium; L: Low

How to select the security policies? coming soon

- Would the threat details uncovered help?
  - <source> + <sec property> leads <policy>
- Would be interesting to apply a preliminary risk analysis?
  - Find out relevant threats which really deserve deep analysis , e. g. attack tree
- What else?



Security Requirements Area Overview

- Misuse case
  - Alexander,
- Threat modeling
  - Lipner
- Problem frames
  - Heisel, Haley
- SQUARE
  - Mead
- CEPAC
  - Attack patterns – McGraw (Cigital)

References so far

[1] I. Alexander. Misuse cases: Use cases with hostile intent. *IEEE Software*, 20(1):58–66, 2003.

[2] R. J. Anderson. *Security Engineering - A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, USA, 2001.

[3] S. Barman. *Writing Information Security Policies*. SAMS, Indianapolis, 2001.

[4] CERT Coordination Center. Carnegie Mellon University. Full statistics, Jan 2008. http://www.cert.org/stats/fullstats.html/.

[5] E. Cole and S. Ring. *Insider threat: protecting the eterprise from sabotage, spying, and theft*. Syngress, 1 edition, 2005.

[6] E. B. Fernandez, M. VanHilst, M. M. L. Petrie, and S. Huang. Defining security requirements through misuse actions. In S. F. Ochoa and G.-C. Roman, editors, *Advanced Software Engineering: Expanding the Frontiers of Software Technology*, volume 219 of *IFIP International Federation for Information Processing*, pages 123–137. Springer Boston, November 2006.

[7] D. Gollmann. *Computer security*. John Wiley & Sons, Inc., New York, NY, USA, 2a edition, 2005.

[8] D. Hatebur, M. Heisel, and H. Schmidt. Analysis and component-based realization of security requirements. In *Proceedings of the International Conference on Availability, Reliability and Security (AReS)*, IEEE Transactions. IEEE, 2008. To be published.

[9] M. G. Jaatun and I. A. Tndel. Covering your assets in software engineering. To appear in IEEE CS in the ARES 2008 proceedings.

[10] G. McGraw. *Software Security: Building Security In*. Addison Wesley Professional, January 23 2006.

[11] H. Mouratidis and P. Giorgini. A methodology to develop secure systems using patterns. In H. Mouratidis and P. Giorgini, editors, *Integrating security and software engineering: Advances and future vision*, chapter I, pages 1–14. Idea Group, Hershey, Pennsylvania, USA, 2006.

[12] C. P. Pfleeger. *Security in Computer*. Prentice Hall, 2002.

[13] S. T. Redwine. Software assurance - a guide to the common body of knowledge to produce, acquire, and sustain secure software. Technical Report Version 1.1, Workforce Education and Training Working Group - US Departments of Homeland Security and Defense, September 2006.

[14] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad. *Security Patterns Integrating Security and Systems Engineering*. John Wiley & Sons Ltd, 2006.

[15] M. Shaheen. The homeland security market essential dynamics and trends, November 2006.

[16] G. Sindre and L. Opdahl. Eliciting security requirements with misuse cases. *Requir. Eng.*, 10(1):34–44, 2005.

[17] F. Swiderski and W. Snyder. *Threat Modeling*. Microsoft Press, July 2004.

[18] I. A. Tøndel, M. G. Jaatun, and P. H. Meland. Security requirements for the rest of us: A survey. *IEEE Software*, 25(1):20–27, 2008.

Thanks’

- Happy international women’s day (march 8th)