SECURE360 conference

JOHN BENNINGHOFF AND KARL BROPHEY

BEHAVIORAL SECURITY MODELING

TUESDAY 1:15 PM

WELCOME TO SECURE360 2012

- Did you remember to scan your badge for CPE Credits? Ask your Room Volunteer for assistance.

- Please complete the Session Survey front and back (this is Room 5), and leave on your seat.
  - Note: "Session" is Tuesday or Wednesday

- Are you tweeting? #Sec360 @transvasive

SECURE360 WORLD RUN/WALK

THANKS!

Behavioral Security Modeling

Eliminating Vulnerabilities by Building Predictable Systems

TRANSVASIVE

Transparent and Pervasive Security

Behavioral Information Security

What is BIS?

Behavioral Security Modeling

a method for describing security requirements using BIS principles

Security Requirements Gap

Traditional Requirements

- Security Architecture
- Non-Functional
- Threats
- Exploits
- Defense in Depth
- Misuse Cases

Well-covered in current articles

“Keep the bad guys from messing with our stuff.”

Functional Requirements

- Business Controls
- Functional
- Least-Privilege
- Abuse
- Quality
- Constraints

Missing from current articles

“What are the good guys allowed to do?”

Functional requirements for robust and secure information systems must define all human/ information interactions permitted by the system.

Approach

- Engage non-technical stakeholders for:
  - Constraints
  - Effect of Constraints
  - Security Actions
  - Post Conditions
- Focus on quality of requirements
- SDLC agnostic

Constraints

Security Constraints are defined as:

Placing limits on interactions between Actors and Objects through defined Actions in information systems

Constraints

- Social
- Information
- Location
- Temporal
- Input

Method

- Opening Questions
- Clarifying Questions
- Uncovering Hidden Constraints
- Patterns

Social Constraints

Defined by “Who you are”

Opening Question:

- “What teams need access to this function to do their jobs?”

Social Constraints

Clarifying Questions:

- *Overly specific requirements (a single person):* "What is it about Alice's job that makes it appropriate for her to have access?"
- *Socially ambiguous roles: "*Do you mean all employees and contractors, or just all employees?"

Social Constraints

Hidden constraints:

- *Exceptions:* “Does everyone on this team need access to this function? What about (specific example)?”
- *Consider usage by external groups: “*Are partners / teams outside of the organization who need access to the function?”

Social Constraints

- Advice: Develop a Social Group Catalog

- Role-Based Access Requirements Pattern
- “Everyone” Anti-Pattern
- Deny Access To… Anti-Pattern

Information Constraints

Defined by “What the information is”

Opening Questions:

- “Can this Action be applied to all data?”
- “Do all users have access to the same data?”

Information Constraints

Clarifying Questions:

- *Identifying social-only restrictions:* "Are people on this team allowed (or disallowed) from accessing this data with just one function, or all functions?"

Information Constraints

- Advice: If you can't avoid combining Action, Object, and Actor into a single constraint, generalize

- Role Based Data Access Requirements Pattern
- "My Data" Pattern

Location and Temporal Constraints

Location: Defined by “Where you are”

Temporal: Defined by “When”

Input Constraints

- Blur the lines between security and quality
- Limits on the direct and indirect input values to an Action
- Limits executing Actions on Objects based on values of Objects provided as inputs to the Action

Go Path and No-Go Path

- Requirements generally define the “Go Path” (Happy Path)
- Constraints must define the “No-Go Path”
- No-Go Path isn’t always “Access Denied”
- Don’t incent users to circumvent controls

Improving Requirements

- Prioritize
- Generalize
- Remove Ambiguity
- Reuse

Security Actions

Functional Requirements must include:

- User Account Management Actions
- User Permissions Management Actions
- End User Security Actions

Post Conditions

- A statement of what must be true when an action is complete
- A sort of formalized hygiene
- Use when potential for integrity issues

Behavioral Security Modeling – What's Next?

- White Paper, now on http://transvasive.com/!
- Field testing: If you're interested, please let us know!
- *Patterns Website (Wiki)*
- *Training, Tools, Extend approach later into the development lifecycle*

Thank You!

John Benninghoff
john@transvasive.com
http://transvasive.com/
Twitter: @transvasive

Karl Brophey
karl@brophey.net

TRANSVASIVE
Transparent and Pervasive Security

BROPHEY CONSULTING
Bridging Technology and Business Strategy