Functional Security Requirements

Building Predictable Systems using Behavioral Security Modeling
“[T]here are known knowns; there are things we know that we know. There are known unknowns; that is to say there are things that, we now know we don't know. But there are also unknown unknowns – there are things we do not know we don't know.” – United States Secretary of Defense, Donald Rumsfeld
“I don’t care about security.”
“I just set up this new folder, and want to give everyone access”

Everyone...

• on my team?
• in IT?
• in the company?
• who is able to access this directory, even anonymously?
Security Requirements Gap

**Traditional Requirements**
- Security Architecture
- Non-Functional
- Threats
- Exploits
- Defense in Depth
- Misuse Cases
- Known Unknowns

Well-covered in current literature

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

**Functional Requirements**
- Business Controls
- Functional
- Least-Privilege
- Abuse
- Quality
- Constraints
- Unknown Unknowns

Missing from current literature

“What are the good guys allowed to do?”
Behavioral Security Modeling

a method for describing and organizing security requirements
Functional requirements for robust and secure information systems must define all human/information interactions permitted by the system.
BSM Approach

- **Constraints**
- Checklist of Questions
- Requirement Patterns
- Go-Path and No-Go Path
BSM Approach

- **Constraints**
- Checklist of Questions
- Requirement Patterns
- Go-Path and No-Go Path

- Social
- Information
- Location
- Temporal
- Input
BSM Approach

- Constraints
- **Checklist of Questions**
- Requirement Patterns
- Go-Path and No-Go Path
BSM Approach

• Constraints
• Checklist of Questions
• **Requirement Patterns**
• Go-Path and No-Go Path
BSM Approach

- Constraints
- Checklist of Questions
- Requirement Patterns
- Go-Path and No-Go Path
Example: Broker Financial

Broker -> Associate -> Clients

Broker -> Associate -> Clients

Operations

Broker -> Clients

Broker -> Clients

Example: Broker Financial

- New Financial Services Firm
- Web-based books & records system
- Broker, Associate, Operations
- Two Offices
- Alternate Universe
Example: Broker Financial

Social Constraints

• Role-Based Access: Broker, Associate, Operations

• Attribute-Based Access: Licensing (Trading Functions for Associates, Brokers)

• No-Go Path: Trading
Example: Broker Financial

Information Constraints

- Role Based Data Access (Clients)
- Dual Controls (Checks)
- “My Data” (Clients)
- No-Go Path: Clients
Example: Broker Financial

Location and Temporal Constraints

- On-Premise Only (Operations)
- During Business Hours (Trading Functions)
- No-Go Path: Trading
Example: Broker Financial

Input Constraints

• Role-Based Transaction Limits (Trading Limits)
• Input Validation (many)
• No-Go Path: Trading
Behavioral Security Modeling – What’s Next?

- Field testing: If you’re interested, please let us know!
- Question Checklist (summary, one-page)
- 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 Brophrey  
karl@brophey.net