Application Security Kung-Fu
Competitive Advantage from Threat Modeling

Akshay Aggarwal
Practice Manager (North America & LATAM)
Akshaya AT Microsoft Dot com
ACE Team
Microsoft Information Security
Agenda

- Background
- Information Security (InfoSec) challenges
- Driving security into development
- Threat Modeling
- Bringing it all together
- Conclusion
Trend of Security Breaches
WHAT ASSETS DOES YOUR ORG CARE ABOUT?
Scenario
Business as Usual

Information Security Truths: Tracking Risk
InfoSec Challenges – Where’s the Data

- Outourced 3rd Party
- In Transit
- In databases
- In spreadsheets
- Through Web applications
- On my Laptop
- On my Phone
- On a network share

Microsoft | Information Security
Process Complexities

Data Classification

Industry Regulation

Shadow Process/Apps

Risk Management
InfoSec Priority

- Valuable data must be protected
- Global regulations must be followed
- The business must remain enabled
IS THERE A PROCESS DRIVING APPLICATION SECURITY?
Driving Security Into Development

Software Development Lifecycle
- Envision
- Design
- Develop
- Test
- Release

IT Security Development Lifecycle
- App Entry/Risk Assessment
- Threat Modeling
- Internal Review
- Pre-Production Assessment
- Post-Production Assessment

- Catalog & Classify
- Identify Controls
- Implement Controls
- Verify Controls
- Monitor Controls

- TAM Enterprise
- CAT.NET
- SPIDER
- Stingray
DO YOU ANALYZE YOUR THREATS?
HOW?
ACE Security

PROCESS

What is Microsoft Application Threat Modeling?

http://go.microsoft.com/fwlink?linkid=77002
Threat Modeling

- The process of proactive identification and enumeration of threats to an application

Activities and Role Participation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ This activity primarily focuses on creating the security architecture of the system</td>
<td>▪ Threat modeling allows system security personnel to communicate the potential damage of security flaws and prioritize remediation efforts</td>
<td>▪ A security design review aims to find any gaps in the design of an application from a secure by design prospective</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Architects</td>
<td>100%</td>
</tr>
<tr>
<td>Business Owners</td>
<td>10%</td>
</tr>
<tr>
<td>System Architects</td>
<td>30%</td>
</tr>
<tr>
<td>Developers</td>
<td>30%</td>
</tr>
<tr>
<td>Security Experts</td>
<td>20%</td>
</tr>
<tr>
<td>Testers</td>
<td>10%</td>
</tr>
</tbody>
</table>
Kung Fu 1: Proactive Security

**Purpose**
- Proactive approaches save $$ & time

**Reason**
- Design flaws identified early in lifecycle
- Focus on business rules rather than technical implementation

**Advantages of TM**
- Build security into plan rather than being reactive

**Example**
- Evaluating feature set at ISV
Kung Fu 2: Due Diligence

**Purpose**
- Compliance is among top CSO/CIO priorities
- Corporate security spend maps to compliance concerns

**Reason**
- No one wants to set the precedence for non-compliance
- Most tangibly quantifiable downside

**Advantages of TM**
- Documented security plan
- Ahead of the curve

**Example**
- Hospital CISO demonstrated due diligence to board after attack
Kung Fu 3: Competitive Differentiator

**Purpose**
- Security becoming increasingly relevant in competitive situations

**Reason**
- Clients want solution secure by design
- Reduce risk profile from app portfolio

**Advantages of TM**
- Demonstrate sophistication of approach
- Clearly documented roadmap & standards

**Example**
- Utility RFP process re-engineered to evaluate vendor security maturity
Kung Fu 4: Security Process Agility

Purpose
- Security comes from incremental changes
- Most organizations struggle with setting a security mindset

Reason
- Culture change is difficult
- Standards and best practices keep changing
- Education is difficult and has lag

Advantages of TM
- Changes to best practice can percolate down
- Teams have just in time info

Example
- Microsoft IT Business Units use TM to drive change
ACE Services


http://blogs.msdn.com/ace_team
Lessons Learned
Microsoft Solution Offerings
Consulting offerings

• Application Security
  – Security Code Reviews
  – Enterprise Threat Modeling
  – Security Guidance Development
  – Application Security Program development

• Infrastructure Services
  – Technical Compliance Management using TCM tool
  – PKI, ISA, RMS security architecture/deployments

• Performance Services
  – Application Performance Testing
  – Building Performance Test Frameworks
  – Active Performance Monitoring
Conclusion
What did we talk about?

Proactive Security
Security Process Agility
Due Diligence
Competitive Differentiator
Contact

How do I find out more?

• Contact info for Microsoft ACE Services
  acesvc@microsoft.com

• Talk to your Microsoft Technical Account Manager or Services Executive

• Akshay blogs at:
  http://blogs.msdn.com/akshay_aggarwal
  http://noFUD.org