

# Product Risk Assessment



## Traditional Microsoft Software Product Development Lifecycle Tasks and Processes



# Product Risk Assessment

- What portions of the project will require ...
  - threat models before release
  - security design reviews
  - penetration testing
  - Fuzz testing



- Security Risk Assessment
- Privacy Impact Rating

# Security Risk Assessment

---

- Setup Questions
  - Which operating systems?
  - Does setup require an Admin password?
- Attack Surface Questions
  - Is your feature installed by default? Why?
- Mobile-Code Questions
- Security Feature-Related Questions
- General Questions
  - Does your application parse files?

Product Risk Assessment

# Security Questionnaire

## Risk Assessment Document

Version 3.1, April 7th, 2006

(Howard and Lipner 2006)

Review Info	
Date questionnaire was filled out:	
Names of people who filled out this questionnaire:	
Who is the primary security contact in your team?	
Component/Product Info	
Component Name:	
Ship vehicle(s):	
Where is your source code?	
Where is your bug database?	
Where are your threat models?	
What OS platforms do you support?	<input type="checkbox"/> Win2000, <input type="checkbox"/> Windows XP, <input type="checkbox"/> Windows Vista, <input type="checkbox"/> Mac, <input type="checkbox"/> *nix, <input type="checkbox"/> Windows CE, <input type="checkbox"/> Other:
Does your application run on down-level platforms?	<input type="checkbox"/> Yes, <input type="checkbox"/> No
General Security	
Does your component work differently in a multi-user terminal services environment?	<input type="checkbox"/> Yes, <input type="checkbox"/> No Explain:
Does your component require the user to be an administrator??	<input type="checkbox"/> Yes, <input type="checkbox"/> No, <input type="checkbox"/> N/A
Do you ship any sample code	<input type="checkbox"/> Yes, <input type="checkbox"/> No
What standard Windows services is your feature dependant on?	<input type="checkbox"/> Don't know, Dependant on:
Do you ship components that take code drops from outside your team?	<input type="checkbox"/> Yes, <input type="checkbox"/> No

# Analyzing the Questionnaire

---

- Need threat model if ...
  - App has a networking interface
  - App has kernel-mode and user-mode interactions
  - Non-Admin interact with higher-privileged process
  - App is a security feature
- If this is a new product, it will require a thorough security design review
- Sample code must meet shipping code quality standards => SDL requirements
- If App parses files or network traffic => fuzzing

Product Risk Assessment

## **Anonymous Data**

Any user data that is not unique or tied to a specific person and cannot be traced back to the person.

This data might include hair color, system configuration, method by which a product was purchased (retail, online, ...), or usage statistics distilled from a large collection of user.

## **Personally identifiable information (PII)**

- Any user data that uniquely identifies a user such as contact information (name, address, phone number, e-mail address, ...)
- Data that is commingled or correlated with the user's PII, for example, demographics stored with the user's PII or with a unique ID that can be linked to the user's PII
- Data that is sensitive PII

## **Sensitive PII (1)**

- Any user data that identifies an individual and could facilitate identity theft or fraud. This data includes social security numbers, tax IDs, credit card numbers, and bank account numbers.
- Data that is commingled or correlated with PII and used as an authorization key, such as password and PINs (personal identification numbers), biometric information (when used to authenticate), mother's maiden name, and so on.

## **Sensitive PII (2)**

- Data that is commingled or correlated with PII and could be used to discriminate, such as sexual preference or sexual lifestyle, political or religious beliefs, ethnicity or race, or trade union membership.
- Data that is commingled or correlated with PII and contains medical history or health records or financial information.
- Data that has breadth and contents that are unknown at the time of collection and could hold sensitive PII; e.g. raw memory dump.

## Privacy Ranking 1

- The application stores PII or transfers PII to the software developer or a third party.
- The application is targeted at children or could be deemed attractive to children.
- The application continuously monitors the user of your application.
- The application installs new software or changes the user's file-type associations, home page, or search page.

## **Privacy Ranking 2**

- If the application transfers anonymous data to the software developer or to a third party.

## **Privacy Ranking 3**

- If the application is not Ranking 1 or 2

# Readings

---

(Howard and Lipner 2006) Howard, Michael, and Steve Lipner. The Security Development LIFECYCLE. Redmond, WA: Microsoft Press, 2006.