

Getting Vulnerabilities Out of Software

Mark Pustilnik
Security Development Lead
Secure Windows Initiative Attack Team
Microsoft
(also a UW PMP alumnus)



Introductions

- Who am I and what do I do?
- A few words about the Secure Windows Initiative team at Microsoft
- <http://www.eweek.com/article2/0,1895,1879502,00.asp>
- What is behind Microsoft's turnaround in security?



Ongoing Process

- Conception – avoid the impossible
- Design – catches *bad bugs*
- Implementation – more prescriptive
- Support – addresses things you miss and emerging threats



Conception

- Case study: DRM solutions
 - What do you expect DRM to do?
 - What are the challenges?
 - Messaging: promises vs. delivery
 - What can realistically be delivered?



Design

- It's all about *security guarantees*
- Case study: security guarantees of on-line backup software



Implementation

- Cookbook analysis (if design is solid)
- Case study: Aren't you glad you authenticated?



Support

- Organizational structure (people)
- Platform support (technology)
- Customer Expectations (management)

