



IBM Software Group

Security Evaluation and Assurance Lessons from Business, Marketing, and HCI

Mary Ellen Zurko, IBM Software Group
Lotus Security Architecture and Strategy
mzurko@us.ibm.com

Lotus software



@business on demand software

A Bit About Lotus Products

- Collaborative application security
 - ▶ Notes/Domino, Portal, Workplace
 - ▶ Enterprise customers
 - ▶ Lots of end user interaction
 - ▶ Internationally geographically distributed development organization
- IBM Lotus Workplace going for EAL2
 - ▶ Email, Calendar, Contacts
 - ▶ Discussion DB, Document management, Web conferences
 - ▶ Learning
 - ▶ No PP
- Web and Java infrastructure
 - ▶ Web edition and Rich client edition user interfaces
 - ▶ Layered on other products from across the company
 - ▶ The top of the infrastructure stack



Cost effective security activities at Lotus

- Architectural involvement from the very beginning
- Checklist at design time coupled with
- Expert review and consultation
- On call expertise for all levels of security (architectural, design, code, configuration, test)
 - ▶ Encourages distributed engagement and responsibility
- Knowledgeable and engaged vulnerability testing and ethical hacking
- Coupled with experts in past and current vulnerabilities
- Point person for (any) vulnerabilities discovered after release



Lessons from Business

- Measure against the real goal
 - ▶ And measure in a way anyone can understand
 - ▶ Create future goals based on measurements

- Measurements for increased security
- Number of vulnerabilities discovered by the CC process
- % of CC evaluated products with a CERT advisory in the last 12 months
 - ▶ Versus the general population of products
- Checklist of Security Function areas covered in an evaluation
 - ▶ In natural language, not FPR_ANO

- Measurements for CC itself
- % of products in the X market with a CC evaluation
 - ▶ % at each assurance level
- % of machines running at least one product with a CC evaluation



Lessons from Marketing

- Increases demand where it counts – where the money is
- Turns it into table stakes – must have on the checklist
- Increases the demand which promotes the development and use
- Predicated on having something to market in the first place
 - ▶ Measurement is important
- “Got Milk?”
- “Michelin: Because so much is riding on your tires.”



Lessons from Human Computer Interaction

- Usability testing of secure deployment configuration
- Early usability testing of PC installations highlighted obvious difficulties
 - ▶ Inserting floppies into random gaps in the front of the machine
- Measure how much of the security configuration was achieved
- And how long it took
- Pressure to make secured deployments intuitive and default
- Encourages automated solutions like “security wizards”

