Application Security

Mike Smith

26/04/10 - Rev.12

Attacks

- Smurf (ICMP)
- Fraggle (UDP)
- SYN - TCP ACK
- DoS
- D-DoS
- Teardrop

Patch Management

1. Infrastructure
2. Research
3. Assess and Test
4. Mitigation - Rollback
5. Deployment - Rollout
6. Validation, Reporting and Logging

Malware

- Worm - replicates without a host
- Virus - needs an application
- Rootkit
- Botnets, RATs, Logic Bomb
- Trogan Horses
- Mobile Code / Java Applets / ActiveX Controls
- Insertion - Avoidance - Eradication - Replication - Trigger - Payload

Distributed Computing

- CORBA
- COM / DCOM - GUID
- SOAP
- EJB
- DCE - UUID

OLTP - ACID

- Atomicity - divide transactions into units of work
- Consistency - follow integrity policy
- Isolation - execute in isolation
- Durable - Once verified, committed on all systems

Capability Maturity Model - CMM I Regularly Drink My Orangejuice

- 1 - Initial
- 2 - Repeatable
- 3 - Defined
- 4 - Managed
- 5 - Optimizing

Database Models

- Relational
  - row = tuple
  - column = attribute
- Hierarchical
- Network
- Object Orientated
- Object Relational

DBMS

- Must implement access controls
- Caution against data inferencing
- Data definition language - DDL
- Data manipulation language - DML
- Query language - QL
- Report generator
- Views
- Aggregation - combining information
- Inference - deduce the full story

Interfaces

- Open Database Connectivity - ODBC
- Object Linking and Embedding - OLE DB
- Java Database Connectivity - JDBC

OOP

- Benefits of OOP
  - Modularity - Autonomous objects and cooperation through messages
  - Deferred Commitment - Internals of objects can be changed independently
  - Reusability - reuse objects from other programs
  - Naturalness - maps to business processes
- OOA - Process of classifying objects
- OOD - Create a representation of the real-world problem
- Polyinstantiation
  - Multiple copies from the same class
  - Government or military used to hide covert operations

SDLC

- I/LDAP/SDx2/II/OM/D
- Initiation
- Fuctional Design Analysis and Planning
- System Design
- Software Development
  - Verification - meets spec?
  - Validation - meets project goal?
- Installation/Implementation
- Operational/Maintenance
- Disposal

SDLC Methodologies

- Waterfall
- Spiral
- Joint Analysis Development - JAD
- Rapid Application Development - RAD
- Cleanroom
- Iterative
- Reuse
- Extreme