Architecting Secure Enterprise

Jayashree Kar, Program Director

February 27, 2007

IMAGINATION ACTION JOY

Agenda

- Security – Few Trends & Projections
- Enterprise Security - Various Aspects
- Case Studies
- Conclusions
- Q&A

About MindTree

- Global Presence
  - USA — New Jersey; Santa Clara; Chicago; Denver; D.C.; Miami
  - Europe — London; Frankfurt; Sweden; Switzerland
  - Australia — Sydney
  - Asia & Middle East — Tokyo; Singapore; Dubai
  - India — Bangalore; Hyderabad; Chennai
- CMMi Level 5 and P-CMM Level 5 — Youngest company in the world to achieve both milestones
- Employees — 4,000+
- Most consistent performer in "Best Employer" surveys — 2004 & 2005

Security – Trends & Projections

- Worldwide security software revenue will increase from $7.4 billion in 2005 to about $12 billion in 2010

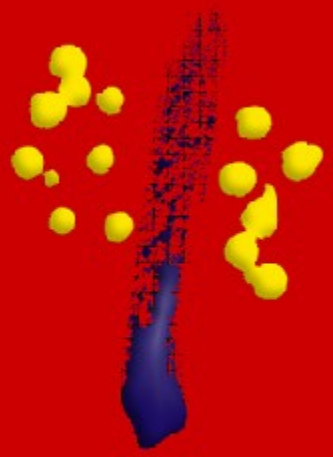
  Source : 21st Sep, 2006, Gartner Reports

- According to research by Gartner and Symantec, close to 90 percent of software attacks are aimed at the application layer

  Source :http://www.adtmag.com/article.aspx?id=18708

- As per a study conducted by Microsoft and Compuware, 66% of security attacks are at Network level, 22% is at application level, 11% are at database level.

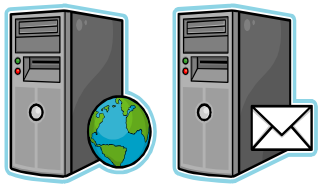
  Source : http://assets.devx.com/extensibility/17879.pdf



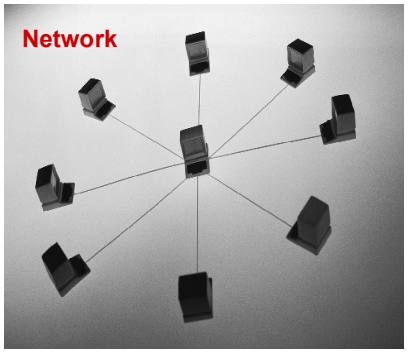
Enterprise Security
- Various Aspects

Typical Enterprise

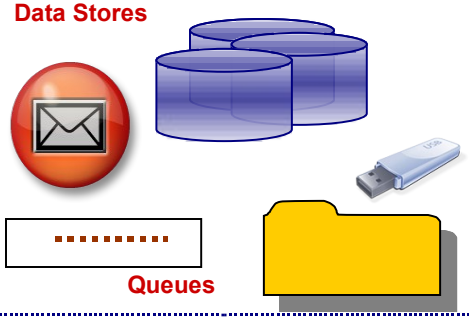
Servers



Network

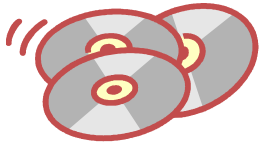


Data Stores



Queues

Applications



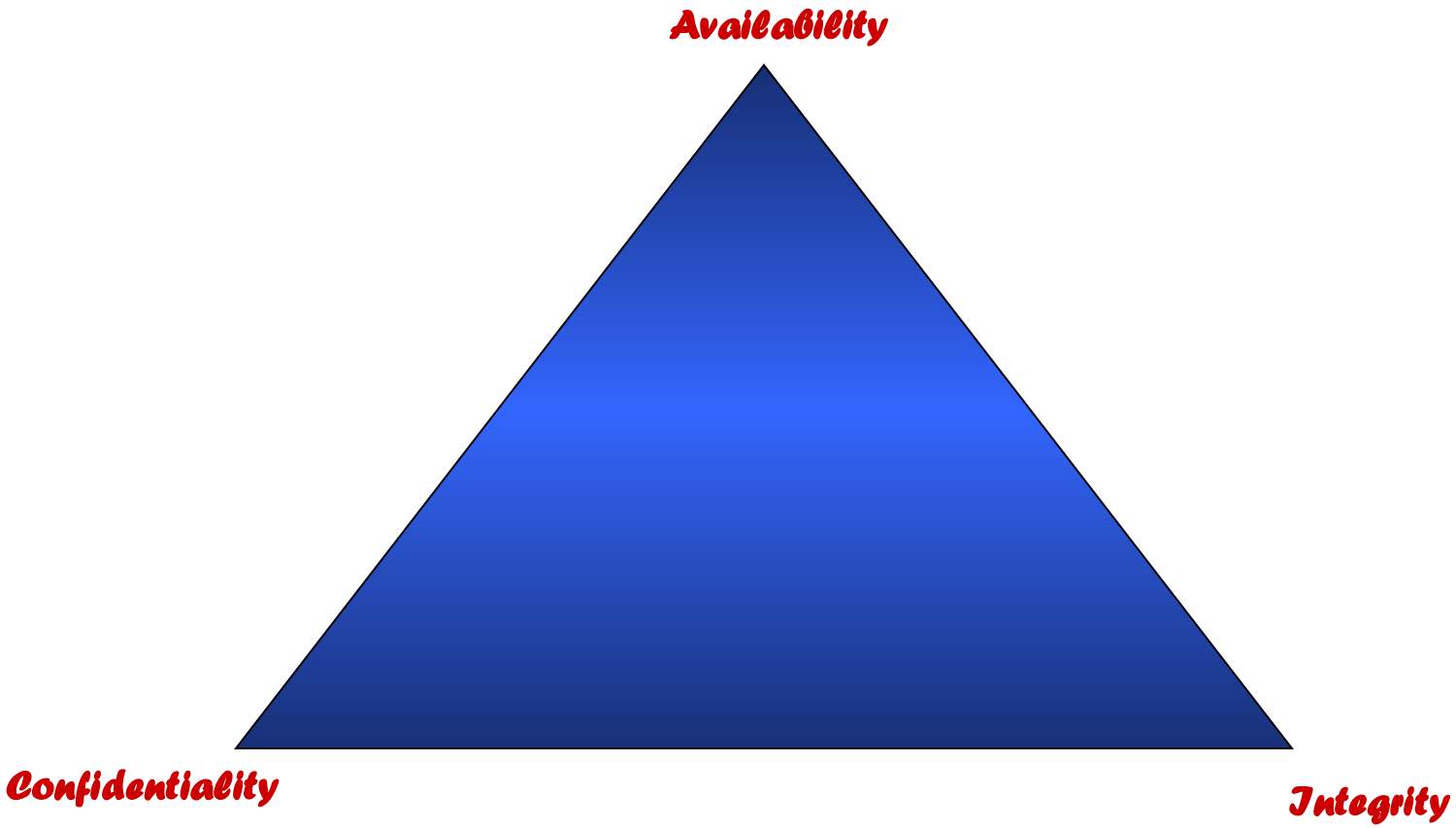
End-Users

Devices

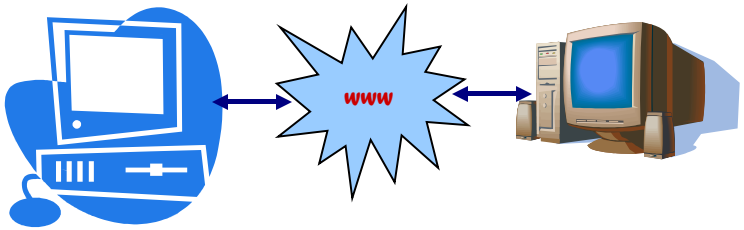
Physical Data

Business Partners

Security Areas

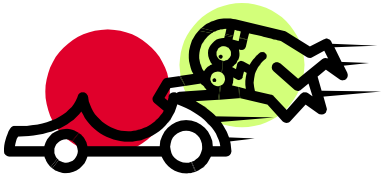


Why the Threat?



Exposure to Public network

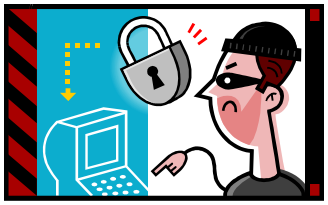
Lack of awareness



Speed to Market

Regulatory compliance Requirements

Sources of Threats



Script Kiddies, Accidental Hackers

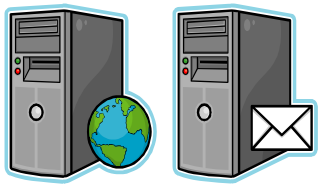
Professional Hackers

Spies

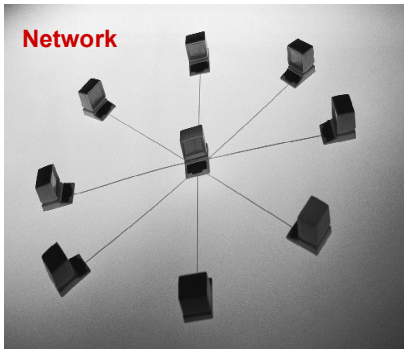
Disgruntled Insiders

Enterprise Security Areas

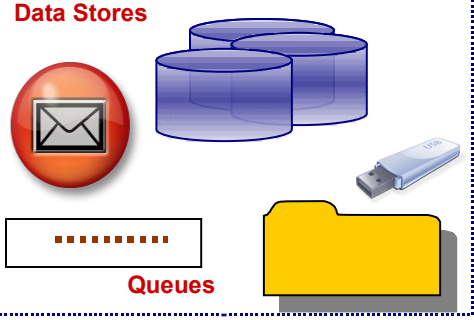
Servers



Network

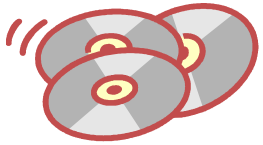


Data Stores



Queues

Applications



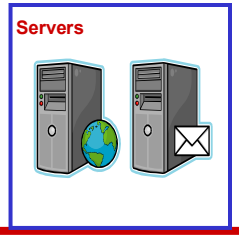
End-Users

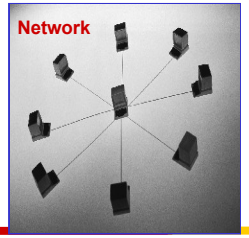
Devices

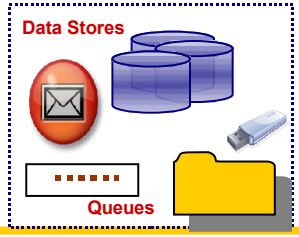
Physical Data

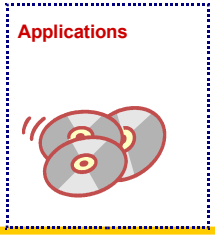
Business Partners

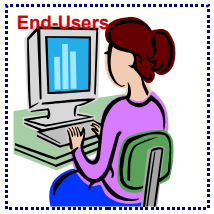
Server Security

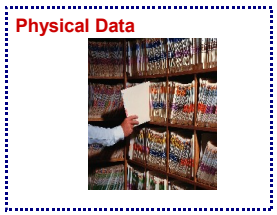








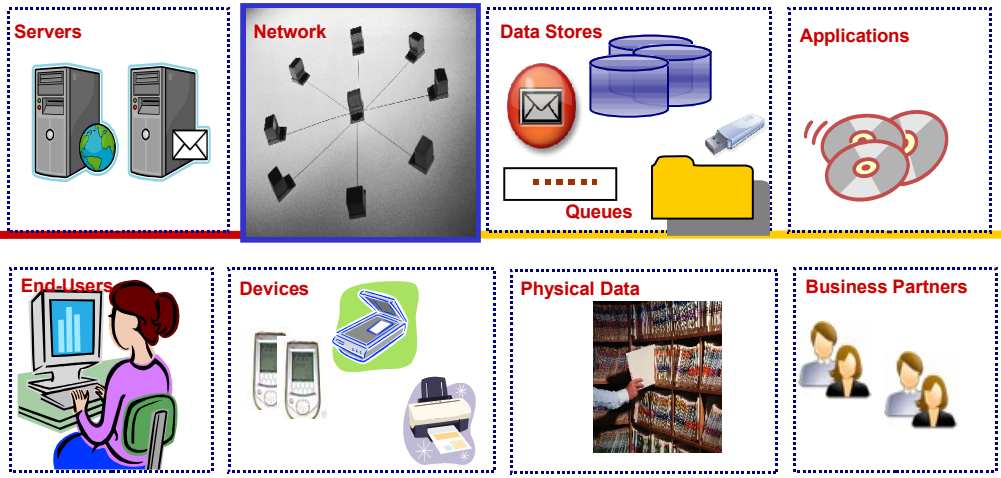




- Vulnerabilities
  - Backdoors
  - Expired Certificates
  - Broken Authentication
  - DoS and DDoS - Distributed Denial of Service
  - Domain Hijacking

- Solutions
  - Strong Policy & Governance
  - Vulnerability Assessments
  - Audit and Alert mechanism

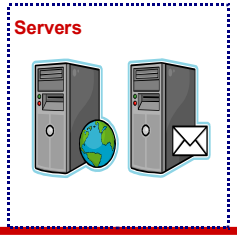
Network Security

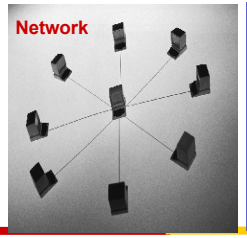


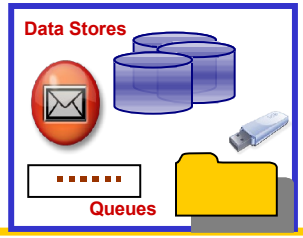
- Vulnerabilities
  - Unblocked Ports
  - Intrusion Prevention Failure
  - Spoofing
  - Sniffing
  - Eavesdropping
  - MITM - Man in the Middle

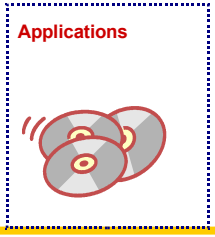
- Solutions
  - Firewall, DMZ, Proxy, VPN
  - MAC ACL
  - DHCP – dynamic host conf protocol
  - Traffic Analysis
  - Data Encryption
  - Hot Swappable Cards
  - Audit and Alert mechanism

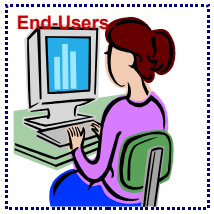
Data Store

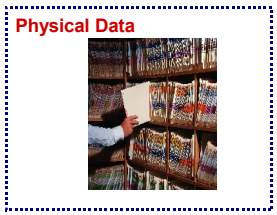








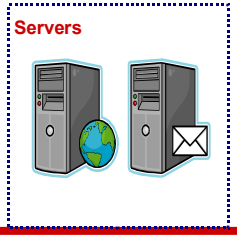


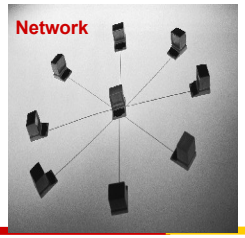


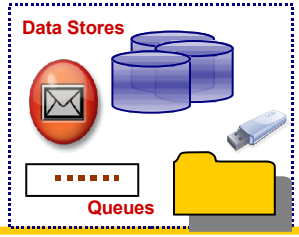
- Vulnerabilities
  - Exposure of
    - User data
    - Configuration data
    - Data in Store
    - Audit and Error Logs
  - Privacy violation

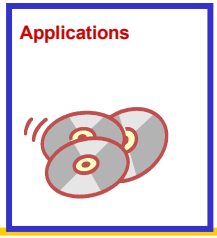
- Solutions
  - Data level authentication & authorization
  - Views and synonyms
  - Encryption
  - Replication and Mirroring
  - Audits and Alerts

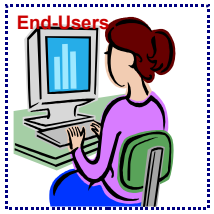
Application Security

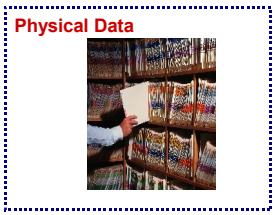








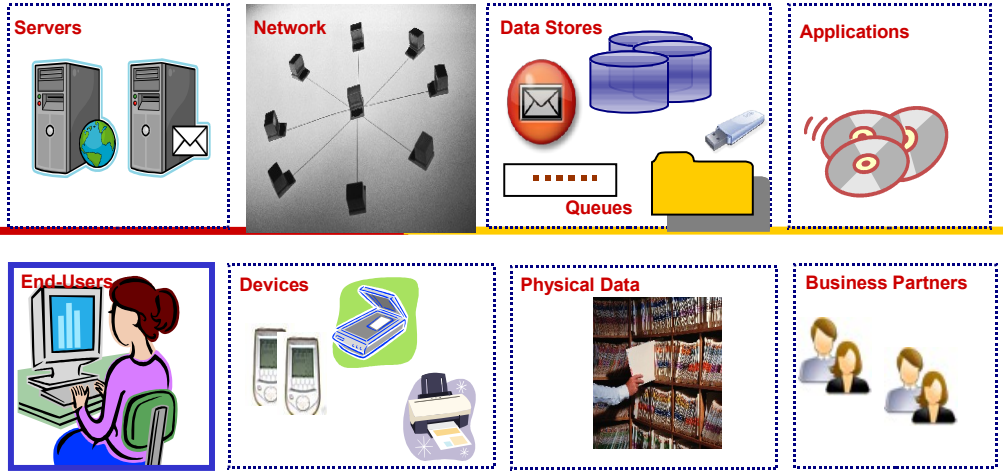




- Vulnerabilities
  - Injections
  - Hijacking
  - Buffer Overflow
  - Cross Site Scripting- XSS
  - Null Byte Attack
  - Race Conditions
  - Improper Error Handling
  - Broken authentication & authorization

- Solutions
  - Partitioning
  - Validation
  - Authentication and Authorization
  - Checklists and Standards
  - Code Scanning
  - Audit and Alerts
  - Awareness Programs

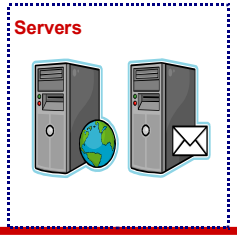
End Users

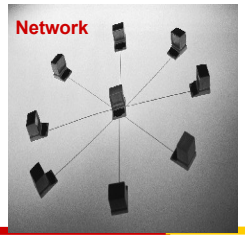


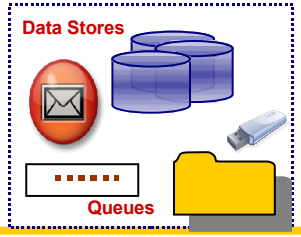
- Vulnerabilities
  - Worms, viruses
  - Trojans
  - Social Engineering

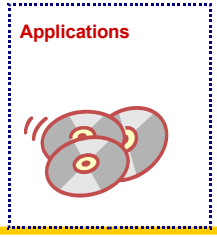
- Solutions
  - Automatic Patch Administration
  - Site Blocking
  - Awareness Programs

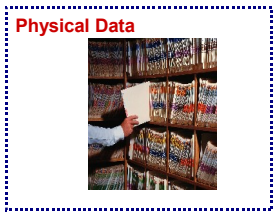
Devices







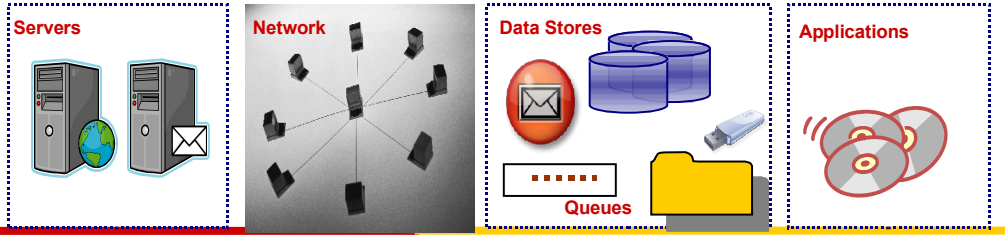




- Vulnerabilities
  - Theft
  - Viruses
  - DoS – denial of service
  - Improper Configuration

- Solutions
  - Regular Patch Updates
  - Remote Monitoring and Management
  - Proper configuration, secure authorization
  - Frequent Backups
  - Periodic Assessment
  - Track new threats & vulnerabilities
  - Security Training

Physical Data

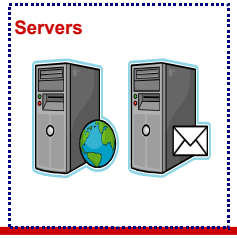


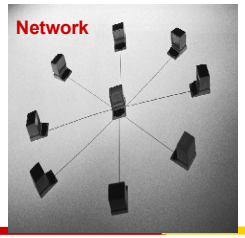
- Vulnerabilities
  - Unwanted Exposure
  - Accidents

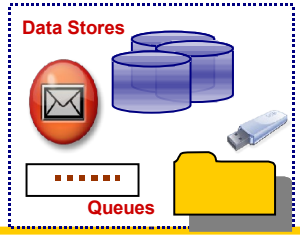
Solutions

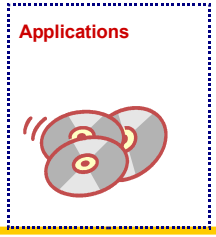
- Data Archival Mechanisms
- Data Destruction Policies

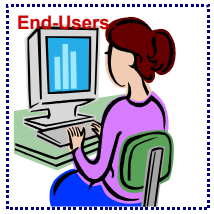
Partner Channel

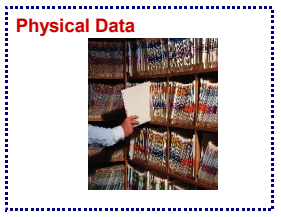








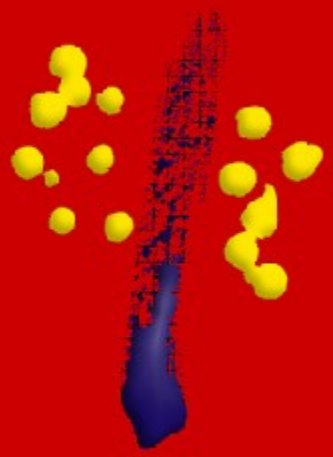




- Vulnerabilities
  - Authentication
  - Privacy violation
  - Authorization violation
  - Data tampering

Solutions

- SSL/TLS
- XML Digital Signatures, XML Encryption
- XACML - Extensible Access Control Markup Language
- SAML
- WS-Security
- ebXML Messaging Service (ebMS)
- Liberty Alliance Project

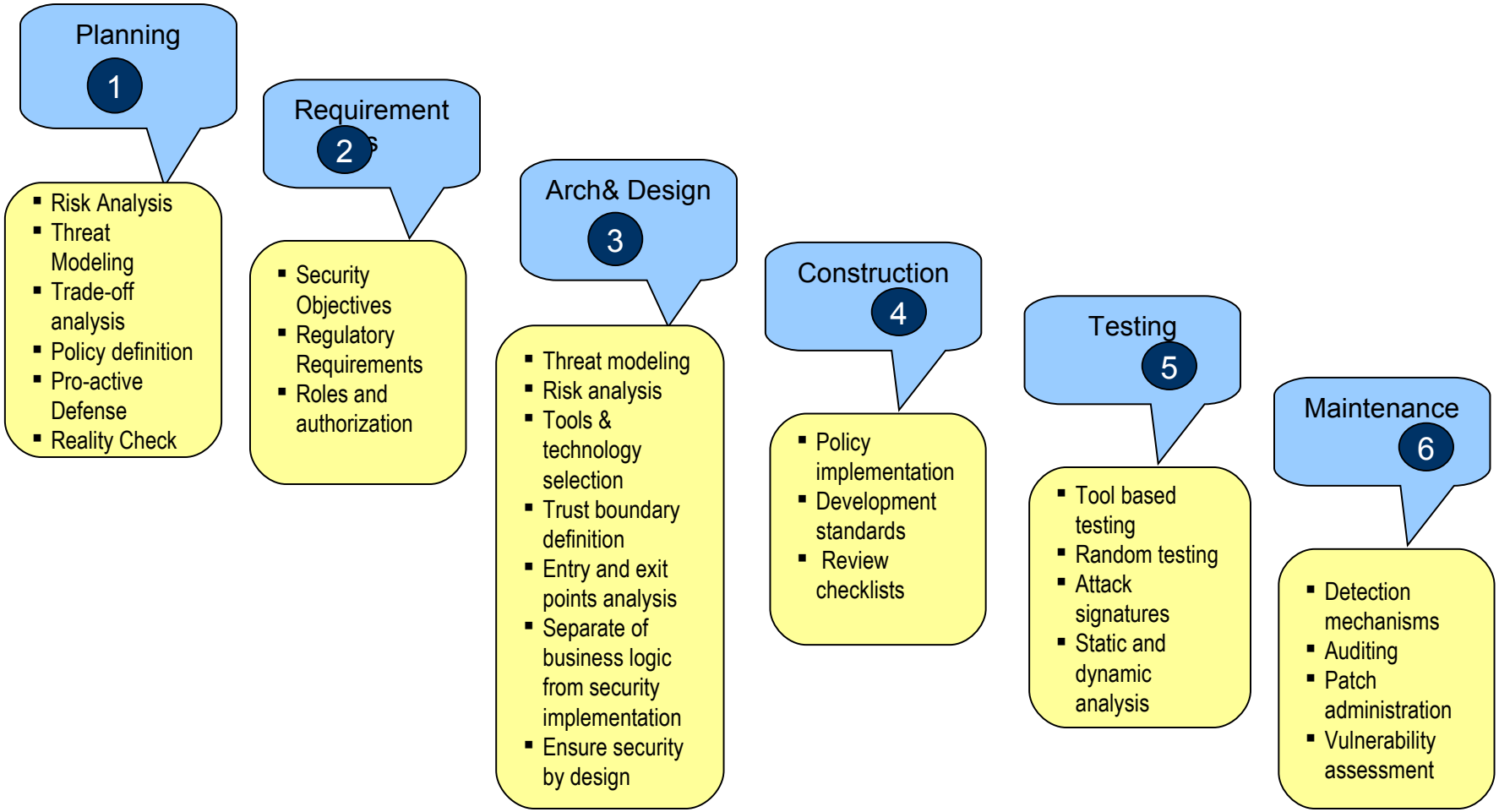


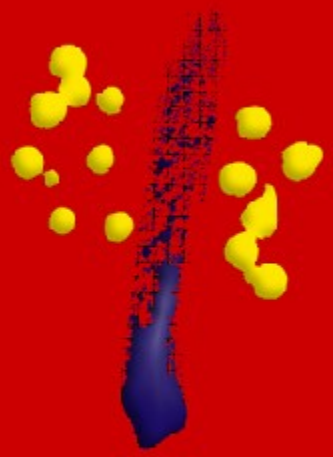
Security in SDLC

Security is not a Product; but a Process

-Bruce Schneier

Security in SDLC





Few Rules for Securing Enterprise

Few Rules for Securing Enterprises

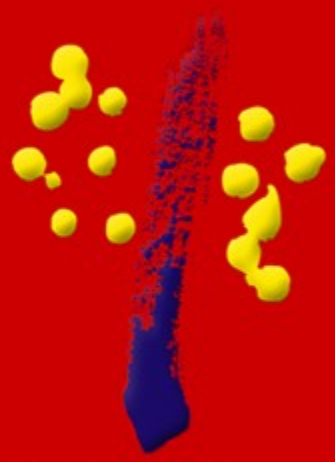
- Don't underestimate the IQ of Hackers
- Understand your Assets, Threats and Risks
- Define the Secure Boundary of the Enterprise
- Understand the Entry and Exit points
- Analyze Input Sources

Few Rules for Securing Enterprises

- Avoid Un-Proven components
- Establish proper Encryption level
- Use White listing vs. Black listing
- Deploy strong Authentication & Authorization
- Use Least Privilege Principle

Few Rules for Securing Enterprises

- Remain vigilant for new threats and vulnerabilities
- Strive for "Defense in Depth"
- Don't ignore any vulnerability for long
- Think like a Hacker
- Don't spend a million bucks to save a dime



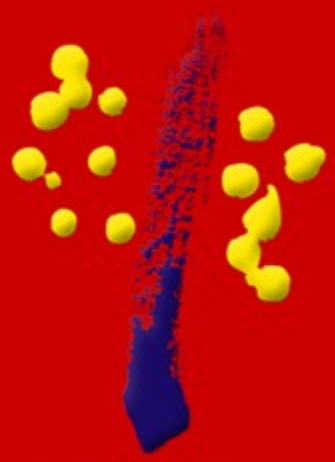
Case Study

Case Study – Secure Project Space, MindTree

- Project Description
  - Used as a sharing platform for projects
- Customer (s)
  - MindTree and MindTree's customers
- Statistics
  - Used by 75+ projects
  - DR Site with backup- can be recovered within minutes
- Server
  - OS-hardening
  - Automatic patch administration
- Network
  - Firewall, proxies
- Data At Rest
  - Cryptography
- Application
  - Authentication, fine grained authorization, auditing, monitoring and alerts

Case Study – Large Insurance ODC

- Project Description
  - Several web applications for internal staffs as well customers and partners
- Customer
  - Large Insurance company in North America
- Statistics
  - Security policy
  - Two DR sites in different regions with hot backups
- Server
  - OS-hardening
  - Automatic patch administration
- Network
  - DMZ, SSL
- Data at Rest
  - Cryptography, views, protected file systems
- Application
  - Authentication, fine grained authorization, security enforced by design, code review, auditing, monitoring and alerts, SSO
- End Users
  - Installation through images
  - Regular Awareness Programs



Conclusions

Conclusions

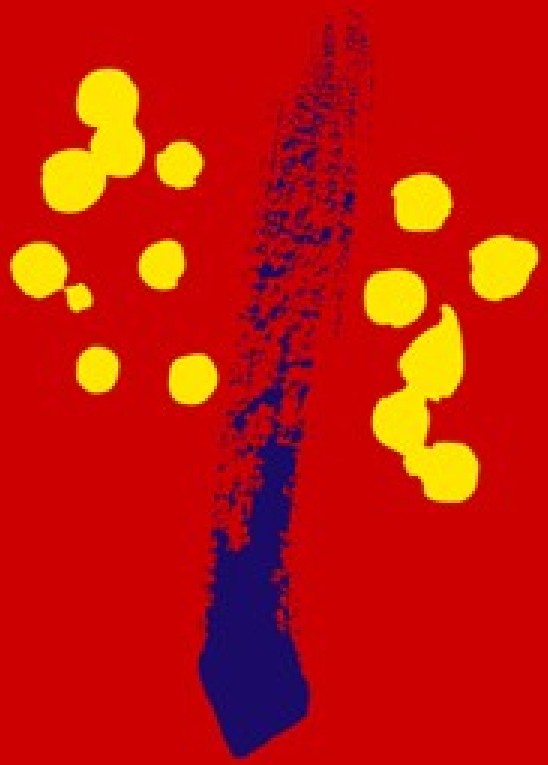
- Don’t underestimate the IQ of hackers
- Security is not a product, but a process
- Social Engineering is a huge threat to security
- You can’t manage things effectively if you can’t measure its efficiency
- Don’t spend a million to save a dime

References & Further Study

- http://searchsecurity.techtarget.com/originalC
- http://secunia.com/multiple_browsers_windo
- Innocent Code by
  - Sverre H. Huseby

Q&A

Contact: Jayashree_kar@mindtree.com



MindTree

CONSULTING