Application Security Trends & Challenges

Mano Paul
CISSP, MCAD, MCSD, CompTIA Network+, ECSA
Software Assurance Advisor, (ISC)²®

mpaul@isc2.org
www.isc2.org
August 2008
<table>
<thead>
<tr>
<th><strong>(ISC)²</strong></th>
<th><strong>Mano Paul</strong></th>
</tr>
</thead>
</table>
| • International Information Systems Security Certification Consortium  
• Established in 1989 as a global not-for-profit leadership organization with nearly 60K members in 135 countries  
• ANSI accredited Gold Standard credentials  
• BoD – Top InfoSec Professionals; tracking the evolving InfoSec workforce. | • (ISC)²’s Software Assurance Advisor  
• ISSA – Industry Representative  
• Founded SecuRisk Solutions, Express Certifications and AppSentinel  
• Invited Speaker @ OWASP, CSI, Catalyst, TRISC, SC World Congress  
• Shark Biologist, Bahamas  
• InfoSec Program Manager – Dell Inc.  
• Contributing Author  
  – Security PnP for MSDN  
  – InfoSec Management Handbook  
  – InfoSec Management Top 10 |
You start coding, I’ll go find out what they want!

-Analyst to Programmer

2b||!2B S3cur3
• Access and Connectivity
• Cornucopia of polymorphic Threats / Hacker Motivations
• Architecture – DNA to SOA; now WOA
• Mobile Computing and Vanishing Perimeters
• Governance, Regulations, Compliance & Privacy Initiatives
• Rich Internet Applications (RIA) – Desktop on the Web

Port 80/443 – The Weakest Link
<Challenges>

- Iron Triangle Constraints
  - Scope (Functionality), Schedules (Deadlines), & Budget (Resources)
  - Bolt-On Vs. Built-In / Afterthought vs. Brainwashed State
- Security viewed as non-functional and an Impediment (not an enabler)
- Attacker’s Advantage vs. Defender’s Dilemma
- Onus on Development Teams, not Security Teams
- Ubiquitous Wild Wild Web (www)
- The Enemy Within
Let’s create that Culture
Thank YOU
Chak De India
Security

(ISC)²

SECURITY TRANSCENDS TECHNOLOGY™