Manoranjan Paul
!= Marijuana Paul
Entertainment Paul
Entertainment + Education == Enlightenment
Entertainment - Education ==

Main Entry: joker [joh-ker] ? Show IPA

Part of Speech: noun

Definition: person who kids, teases

Synonyms: actor, banana, buffoon, card*, clown, comedian, comic, cutup, droll, farceur, fool, funster, gagster, humorist, jester, jokesmith, jokester, josh, kidder, life of the party, prankster, punster, quipster, second banana, stand-up comic, stooge, straight person, top banana, trickster, wag, wisecracker, wit

* = informal/non-formal usage
wise
cracker
wise
is wise
Christian
“L33t”
“L4m3”
After 2 near death calls

Christian
Teach Security
Teach Christ
Teach Security in Christ
Advisor

Software Assurance
And a few more

- MCAD
- MCSD
- ECSA
- CompTIA Network +
SecuRisk Solutions

Training
Products
Consulting

SecuRisk Solutions Framework

PROGRAM INSTRUCTOR CBT CERTIFICATION CURRICULUM DEVELOPMENT

AWARENESS TRAINING EDUCATION

SMART Learning Framework PRODUCTS

SECURITY SOFTWARE CONSULTING

*SMART - Skills Measuring Assessment Reinforced Training

Express Certifications
Certification Practice Tests
CISSP
CSSLP
SSCP
CAP
Hackers hit

“What’s been taken is bits of data that the
right put together into an identity.”

ZU 0666 '0, 0); DROP DATABASE TABLE;

CSRF
‘dash4rk’
2nd Degree Brown Belt
Black Belt
My son once asked me “Dada, Are I Famous?”
S. OFFICIALS THAT IF ISRAEL DECIDES TO LAUNCH A PRE-EMPTIVE STRIKE AGAINST IRANIAN NUCLEAR FACILITIES.
NOT ME

PLAYBOY

STEPHEN KING, TOM McGuane,
WILLIAM F. BUCKLEY, JR.,
LEONARD MICHAELS, LARRY
L. KING, D. KEITH MANO,
PAAU ERDMAN, G. GORDON
Liddy, EDDIE MURPHY.

Censored

Censored

So who am I?
Love my Savior,
Love my Spouse,
Love my Sons,
Love Shaolin,
Love Sharks,
Love Security
Mano ‘dash4rk’ Paul
The 7 Qualities of Highly Secure Software
Disclaimer

• !Pimp my book talk
  ◦ One time on a flight … someone asked me
    • What is this book about?
    • Is it any good?
  
• All opinions expressed are my own and not reflective of my employer …. Wait a minute!

• Tweet/Facebook/Blogs … permission?
What we ...

- Produce
  - Insecure (Hackable) Software
- Need
  - Highly Secure Software
What is this talk about?

- Not about
  - 7 things I need to put in my code (software)
- About
  - 7 things you should take into account when
    - Designing
    - Developing
    - Deploying
    - Software.
- Technical – Operations – Management focused
7 Myths to bust

• #1 – We have a firewall
• #2 – We use SSL
• #3 – We have IDS/IPS
• #4 – We are not be accessible from the Internet
• #5 – We have never been compromised
• #6 – Security is “Not my job”
• #7 – Security adds little/no business value
What is Highly Secure Software?

- Hacker-proof
- 3Rs of Software Assurance (Trust)
  - Reliable
  - Resilient
  - Recoverable
007 …

- #1 – Security is Built In, Not Bolted On
- #2 – Functionality Maps to a Security Plan
- #3 – Includes Foundational Assurance Elements
- #4 – Is Balanced
- #5 – Incorporates Security Requirements
- #6 – Is Developed Collaboratively
- #7 – Is Adaptable
#1 – Security is Built In, Not Bolted On

- The Ant and the Grasshopper
- Be proactive not reactive
- Be strategic and not just tactical (Tool centric)
Security Development Lifecycle

- Rotation/Archival
- Secure Disposal
- Training
- Lessons Learned
- Security Requirements
- Security Plan
- Attack Surface Eval.
- Threat Modeling
- Security Arch. Review
- Secure Coding
- Static Analysis
- Dynamic Analysis
- Assurance Testing
- C&A
- Release
- Secure Installation
- V&V.
- Continuous Monitoring
- Design
- Implementation
- Testing
- C&A
- Continuous Monitoring
- Secure Disposal

Building Security In

- MOM in Cybercrime
  - Motive ? Hacker Motivations
  - Opportunities < Reduced Attack Surface
  - Means < Controls to Mitigate

- Security Processes and Implementing Controls

- Integrated with the SDLC
  - Requirements to Release … is there more?
#2 – Functionality Maps to a Security Plan

- Breaking the Tape
- Begin with the End in Mind
  - How “secure” is your software going to be?
- Functionality $\leftrightarrow$ Controls in Security Plan
Security Plan

- Framework for ‘Assurance’ Foundation
- Failing to plan = planning to Fail
- Overview of applicable security requirements
  - External (GRC+P)
  - Internal (Policies/Standards)
- Controls
  - Safeguards / Countermeasures
  - Technical (System) / Operational (People) / Management (Risk based)
Mapped Software

• Functionality: Each user must have an unique account for interacting with the software.
• Controls: Unique usernames and passwords
• Security Requirements: Remove test and default accounts before release (PCI DSS 6.3.1)
• Threat: Impersonation and Repudiation
#3 – Includes Foundational Assurance Elements

- What lies beneath?
- Put first things first
First things First

CONFIDENTIALITY  INTEGRITY  AVAILABILITY

AUTHENTICATION  AUTHORIZATION  AUDITING
#4 – Is Balanced

- The Clown Fish and the Anemone
- Think Win/Win

Balancing what?

- Risk and Reward
  - Security Lingo (ROI)
- Functionality and Assurance
  - Iron Triangle Triple Constraints
  - “It is a real trade off. You always want the functionality and you always know you are providing opportunities so you need to take that into account and try to build in additional security every time. It is a race”

Richard ‘Dickie’ George
Technical Director, NSA
### Balancing what (contd.)

#### Threats and Controls

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Threat</th>
<th>Control(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overflow</td>
<td>strlen &lt;= bytesize, safe APIs ...</td>
</tr>
<tr>
<td>2</td>
<td>Injection Flaws</td>
<td>Parameterized Queries, Validate input ...</td>
</tr>
<tr>
<td>3</td>
<td>XSS</td>
<td>Response Encoding, Validate Request ...</td>
</tr>
<tr>
<td>4</td>
<td>CSRF</td>
<td>Session specific tokens, POST vs. GET ...</td>
</tr>
<tr>
<td>5</td>
<td>DoS</td>
<td>Load Balancing, Replication ...</td>
</tr>
<tr>
<td>6</td>
<td>Repudiation</td>
<td>Logging, Code signing ...</td>
</tr>
<tr>
<td>7</td>
<td>Reversing</td>
<td>Obfuscation, IsDebuggerPresent API</td>
</tr>
</tbody>
</table>
#5 – Incorporates Security Requirements

- Lost in translation
  - Send reinforcements, we’re going to advance.
  - Send three and four pence, we’re going to a dance.
- Seek First to understand, then to be understood
Security Requirements

External
- Regulations & Compliance
  - SOX
  - HIPAA
  - GLBA
  - FISMA
- Industry Standards
  - ISO
  - NIST
  - PCI
  - OASIS
- Privacy
  - COPPA

Internal
- Company Governance
- Business Functionality

Data Classification
Subject-Object Matrix
Use / Abuse Case Modeling

#6 – Is Collaboratively Developed

- There is no ‘I’ in Team
- Synergize
Whose viewpoint?

Highly Secure Software
#7 – Is Adaptable

- The shark is a Polyphyodont
- Sharpen the Saw
Adaptable Software

• Law of resiliency degradation
• Adaptable to
  ◦ Technology
  ◦ Threats
  ◦ Talents
• Begin with the Future in mind
  ◦ Predictive not just proactive
More information Questions?

Book Signing
Contact!

If You (Liked the presentation ||
Did not like the presentation ||
Need Encore(other) presentation for your company ||
Have Security Program Development Consulting Needs ||
Have Security Product Development/Evaluations Needs ||
Have Awareness, Training & Education Needs ||
Have Certification Needs)
{
    Contact me;
}
else
{
    Have a great day!
}
finally
{
    Thankyou();
    BuildHighlySecureSoftware();

    LinkedIn
    Facebook
    Twitter (@manopaul)

    Email
    mano(dot)paul(at)securisksolutions(dot)com
    mano(dot)paul(at)expresscertifications(dot)com