Wild Wild Wild
(WWW)
Security Planet

Manoranjan (Mano) Paul
CSSLP, CISSP, AMBCI, ECSA, MCSD, MCAD, CompTIA Network+
</Who am I? – The ABCDs>

- Author
  - Official (ISC)^2 Guide to the CSSLP^CM
  - Information Security Management Handbook
- Advisor - Software Assurance, (ISC)^2
- Biologist (Shark)
- Christian - Hidden Treasures Blog
- CEO - SecuRisk Solutions & Express Certifications
- Dell - Application Security Program Engineer/Manager
- dash4rk - SharkTalk™ podcaster
</Who I am NOT? – Seriously>
</What I do?>

- SecuRisk Solutions
  - Education
  - Consulting
  - Products

- Express Certifications
  - Self Assessments / Practice Exams
    - CISSP (2007)
    - SSCP (2007)
    - BCI Certificate (2009)
    - CSSLP (2010)
    - CAP (2010)

Copyright 2007-2010. SecuRisk Solutions
</A Wild + Wonderful World>
</Shakespearean Security>

- All the World’s a Stage  (As you like It)
- The ides of …  (Julius Caesar)
  - Digital Pearl Harbor
- Method in the Madness (Hamlet)

What is the Question?

2B || !2B
Secure
It's a jungle out there

“... organisms keep themselves safe in a world that's every bit as unpredictable as our world”

Raphael Sagarin
Author of Natural Security
Ignoring known vulnerabilities in your software is akin to sticking your head in the sand …

Accept, Transfer, Mitigate, or Avoid Risk.
</Sharks and Candirus>

- External – Attacks from the outside
- Sharks

- Internal – Something Fishy Inside
- Candiru (Parasitic)
</Sleeping NOT so beauty>

- Lungfish aestivation

As the water level falls lungfish burrow into the bottom mud to form a cocoon and aestivate through the dry season.

- Logic Bombs
<Sharks at Sea and on Land>

**Sharks**
- Sharp teeth
- Cartilaginous body
  - Flexibility
  - Muscular efficiency
- Attack
  - Weaker organisms
- Picky eaters
- Deadly consequences

**Hackers**
- Sharp skills
- No backbone
  - Adaptive
  - Path of least resistance
- Attack
  - Vulnerable organizations
- Selective
- Deadly consequences

Copyright 2007-2010. SecuRisk Solutions
Have you seen a school of sharks?
- Sharks are usually asocial in nature, although some sharks are observed to be in schools.

Hackers
- Psychologically prefer individuality, independence and anonymity (nicknames)
- With a strong need to belong to a larger social group
- Cyber-criminals and cyber-terrorists are organized.
<Attack behavior>

- Sharks
  - Pattern: Circles prey before moving in
  - Motive: Usually unintentional

- Hackers
  - Pattern: Reconnaissance activities
  - Motive: Usually intentional
<Attack Patterns: Recon to Root>

- **Probe** (Reconnaissance)
  - Mining
  - Scanning
  - Fingerprinting
  - Social Networking

- **Penetrate**
  - Bruteforceing
  - Overflow
  - Injection

- **Persist**

- **Propagate**

- **Paralyze (r00t)**
  - Rootkits
  - cmd prompt access
The Top 5 most dangerous sharks>

- **5 - Shortfin Mako Shark**
  - Fastest Shark – you can’t out-swim it

- **4 - Oceanic Whitetip Shark**
  - Opportunists – 1st at a shipwreck site

- **3 - Tiger Shark**
  - Garbage collectors of the sea

- **2 - Bull Shark**

- **1 - Great White Shark**

Which among the top 5 poses the greatest threat to humans?
The MOST dangerous hacker

- The one who can operate in different environments
  - Network
    - Understands perimeter defenses, operations and circumvention techniques
  - Hosts
    - Understand OS protection, patching and penetration
  - Applications / Software
    - Understands programming, secure coding and how to break software
From monolithic applications to smaller disconnected and modular services/apis/apps.
What do Kangaroos and Sharks have in common?

- Kangaroos cannot walk backwards
- Sharks can only swim forward
  - Must keep swimming, must keep swimming
  - No reversing

- Hackers on the other hand can reverse engineer.
Fish are friends not …>

- Can't really say that about hackers ...
- Can you?
- So we need to defend ourselves …
</pH – potentially Hackable>

- pH is
  - the measure of acidity/alkalinity
- Security pH-ilosophy should be to NEUTRALIZE threats with controls
- Any imbalance will lead to potentially Hackable software
Necessary protections should be built in the software layered with defense in depth, starting with the perimeter.
Sharks are Polyphyodont animals; no dentist needed

Our defenses need to be similar
  ◦ Continuously effective
  ◦ Validation and Verification (V&V) activities
</Holistic defense>

- Hammerhead Shark
- Owl

- $360^0$ (Holistic) Security
  - People, Process and Technology
  - Network, Hosts and Application
  - Tactical and Strategic
Some aquatic mammals sleep by shutting ONLY one side of their brain at a time.
Security should always be vigilant (conscious).
</The Bear Bare Necessities>

![Crossword Puzzle]

<table>
<thead>
<tr>
<th>Down</th>
<th>Across</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Synonym: Sensitivity; Antonym: Disclosure</td>
<td>5. Who is making the request?</td>
</tr>
<tr>
<td>3. Synonym: Criticality; Antonym: Destruction</td>
<td></td>
</tr>
<tr>
<td>4. Synonym: Accuracy; Antonym: Alteration</td>
<td></td>
</tr>
</tbody>
</table>
A myth to kill …

Source: End to End security, or why you shouldn’t drive your motorcycle naked?
By Vittorio Bertocci
Secure software should be:

- Modular (Unit)
- Highly Cohesive (discrete functions)
- Loosely Coupled (no dependencies)
The Horse Shoe Crab (Limulus) is said to have a third eye.

Secure Software should allow for Extra Vigilance (Auditing)!
<Defensive Strategies …>
According to the CBS News, which of the following is more dangerous than Sharks?

- Dogs
- Cars
- Sand
- Stroke

Side Channel attacks

To sum up…/

2B || !2B
Secure Naturally
Incorporating the Bare Necessities
so that your software is NOT potentially Hackable
That is the Question

- A Wild Wild Wild (WWW) Security Planet -
We live in, but it is a Wonderful Planet.
<Thank you>

Did I live up to my name?
```csharp
If (Liked_the_presentation)
{
    Contact me;
}
else
{
    Have a great day;
}
finally
{
    Thank you;
}
• LinkedIn
• Facebook
• Twitter
• SharkTalk podcast
• Email
    • mano(dot)paul(at)securisksolutions(dot)com
    • mano(dot)paul(at)expresscertifications(dot)com
```
SharkTalk™ and Hidden Treasures

- **SharkTalk**
  - iTunes: itpc://feeds.feedburner.com/SharkTalk
  - RSS: http://feeds.feedburner.com/SharkTalk

- **Hidden Treasures**
  - http://www.facebook.com/getPearls
  - http://thepauls.wordpress.com
© Copyright Attribution

- JAWS Movie
- PowerPoint Template from Indezine.
- Images.Google.Com
- Flickr