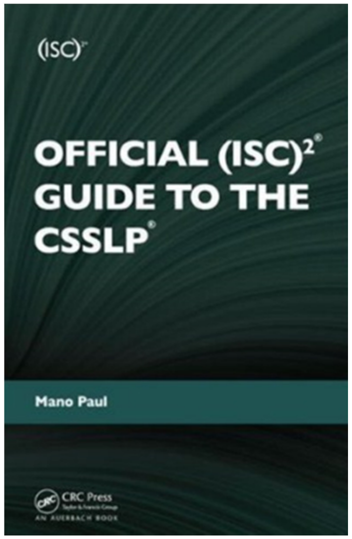
# Wild Wild Wild (WWW) Security Planet

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$^{TM}$ podcaster



(ISC)$^2$

OFFICIAL (ISC)$^2$ GUIDE TO THE CSSLP

Mano Paul

CRC Press
AN AUERBACH BOOK

Copyrighted Material

Information Security Management Handbook

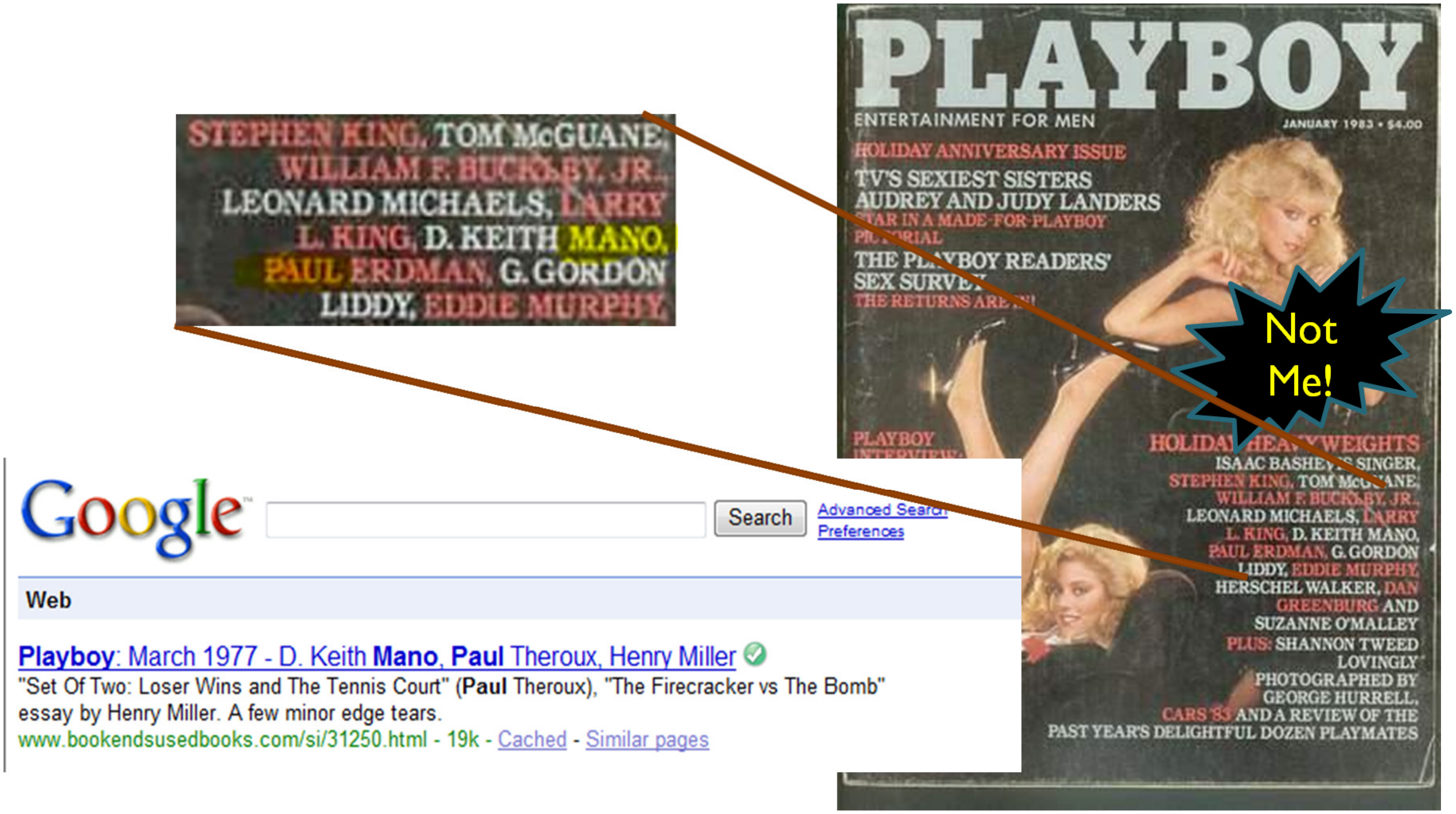
Sixth Edition

Edited by
Harold F. Tipton, CISSP · Micki Krause, CISSP

Volume 3

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

# </Who I am NOT? – Seriously>


STEPHEN KING, TOM McGUANE, WILLIAM F. BUCKLEY, JR., LEONARD MICHAELS, LARRY L. KING, D. KEITH MANO, PAUL ERDMAN, G. GORDON LIDDY, EDDIE MURPHY
PLAYBOY
ENTERTAINMENT FOR MEN
JANUARY 1983 • $4.00
HOLIDAY ANNIVERSARY ISSUE
TV'S SEXIEST SISTERS AUDREY AND JUDY LANDERS STAR IN A MADE-FOR-PLAYBOY PICTORIAL
THE PLAYBOY READERS' SEX SURVEY THE RETURNS ARE IN!
PLAYBOY INTERVIEW
HOLIDAY HEAVYWEIGHTS ISAAC BASHEVIS SINGER, STEPHEN KING, TOM McGUANE, WILLIAM F. BUCKLEY, JR., LEONARD MICHAELS, LARRY L. KING, D. KEITH MANO, PAUL ERDMAN, G. GORDON LIDDY, EDDIE MURPHY, HERSCHEL WALKER, DAN GREENBURG AND SUZANNE O'MALLEY
PLUS: SHANNON TWEED LOVINGLY PHOTOGRAPHED BY GEORGE HURRELL, CARS '83 AND A REVIEW OF THE PAST YEAR'S DELIGHTFUL DOZEN PLAYMATES
Not Me!
Google
Search
Advanced Search
Preferences
Web

**Playboy**: March 1977 - D. Keith **Mano**, **Paul** Theroux, Henry Miller

"Set Of Two: Loser Wins and The Tennis Court" (**Paul** Theroux), "The Firecracker vs The Bomb" essay by Henry Miller. A few minor edge tears.

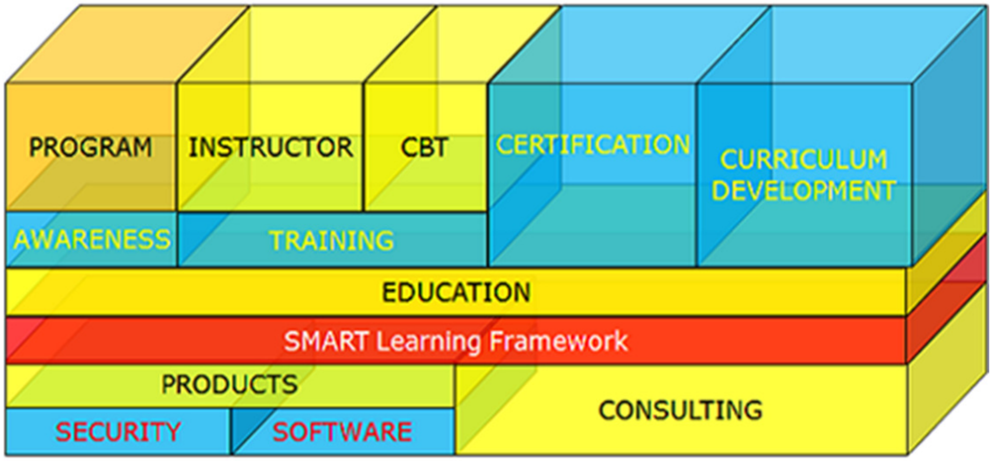
www.bookendsusedbooks.com/si/31250.html - 19k - Cached - Similar pages

# </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)

SecuRisk Solutions Framework



*SMART - Skills Measuring Assessment Reinforced Training

# </A Wild + Wonderful World>

CHICHEN ITZA, MEXICO
CHRIST REDEEMER, BRASIL
COLOSSEUM, ITALY
TAJ MAHAL, INDIA
GREAT WALL OF CHINA
PETRA, JORDAN
07.07.2007
LISBON
OFFICIAL DECLARATION OF
THE NEW 7 WONDERS
OF THE WORLD
MACHU PICCHU, PERU

# </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

# </A Wild World … >

**It’s a jungle out there**

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

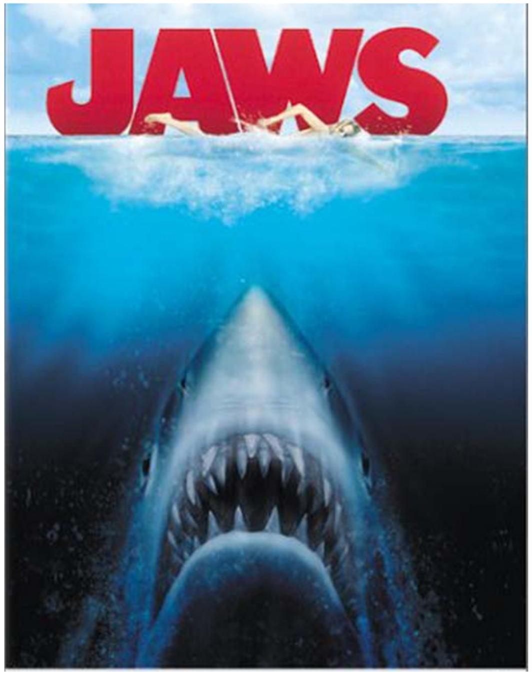
Raphael Sagarin<br>
Author of Natural Security

# </Head in the Sand>

- Ignoring known vulnerabilities in your software is akin to sticking your head in the sand …
- Accept, Transfer, Mitigate, or Avoid Ri$k.

# </Sharks and Candirus>

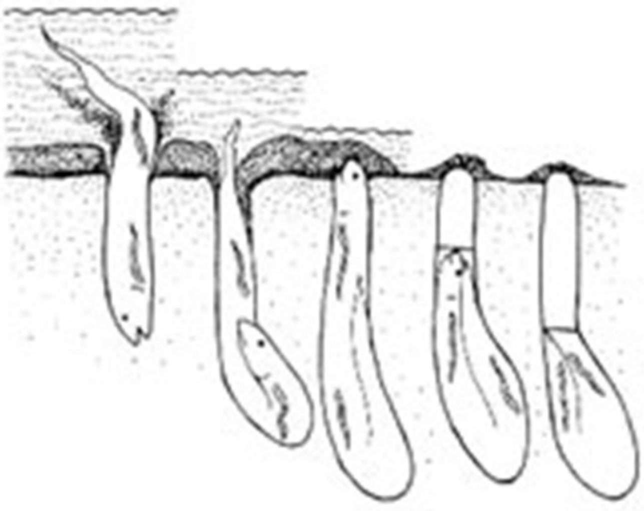
- External – Attacks from the outside
- Sharks



- 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

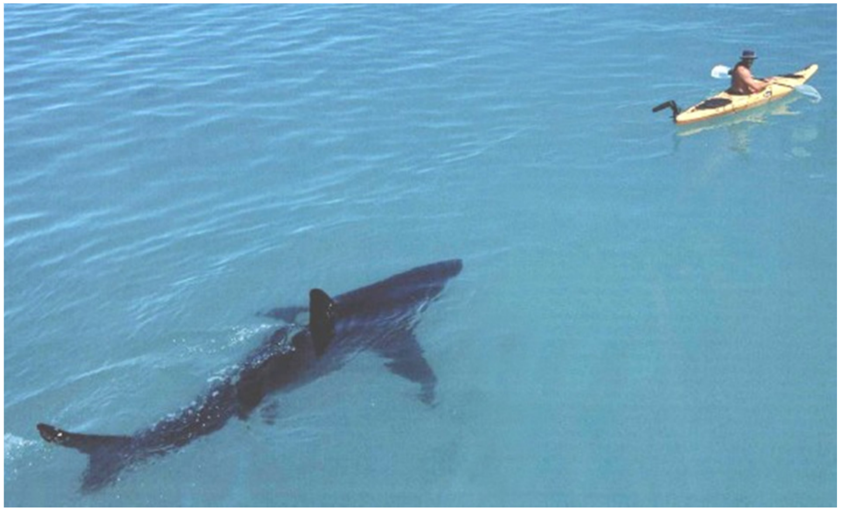
# </Shark school!>

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

- Hackers
  - Psycholog dence and anon
  - With a st ocial group
  - Cyber-cri organized

# </Attack behavior>

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



- Hackers
  - Pattern: Reconnaissance activities
  - Motive: Usually intentional

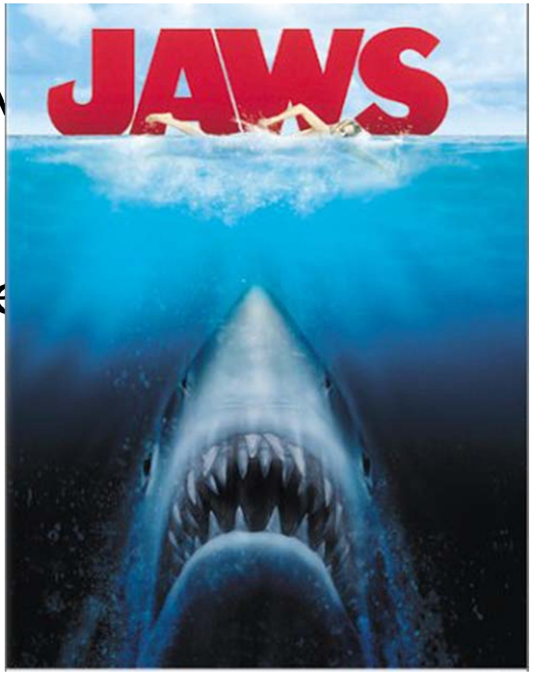
# </Attack Patterns: Recon to Root>

- Probe (Reconnaissance)
  - Mining
  - Scanning
  - Fingerprinting
  - Social Networking
- Penetrate
  - Bruteforcing
  - Overflow
  - Injection

- Persist
- Propagate
- Paralyze (r00t)
  - Rootkits
  - cmd prompt access

# </The Top 5 most dangerous sharks>

- 5 - Shortfin Mako Shark
  - Fastest Shark – you cant out-s
- 4 - Oceanic Whitetip Shark
  - Opportunists – 1st at a shipwre
- 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?



Copyright 2007-2010. SecuRisk Solutions

# </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

# </Architectures – Large and Small>

From monolithic applications to smaller disconnected and modular services/apis/apps.

# </Sharks and Kangaroos>

- 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 …>

- Cant 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

# </Defensive Dams>

- Necessary protections should be built in the software layered with defense in depth, starting with the perimeter.

# </Layered defense>

- Sharks are Polyphyodont animals; no dentist needed

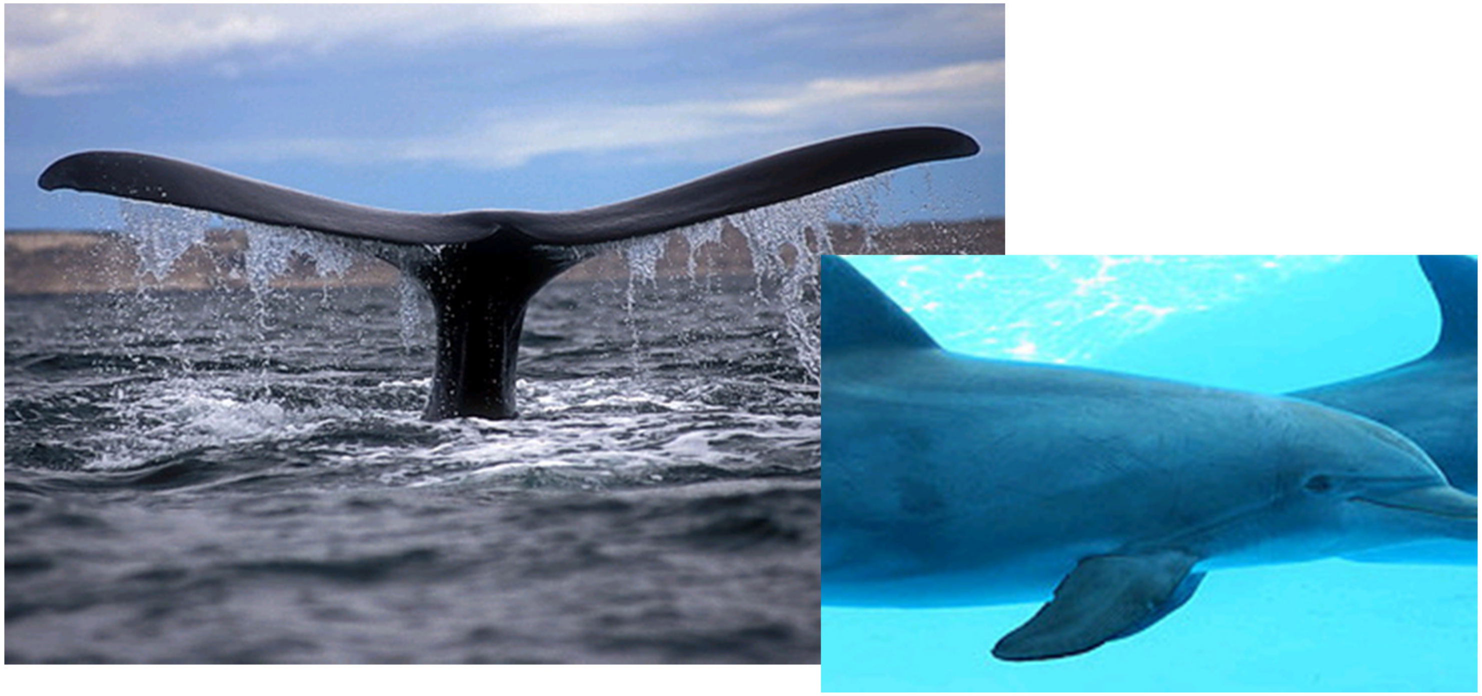
- Our defenses need to be similar
  - Continuously effective
  - Validation and Verification (V&V) activities

# </Holistic defense>

- Hammerhead Shark
- Owl

- $360^0$ (Holistic) Security
  - People, Process and Technology
  - Network, Hosts and Application
  - Tactical and Strategic

# </Sleep-Swimming>



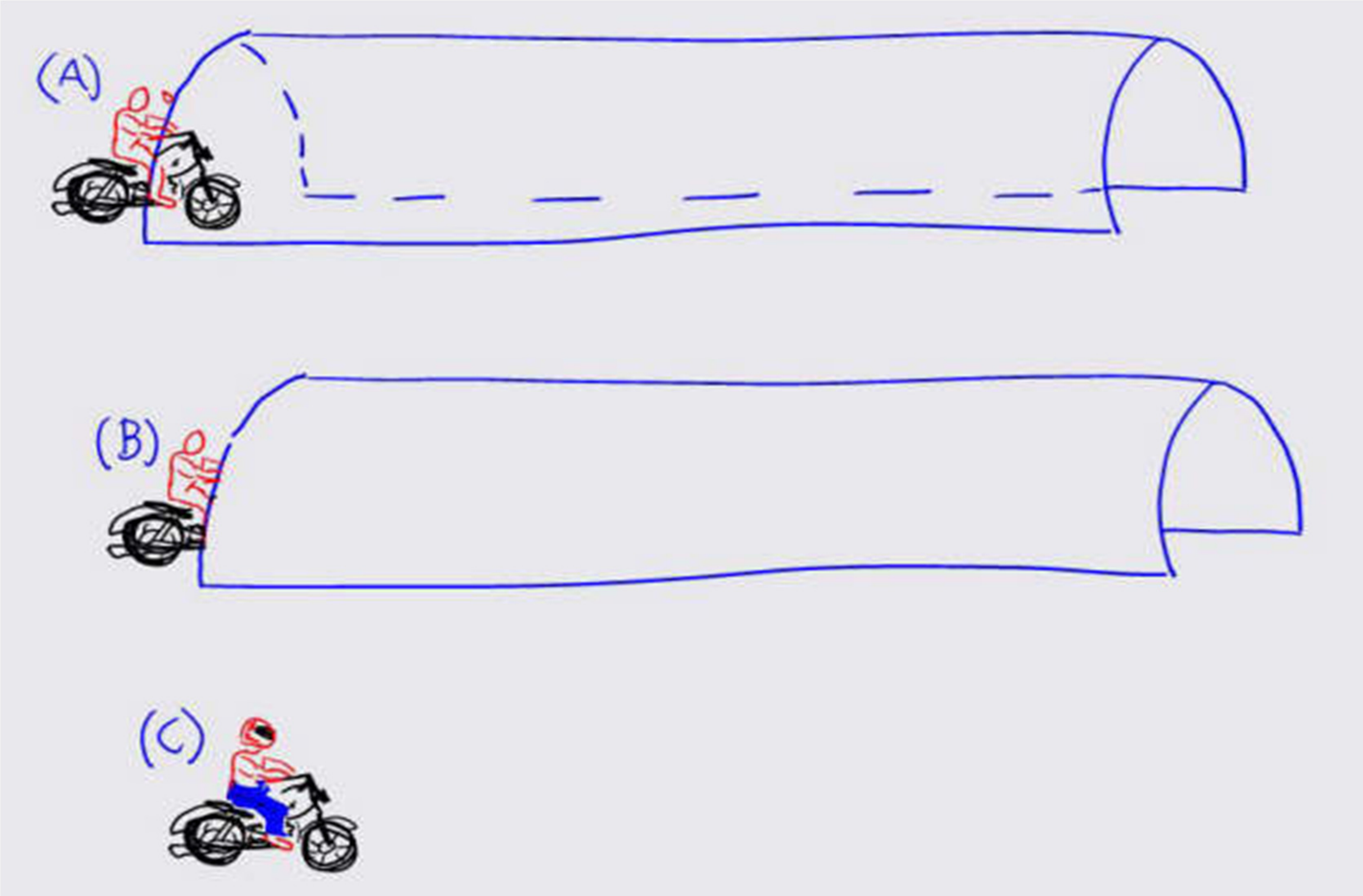
- Some aquatic mammals sleep by shutting ONLY one side of their brain at a time.
- Security should always be vigilant (conscious).

# </The ~~Bear~~ Bare Necessities>

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ■ | ■ | ■ | ■ | 1 C | ■ | ■ | 2 A | ■ | ■ | ■ | ■ | ■ | ■ |
| ■ | ■ | ■ | ■ | O | ■ | ■ | U | ■ | 3 A | ■ | ■ | ■ | ■ |
| ■ | ■ | ■ | ■ | N | ■ | ■ | T | ■ | V | ■ | ■ | ■ | ■ |
| ■ | ■ | ■ | ■ | F | ■ | ■ | H | ■ | A | ■ | ■ | ■ | ■ |
| ■ | ■ | ■ | ■ | I | ■ | ■ | O | ■ | I | ■ | ■ | ■ | ■ |
| ■ | ■ | ■ | ■ | D | ■ | ■ | R | ■ | L | ■ | ■ | ■ | 4 I |
| 5 A | U | T | H | E | N | T | I | C | A | T | I | O | N |
| ■ | ■ | ■ | ■ | N | ■ | ■ | Z | ■ | B | ■ | ■ | ■ | T |
| ■ | ■ | ■ | ■ | T | ■ | ■ | A | ■ | I | ■ | ■ | ■ | E |
| ■ | ■ | ■ | ■ | I | ■ | ■ | T | ■ | L | ■ | ■ | ■ | G |
| ■ | ■ | ■ | ■ | 6 A | U | D | I | T | I | N | G | ■ | R |
| ■ | ■ | ■ | ■ | L | ■ | ■ | O | ■ | T | ■ | ■ | ■ | I |
| ■ | ■ | ■ | ■ | I | ■ | ■ | N | ■ | Y | ■ | ■ | ■ | T |
| ■ | ■ | ■ | ■ | T | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | Y |
| ■ | ■ | ■ | ■ | Y | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |

| Down | Across |
|---|---|
| 1. Synonym: Sensitivity; Antonym: Disclosure | 5. Who is making the request? |
| 2. Rights and Privileges of the Requestor | 6. Historical Evidence |
| 3. Synonym: Criticality; Antonym: Destruction | |
| 4. Synonym: Accuracy; Antonym: Alteration | |

# </A myth to kill …>



Source: End to End security, or why you shouldn't drive your motorcycle naked?
By Vittorio **Bertocci**

# </Bee-Having Software>

Secure software should be

- Modular (Unit)
- Highly Cohesive (discreet functions)
- Loosely Coupled (no dependencies)

# </The Third Eye>

- The Horse Shoe Crab (Limulus) is said to have a third eye.
- Secure Software should allow for Extra Vigilance (Auditing)!

# </Defensive Strategies …>

- Against Sharks
  - Stay on land
  - Swim in a Swi
  - Cages
  - Chain Suit
  - Stun Gun
- Against Hackers
  - Risk Avoidance

# </More dangerous than Sharks?>

- According to the CBS News, which of the following is more dangerous than Sharks?
  - Dogs
  - Cars
  - Sand
  - Stroke

- Side Channel attacks
  - "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow," by Shuo Chen, Rui Wang, XiaoFeng Wang, and Kehuan Zhang.

# </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?

# </Cont@ct!/>

```
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