OWASP AppSensor
The Future of Application Security

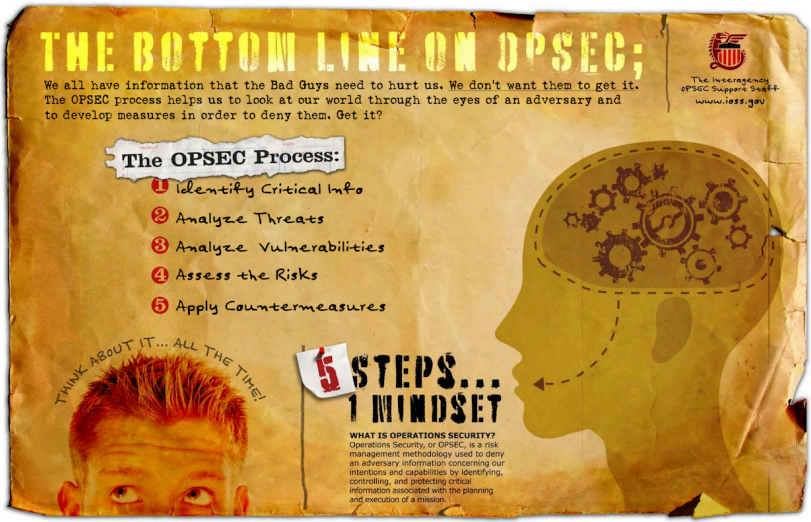
Dennis Groves, MSc
dennis.groves@owasp.org

November 15, 2013

About Me

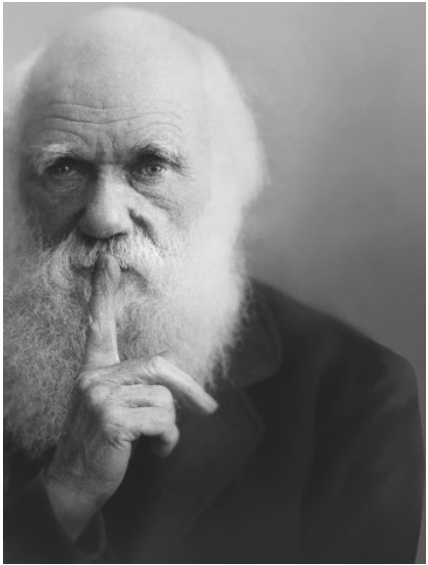
A Thought Experiment

OPSEC


THE BOTTOM LINE ON OPSEC;
We all have information that the Bad Guys need to hurt us. We don't want them to get it. The OPSEC process helps us to look at our world through the eyes of an adversary and to develop measures in order to deny them. Get it?
The Interagency OPSEC Support Staff
www.ioss.gov
The OPSEC Process:
1 Identify Critical Info
2 Analyze Threats
3 Analyze Vulnerabilities
4 Assess the Risks
5 Apply Countermeasures
THINK ABOUT IT... ALL THE TIME!
5 STEPS... 1 MINDSET
WHAT IS OPERATIONS SECURITY?
Operations Security, or OPSEC, is a risk management methodology used to deny an adversary information concerning our intentions and capabilities by identifying, controlling, and protecting critical information associated with the planning and execution of a mission.

1: Identify Critical Info

Know Yourself



"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change."

Vitorian Duel

Use Time Based Security Metrics

Use Time Based Security Metrics

Theorem

Protection time must be greater than or equal to detection time plus reaction time.

(1) $$P_t \geq D_t + R_t$$

Wester Duel

Know your Opponent

Pistol Duel

- Novice Shooter
- Weekend Shooter
- Professional Shooter
- Quick Draw Champion

Application

- Script Kiddies
- Hacktivists
- Criminals
- Disgruntled Employee
- Corporate Spy
- Cyber Warrior

Out Gunned

2: Analyze Threats

Pistol Duel

- Handgun Skills
- Nervousness
- Psychological Readiness

Application

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

3: Analyze Vulnerabilities

Pistol Duel

- Jam
- Misfire
- Backfire

The OWASP Top-10

- A1 Injection
- A3 Cross-Site Scripting
- A5 Security Misconfiguration
- A7 Missing Access Control

4: Analyze Risks

The probable frequency and probable magnitude of future loss

(2) $\text{Risk} = P(\text{Impact})$

(3) $\text{Risk} = P(\text{Impact} * \text{Vulnerability})$

(4) $\text{Risk} = \text{Impact} * \text{Vulnerability} * \text{Threat}$

(5) $\text{Risk} = P(\text{Impact} * \text{Vulnerability} * \text{Threat})$

(6) $$\text{Risk} = \frac{\text{Impact} * \text{Vulnerability} * \text{Threat}}{\text{Countermeasures}}$$

(7) $$\text{Risk} = \text{Impact} * \frac{P(\text{Threat}) * P(\text{Vulnerability})}{\text{Countermeasures}}$$

5: Apply Countermeasures

- Tolerate: Do nothing.
- Transfer: Outsource the risk.
- Terminate: Eliminate the asset.
- Treat: Reduce the risk.

Risk Reduction Methods

Reducing the risk (treatment) is the most common strategy used today.

- Reduce the probability of a threat.
- Reduce the probability of a vulnerability.

Reduce Attack Surface

Pistol Duel

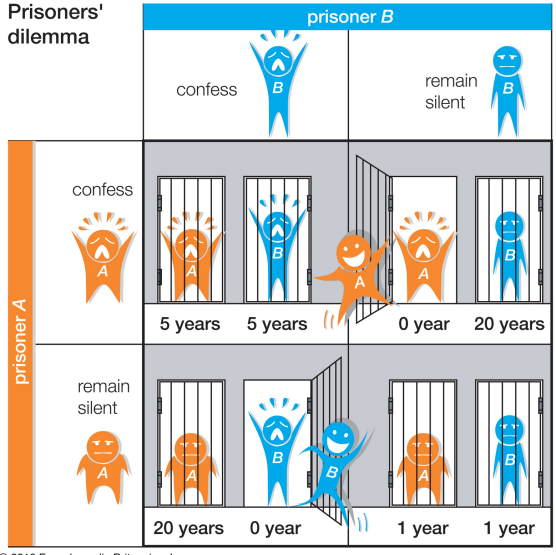
- Turn To The Side
- Crouch Down Low
- ???

Application

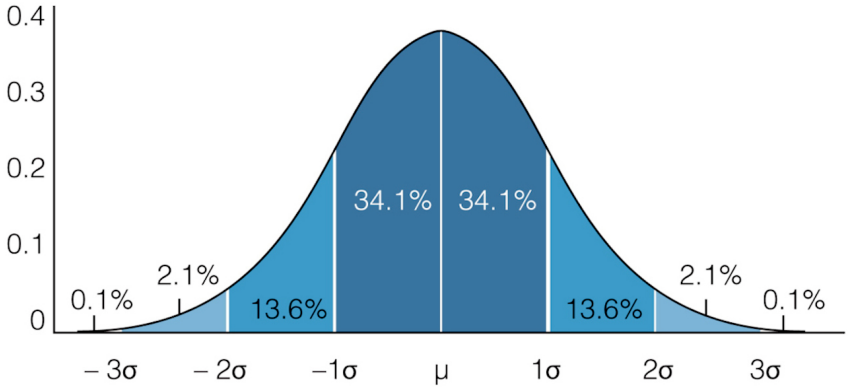
- Penetration Testing
- Code Review
- Patching

Predicting the Future

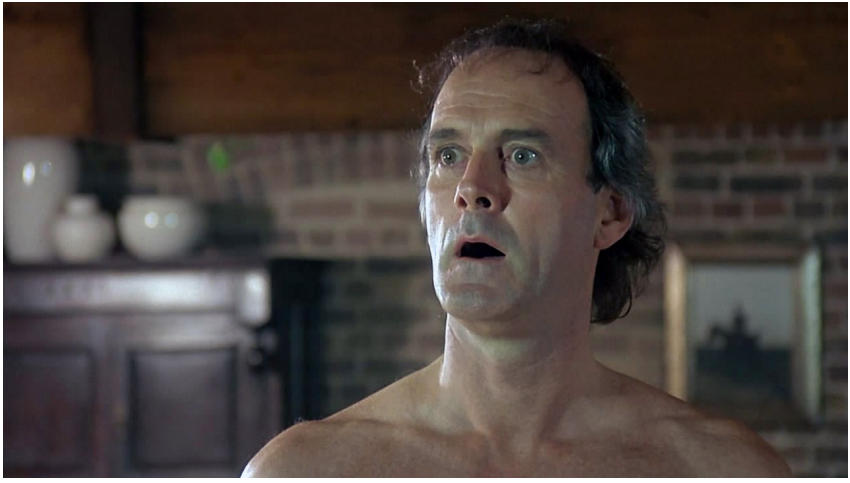
Reluctance to Trust



Basic Statistics



Now For Something Completely Different



Risk Optimization

Risk Optimisation is rarely practiced, but highly effective method.

- Reduce the impact of an event

Bullet Proof Vest

Security Principles

- Know Yourself
- Use Time Based Security
- Know your Opponent
- Reduce Attack Surface
- Reluctance to Trust
- Add Impact Reduction
- Use Separation of Duty

How Can You Help?

- Join the Mailing List and Participate
- Help us develop reference implementations
- Tell your friends, and employers

Obrigado!

Questions?