OWASP AppSensor, The Future of Application Security

OWASP AppSensor
The Future of Application Security

Dennis Groves, MSc

dennis.groves@owasp.org

February 17, 2013

Contents

Who am I?

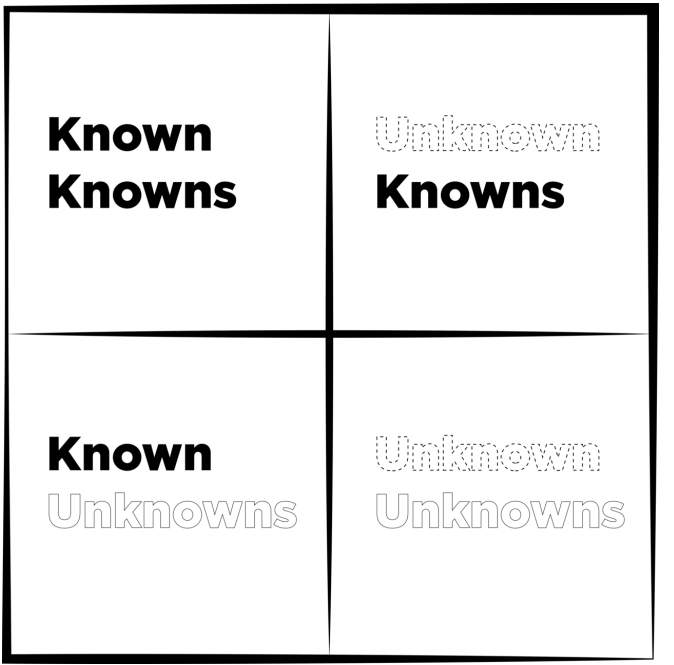
About Me

When was I born?

What is my Bloodtype?

Donald Rumsfeld

"There are known knowns; there are things we know that we know. There are known unknowns; that is to say there are things that, we now know we don't know. But there are also unknown unknowns – there are things we do not know we don't know."


Known
Knowns
Unknown
Knowns
Known
Unknowns
Unknown
Unknowns

Mark Twain

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

Security Management

A Risk Based Approach

Risk

The probable frequency and probable magnitude of future loss

$$Risk = P(Impact) \tag{1}$$

A Brief History of Risk

$$Risk = P(Impact * Vulnerability) \tag{2}$$

A Brief History of Risk

$$Risk = P(Impact * Vulnerability) \tag{2}$$

$$Risk = Impact * Vulnerability * Threat \tag{3}$$

A Brief History of Risk

$$Risk = P(Impact * Vulnerability) \tag{2}$$

$$Risk = Impact * Vulnerability * Threat \tag{3}$$

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

A Brief History of Risk

$$Risk = P(Impact * Vulnerability) \tag{2}$$

$$Risk = Impact * Vulnerability * Threat \tag{3}$$

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

$$Risk = \frac{Impact * Vulnerability * Threat}{Countermeasures} \tag{5}$$

A Brief History of Risk

$$Risk = P(Impact * Vulnerability) \tag{2}$$

$$Risk = Impact * Vulnerability * Threat \tag{3}$$

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

$$Risk = \frac{Impact * Vulnerability * Threat}{Countermeasures} \tag{5}$$

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

Risk Treatments

- Tolerate: Do nothing.

Risk Treatments

- Tolerate: Do nothing.
- Transfer: Outsource the risk.

Risk Treatments

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

Risk Treatments

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

Risk Reduction Methods

- Reduce the probability of a threat.

Risk Reduction Methods

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

Risk Reduction Methods

- Reduce the probability of a threat.
- Reduce the probability of a vulnerability.
- Reduce the impact of an event?

Security Operations

Time Based Security

Theorem

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

$$P_t \geq D_t + R_t \tag{7}$$

OWASP AppSensor

OWASP AppSensor

Moving Detection & Reaction into the Application

AppSensor Overview

This is a high-level overview of the concept and why it is different.

AppSensor Contributors

Michael Coates, Colin Watson, John Melton Ryan Barnett, Simon Bennetts, Marc Chisinevski, Robert Chonjnacki, August Detlefsen, Sean Fay, Randy Janida, Alex Lauerman, Manuel Arredondo, Bob Maier, Craig Munson, Giri Nambari, Abdul Rauf, Jay Reynolds, Eric Sheridan, John Steven, Alex Thissen, Don Thomas, Kevin Wall, Mehmet Yilmaz, Jim Manico, Dinis Cruz, myself and many, many others...

Conventional Defensive Measures

- Perimeter Defence

Conventional Defensive Measures

- Perimeter Defence
- Cryptographic Communications

Conventional Defensive Measures

- Perimeter Defence
- Cryptographic Communications
- Anti-Virus (AV)

Conventional Defensive Measures

- Perimeter Defence
- Cryptographic Communications
- Anti-Virus (AV)
- Intrusion Detection/Prevention Systems (IDS/IPS)

Perimeter Defence

- Packet Filters

Perimeter Defence

- Packet Filters
- Firewalls

Perimeter Defence

- Packet Filters
- Firewalls
- Application Layer (WAF)

Cryptographic Communications

- SSL 1.0 - 2.0 - 3.0

Cryptographic Communications

- SSL 1.0 - 2.0 - 3.0
- TLS 1.0 - 1.1 - 1.2

Anti-Virus

- The system is already compromised!

Anti-Virus

- The system is already compromised!

$$P_t \geq D_t + R_t \tag{8}$$

Anti-Virus

- The system is already compromised!

$$P_t \geq D_t + R_t \tag{8}$$

- Anti-Virus is the same as giving up. ;)

Intrusion Detection/Prevention Systems

- Host Based - Tripwire etc..

Intrusion Detection/Prevention Systems

- Host Based - Tripwire etc..
- Network Based - Snort etc..

Intrusion Detection/Prevention Systems

- Host Based - Tripwire etc..
- Network Based - Snort etc..
- Application Based - OWASP AppSensor

Application Defensive Measures

- Attack-Aware Detection

Application Defensive Measures

- Attack-Aware Detection
- Normal and Malicious Behavior

Application Defensive Measures

- Attack-Aware Detection
- Normal and Malicious Behavior
- Evasion and Unknown Attacks

AppSensor Detection Points

Type	Code	Name
Signature	RE	Request Exceptions
	AE	Authentication Exceptions
	SE	Session Exceptions
	ACE	Access Control Exceptions
	IE	Input Exceptions
	EE	Encoding Exceptions
	CIE	Command Injection Exceptions
	FIO	File IO Exceptions
	HT	Honey Trap
Behavioural	UTE	User Trend Exceptions
	STE	System Trend Exceptions
	RP	Reputation

AppSensor Rich Response

Response Type	Examples
Logging Change	Full stack trace of error messages logged
	Record DNS data on user's IP address
Account Logout	Session terminated and user redirected
	Session terminated only (no redirect)
Account Lockout	User account locked permanently
	One user's IP address range blocked
Application Disabled	Website shut down and replaced with static page
	Application taken offline

Define

This is the set of chapters that is of interest to Management. Why do they want an OWASP AppSensor and what is the set of actions they need to put in place to instantiate the OWASP AppSensor.

Design

This is the set of chapters that is of interest to Software Architects. What are the various requirements for an OWASP AppSensor and what the design trade-offs in different deployment configurations of the OWASP AppSensor.

Develop

This is the set of chapters that is of interest to Software Engineers (Developers). What is required for a developer to develop an OWASP AppSensor. Additionally, I imagine this is also about how to test the code to verify that it manages the exceptions as required

Deploy

This is the set of chapters that is of interest to Operations. How do you deploy, tune and configure the OWASP AppSensor?

Future AppSensor Developments

- AppSensor-core

Future AppSensor Developments

- AppSensor-core
- AppSensor-ws-soap

Future AppSensor Developments

- AppSensor-core
- AppSensor-ws-soap
- AppSensor-ws-rest

Future AppSensor Developments

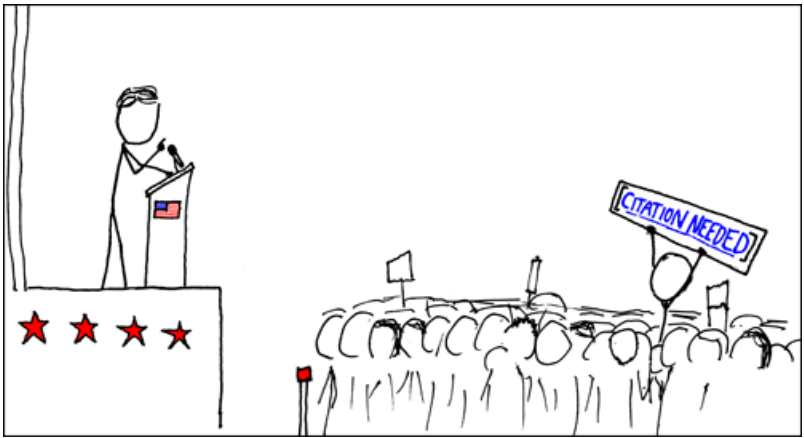
- AppSensor-core
- AppSensor-ws-soap
- AppSensor-ws-rest
- AppSensor Handbook

How Can You Help?

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

Bibliography

Bibliography



Thank You!

Please send feedback to dennis.groves@owasp.org

- What did you like most?

Thank You!

Please send feedback to dennis.groves@owasp.org

- What did you like most?
- What did you like least?

Thank You!

Please send feedback to dennis.groves@owasp.org

- What did you like most?
- What did you like least?
- What can be improved?

Dennis Groves