OWASP AppSensor
The Future of Application Security

Dennis Groves, MSc

dennis.groves@owasp.org

June 2, 2013

Nasreddin Hodja

One day Nasreddin Hodja's donkey was stolen. When they heard this, the village people all came to the Hodja and began to ask questions such as, "Oh, why didn't you bolt the stable door?" "Why didn't you build the walls higher?" "Can anyone sleep so soundly?" In reply the Hodja said, "Yes, you're right. It's my fault, of course, not the thief's."

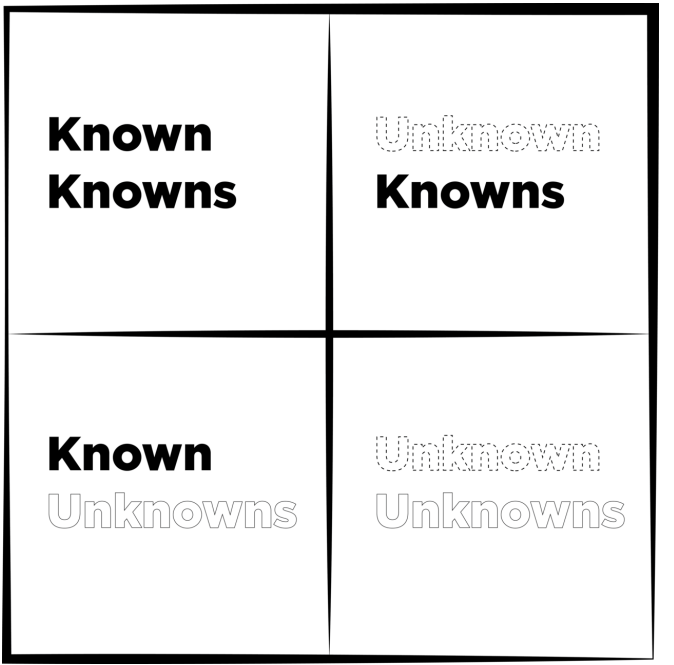
Contents

Who am I?

About Me

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

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

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

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

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

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

Scott Adams

There are many methods for predicting the future. For example, you can read horoscopes, tea leaves, tarot cards, or crystal balls. Collectively, these methods are known as "nutty methods." Or you can put well-researched facts into sophisticated computer models, more commonly referred to as "a complete waste of time."

Risk Treatments

- 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.

Risk Reduction Methods

Risk Optimisation is rarely practiced, but highly effective method.

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

Perimeter Defence

- Packet Filters
- Firewalls
- Application Layer (WAF)

Cryptographic Communications

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

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

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

Future AppSensor Developments

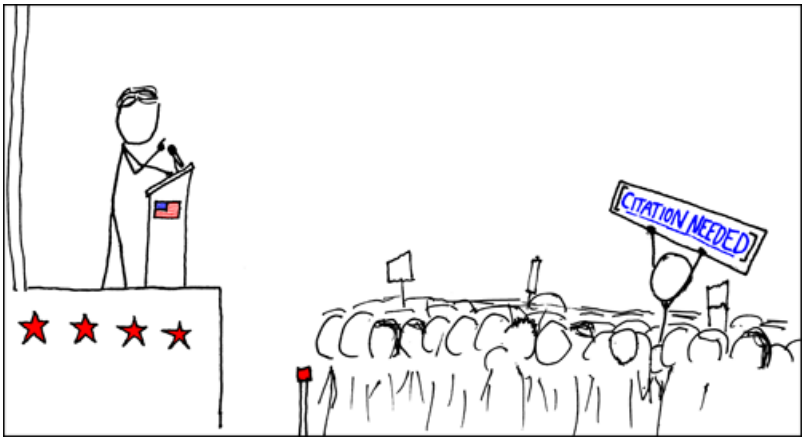
- AppSensor-core
- AppSensor-ws-soap
- AppSensor-ws-rest
- AppSensor Handbook

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

Dennis Groves