Cornucopia

Ecommerce Website Edition v1.20-EN

OWASP Cornucopia is a mechanism to assist software development teams identify security requirements in Agile, conventional and formal development processes

Author

Colin Watson

Index

Introduction

The idea behind Cornucopia is to help development teams, especially those using Agile methodologies, to identify application security requirements and develop security-based user stories. Although the idea had been waiting for enough time to progress it, the final motivation came when SAFECode published its Practical Security Stories and Security Tasks for Agile Development Environments in July 2012.

The Microsoft SDL team had already published its super Elevation of Privilege: The Threat Modeling Game (EoP) but that did not seem to address the most appropriate kind of issues that web application development teams mostly have to address. EoP is a great concept and game strategy, and was published under a Creative Commons Attribution License.

Cornucopia Ecommerce Website Edition is based on the concepts and game ideas in EoP, but those have been modified to be more relevant to the types of issues ecommerce website developers encounter. It attempts to introduce threat-modelling ideas into development teams that use Agile methodologies, or are more focused on web application weaknesses than other types of software vulnerabilities or are not familiar with STRIDE and DREAD.

Cornucopia Ecommerce Website Edition is referenced as an information resource in the PCI Security Standard Council's Information Supplement PCI DSS E-commerce Guidelines, v2, January 2013.

The card deck (pack)

Instead of EoP's STRIDE suits (sets of cards with matching designs), Cornucopia suits are based on the structure of the OWASP Secure Coding Practices - Quick Reference Guide (SCP), but with additional consideration of sections in the OWASP Application Security Verification Standard, the OWASP Testing Guide and David Rook's Principles of Secure Development. These provided five suits, and a sixth called "Cornucopia" was created for everything else:

- Data validation and encoding (VE)
- Authentication (AT)
- Session management (SM)
- Authorization (AZ)
- Cryptography (CR)
- Cornucopia (C)

Similar to poker-playing cards, each suit contains 13 cards (Ace, 2-10, Jack, Queen and King) but, unlike EoP, there are also two Joker cards. The content was mainly drawn from the SCP.

Mappings

The other driver for Cornucopia is to link the attacks with requirements and verification techniques. An initial aim had been to reference CWE weakness IDs, but these proved too numerous, and instead it was decided to map each card to CAPEC software attack pattern IDs which themselves are mapped to CWEs, so the desired result is achieved.

Each card is also mapped to the 36 primary security stories in the SAFECode document, as well as to the OWASP SCP v2, ASVS v3.0.1 and AppSensor (application attack detection and response) to help teams create their own security-related stories for use in Agile processes.

Game strategy

Apart from the content differences, the game rules are virtually identical to those for EoP.

Provide feedback

If you have ideas or feedback on the use of OWASP Cornucopia, please share them. Even better if you create alternative versions of the cards, or produce professional print-ready versions, please share that with the volunteers who created this edition and with the wider application development and application security community.

The best place to use to discuss or contribute is the mailing list for the OWASP project:

- Mailing list
https://lists.owasp.org/mailman/listinfo/owasp_cornucopia
- Project home page
https://www.owasp.org/index.php/OWASP_Cornucopia

All OWASP documents and tools are free to download and use. OWASP Cornucopia is licensed under the Creative Commons Attribution-ShareAlike 3.0 license.

Instructions

The text on each card describes an attack, but the attacker is given a name, which is unique across all the cards. The name can represent a computer system (e.g., the database, the file system, another application, a related service, a botnet), an individual person (e.g., a citizen, a customer, a client, an employee, a criminal, a spy), or even a group of people (e.g., a competitive organization, activists with a common cause). The attacker might be remote in some other device/location, or local/internal with access to the same device, host or network as the application is running on. The attacker is always named at the start of each description. An example is:

William has control over the generation of session identifiers

This means the attacker (William) can create new session identifiers that the application accepts.

The attacks were primarily drawn from the security requirements listed in the SCP, v2 but then supplemented with verification objectives from the OWASP "Application Security Verification Standard for Web Applications," the security focused stories in SAFECode's "Practical Security Stories and Security Tasks for Agile Development Environments," and finally a review of the cards in EoP.

Lookups between the attacks and five resources are provided on most cards:

- Requirements in "Secure Coding Practices (SCP) - Quick Reference Guide," v2, OWASP, November 2010

https://www.owasp.org/index.php/File:OWASP_SCP_Quick_Reference_Guide_v2.pdf

- Verification IDs in "Application Security Verification Standard (ASVS) for Web Applications", OWASP, 2016

https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

- Attack detection points IDs in "AppSensor," OWASP, August 2012

https://www.owasp.org/index.php/AppSensor_DetectionPoints

- IDs in "Common Attack Pattern Enumeration and Classification (CAPEC)," v2.6, Mitre Corporation, November 2015

http://capec.mitre.org/data/archive/capec_v2.8.zip

- Security-focused stories in "Practical Security Stories and Security Tasks for Agile Development Environments," SAFECode, July 2012

http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf

OWASP
Open Web Application Security Project

Project Acknowledgements

- Colin Watson and Dario De Filippis
- Blackfoot UK Limited for the print-ready card designs
- Tom Brennan and OWASP for the box and leaflet
- OWASP employees especially Kate Hartmann
- Oana Cornea and other participants at the AppSec EU 2015

(continued on page 16)

A look-up means the attack is included within the referenced item, but does not necessarily encompass the whole of its intent. For structured data like CAPEC, the most specific reference is provided but sometimes a cross-reference is provided that also has more specific (child) examples. There are no lookups on the six Aces and two Jokers. Instead these cards have some general tips in italicized text.

It is possible to play Cornucopia in many different ways. Here is one way.

A - Preparations

A1. Use the cards in this pack

A2. Identify an application or application process to review; this might be a concept, design or an actual implementation

A3. Create a data flow diagram, user stories, or other artefacts to help the review

A4. Identify and invite a group of 3-6 architects, developers, testers and other business stakeholders together and sit around a table (try to include someone fairly familiar with application security)

A5. Have some prizes to hand (gold stars, chocolate, pizza, beer or flowers depending upon your office culture)

B - Play

One suit - Cornucopia - acts as trumps. Aces are high (i.e., they beat Kings). It helps if there is a non-player to document the issues and scores.

B1. Remove the Jokers and a few low-score (2, 3, 4) cards from Cornucopia suit to ensure each player will have the same number of cards.

B2. Shuffle the deck and deal all the cards.

B3. To begin, choose a player randomly who will play the first card - they can play any card from their hand except from the trump suit - Cornucopia.

B4. To play a card, each player must read it out aloud, and explain (see the online Wiki Deck for tips) how the threat could apply (the player gets a point for attacks that might work which the group thinks is an actionable bug) - do not try to think of mitigations at this stage, and do not exclude a threat just because of a belief that it is already mitigated - someone note the card and record the issues raised

B5. Play clockwise, each person must play a card in the same way; if you have any card of the matching lead suit you must play one of those, otherwise they can play a card from any other suit. Only a higher card of the same suit, or the highest card in the trump suit Cornucopia,wins the hand.

B6. The person who wins the round, leads the next round (i.e., they play first), and thus defines the next lead suit.

B7. Repeat until all the cards are played.

C - Scoring

The objective is to identify applicable threats, and win hands (rounds):

C1. Score +1 for each card you can identify as a valid threat to the application under consideration.

C2. Score +1 if you win a round.

C3. Once all cards have been played, whoever has the most points wins.

D - Closure

D1. Review all the applicable threats and the matching security requirements.

D2. Create user stories, specifications and test cases as required for your development methodology.

Alternative game rules

If you are new to the game, remove the Aces and two Joker cards to begin with. Add the Joker cards back in once people become more familiar with the process. Apart from the "trumps card game" rules described above which are very similar to the EoP, the deck can also be played as the "twenty-one card game" (also known as "pontoon" or "blackjack") which normally reduces the number of cards played in each round.

Practice on an imaginary application, or even a future planned application, rather than trying to find fault with existing applications until the participants are happy with the

usefulness of the game.

Consider just playing with one suit to make a shorter session – but try to cover all the suits for every project. Or even better just play one hand with some pre-selected cards, and score only on the ability to identify security requirements. Perhaps have one game of each suit each day for a week or so, if the participants cannot spare long enough for a full deck.

Some teams have preferred to play a full hand of cards, and then discuss what is on the cards after each round (instead of after each person plays a card).

Another suggestion is that if a player fails to identify the card is relevant, allow other players to suggest ideas, and potentially let them gain the point for the card. Consider allowing extra points for especially good contributions.

You can even play by yourself. Just use the cards to act as thought-provokers. Involving more people will be beneficial though.

In Microsoft's EoP guidance, they recommend cheating as a good game strategy.

Development framework-specific modified card decks

At the end of 2012, the OWASP Framework Security Matrix was published which documents built in security controls in some commonly used languages and frameworks for web and mobile application development. With certain provisos it is useful to consider how using these controls can simplify

the identification of additional requirements – provided of course the controls are included, enabled and configured correctly.

Consider removing the following cards from the decks if you are confidence they are addressed by the way you are using the language/framework. Items in parentheses are "maybes."

Internal coding standards and libraries

Add your own list of excluded cards based on your organisation's coding standards (provided they are confirmed by appropriate verification steps in the development lifecycle).

Your coding standards and libraries		
Data validation and encoding	Session management	Cryptography
[your list]	[your list]	[your list]
Authentication	Authorisation	Cornucopia
[your list]	[your list]	[your list]

Compliance requirement decks

Create a smaller deck by only including cards for a particular compliance requirement.

Compliance requirement		
Data validation and encoding	Session management	Cryptography
[your list]	[your list]	[your list]
Authentication	Authorisation	Cornucopia
[your list]	[your list]	[your list]

Frequently asked questions

1. Can I copy or edit the game?

Yes of course. All OWASP materials are free to do with as you like provided you comply with the Creative Commons Attribution-ShareAlike 3.0 license. Perhaps if you create a new version, you might donate it to the OWASP Cornucopia Project?

2. How can I get involved?

Please send ideas or offers of help to the project's mailing list.

3. How were the attackers' names chosen?

EoP begins every description with words like "An attacker can..." These have to be phrased as an attack but I was not keen on the anonymous terminology, wanting something more engaging, and therefore used personal names. These can be thought of as external or internal people or aliases for computer systems. But instead of just random names, I thought how they might reflect the OWASP community aspect. Therefore, apart from "Alice and Bob," I use the given (first) names of current and recent OWASP employees and board members (assigned in no order), and then randomly selected the remaining 50 or so names from the current list of paying individual OWASP members.

No name was used more than once, and where people had provided two personal names, I dropped one part to try to ensure no-one can be easily identified. Names were not deliberately allocated to any particular attack, defence or requirement. The cultural and gender mix simply reflects theses sources of names, and is not meant to be world-representative.

4. Why aren't there any images on the card faces?

There is quite a lot of text on the cards, and the cross-referencing takes up space too. But it would be great to have additional design elements included. Any volunteers?

5. Are the attacks ranked by the number on the card?

Only approximately. The risk will be application and organization dependent, due to varying security and compliance requirements, so your own severity rating may place the cards in some other order than the numbers on the cards.

6. How long does it take to play a round of cards using the full deck?

This depends upon the amount of discussion and how familiar the players are with application security concepts. But perhaps allow 1.5 to 2.0 hours for 4-6 people.

OWASP
Open Web Application Security Project

Project Acknowledgements

- Microsoft SDL Team for the Elevation of Privilege Threat Modelling Game, published under a Creative Commons Attribution license, as the inspiration for Cornucopia and from which many ideas, especially the game theory, were copied.
- Keith Turpin and contributors to the "OWASP Secure Coding Practices – Quick Reference Guide," originally donated to OWASP by Boeing, which is used as the primary source of security requirements information to formulate the content of the cards.
- Contributors, supporters, sponsors and volunteers to the OWASP ASVS, AppSensor and Web Framework Security Matrix projects, Mitre's Common Attack Pattern Enumeration and Classification (CAPEC), and SAFECode's "Practical Security Stories and Security Tasks for Agile Development Environments" which are all used in the cross-references provided.