



## Elevation of Privilege Anleitung

Artikulieren Sie Bedrohungen klar und nachvollziehbar. Bedrohungen müssen testfähig/überprüfbar sein. Überlegen Sie, wie. Bedrohungen sollen innerhalb des Systems adressierbar sein. Streit um die Gültigkeit einer Bedrohung können Sie mit der Frage auflösen: "Würden wir einen Bugreport, ein Feature-Request oder eine Design-Änderung hierfür akzeptieren?". Ist die Antwort "ja", handelt es sich um eine relevante Bedrohung. Dies bedeutet nicht, dass Bedrohungen außerhalb dieser Betrachtung nicht real sind. Es hilft lediglich, sich auf adressierbare Bedrohungen zu konzentrieren. Bedrohungen die einleiten mit "Ein Angreifer könnte..." werden erläutert im Stile "..und zwar wie folgt...". Karten mit "Ihr Code..." werden wie folgt vorgetragen: "Unser Code... und zwar wie folgt".

Das Kartendeck enthält einige Spezialkarten: Trümpfe und offene Bedrohungen. EoP Karten sind Trümpfe. Sie gewinnen die Runde, auch wenn sie einen niedrigeren Wert haben, als die Suite/Farbe, mit der die Runde begonnen wurde. Asses sind offene Bedrohungen. Wer ein Ass spielt, muss eine Bedrohung finden, die auf keiner anderen Karte steht und versuchen, sie auf das System anzuwenden.

Wenn alle Karten gespielt sind, gewinnt der Spieler mit der höchsten Punktezahl.

**Viel Spaß beim Spielen!**

# Anleitung



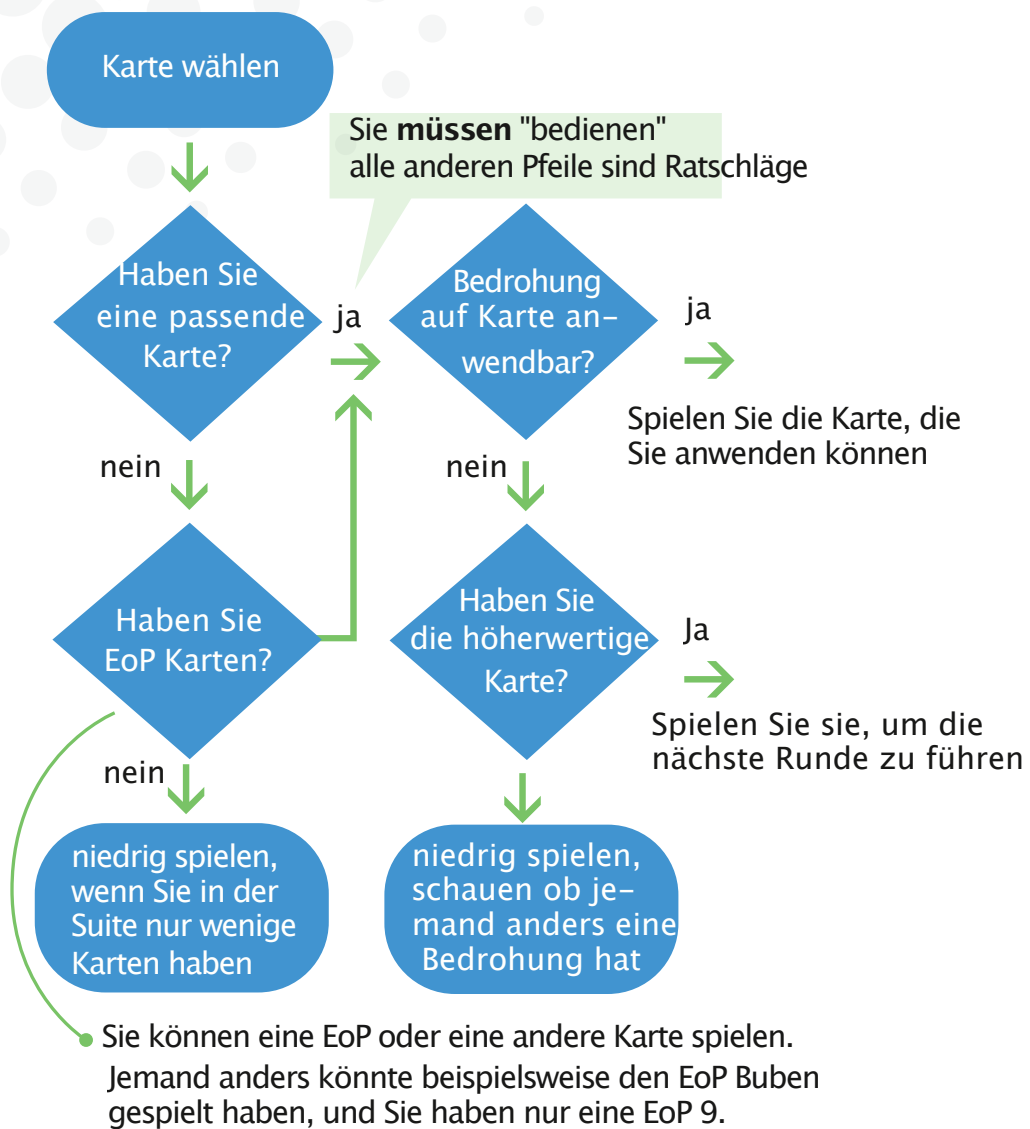
### Inhalt:

- 2 Karten mit der Spielanleitung
- 1 Karte mit einem Strategie-Diagramm
- 6 STRIDE "Suites" von Spielkarten
  1. Spoofing: 2-K, Ace
  2. Tampering: 3-K, Ace
  3. Repudiation: 2-K, Ace
  4. Information Disclosure: 2-K, Ace
  5. Denial of Service: 2-K, Ace
  6. Elevation of Privilege: 5-K, Ace (Trump cards)
- **6** STRIDE Threat Reference cards
- **1** About Threat Modeling and SDL card

© 2010 Microsoft Corporation. This work is licensed under the Creative Commons Attribution 3.0 United States License. To view the full content of this license, visit **<http://creativecommons.org/licenses/by/3.0/us/>** or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

# Anleitung

# Strategie



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege



**Microsoft®**

elevation of privilege





## Spoofing Fortsetzung

- 10. Ein Angreifer kann wählen, dass eine schwächere oder gar keine Authentisierung genutzt wird.
- J. Ein Angreifer kann die auf einem Client gespeicherten Credentials stehlen und wieder verwenden..
- Q. Ein Angreifer kann den Mechanismus angreifen, mit dem Passwörter zurückgesetzt oder aktualisiert werden (Account Recovery erfordert nicht die Eingabe des alten Passworts).
- K. Ihr System wird mit einem Default Adminpasswort ausgeliefert und erzwingt nicht die Änderung des Passworts.
- A. Sie haben einen neuen Spoofing Angriff erfunden.

# Spoofing



## Tampering Fortsetzung

- J.** Ein Angreifer kann auf eine Ressource schreiben, weil es keine ACLs gibt, oder weil jeder berechtigt ist (world writable).
- Q.** Ein Angreifer kann Parameter über eine Trust Boundary hinweg ändern, nachdem sie validiert wurde (z.B. in einem hidden field, in HTML, oder einem Pointer an eine kritische Speicherstelle im RAM übergeben).
- K.** Ein Angreifer kann Code mithilfe eines Extension Points einbinden.
- A.** Sie haben einen neuen Tampering Angriff erfunden.

# Tampering



## Repudiation Fortsetzung

- 10. Ein Angreifer kann beliebige Logdaten in ein Logsystem einschleusen, weil die Logquellen nicht oder nur schwach authentisiert werden.
- J.** Ein Angreifer kann unbemerkt Logs editieren oder löschen.
- Q.** Ein Angreifer kann abstreiten, etwas getan zu haben und es gibt keine brauchbaren Daten, um das Gegenteil zu beweisen.
- K.** Das System hat keine Logs.
- A.** Sie haben einen neuen Repudiation Angriff erfunden.

# Repudiation





## Information Disclosure Fortsetzung

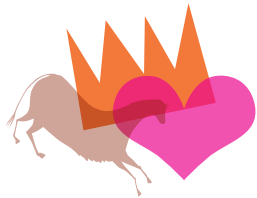
- 9. Ein Angreifer kann sensible Informationen in einer Datei lesen, weil deren Zugriffsrechte falsch gesetzt sind (schwache ACLs).
- 10. Ein Angreifer kann mangels Zugriffsbeschränkungen eine sensible Datei lesen.
- J. Ein Angreifer kann den statischen Schlüssel finden, der zur Verschlüsselung genutzt wird.
- Q. Ein Angreifer kann einen Kommunikationskanal vollständig mitlesen, weil dieser unverschlüsselt ist.
- K. Ein Angreifer kann Netzwerkinformationen lesen, weil keine Kryptografie genutzt wird.
- A. Sie haben einen neuen Information Disclosure Angriff erfunden.



## Denial of Service cont.

- 8. Ein Angreifer kann einen Server unverfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat (Server, authentisiert, persistent).
- 9. Ein Angreifer kann einen Client unverfügbar machen, ohne dass eine Authentisierung stattgefunden hat, und das Problem besteht nach dem Angriff fort (Client, anonym, persistent).
- 10. Ein Angreifer kann, ohne zu authentisieren, einen Server unverfügbar machen. Das Problem besteht fort, nachdem der Angriff aufgehört hat (Server, anonym, persistent).
- J. Ein Angreifer kann das Logging-Subsystem außer Betrieb setzen.
- Q. Ein Angreifer kann eine verwundbare Systemkomponente missbrauchen, um eine (volumenbasierte) DoS Attacke um den Faktor 10 zu verstärken.
- K. Ein Angreifer kann eine verwundbare Systemkomponente missbrauchen, um ein DoS Attacke mehr als 100fach zu verstärken.
- A. Sie haben eine neue Denial of Service Attacke erfunden.

# Denial of Service



# Elevation of Privilege



# SDL

The Elevation of Privilege game is a fun and easy way to get started understanding the security of your systems by threat modeling. As you discover and correct design-level security problems, it's worth thinking about the other ways security issues can creep into your code. Microsoft has a large collection of free resources available to help you get started with the Security Development Lifecycle (SDL).

To learn more about threat modeling and the Microsoft Security Development Lifecycle, visit our website at [microsoft.com/sdl/](https://microsoft.com/sdl/)

**Microsoft®**

Security Development Lifecycle