

# Instructions



## Elevation of Privilege Instructions

Threats should be articulated clearly, testable, and addressable. In the event that a threat leads to an argument, you can resolve it by asking the question: "Would we take an actionable bug, feature request or design change for this?" If the answer is yes, it is a real threat. (This doesn't mean that threats outside of that aren't real. It's simply a way to focus discussion on actionable threats.) Questions that start with "There's a way" should be read as "There's a way, and here's how..." while questions that start with "Your code" should be read "The code we're collectively creating, and here's how."

The deck contains a number of special cards: trumps and open threats. EoP cards are trumps; they take the trick even if they have a lower value than the suit that was led. The ace of each suit is an open threat card. When played, the player must identify a threat not listed on another card.

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

**Remember to have fun!**

## Instructions 1

### Elevation of Privilege Instructions

Draw a diagram of the system you want to threat model before you deal the cards.

Deal the deck to 3-6 players. Play starts with the 2 of Tampering. Play clockwise, and each player in turn continues using the suit if they have a card in that suit. If the player doesn't have a card from that suit, the player can use another suit. Each round is won by the highest card played in the suit that was led, unless an Elevation of Privilege (EoP) card is played. In that case the high value EoP card wins.

To play a card, read the card, announce your threat and record it. If the player can't link the threat to the system, play proceeds.

The winner of a hand selects the card (and suit) to lead the next hand. Take a few minutes between hands to think about threats.

**Notes:**  
1 for a threat on your card. +1 for taking the trick

### Contents:

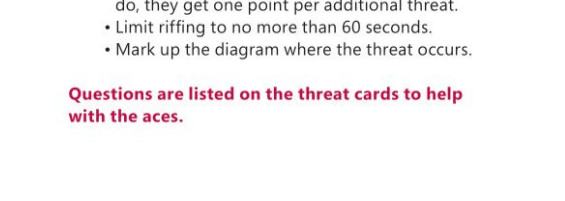
- 2 Instruction cards
- 1 Strategy Diagram card
- 15 STRIDE Threat cards (suits)
  1. Spoofing: 2-K, Ace
  2. Tampering: 2-K, Ace
  3. Repudiation: 2-K, Ace
  4. Information Disclosure: 2-K, Ace
  5. Denial of Service: 2-K, Ace
  6. Elevation of Privilege: 2-K, Ace (Trump cards)
- 15 STRIDE Threat Reference cards
- 1 About Threat Modeling card

Portions © 2010 Microsoft Corporation. This game was invented by Adam Shostack at Microsoft. The original EoP deck was produced by Microsoft.  
This edition © 2021 Agile Stationery Limited. This edition is not publicly licensed. The publication of works derived from new material in the deck is not permitted without prior consent.

## Instructions

## Instructions

## Instructions



## Instructions 2

### Elevation of Privilege Variants

- Optional variants:**
- You may pass cards after the third trick. This is helpful if you have cards that you can't tie to the system. Someone else may be able to.
  - Double the number of points, and give one point for threats on other people's cards.
  - Other players may "sift" on the threat and if they do, they get one point per additional threat.
  - Limit rifling to no more than 60 seconds.
  - Mark up the diagram where the threat occurs.
- Questions are listed on the threat cards to help with the ace.**

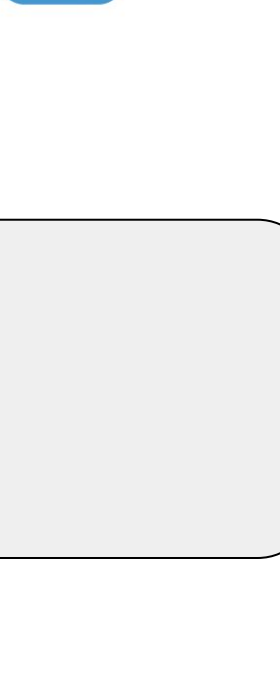
### Strategy



### Context



### Play



## Instructions

In the bottom left hand corner during game play



Click to open rule book

Click to see full controls of Tabletopia



Click to see full controls of Tabletopia

Actions	Controls
Adjust camera position	Left Click & Hold or WASD keys
Adjust camera perspective	Right Click & Hold
Read/Zoom in on card	1. Hover over a card and click space 2. This allows you to better read the card, while not changing its position. 3. Click space button again to unzoom
Deal all cards to players	Right Click Deck >> Deal >> Select highest # (Repeat until all cards are dealt)
Move card	Left Click & Hold on while hovering over a card
Flip card	F key
Put a card in your hand on table	Drag card to bottom of screen until you see blue bar
Draw # card(s) from deck	Right Click Deck >> Draw >> Select #

# Appendix

**Spoofing**

2. An attacker could take over the port or socket that the server normally uses.
3. An attacker could try one credential after another and there's nothing to slow them down (online or offline).
4. An attacker can anonymously connect because we expect authentication to be done at a higher level.
5. An attacker can confuse a client because there are too many ways to identify a server.
6. An attacker can spoof a server because identifiers aren't stored on the client and checked for consistency on re-connection (that is, there's no key persistence).
7. An attacker can connect to a server or peer over a link that isn't authenticated (and encrypted).
8. An attacker could steal credentials stored on the server and reuse them (for example, a key is stored in a world readable file).
9. An attacker who gets a password can reuse it (use stronger authenticators).

continued on back

**Spoofing cont.**

10. An attacker can choose to use weaker or no authentication.
- J. An attacker could steal credentials stored on the client and reuse them.
- Q. An attacker could go after the way credentials are updated or recovered (account recovery doesn't require disclosing the old password).
- K. Your system ships with a default admin password and doesn't force a change.
- A. You've invented a new Spoofing attack.

**Tampering**

2. An attacker can take advantage of your custom key exchange or integrity control which you built instead of using standard crypto.
3. An attacker can modify your build system and produce signed builds of your software.
4. Your code makes access control decisions all over the place, rather than with a security kernel.
5. An attacker can replay data without detection because your code doesn't provide timestamps or sequence numbers.
6. An attacker can write to a data store your code relies on.
7. An attacker can bypass permissions because you don't make names canonical before checking access permissions.
8. An attacker can manipulate data because there's no integrity protection for data on the network.
9. An attacker can provide or control state information.

continued on back

**Tampering cont.**

10. An attacker can alter information in a data store because it has weak/open permissions or includes a group which is equivalent to everyone ("anyone with a Facebook account").
- J. An attacker can write to some resource because permissions are granted to the world or there are no ACLs.
- Q. An attacker can change parameters over a trust boundary and after validation (for example, an important parameter in a hidden field in HTML, passing a pointer to critical memory).
- K. An attacker can load code inside your process via an extension point.
- A. You've invented a new Tampering attack.

**Repudiation**

2. An attacker can pass data through the log to attack a log reader, and there's no documentation of what sorts of validation are done.
3. A low privilege attacker can read interesting security information in the logs.
4. An attacker can alter files or messages because the digital signature system you're implementing is weak, or uses MACs where it should use a signature.
5. An attacker can alter log messages on a network because they lack strong integrity controls.
6. An attacker can create a log entry without a timestamp (or no log entry is timestamped).
7. An attacker can make the logs wrap around and lose data.
8. An attacker can make a log lose or confuse security information.
9. An attacker can use a shared key to authenticate as different principals, confusing the information in the logs.

continued on back

**Repudiation cont.**

10. An attacker can get arbitrary data into logs from unauthenticated or weakly authenticated outsiders without validation.
- J. An attacker can edit logs and there's no way to tell (perhaps because there's no heartbeat option for the logging system).
- Q. An attacker can say "I didn't do that," and you would have no way to prove them wrong.
- K. The system has no logs.
- A. You've invented a new Repudiation attack.

**Information Disclosure**

2. An attacker can brute-force file encryption because there's no defense in place (example defense: password stretching).
3. An attacker can see error messages with security-sensitive content.
4. An attacker can read content because messages (for example, an email or HTTP cookie) aren't encrypted even if the channel is encrypted.
5. An attacker may be able to read a document or data because it's encrypted with a non-standard algorithm.
6. An attacker can read data because it's hidden or obscured (for undo or change tracking) and the user might forget that it's there.
7. An attacker can act as a "man in the middle" because you don't authenticate endpoints of a network connection.
8. An attacker can access information through a search index, logger, or other such mechanism.

continued on back

**Information Disclosure cont.**

9. An attacker can read sensitive information in a file with permissive permissions.
10. An attacker can read information in files or databases with no access controls.
- J. An attacker can discover the fixed key being used to encrypt.
- Q. An attacker can read the entire channel because the channel (for example, HTTP or SMTP) isn't encrypted.
- K. An attacker can read network information because there's no cryptography used.
- A. You've invented a new Information Disclosure attack.

**Denial of Service**

2. An attacker can make your authentication system unusable or unavailable.
3. An attacker can drain our easily replaceable battery (battery, temporary)
4. An attacker can drain a battery that's hard to replace (sealed in a phone, an implanted medical device, or in a hard to reach location) (battery, persist)
5. An attacker can spend our cloud budget (budget, persist)
6. An attacker can make a server unavailable or unusable without ever authenticating but the problem goes away when the attacker stops (server, anon, persist, temporary)
7. An attacker can make a client unavailable or unusable and the problem persists after the attacker goes away (client, auth, persist)
8. An attacker can make a server unavailable or unusable and the problem persists after the attacker goes away (server, auth, persist)

continued on back

**Denial of Service cont.**

9. An attacker can make a client unavailable or unusable without ever authenticating and the problem persists after the attacker goes away (client, anon, persist)
10. An attacker can make a server unavailable or unusable without ever authenticating and the problem persists after the attacker goes away (server, anon, persist)
- J. An attacker can cause the logging subsystem to stop working.
- Q. An attacker can amplify a Denial of Service attack through this component with amplification on the order of 10 to 1.
- K. An attacker can amplify a Denial of Service attack through this component with amplification on the order of 100 to 1.
- A. You've invented a new Denial of Service attack.

**Elevation of Privilege (EoP)**

2. An attacker has compromised a key technology supplier.
3. An attacker can access the cloud service which manages your devices.
4. An attacker can escape from a container or other sandbox.
5. An attacker can force data through different validation paths which give different results.
6. An attacker could take advantage of permissions you ask for, but don't use.
7. An attacker can provide a pointer across a trust boundary rather than data which can be validated.
8. An attacker can enter data that is checked while still under the attacker's control and used later on the other side of a trust boundary.
9. There's no reasonable way for callers to figure out what validation of tainted data you perform before passing it to them.

continued on back

**Elevation of Privilege (EoP) cont.**

10. There's no reasonable way for a caller to figure out what security assumptions you make.
- J. An attacker can reflect input back to a user, like cross-site scripting.
- Q. You include user-generated content within your page, possibly including the content of random URLs.
- K. An attacker can inject a command that the system will run at a higher privilege level.
- A. You've invented a new Elevation of Privilege attack.

**About**

Threat Modeling

The Elevation of Privilege game is designed to be the easiest way to start looking at your design from a security perspective. It's one way to threat model, intended to be picked up and used by any development group. Because the game uses STRIDE threats, it gives you a framework for thinking, and specific actionable examples of those threats.

STRIDE stands for:  
 Spoofing: Impersonating something or someone else.  
 Tampering: Modifying data or code.  
 Repudiation: Claiming not to have performed an action.  
 Information Disclosure: Exposing information to someone not authorized to see it.  
 Denial of Service: Denying or degrading service to users.  
 Elevation of Privilege: Gain capabilities without proper authorization.

For more about the game, please visit <https://shostack.org/games/elevation-of-privilege>

Published by Agile Stationery [aj@stationery.com](mailto:aj@stationery.com)

**About**

Threat Modeling

The Elevation of Privilege game is designed to be the easiest way to start looking at your design from a security perspective. It's one way to threat model, intended to be picked up and used by any development group. Because the game uses STRIDE threats, it gives you a framework for thinking, and specific actionable examples of those threats.

STRIDE stands for:  
 Spoofing: Impersonating something or someone else.  
 Tampering: Modifying data or code.  
 Repudiation: Claiming not to have performed an action.  
 Information Disclosure: Exposing information to someone not authorized to see it.  
 Denial of Service: Denying or degrading service to users.  
 Elevation of Privilege: Gain capabilities without proper authorization.

For more about the game, please visit <https://shostack.org/games/elevation-of-privilege>

Published by Agile Stationery [aj@stationery.com](mailto:aj@stationery.com)