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 3 of Tampering. Play clockwise, and each player in turn follows in the suit if they have a card in the suit. If they don't have that suit, they can play another suit. The high card played takes the trick, with Elevation of Privilege taking precedence over the suit lead. Only Elevation of Privilege (EoP) or the lead suit can take a trick.

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.

Take few minutes between hands to think about threats.

Points:

1 for a threat on your card, +1 for taking the trick

Instructions

Elevation of Privilege Instructions

Threats should be articulated clearly, testable, and addressable. In the event that a threat leads to an argument, the threat should resolve by asking the question: "Would we take an actionable bug, feature request or design change for that?" 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 are 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

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 "riff" on the threat and if they do, they get one point per additional threat.
- Limit riffing to no more than 60 seconds.
- Mark up the diagram with where the threat occurs.

Questions are listed on the threat cards to help with the Aces.

Thanks to Laurie Williams for inspiration.

Instructions

Context

Share the rules

Deal the deck to start play

Play

Wrap up

Play

Whoever has 3 of Tampering starts

Whoever has 3 of Tampering:

Play card

Document issue

Have all players played in this hand?

If no:
Play proceeds to next (clockwise) player

If yes:
Play starts with winner of the just-ended hand

(Taking 3 minutes to consider cards may improve flow)

Strategy: see reverse

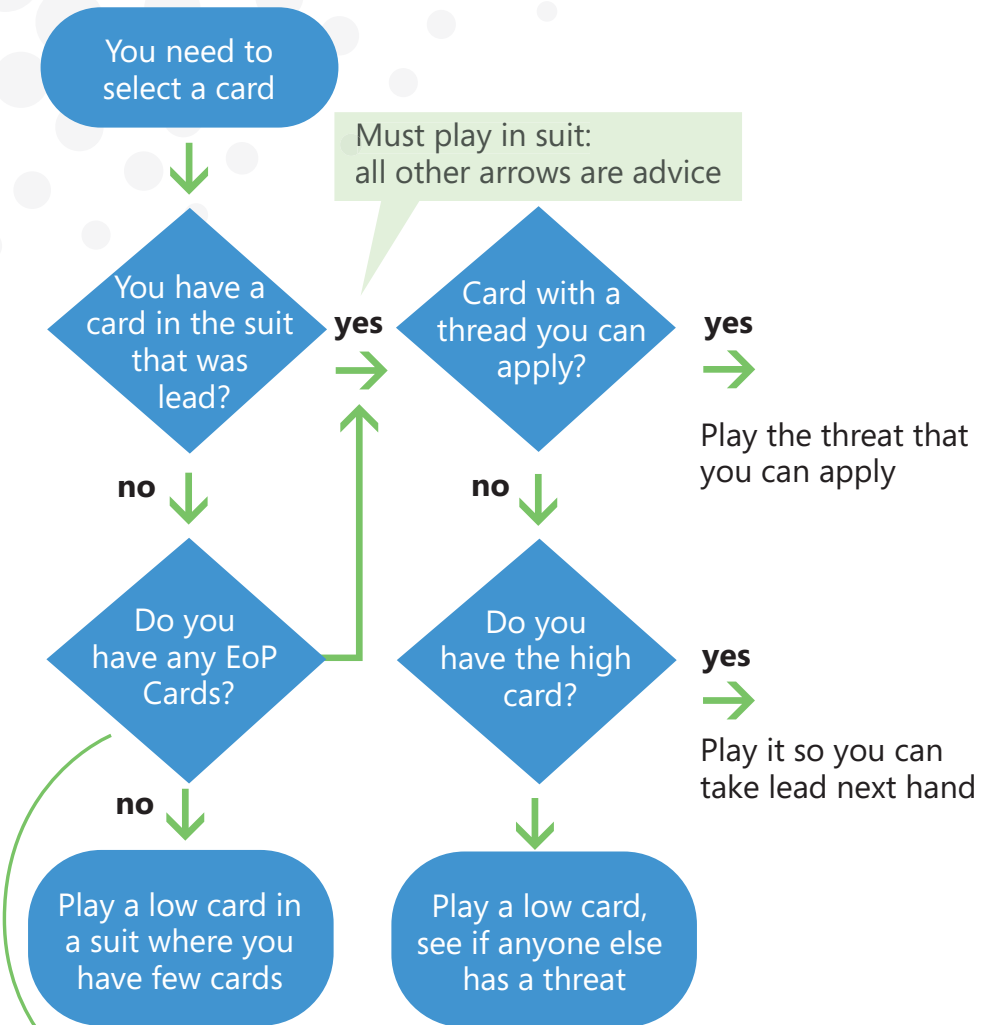
yes

Record hand

Is there time for another hand?

Wrap up

Strategy



Choice: Play EoP or another card. For example, someone else may have played the Jack of EoP, and you only have a 9.

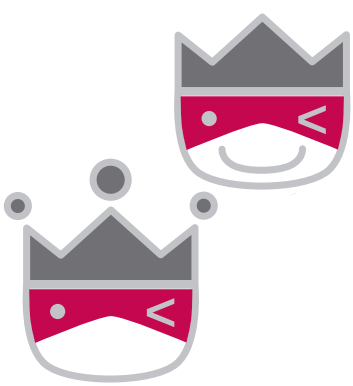
Microsoft®

elevation of privilege

2

Usurpation

Un attaquant peut squatter le port ou le socket que le serveur utilise normalement.



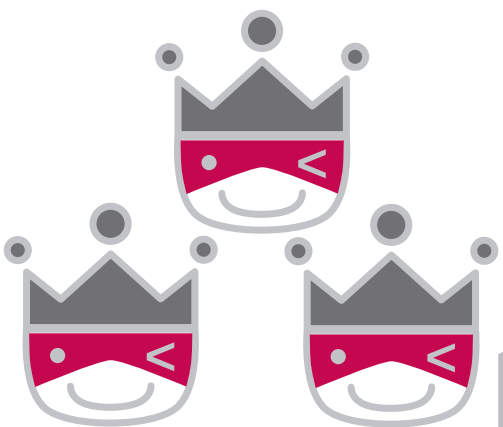
Spoofing

An attacker could squat on the random port or socket that the server normally uses

3

Usurpation

Un attaquant peut essayer des identifiants / mot de passe un après l'autre et il n'y a rien qui le ralentisse (en ligne ou hors ligne)



Spoofing

An attacker could try one credential after another and there's nothing to slow them down (online or offline)

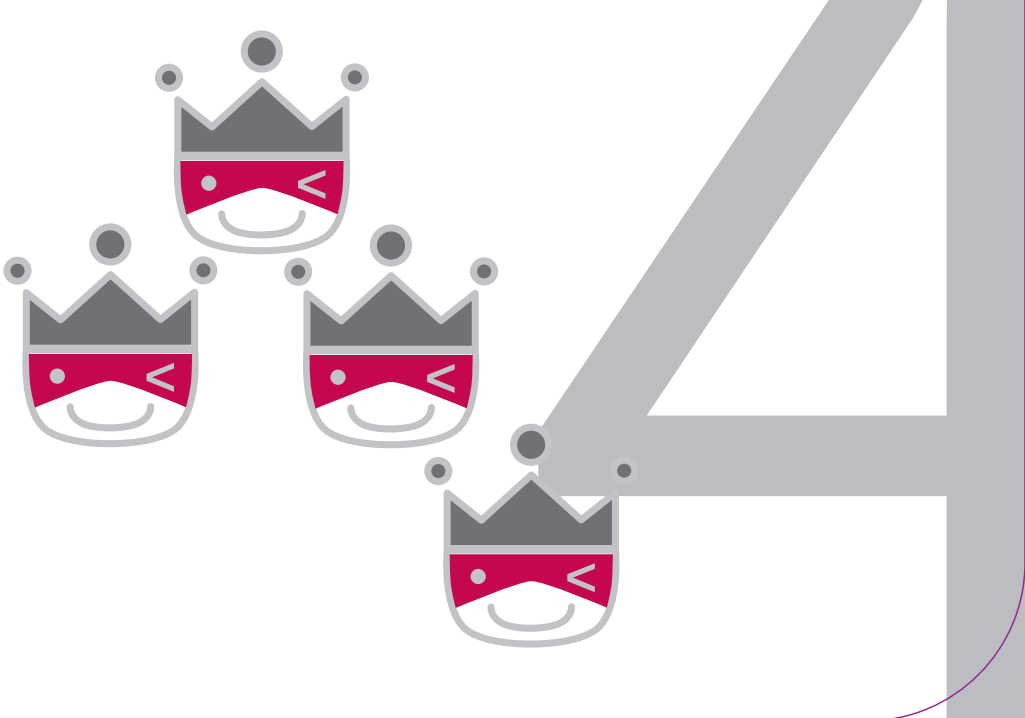
4

Usurpation

Un attaquant peut se connecter anonymement, car nous assumons que l'authentification a été faite à un plus haut niveau.

Spoofing

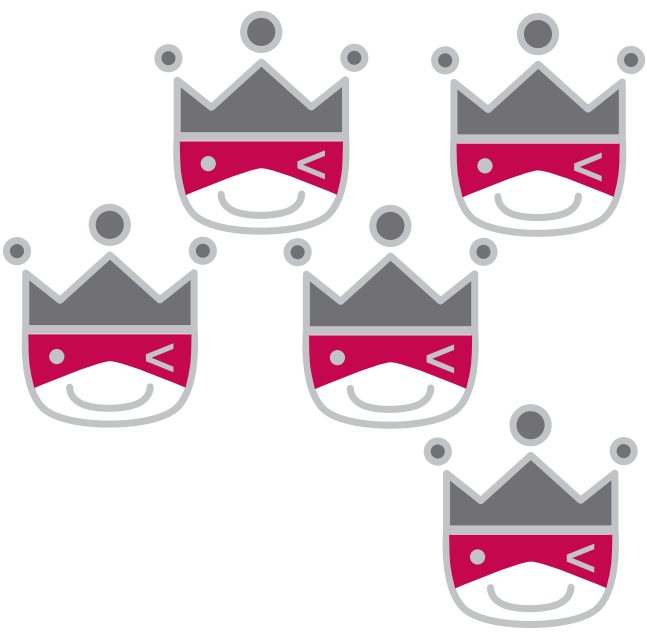
An attacker can anonymously connect, because we expect authentication to be done at a higher level



5

Usurpation

Un attaquant peut confondre un client, car il y a trop de façons d'identifier un serveur



Spoofing

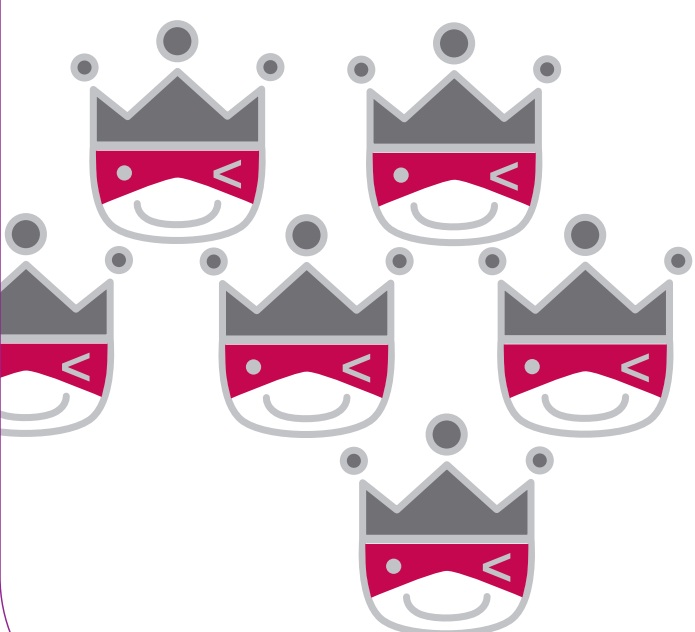
An attacker can confuse a client because there are too many ways to identify a server

6 Usurpation

Un attaquant peut se faire passer pour un serveur, car l'identifiant n'est pas stocké sur le client et il n'y a pas de vérification de cohérence à la reconnexion (c'est-à-dire pas de persistance de clé)

Spoofing

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)



6

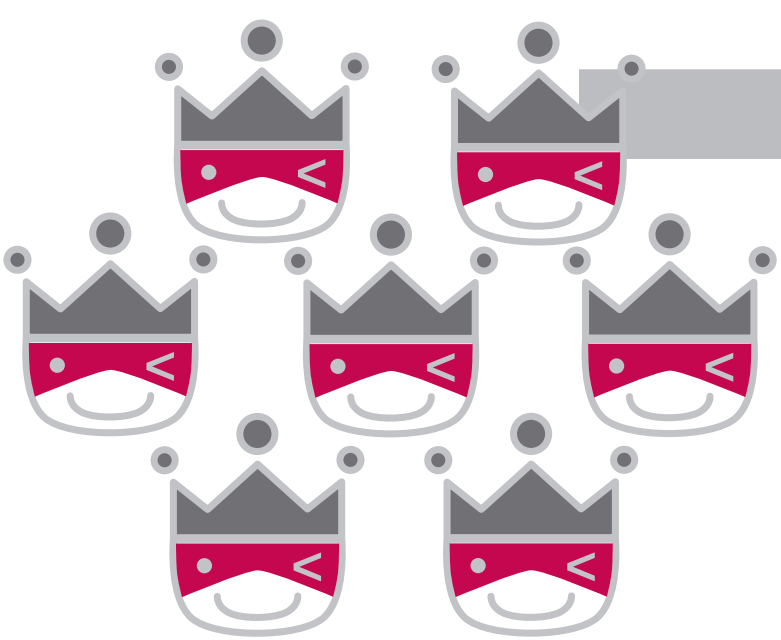
7

Usurpation

Un attaquant peut se connecter à un serveur ou peut voir passer une connexion non authentifiée (et non encrypté).

Spoofing

An attacker can connect to a server or peer over a link that isn't authenticated (and encrypted)



8

Usurpation

Un attaquant peut voler des identifiants / mots de passe stockés sur le serveur et les réutiliser (par exemple, une clé stockée dans un fichier en lecture pour tous)

Spoofing

An attacker could steal credentials stored on the server and reuse them (for example, a key is stored in a world readable file)

9

Usurpation

Un attaquant qui obtient un mot de passe peut le réutiliser (Utiliser des authentificateurs plus fort)

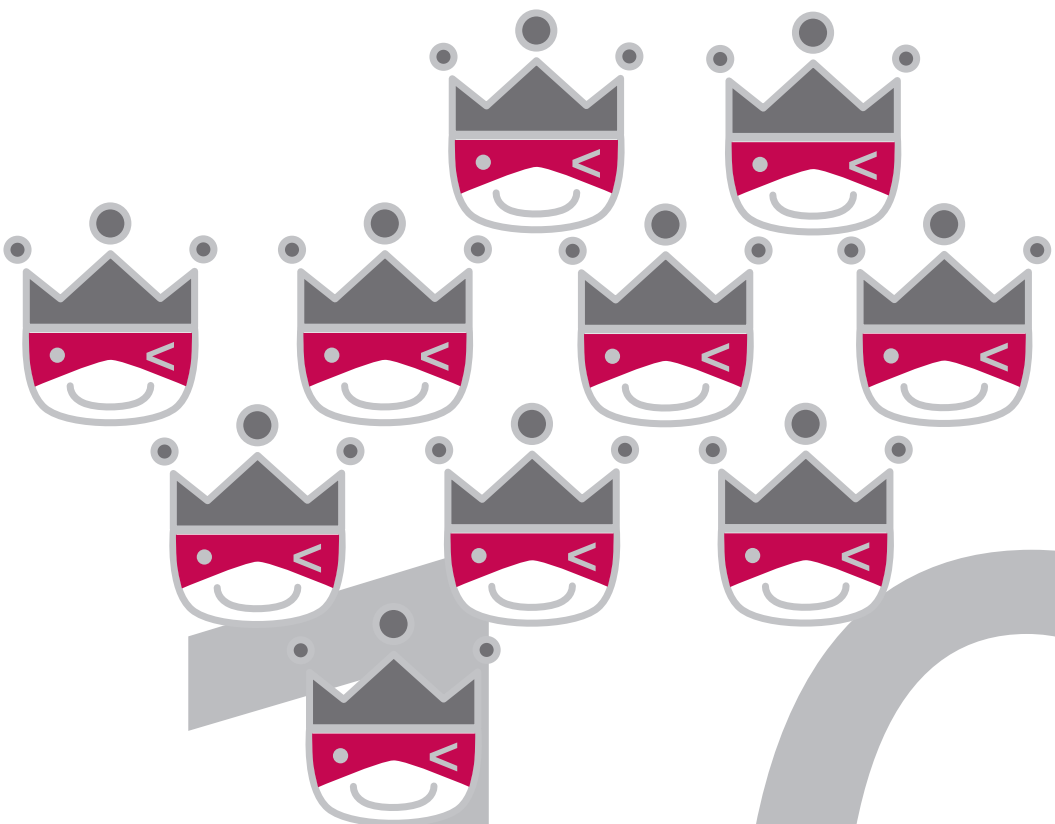
Spoofing

An attacker who gets a password can reuse it (Use stronger authenticators)

10

Usurpation

Un attaquant peut choisir d'utiliser une authentification plus faible ou pas d'authentification



Spoofing

An attacker can choose to use weaker or no authentication

J

Usurpation

Un attaquant peut voler des identifiants / mots de passe sur le client et les réutiliser

Spoofing

An attacker could steal credentials stored on the client and reuse them

Usurpation

Un attaquant peut tenter d'obtenir des identifiants / mot de passe basé sur la façon qu'ils sont mis à jour ou restaurés (par exemple, la récupération d'un compte ne requiert pas de fournir l'ancien mot de passe)

Spoofing

An attacker could go after the way credentials are updated or recovered (account recovery doesn't require disclosing the old password)

K

Usurpation

Votre système vient avec un mot de passe administrateur par défaut et ne force pas de changement

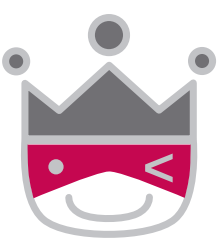
Spoofing

Your system ships with a default admin password, and doesn't force a change

A

Usurpation

Vous avez inventé une nouvelle attaque d'usurpation



Spoofing

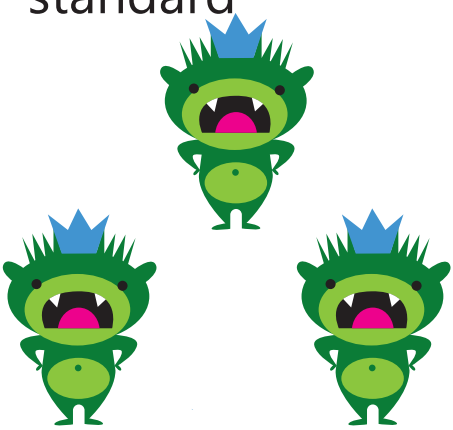
You've invented a new Spoofing attack

A

3

Falsification

Un attaquant peut tirer avantage de votre échange de clé maison ou de contrôle d'intégrité que vous avez développé au lieu d'utiliser de la cryptographie standard



Tampering

An attacker can take advantage of your custom key exchange or integrity control which you built instead of using standard crypto

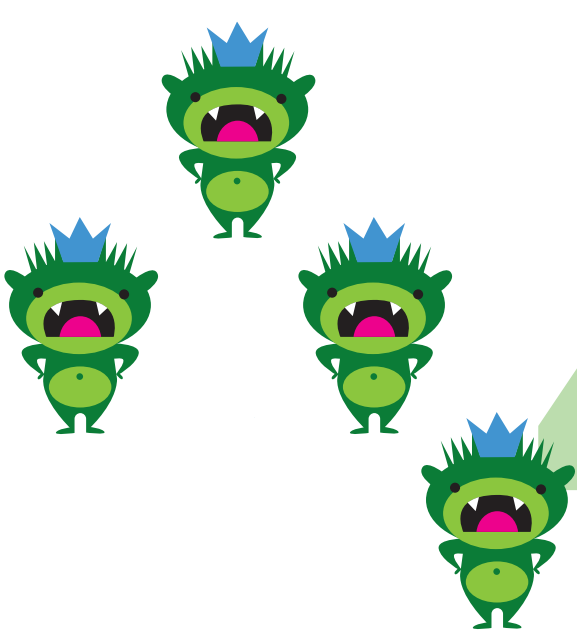
4

Falsification

Votre code fait des décisions de contrôle d'accès à pleins endroits, au lieu d'utiliser un noyau de sécurité

Tampering

Your code makes access control decisions all over the place, rather than with a security kernel

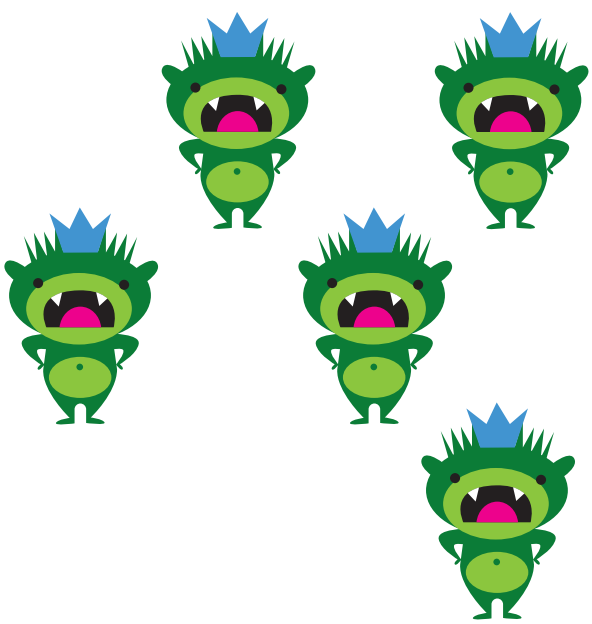


4

5

Falsification

Un attaquant peut rejouer des données sans être détecté parce que votre code ne produit pas de timestamp ou de nombres séquentiels



Tampering

An attacker can replay data without detection because your code doesn't provide timestamps or sequence numbers

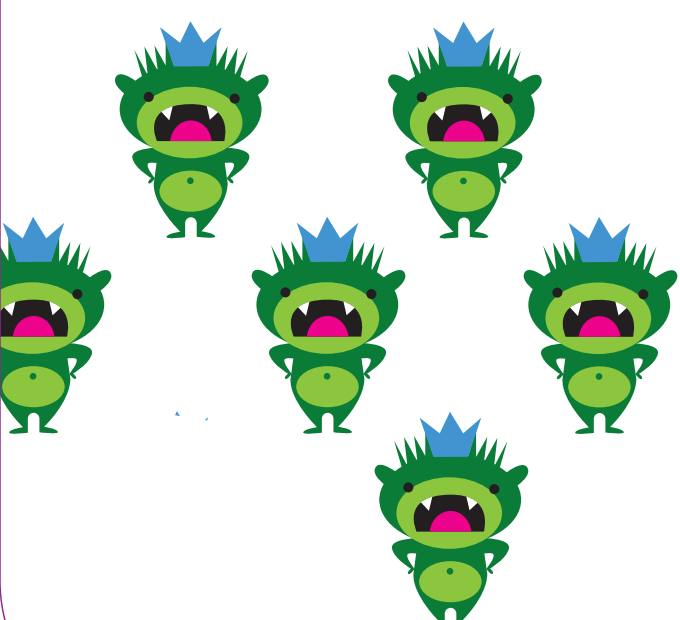
6

Falsification

Un attaquant peut écrire dans un stockage de données sur lequel votre code repose

Tampering

An attacker can write to a data store your code relies on



6

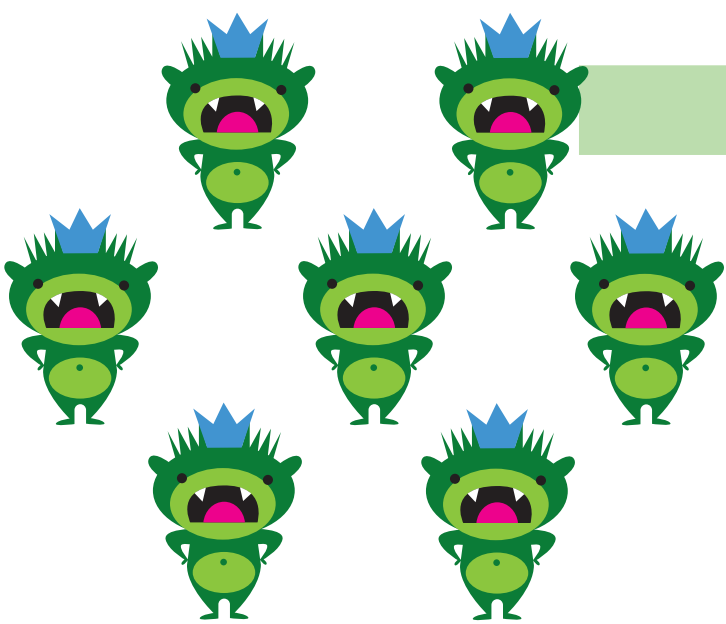
Falsification

7

Un attaquant peut contourner les permissions parce que vous ne standardisez pas les noms avant de vérifier les permissions d'accès

Tampering

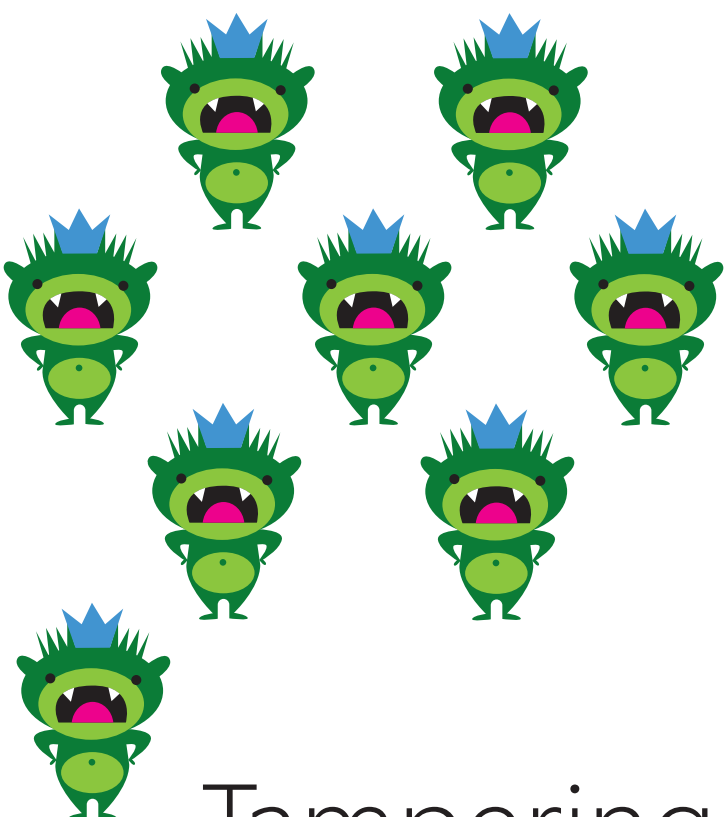
An attacker can bypass permissions because you don’t make names canonical before checking access permissions



8

Falsification

Un attaquant peut manipuler les données, car il n'y a pas de protection d'intégrité des données sur le réseau



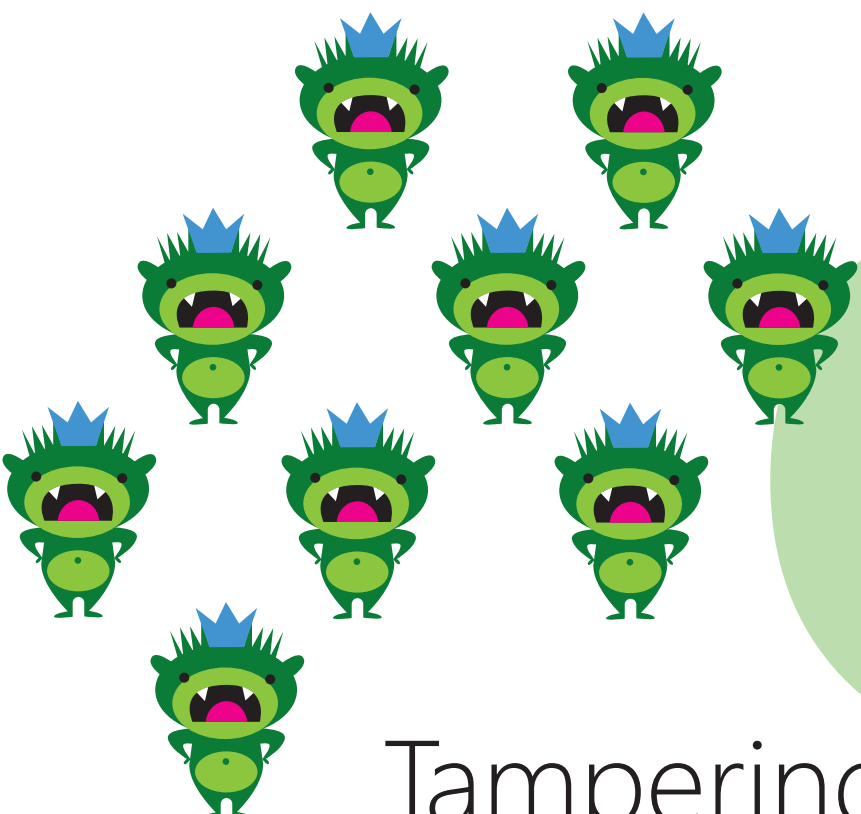
Tampering

An attacker can manipulate data because there's no integrity protection for data on the network

9

Falsification

Un attaquant peut fournir ou contrôler l'état de l'information

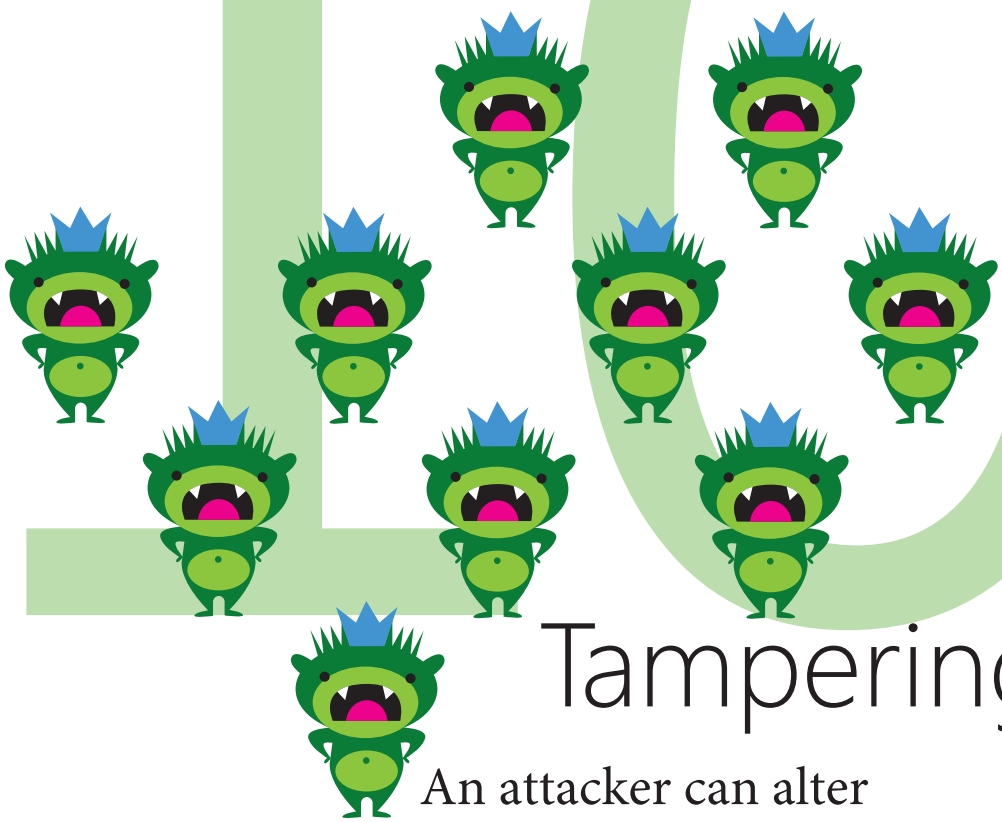


Tampering

An attacker can provide or control state information

Falsification

Un attaquant peut altérer l'information dans un stockage de données, car il a des permissions faibles ou ouvertes ou inclus un groupe qui équivaut à tout le monde ("n'importe qui avec un compte Facebook")



Tampering

An attacker can alter information in a data store because it has weak ACLs or includes a group which is equivalent to everyone ("all Live ID holders")

J

Falsification

Un attaquant peut écrire sur certaines ressources, car les permissions sont données à tous ou il n'y a pas de liste de contrôle d'accès (ACL)

Tampering

An attacker can write to some resource because permissions are granted to the world or there are no ACLs

Falsification

Q

Un attaquant peut changer les paramètres au-delà d'une frontière de confiance et après validation (par exemple, des paramètres importants dans des champs cachés HTML, ou passer un pointeur dans une zone de mémoire critique)
Frontière de confiance: par exemple la limite entre internet et réseau interne

Tampering

An attacker can change parameters over a trust boundary and after validation (for example, important parameters in a hidden field in HTML, or passing a pointer to critical memory)

Falsification

K

Un attaquant peut charger du code à l'intérieur de vos processus via un point d'extension (méthode pour augmenter les fonctionnalités d'une application sans modifier le code)

Tampering

An attacker can load code inside your process via an extension point

A

Falsification

Vous avez inventé une nouvelle attaque pour faire de la falsification

Tampering

You've invented a new Tampering attack

Répudiation

2

Un attaquant peut passer des données au travers du log pour attaquer un lecteur de logs, et il n'y a pas de documentation de quel type de validation sont faite

Repudiation

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

2

Répudiation

3

Un attaquant avec de bas privilèges peut lire de l'information de sécurité intéressante dans les logs

Repudiation

A low privilege attacker can read interesting security information in the logs

3

Répudiation

4

Un attaquant peut altérer les signatures digitales, car le système de signature digitale que vous utilisez est faible ou utilise des MAC (Message Authentication Code: garanti intégrité, mais pas non-répudiation) quand il devrait utiliser des signatures

Repudiation

An attacker can alter digital signatures because the digital signature system you're implementing is weak, or uses MACs where it should use a signature

Répudiation

5

Un attaquant peut altérer les messages du log dans un réseau, car il manque des contrôles d'intégrité forts

Repudiation

An attacker can alter log messages on a network because they lack strong integrity controls

Répudiation

6

Un attaquant peut créer une entrée de log sans timestamp (ou les entrées de logs n'ont pas de timestamp)

Repudiation

An attacker can create a log entry without a timestamp (or no log entry is timestamped)

Répudiation

7

Un attaquant peut faire en sorte que le log perd des données (par exemple remplir le log pour effacer les données les plus vieilles)

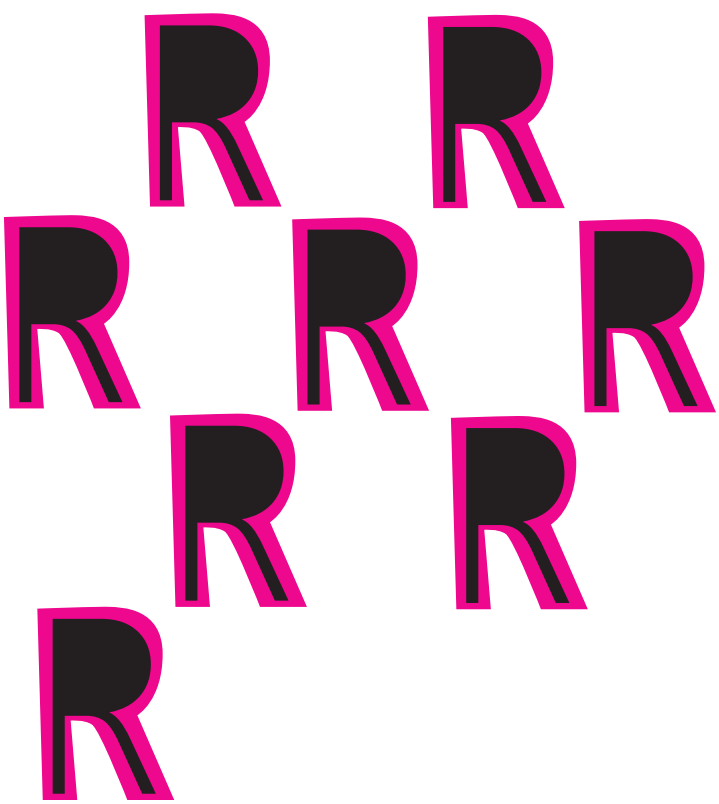
Repudiation

An attacker can make the logs wrap around and lose data

Répudiation

8

Un attaquant peut faire en sorte que le log perde ou mélange les informations de sécurités



Repudiation

An attacker can make a log lose or confuse security information

Répudiation

9

Un attaquant peut utiliser une clé partagée pour s'authentifier en tant qu'un principal (entité qu'un système informatique peut utiliser pour s'authentifier), mélangeant les informations du logs

Repudiation

An attacker can use a shared key to authenticate as different principals, confusing the information in the logs

Répudiation

10

Un attaquant peut écrire des données arbitraires dans le log à partir d'un utilisateur non authentifié ou faiblement authentifié sans validation

Repudiation

An attacker can get arbitrary data into logs from unauthenticated (or weakly authenticated) outsiders without validation

J

Répudiation

Un attaquant peut modifier le log et il n'y a pas de façon de le savoir (peut être qu'il n'y a pas d'options heartbeat pour le système de log)

Repudiation

An attacker can edit logs and there's no way to tell (perhaps because there's no heartbeat option for the logging system)

Répudiation

Q

Un attaquant peut dire "Ce n'est pas moi qui l'ai fait" et il n'y a pas de moyens de prouver qu'il a tort

Repudiation

An attacker can say “I didn’t do that,” and you’d have no way to prove them wrong

Répudiation

Le système n'a pas de log

K

Repudiation

The system has no logs

logs = 0

Répudiation

A

Vous avez inventé une nouvelle attaque de répudiation

Repudiation

You’ve invented a new Repudiation attack

2 Divulgation d'information

Un attaquant peut brute-forcer l'encryption d'un fichier, car il n'y a pas de défense en place (exemple de défense, password stretching)

Information Disclosure

An attacker can brute-force file encryption because there's no defense in place (example defense: password stretching)

3

Divulgation d'information

Un attaquant peut voir un message d'erreur avec du contenu de sécurité sensible

Information Disclosure

An attacker can see error messages with security sensitive content

4 Divulgation d'information

Un attaquant peut lire le contenu, car les messages (comme courriel ou cookie HTTP) ne sont pas encryptés même si le canal est encrypté

Information Disclosure

An attacker can read content because messages (say, an email or HTTP cookie) aren't encrypted even if the channel is encrypted

5 Divulgation d'information

Un attaquant peut être capable de lire un document ou des données car c'est encrypté avec un algorithme non standard

Information Disclosure

An attacker may be able to read a document or data because it's encrypted with a non-standard algorithm

6 Divulgation d'information

Un attaquant peut lire une donnée, car elle est cachée ou occultée (pour l'annulation ou le suivi des changements) et l'utilisateur peut oublier que c'est là

Information Disclosure

An attacker can read data because it’s hidden or occluded (for undo or change tracking) and the user might forget that it’s there

7

Divulgation d'information

Un attaquant peut agir comme 'man in the middle', car les appareils qui se connectent au réseau ne sont pas authentifiés

Information Disclosure

An attacker can act as a ‘man in the middle’ because you don’t authenticate endpoints of a network connection

8

Divulgation d'information

Un attaquant peut accéder à de l'information via un indexer de recherche, un journaliseur ou un autre mécanisme de ce type

Information Disclosure

An attacker can access information through a search indexer, logger, or other such mechanism

9

Divulgation d'information

Un attaquant peut lire de l'information sensible dans un fichier avec permission permissive

Information Disclosure

An attacker can read sensitive information in a file with bad ACLs

10

Divulgation d'information

Un attaquant peut lire de l'information dans des fichiers ou bases de données qui n'ont pas de contrôle d'accès

Information Disclosure

An attacker can read information in files with no ACLs

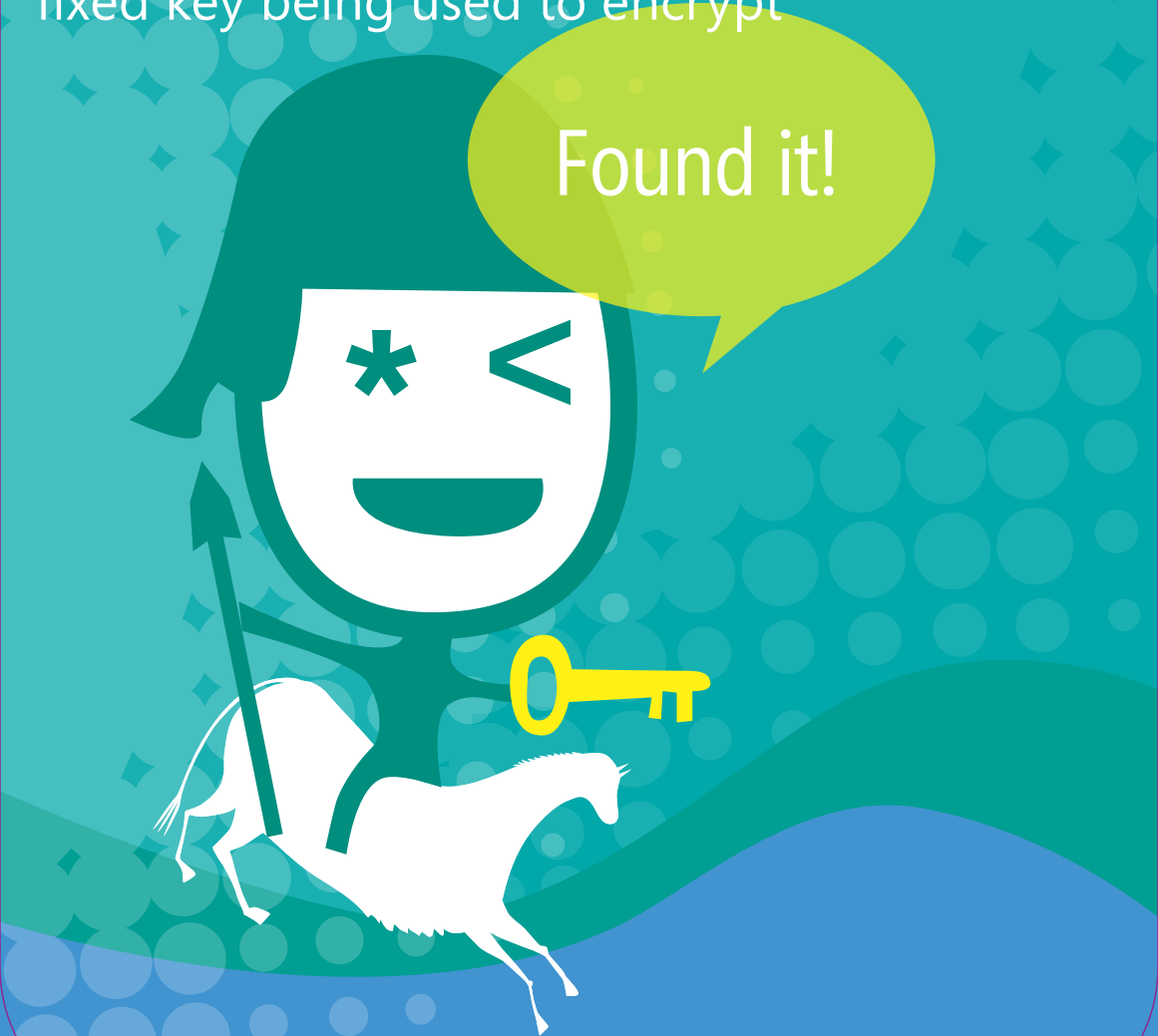
J

Divulgation d'information

Un attaquant peut découvrir les clés fixes qui sont utilisées pour encrypter

Information Disclosure

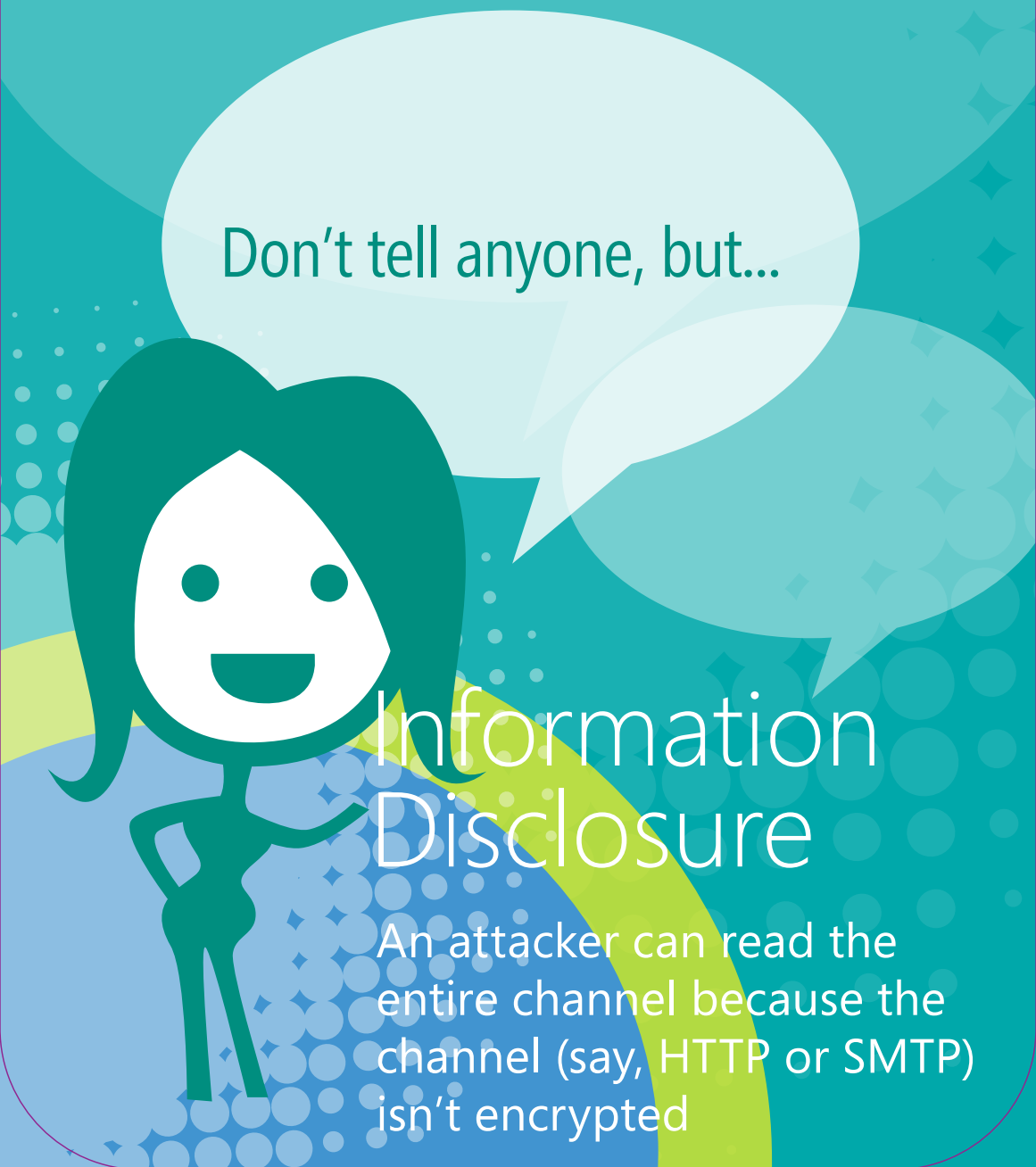
An attacker can discover the fixed key being used to encrypt



Q

Divulgation d'information

Un attaquant peut lire l'entièreté du canal, car le canal (comme HTTP ou SMTP) n'est pas encrypté



Information Disclosure

An attacker can read the entire channel because the channel (say, HTTP or SMTP) isn’t encrypted

K

Divulgation d'information

Un attaquant peut lire les informations réseau, car la cryptographie n'est pas utilisée

Information Disclosure

An attacker can read network information because there's no cryptography used

Divulgation d'information

A

Vous avez inventé une nouvelle attaque de divulgation d'information

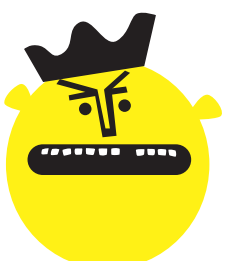
Information Disclosure

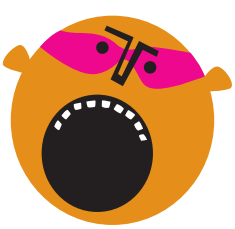
You've invented a new Information Disclosure attack

Déni de service

2

Un attaquant peut rendre votre système d'authentification inutilisable ou non disponible





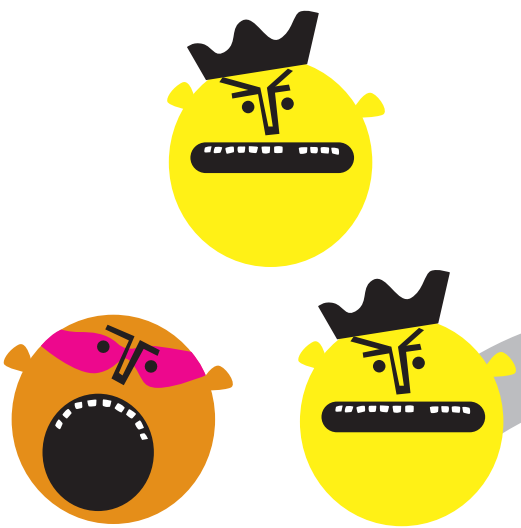
Denial of Service

An attacker can make your authentication system unusable or unavailable

Déni de service

3

Un attaquant peut rendre votre client inutilisable ou non disponible mais le problème cesse lorsque l'attaquant arrête



Denial of Service

An attacker can make a client unavailable or unusable but the problem goes away when the attacker stops

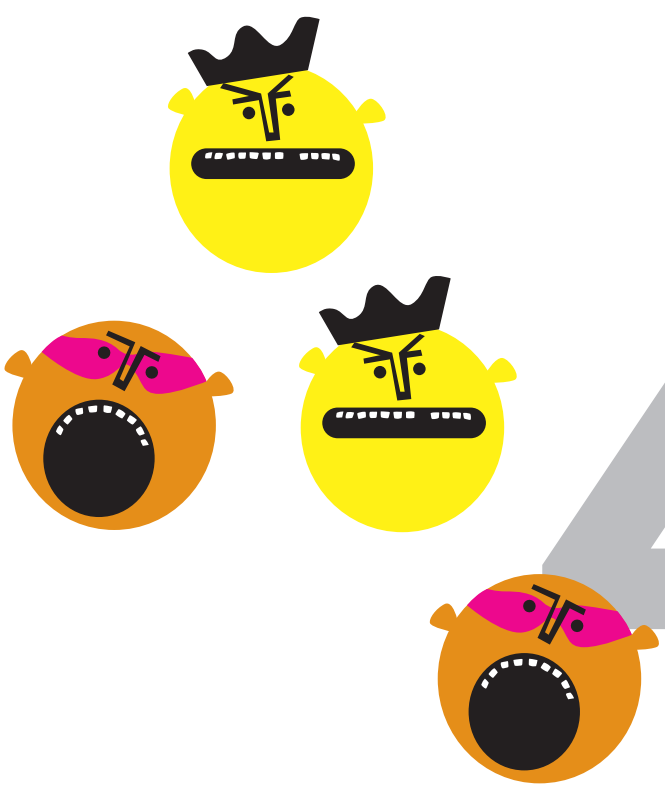
Déni de service

4

Un attaquant peut rendre votre serveur inutilisable ou non disponible mais le problème cesse lorsque l'attaquant arrête

Denial of Service

An attacker can make a server unavailable or unusable but the problem goes away when the attacker stops

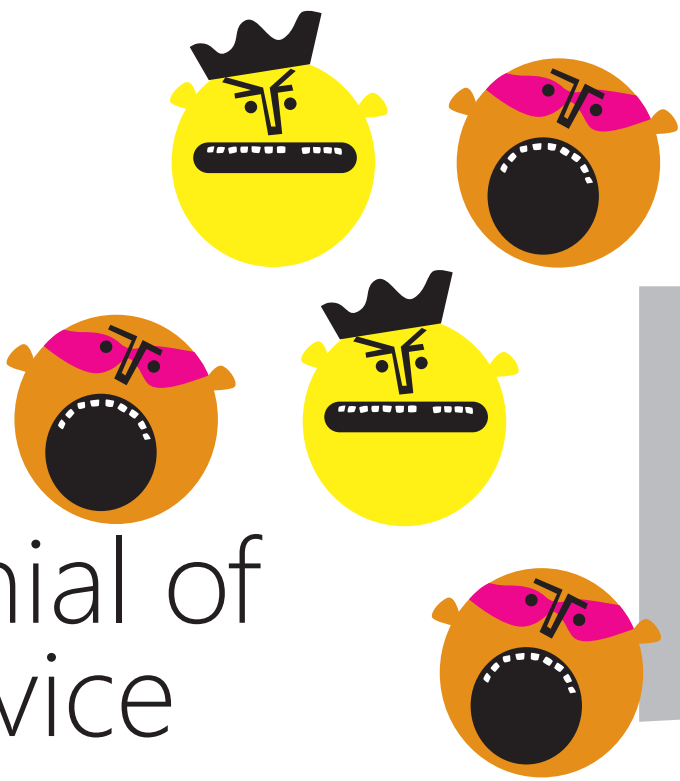


4

Déni de service

5

Un attaquant peut rendre votre client inutilisable ou non disponible sans jamais s'authentifier mais le problème cesse lorsque l'attaquant arrête



Denial of Service

An attacker can make a client unavailable or unusable without ever authenticating but the problem goes away when the attacker stops

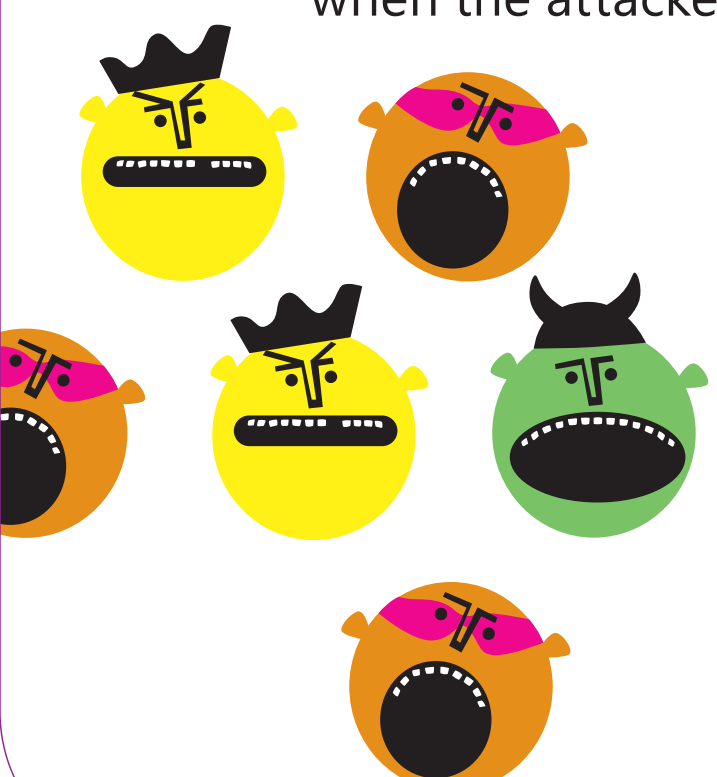
Déni de service

6

Un attaquant peut rendre votre serveur inutilisable ou non disponible sans jamais s'authentifier mais le problème cesse lorsque l'attaquant arrête

Denial of Service

An attacker can make a server unavailable or unusable without ever authenticating but the problem goes away when the attacker stops



6

Déni de service

7

Un attaquant peut rendre votre client inutilisable ou non disponible et le problème persiste lorsque l'attaquant arrête

Denial of Service

An attacker can make a client unavailable or unusable and the problem persists after the attacker goes away

Déni de service

8

Un attaquant peut rendre votre serveur inutilisable ou non disponible et le problème persiste lorsque l'attaquant arrête

Denial of Service

An attacker can make a server unavailable or unusable and the problem persists after the attacker goes away

Déni de service

9

Un attaquant peut rendre votre client inutilisable ou non disponible sans jamais s'authentifier et le problème persiste lorsque l'attaquant arrête

Denial of Service

An attacker can make a client unavailable or unusable without ever authenticating and the problem persists after the attacker goes away

Déni de service

10

Un attaquant peut rendre votre serveur inutilisable ou non disponible sans jamais s'authentifier et le problème persiste lorsque l'attaquant arrête

Denial of Service

An attacker can make a server unavailable or unusable without ever authenticating and the problem persists after the attacker goes away

Déni de service

J

Un attaquant peut faire cesser de fonctionner le sous-système de journalisation

Denial of Service

An attacker can cause the logging subsystem to stop working

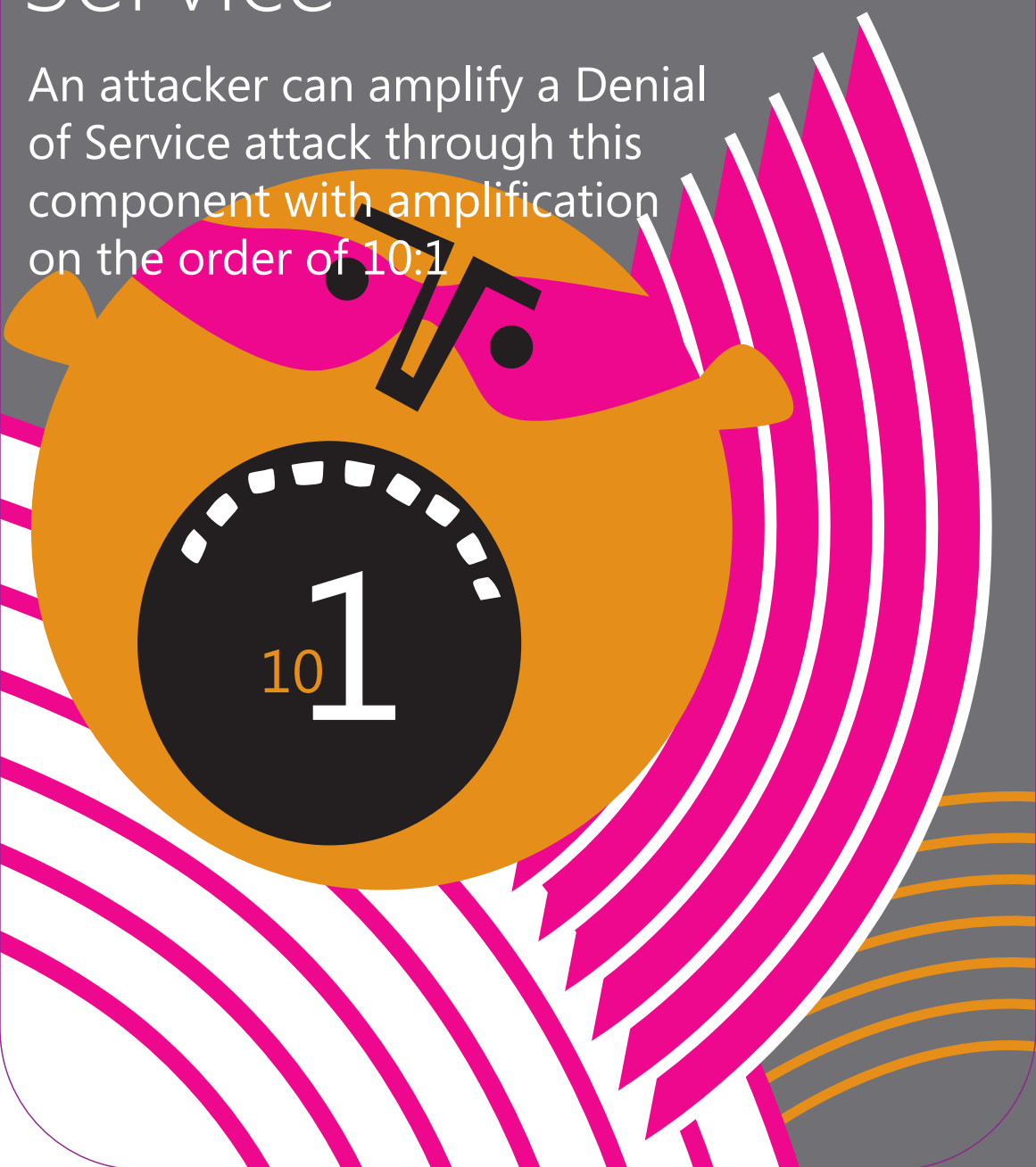
Déni de service

Q

Un attaquant peut amplifier l'attaque de déni de service par l'intermédiaire de cette composante avec une amplification de l'ordre de 10 à 1

Denial of Service

An attacker can amplify a Denial of Service attack through this component with amplification on the order of 10:1



Déni de service

K

Un attaquant peut amplifier l'attaque de déni de service par l'intermédiaire de cette composante avec une amplification de l'ordre de 100 à 1

An attacker can amplify a Denial of Service attack through this component with amplification on the order of 100:1

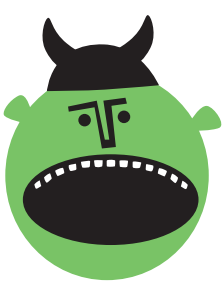
Déni de service

A

Vous avez inventé une nouvelle attaque de déni de service

Denial of Service

You've invented a new Denial of Service attack

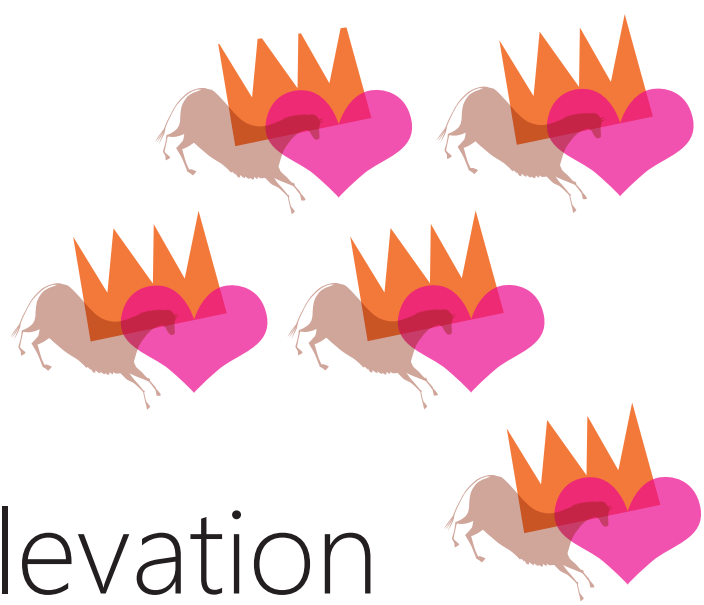


A

5

Élévation de privilège

Un attaquant peut forcer les données par différents chemins de validation pour obtenir de différents résultats



Elevation of Privilege

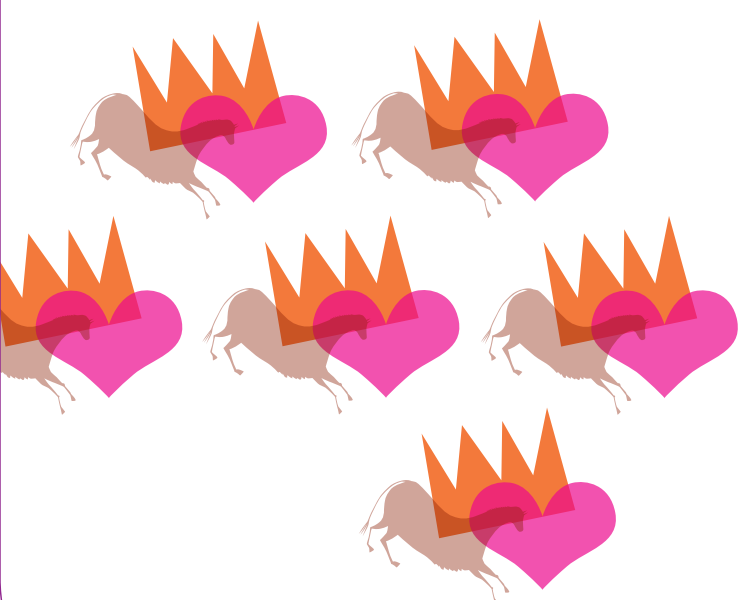
An attacker can force data through different validation paths which give different results

6 Élévation de privilège

Un attaquant peut prendre avantage de permission .NET que vous mettez en place, mais n'utilisez pas

Elevation of Privilege

An attacker could take advantag e of .NET per mis s ions you ask for, but don’t use



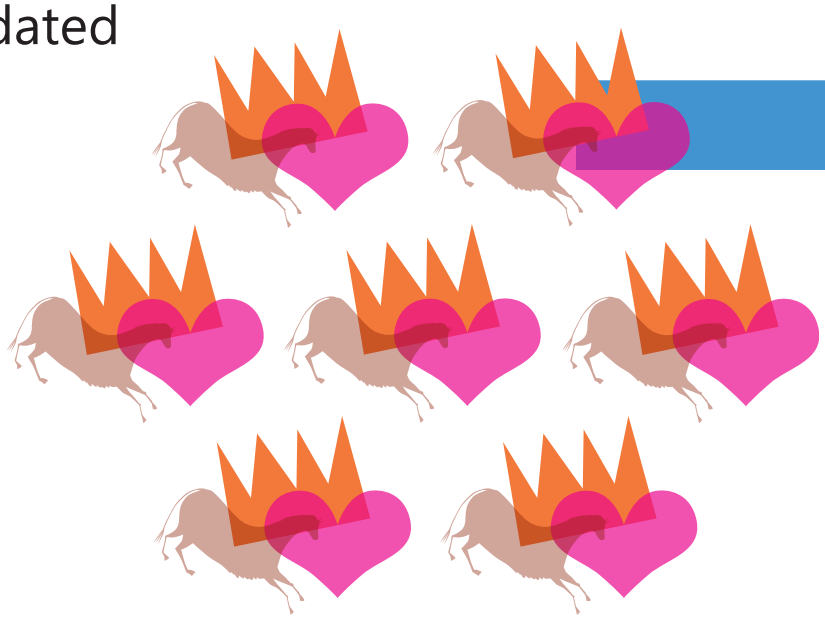
7

Élévation de privilège

Un attaquant peut fournir un pointeur au-delà d'une frontière de confiance, plutôt que des données qui peuvent être validées

Elevation of Privilege

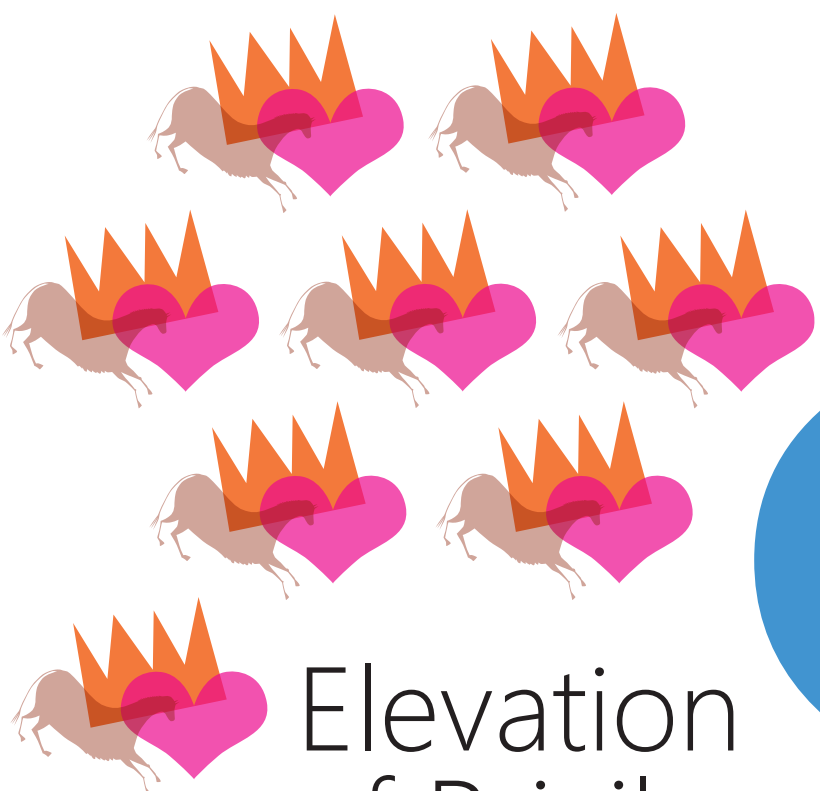
An attacker can provide a pointer across a trust boundary, rather than data which can be validated



8

Élévation de privilège

Un attaquant peut saisir des données qui sont vérifiées lorsque toujours sous leur contrôle et utilisées au-delà d'une frontière de confiance



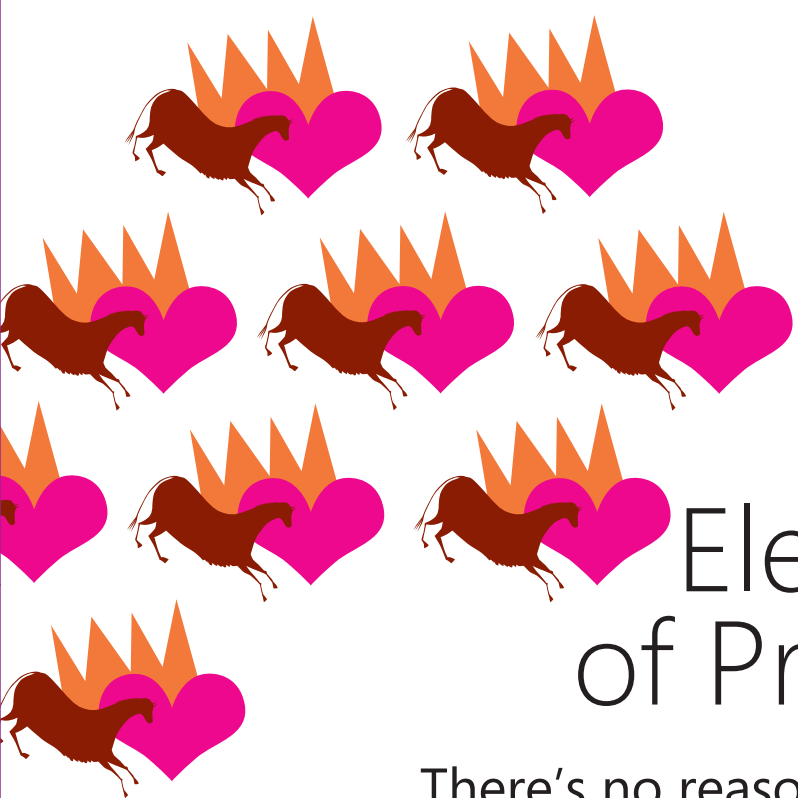
Elevation of Privilege

An attacker can enter data that is checked while still under their control and used later on the other side of a trust boundary

9

Élévation de privilège

Il n'y a pas de façon raisonnable pour un appelant de déterminer quelle validation de pollution de données vous faites avant de transmettre la donnée



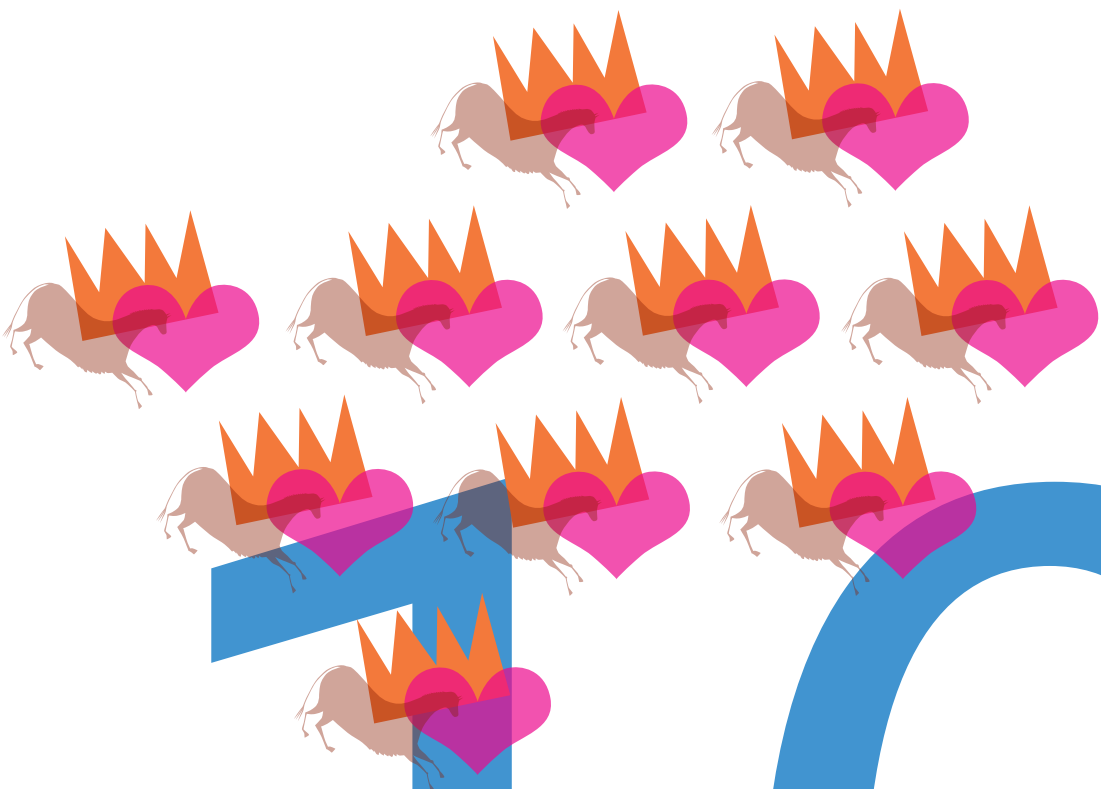
Elevation of Privilege

There’s no reasonable way for a caller to figure out what validation of tainted data you perform before passing it to them

10

Élévation de privilège

Il n'y a pas de façon raisonnable pour un appelant de déterminer quelles assomptions de sécurité vous faites



Elevation of Privilege

There's no reasonable way for a caller to figure out what security assumptions you make

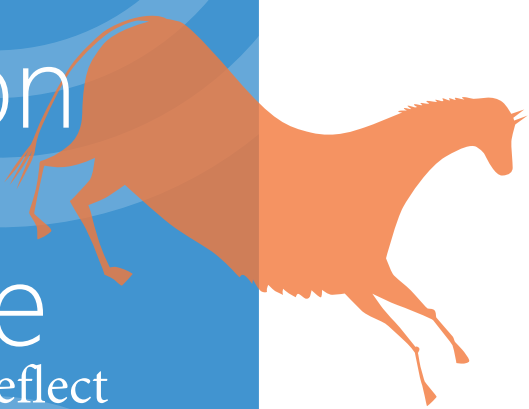
J

Élévation de privilège

Un attaquant peut réfléchir des valeurs saisies à l'utilisateur, comme du cross site scripting

Elevation of Privilege

An attacker canreflect input back to user, like cross site scripting



Q

Élévation de privilège

Du contenu généré par l'utilisateur est inclus dans la page, avec possiblement l'inclusion de contenu de n'importe quelle URL

Elevation of Privilege

You include user-generated content within your page, possibly including the content of random URLs

K

Élévation de privilège

Un attaquant peut injecter une commande dans le système qui va être exécuté à un plus haut niveau de privilège

Elevation of Privilege

An attacker can inject a command that the system will run at a higher privilege level

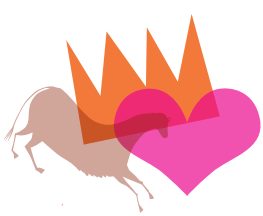
A

Élévation de privilège

Vous avez inventé une nouvelle attaque d'élévation de privilège

Elevation of Privilege

You've invented a new Elevation of Privilege attack



A

Spoofing

2. An attacker could squat on the random 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)

10. An attacker can choose to use weaker or no authentication

continued on back

Spoofing

Spoofing cont.

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

3. An attacker can take advantage of your custom key exchange or integrity control which you built instead of using standard crypto

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

10. An attacker can alter information in a data store because it has weak ACLs or includes a group which is equivalent to everyone ("all LIve ID holders")

J. An attacker can write to some resource because permissions are granted to the world or there are no ACLs

continued on back

Tampering

Tampering cont.

Q. An attacker can change parameters over a trust boundary and after validation (for example, important parameters in a hidden field in HTML, or 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

R

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 digital signatures 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 time-stamp (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

10. An attacker can get arbitrary data into logs from unauthenticated (or weakly authenticated) outsiders without validation

continued on back

Repudiation

R

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'd 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 (say, 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 occluded (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 indexer, logger, or other such mechanism

9. An attacker can read sensitive information in a file with bad ACLs

10. An attacker can read information in files with no ACLs

continued on back

Information Disclosure

Information Disclosure cont.

J. An attacker can discover the fixed key being used to encrypt

Q. An attacker can read the entire channel because the channel (say, 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 make a client unavailable or unusable but the problem goes away when the attacker stops **(client, authenticated, temporary)**

4. An attacker can make a server unavailable or unusable but the problem goes away when the attacker stops **(server, authenticated, temporary)**

5. An attacker can make a client unavailable or unusable without ever authenticating but the problem goes away when the attacker stops **(client, anonymous, temporary)**

6. An attacker can make a server unavailable or unusable without ever authenticating but the problem goes away when the attacker stops **(server, anonymous, temporary)**

7. An attacker can make a client unavailable or unusable and the problem persists after the attacker goes away **(client, authenticated, persistent)**

8. An attacker can make a server unavailable or unusable and the problem persists after the attacker goes away **(server, authenticated, persistent)**

9. An attacker can make a client unavailable or unusable without ever authenticating and the problem persists after the attacker goes away **(client, anonymous, persistent)**

continued on back

Denial of Service

Denial of Service cont.

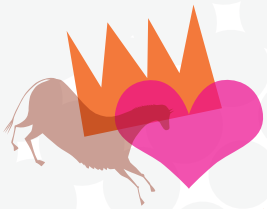
10. An attacker can make a server unavailable or unusable without ever authenticating and the problem persists after the attacker goes away **(server, anonymous, persistent)**

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 10:1

K. An attacker can amplify a Denial of Service attack through this component with amplification on the order of 100:1

A. You've invented a new Denial of Service attack



Elevation of Privilege (EoP)

5. An attacker can force data through different validation paths which give different results

6. An attacker could take advantage of .NET 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 their control and used later on the other side of a trust boundary

9. There's no reasonable way for a caller to figure out what validation of tainted data you perform before passing it to them

10. There's no reasonable way for a caller to figure out what security assumptions you make

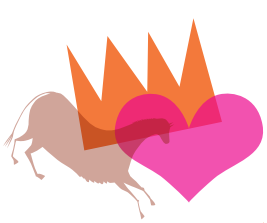
J. An attacker can reflect input back to a user, like cross site scripting

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

Elevation of Privilege



Elevation of Privilege

About

Threat Modeling

Elevation of Privilege 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 it uses the 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 to have not performed an action

Information Disclosure Exposing information to someone not authorized to see it

Denial of Service Deny or degrade service to users

Elevation of Privilege Gain capabilities without proper authorization

At www.microsoft.com/security/sdl/eop we have resources for you including videos, score sheets and tips and tricks for playing.

About

SDL

Elevation of Privilege 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/

Microsoft®

Security Development Lifecycle