IDENTIFYING ATTACK GOALS

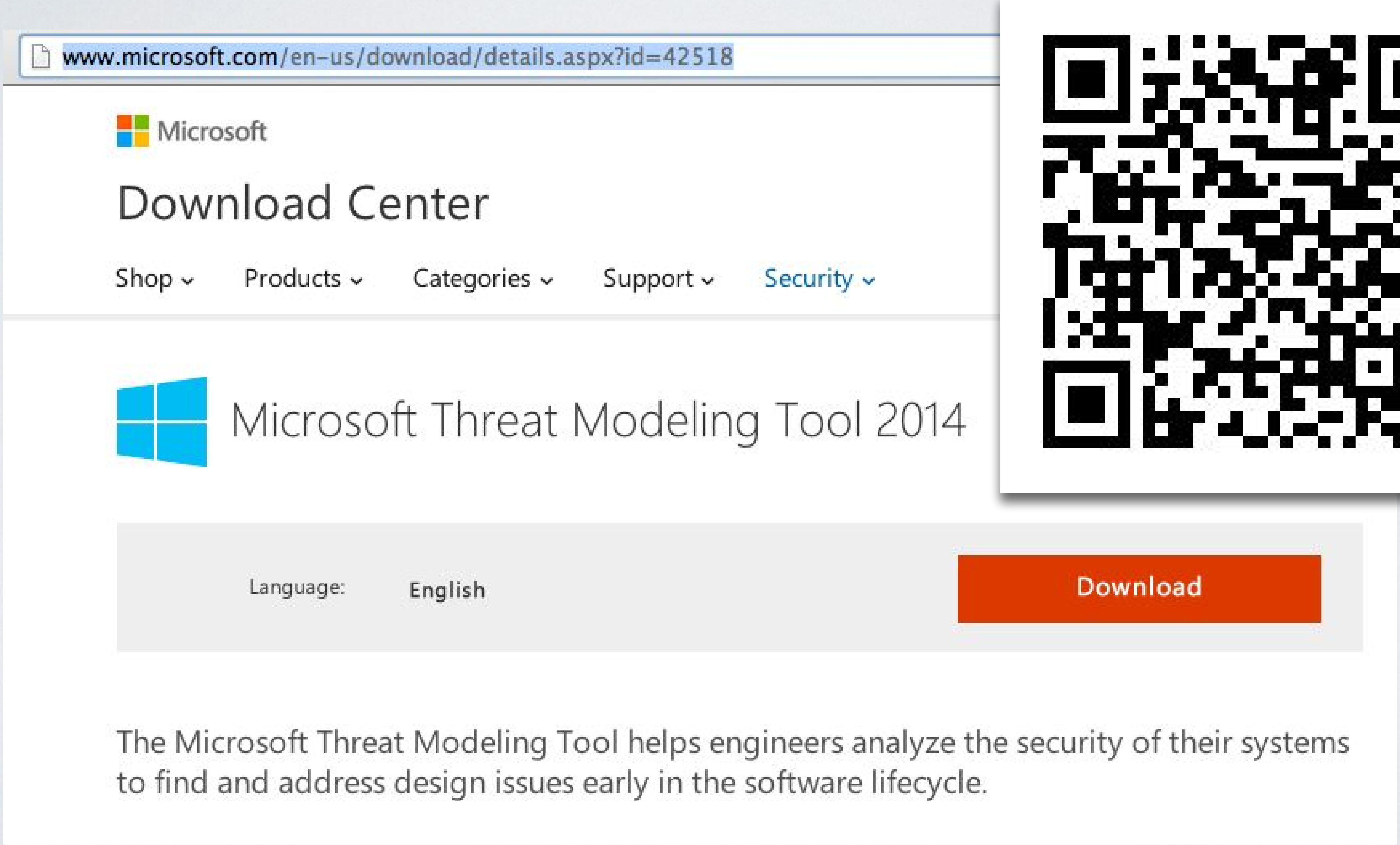
Assets, Entry Points and Data Flow Analysis

Threat Modeling

Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker's perspective**,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

DATA FLOW TOOL

VISIO FOR THREAT MODELS



www.microsoft.com/en-us/download/details.aspx?id=42518

Microsoft

Download Center

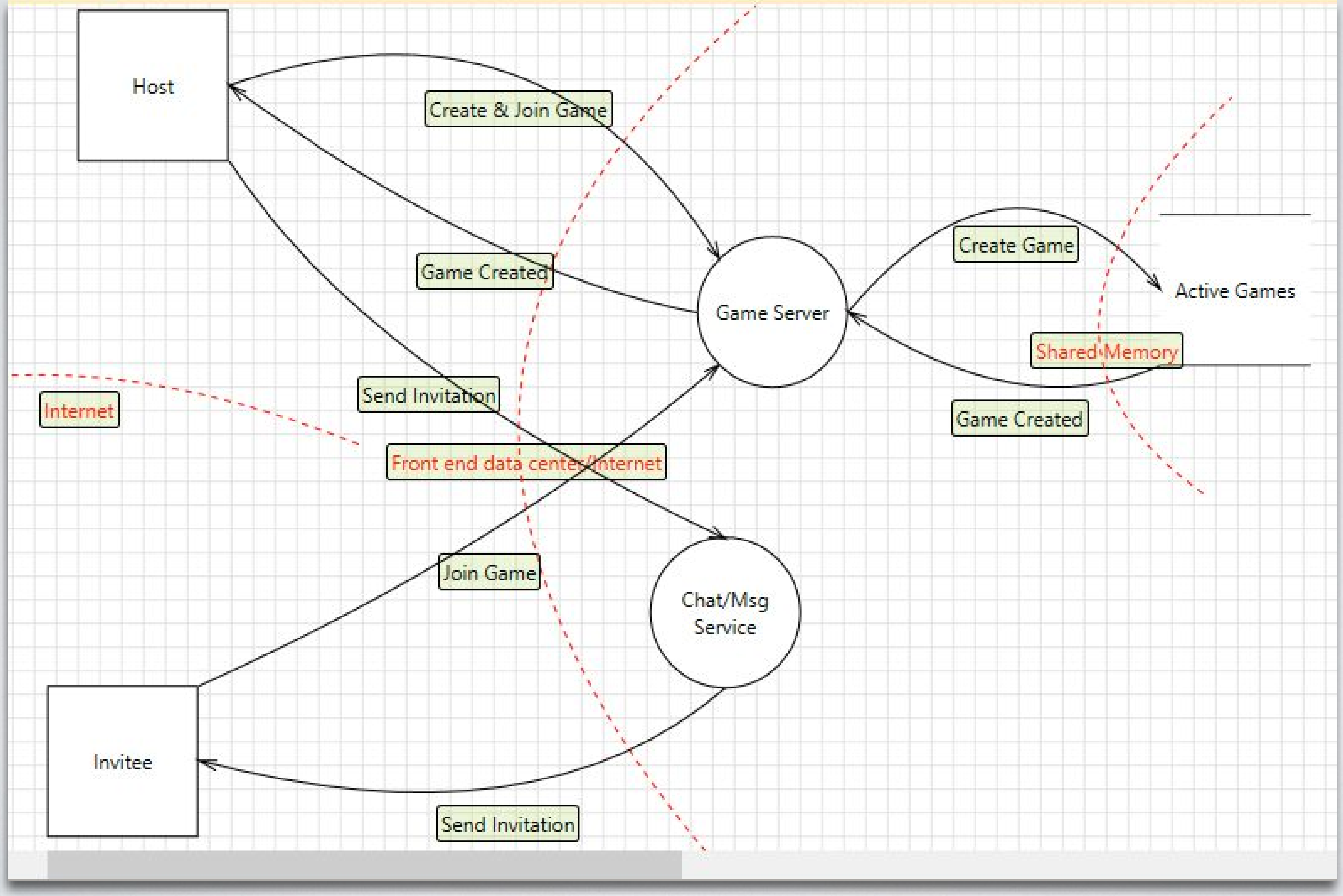
Microsoft Threat Modeling Tool 2014

Language: English

The Microsoft Threat Modeling Tool helps engineers analyze the security of their systems to find and address design issues early in the software lifecycle.

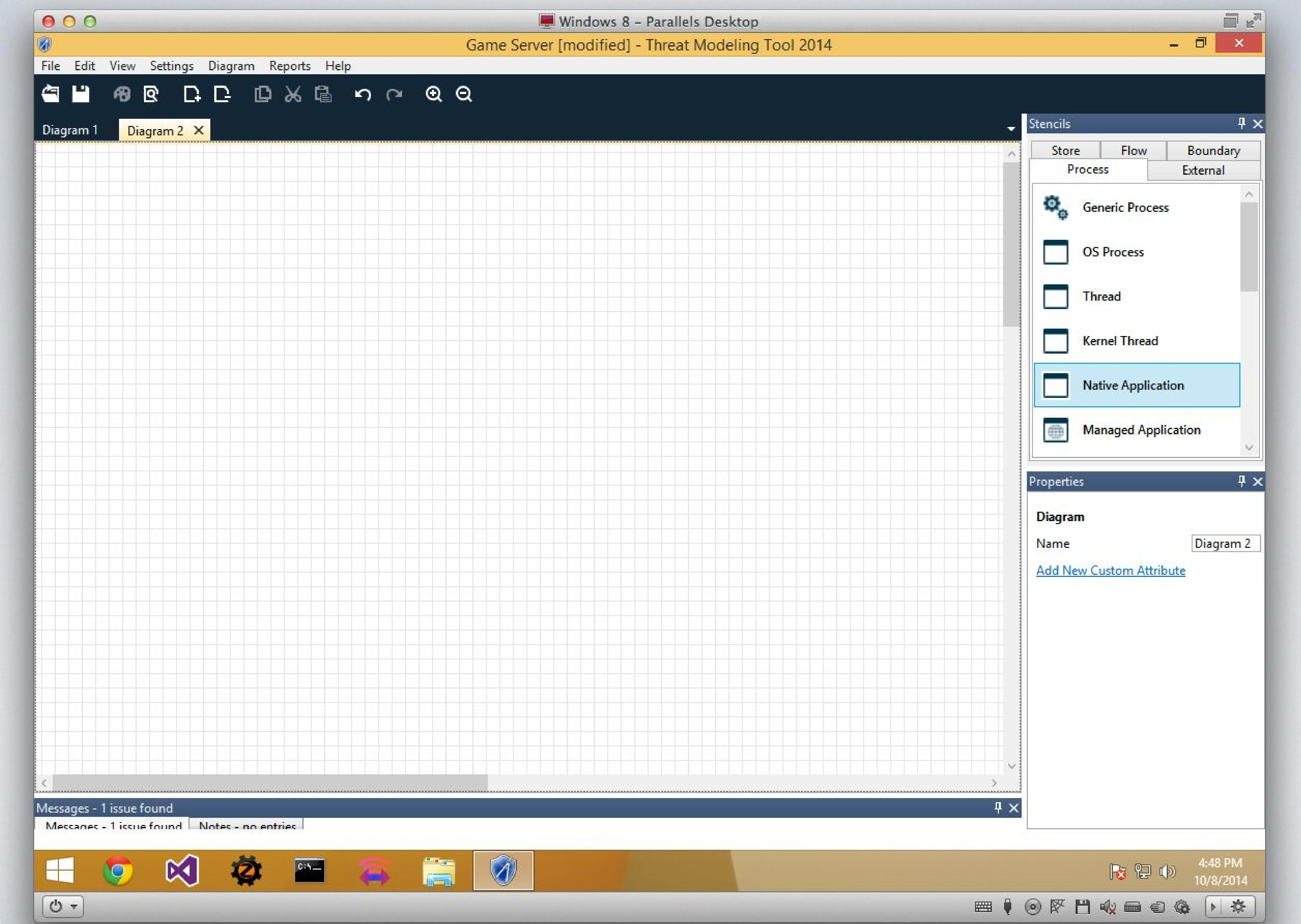
THREATS COME FROM DATA

DATA FLOW DIAGRAMS



ELEMENTS

- Processes: Code (*not* an OS process)
- External Interactors: A source or sink of data that's outside your control (e.g., the client)
- Data Stores: Something that holds data—memory, a file, a database
- Data Flow: The transfer of data from one element to another
- Trust Boundary: Border between two elements that do not trust each other

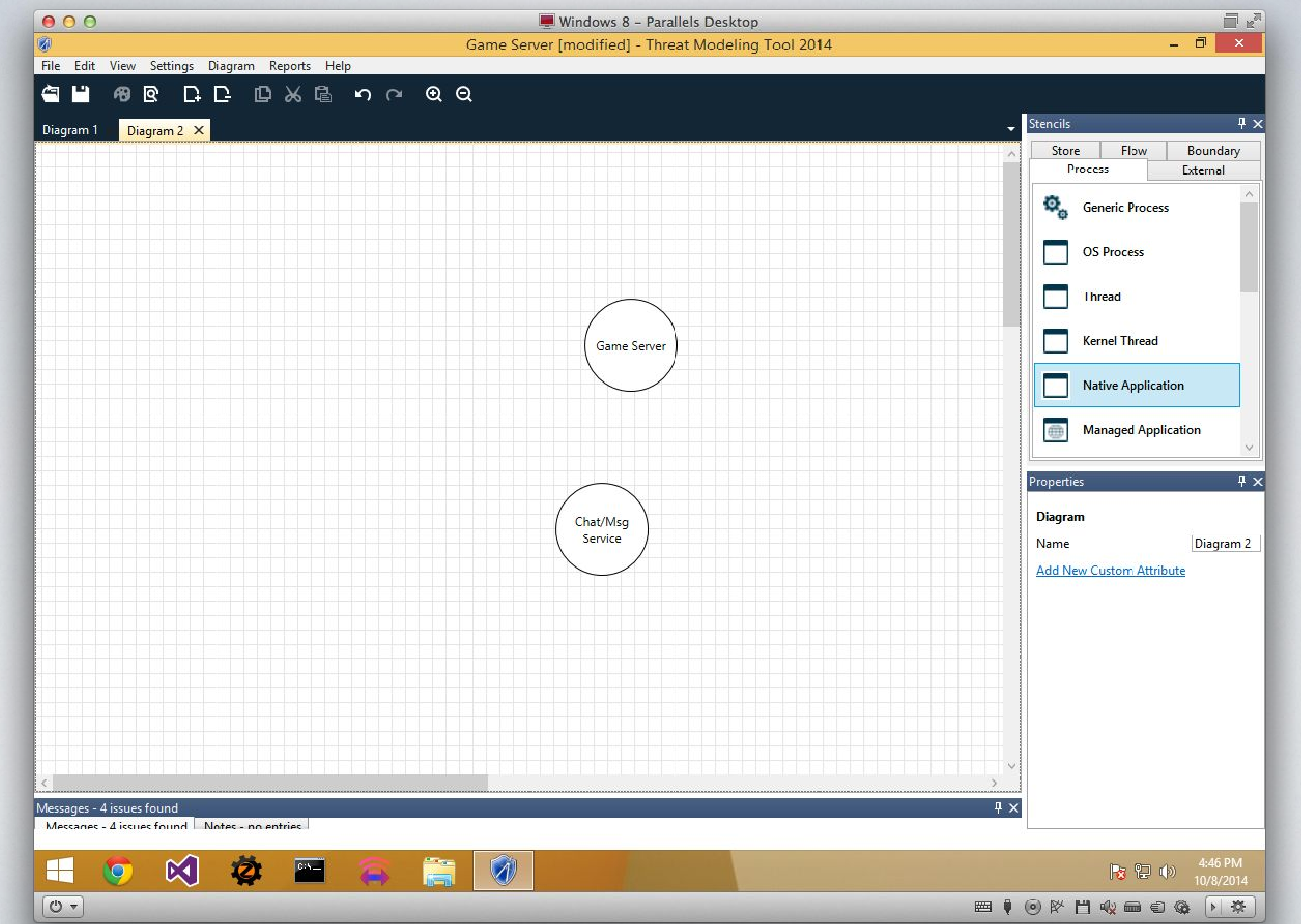


Diagram

Name: Diagram 2

Add New Custom Attribute

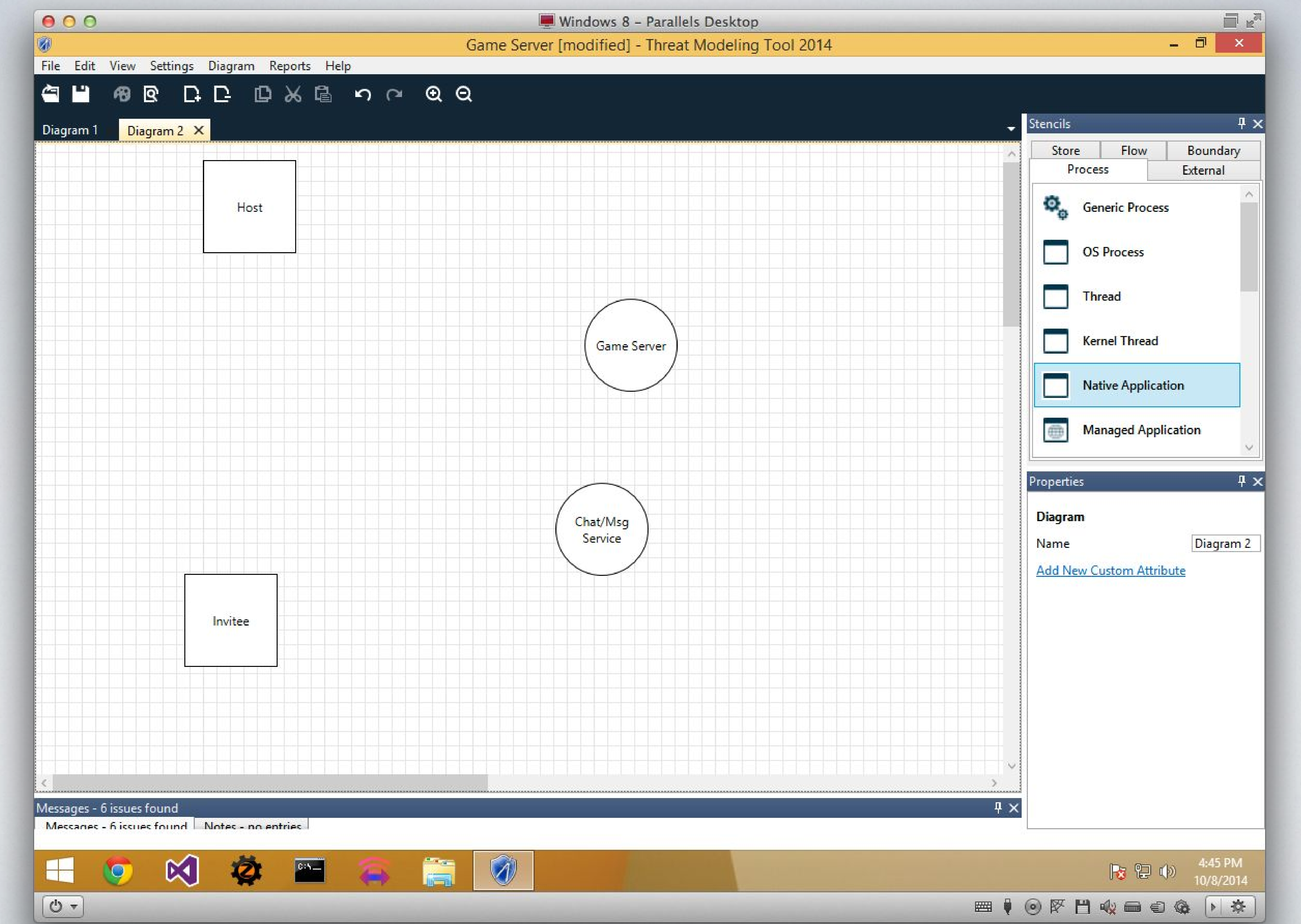
Messages - 1 issue found



Diagram

Name: Diagram 2

Messages - 4 issues found



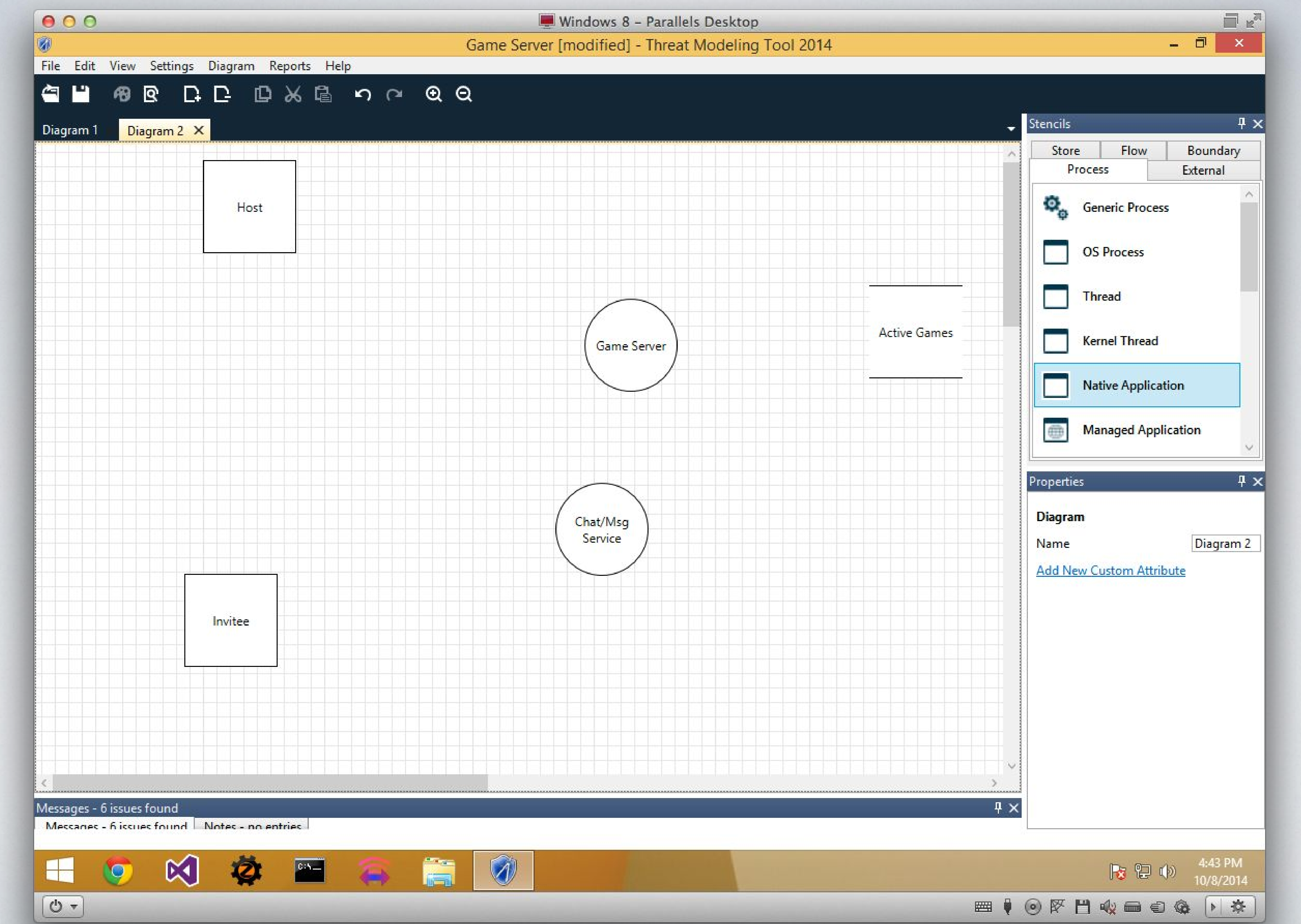
Windows 8 – Parallels Desktop

Game Server [modified] - Threat Modeling Tool 2014

Diagram

Name: Diagram 2

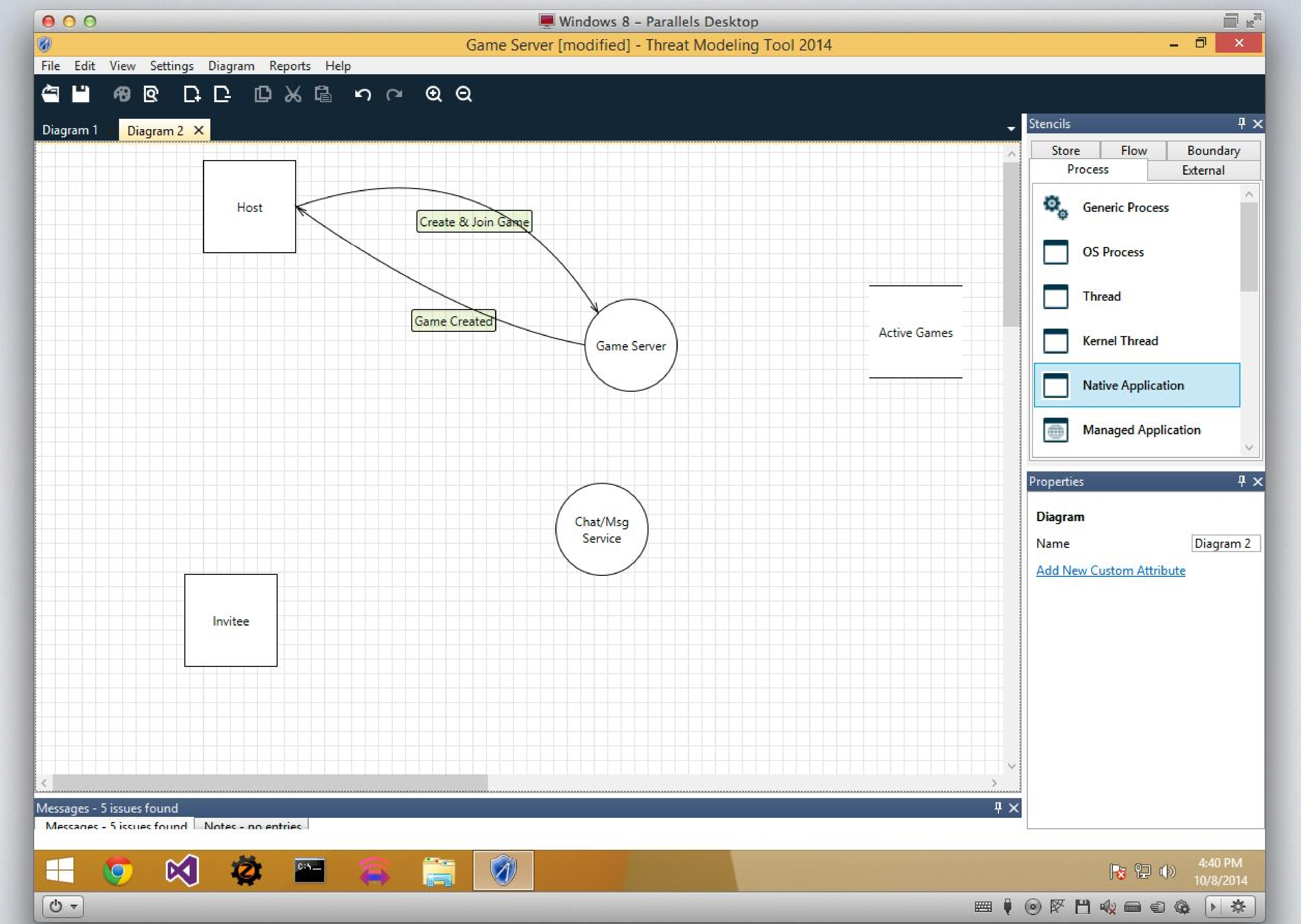
Messages - 6 issues found



Messages - 6 issues found

Diagram

Name: Diagram 2

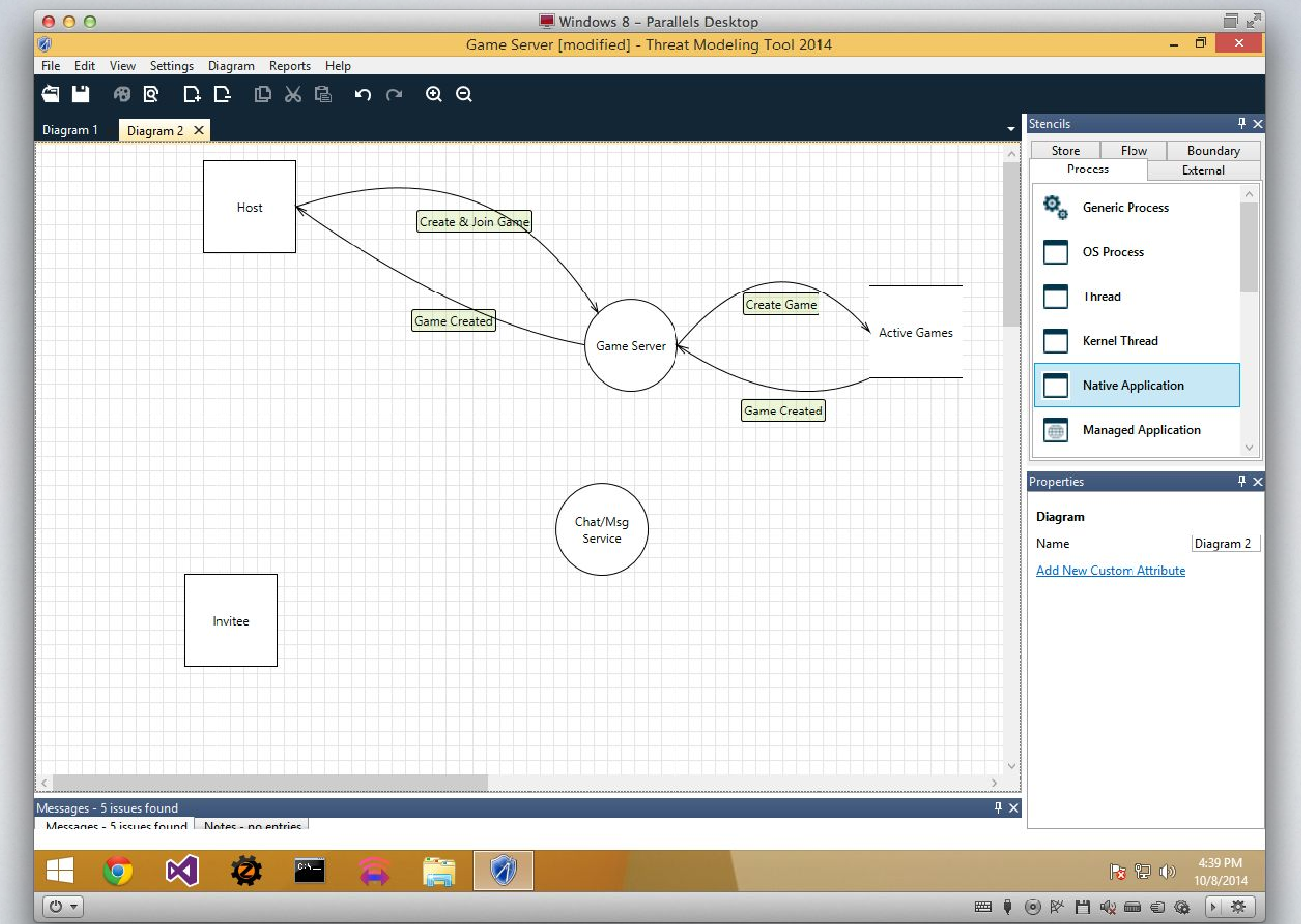


Diagram

Name: Diagram 2

Messages - 5 issues found

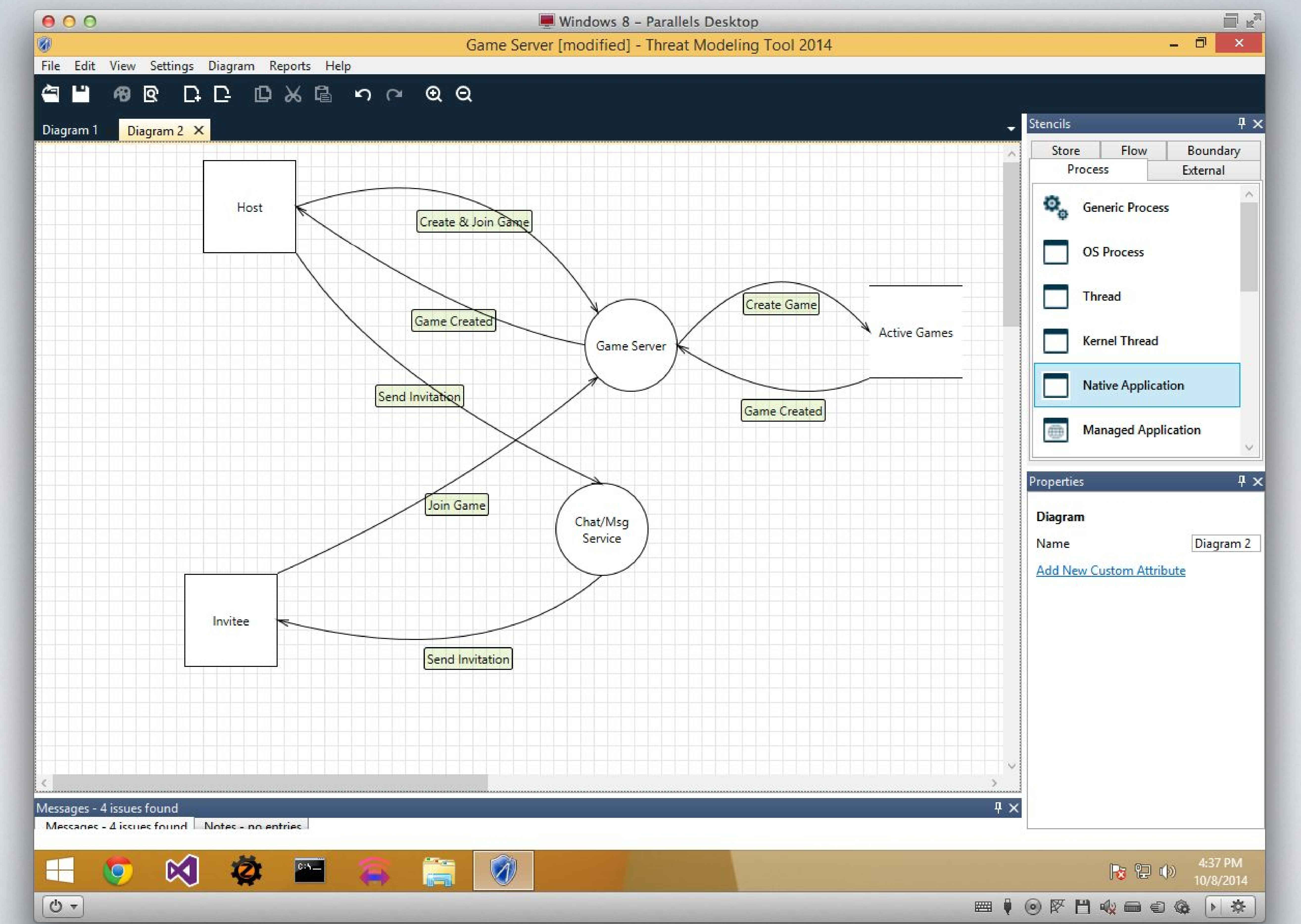
Messages - 5 issues found | Notes - no entries

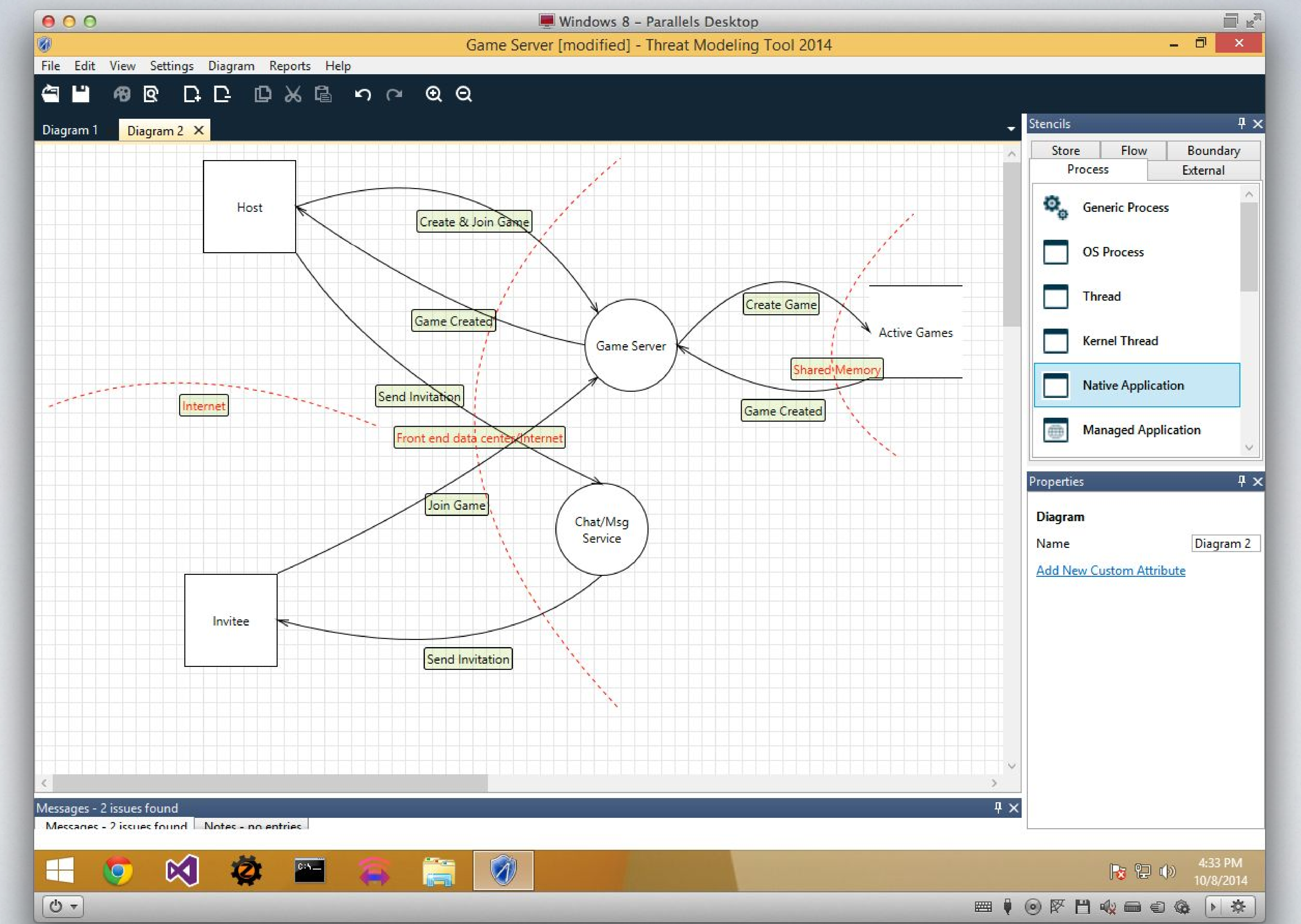


Name: Diagram 2

Messages - 5 issues found

Messages - 5 issues found

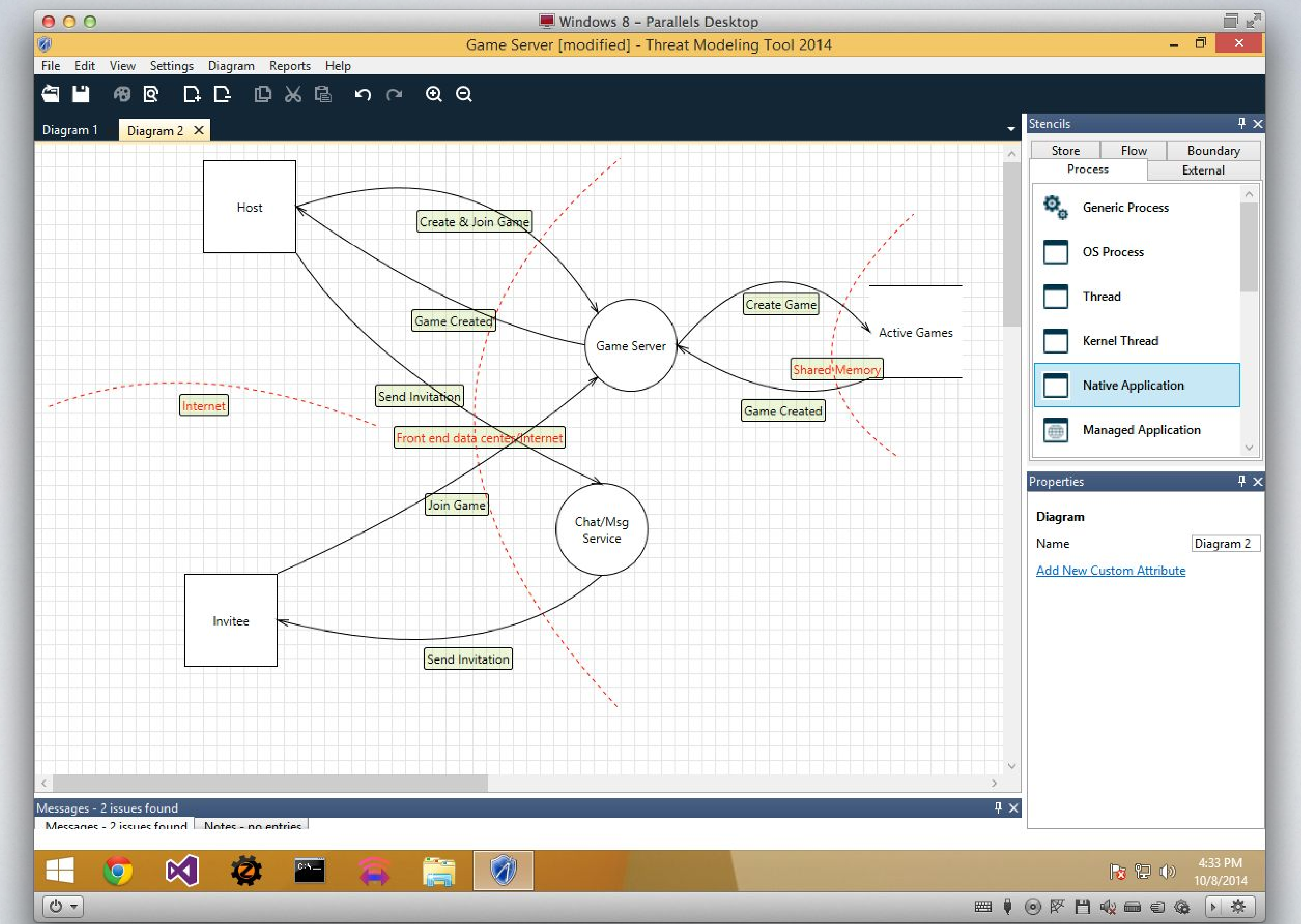

Windows 8 – Parallels Desktop
Game Server [modified] - Threat Modeling Tool 2014
File
Edit
View
Settings
Diagram
Reports
Help
Diagram 1
Diagram 2
Host
Create & Join Game
Game Created
Send Invitation
Game Server
Create Game
Active Games
Game Created
Join Game
Chat/Msg Service
Invitee
Send Invitation
Stencils
Store
Flow
Boundary
Process
External
Generic Process
OS Process
Thread
Kernel Thread
Native Application
Managed Application
Properties
Diagram
Name
Diagram 2
Add New Custom Attribute
Messages - 4 issues found
Messages - 4 issues found
Notes - no entries
4:37 PM
10/8/2014



Messages - 2 issues found

Diagram

Name: Diagram 2



Diagram

Name Diagram 2

Add New Custom Attribute

Messages - 2 issues found

EASY MISTAKES

- ***It's not a flowchart!***
- All data flows must begin or end at a process.
- A process that has input flows but no output flows is a black hole.
- A process that has output but no input is a miracle.
- Make sure each process has all the data needed to create any output flows.

- Threats come from data, so we document *what our data is*, *where it comes from*, *where it goes to* and *what we do with it.*

- A DFD has five kinds of elements: processes, external interactors, data stores, data flows and trust boundaries.

LIVE DEMO

EVALUATING RISKS

Attack Trees

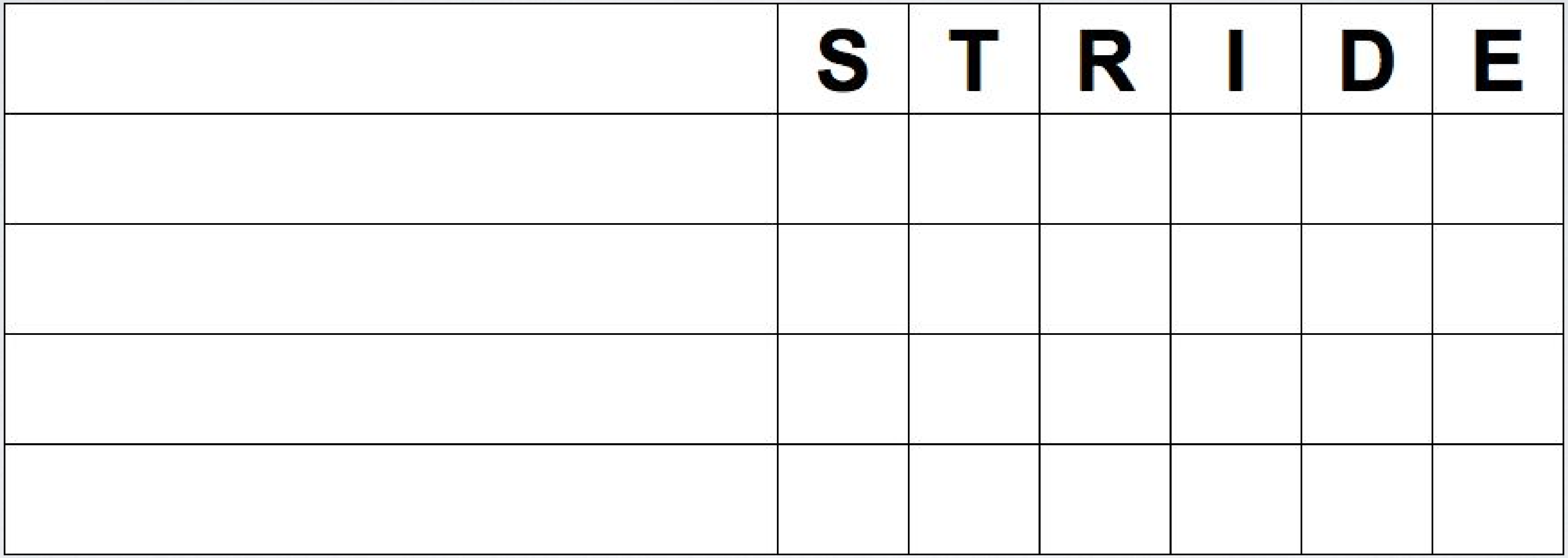
Threat Modeling

Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker’s perspective**,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

THREATS =
STRIDE X DFD ELEMENTS

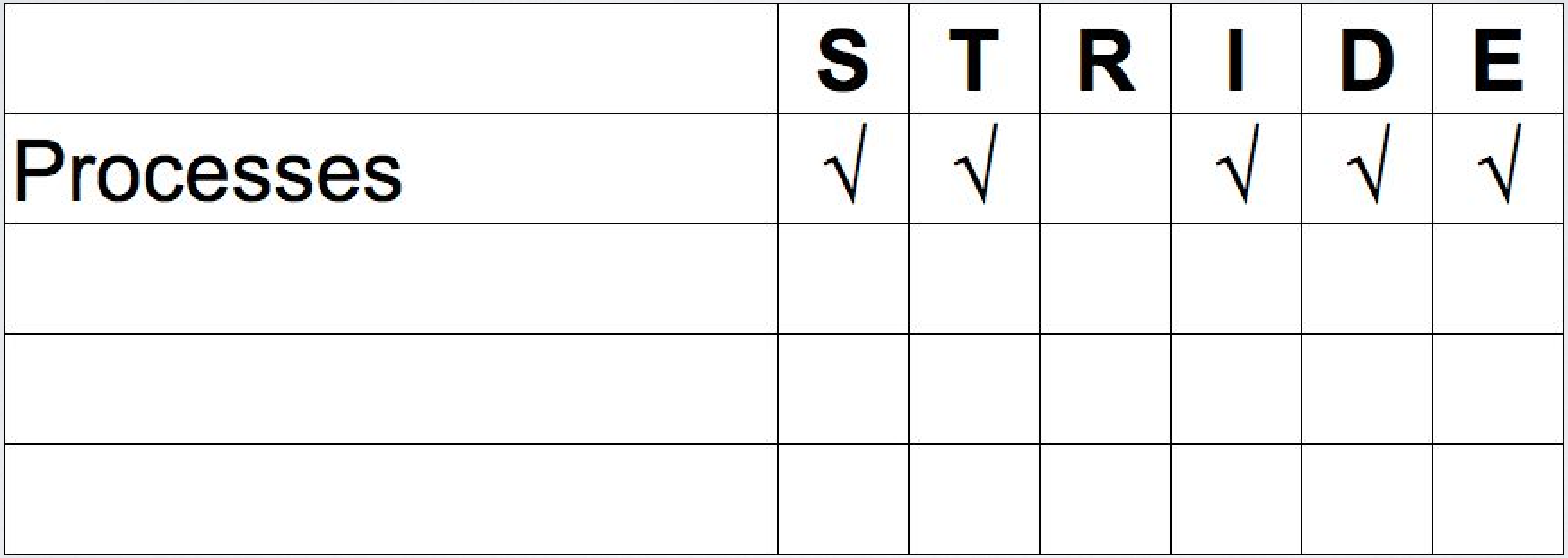
“STRIDE per Element”

STRIDE X ELEMENTS



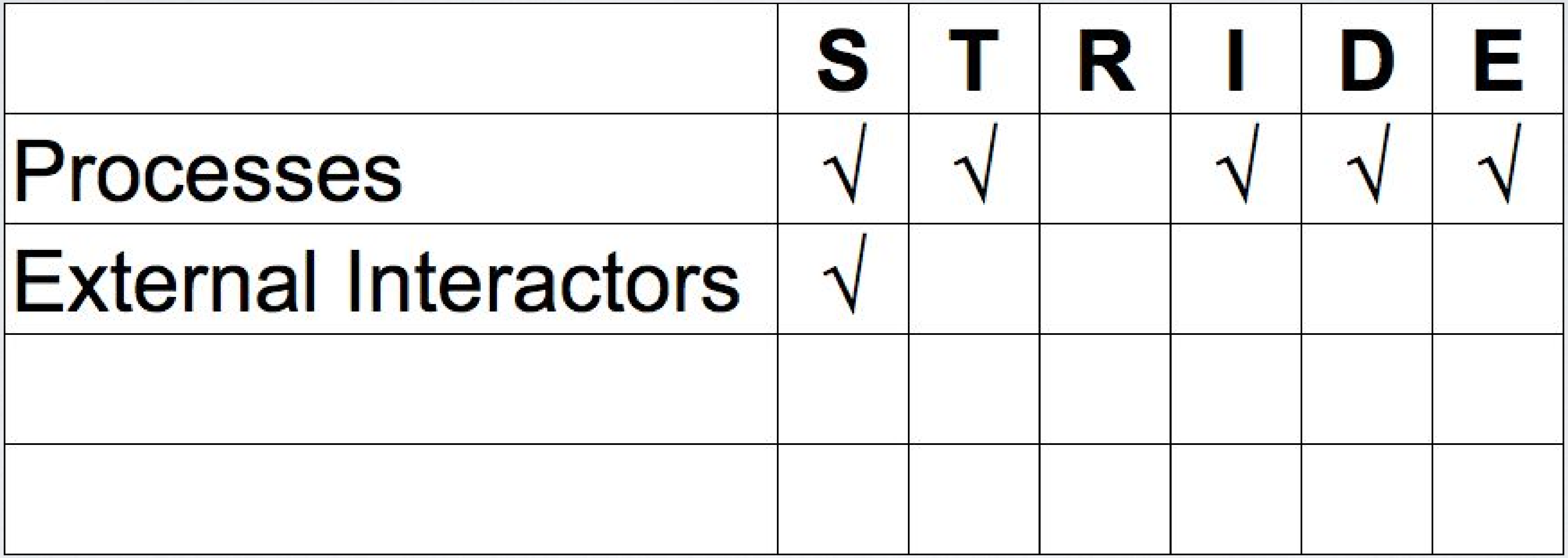
	S	T	R	I	D	E

STRIDE X ELEMENTS



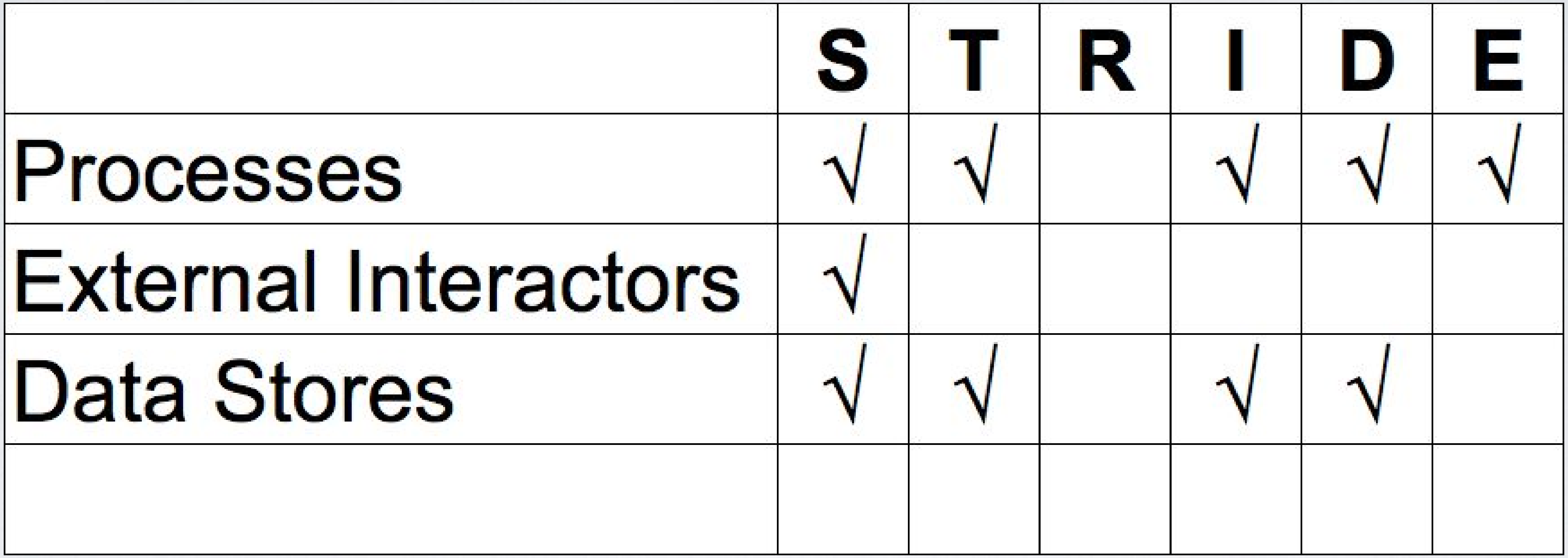
	S	T	R	I	D	E
Processes	√	√		√	√	√

STRIDE X ELEMENTS



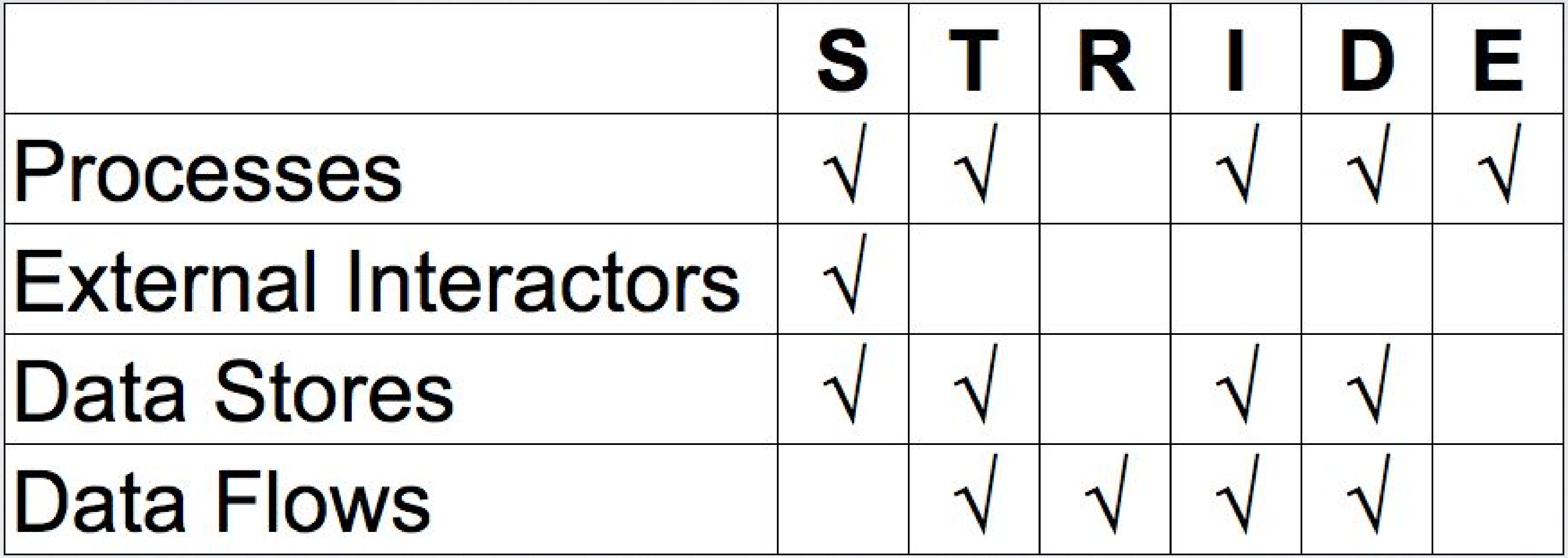
	S	T	R	I	D	E
Processes	√	√		√	√	√
External Interactors	√					

STRIDE X ELEMENTS

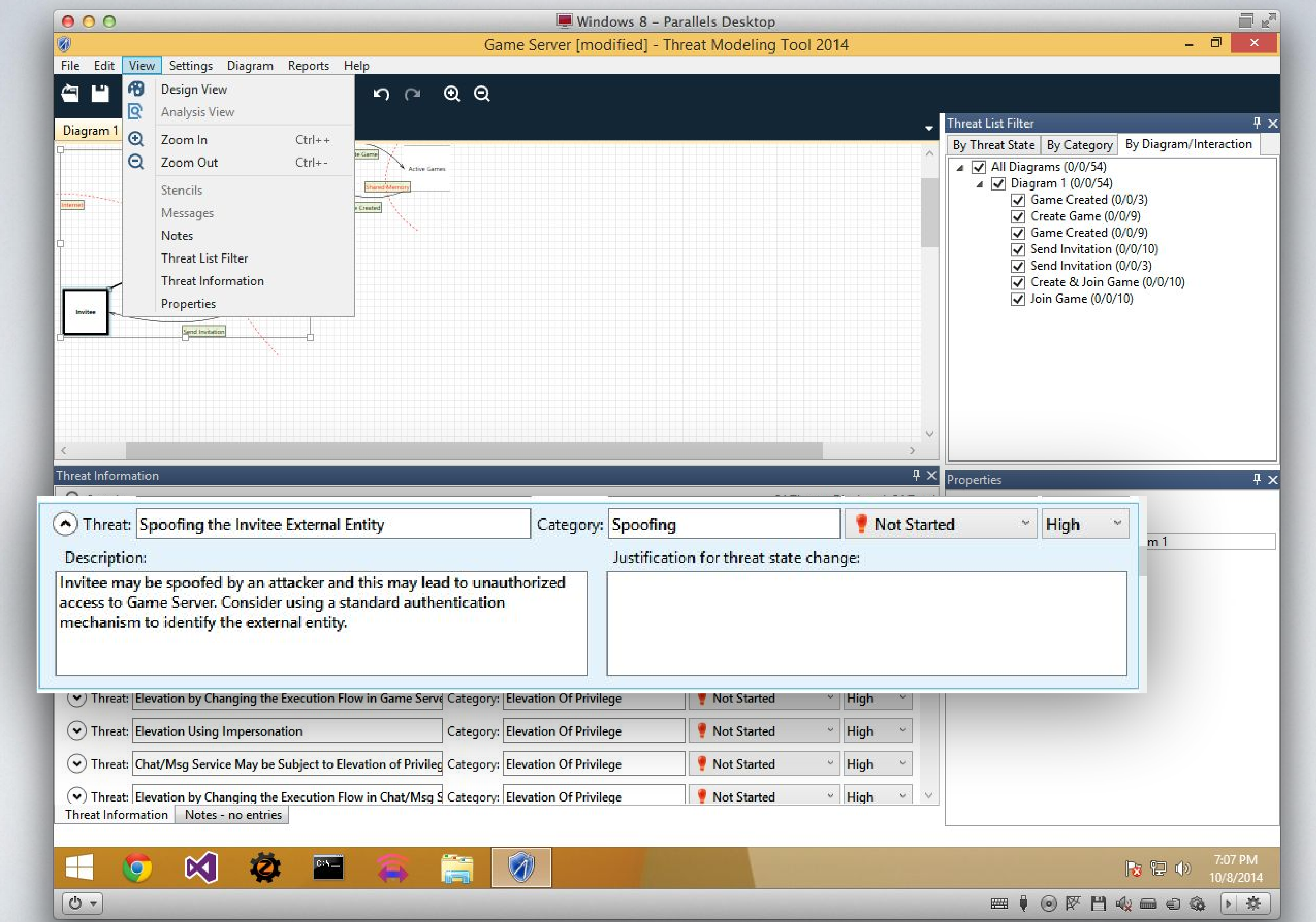


	S	T	R	I	D	E
Processes	√	√		√	√	√
External Interactors	√					
Data Stores	√	√		√	√	

STRIDE X ELEMENTS



	S	T	R	I	D	E
Processes	√	√		√	√	√
External Interactors	√					
Data Stores	√	√		√	√	
Data Flows		√	√	√	√	



☑ All Diagrams (0/0/54)
☑ Diagram 1 (0/0/54)
☑ Game Created (0/0/3)
☑ Create Game (0/0/9)
☑ Game Created (0/0/9)
☑ Send Invitation (0/0/10)
☑ Send Invitation (0/0/3)
☑ Create & Join Game (0/0/10)
☑ Join Game (0/0/10)

Threat: Spoofing the Invitee External Entity Category: Spoofing Not Started High

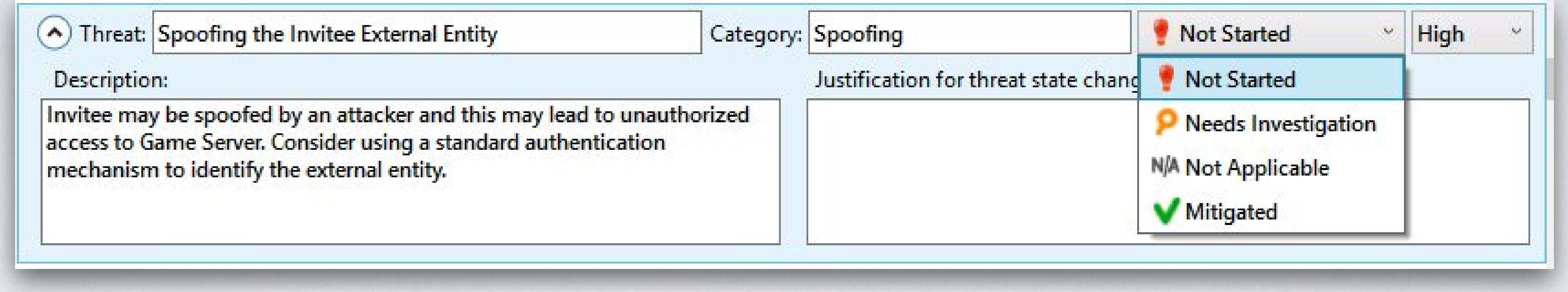
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state change:

Threat: Elevation by Changing the Execution Flow in Game Serve	Category: Elevation Of Privilege	Not Started	High
Threat: Elevation Using Impersonation	Category: Elevation Of Privilege	Not Started	High
Threat: Chat/Msg Service May be Subject to Elevation of Privileg	Category: Elevation Of Privilege	Not Started	High
Threat: Elevation by Changing the Execution Flow in Chat/Msg S	Category: Elevation Of Privilege	Not Started	High

PRIORITIZE AND NARROW SCOPE



Threat: Spoofing the Invitee External Entity

Category: Spoofing

Not Started

High

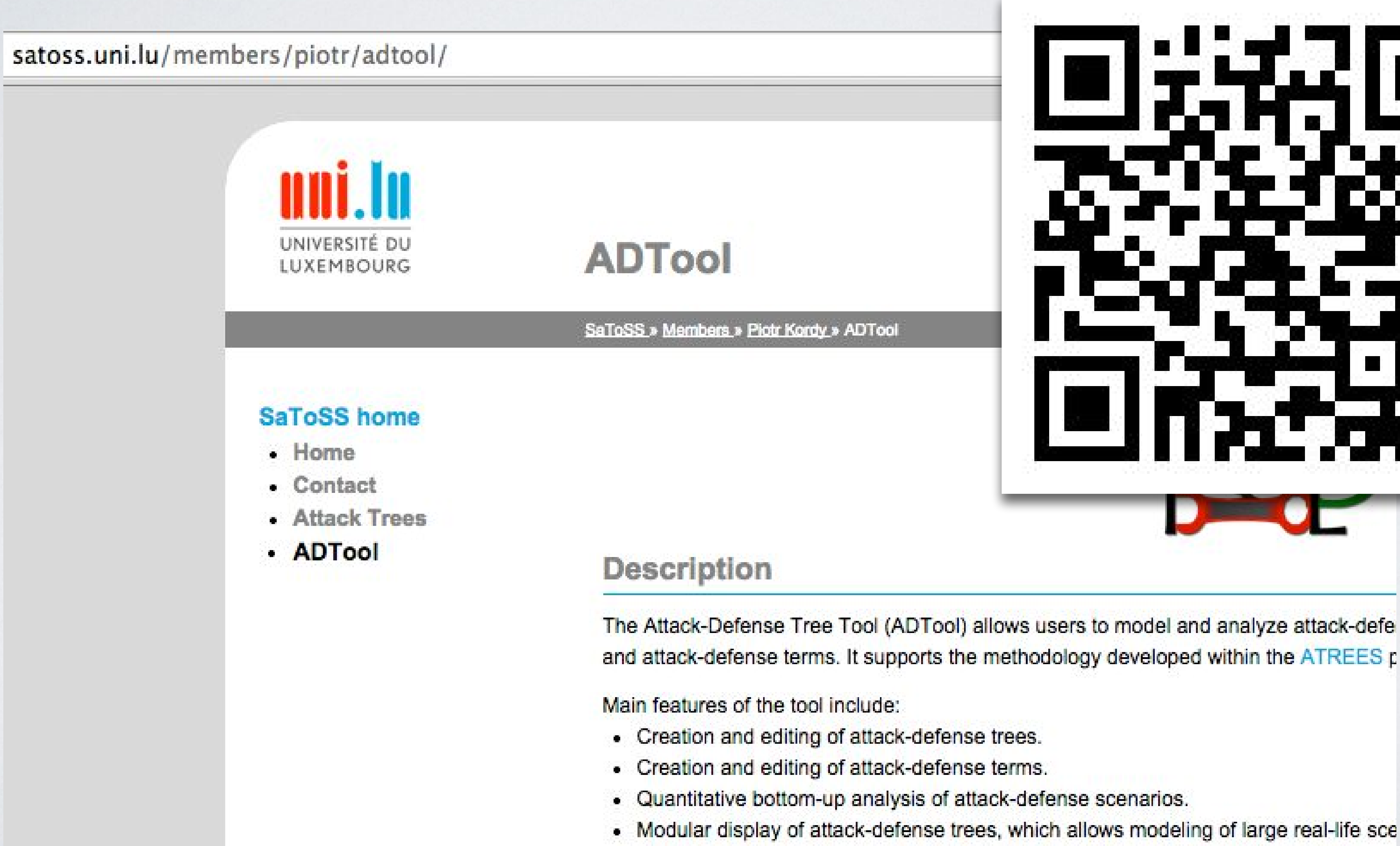
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang

- Not Started: Haven’t looked at it at all yet.
- Needs Investigation: Attack trees in progress.
- Not Applicable: Not a concern.
- Mitigated: Attack tree complete and mitigated.

ATTACK TREE TOOL



satoss.uni.lu/members/piotr/adtool/

uni.lu UNIVERSITÉ DU LUXEMBOURG

ADTool

SaToSS » Members » Piotr Kordy » ADTool

SaToSS home

- Home
- Contact
- Attack Trees
- ADTool

Description

The Attack-Defense Tree Tool (ADTool) allows users to model and analyze attack-defe and attack-defense terms. It supports the methodology developed within the ATREES p

Main features of the tool include:

- Creation and editing of attack-defense trees.
- Creation and editing of attack-defense terms.
- Quantitative bottom-up analysis of attack-defense scenarios.
- Modular display of attack-defense trees, which allows modeling of large real-life sce

ATTACK TREES

- Answers the question “What has to be true for an attacker to successfully perform this attack?”
- Conceptually an if statement:

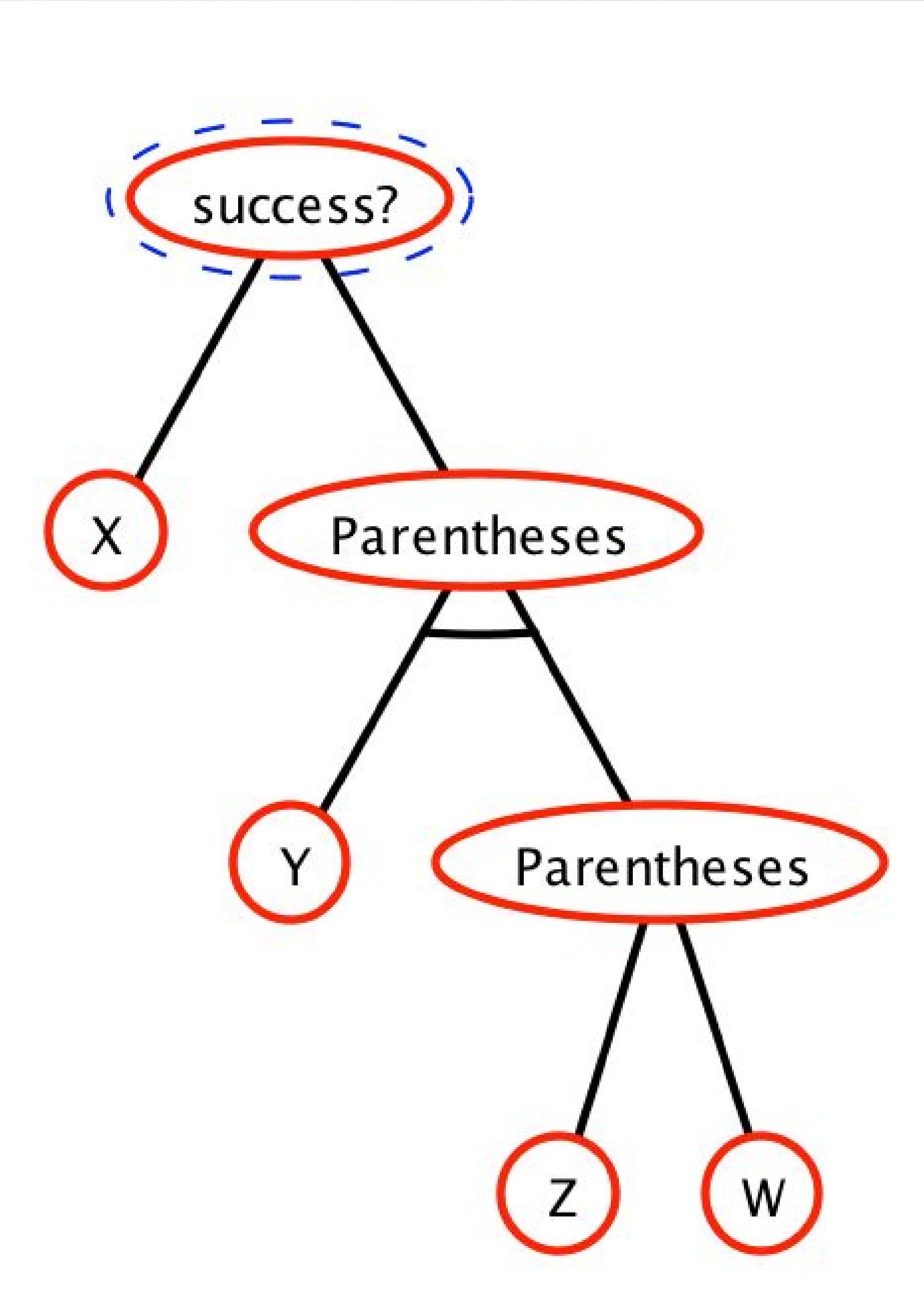
```
bool success = X || (Y && (Z || W));
```

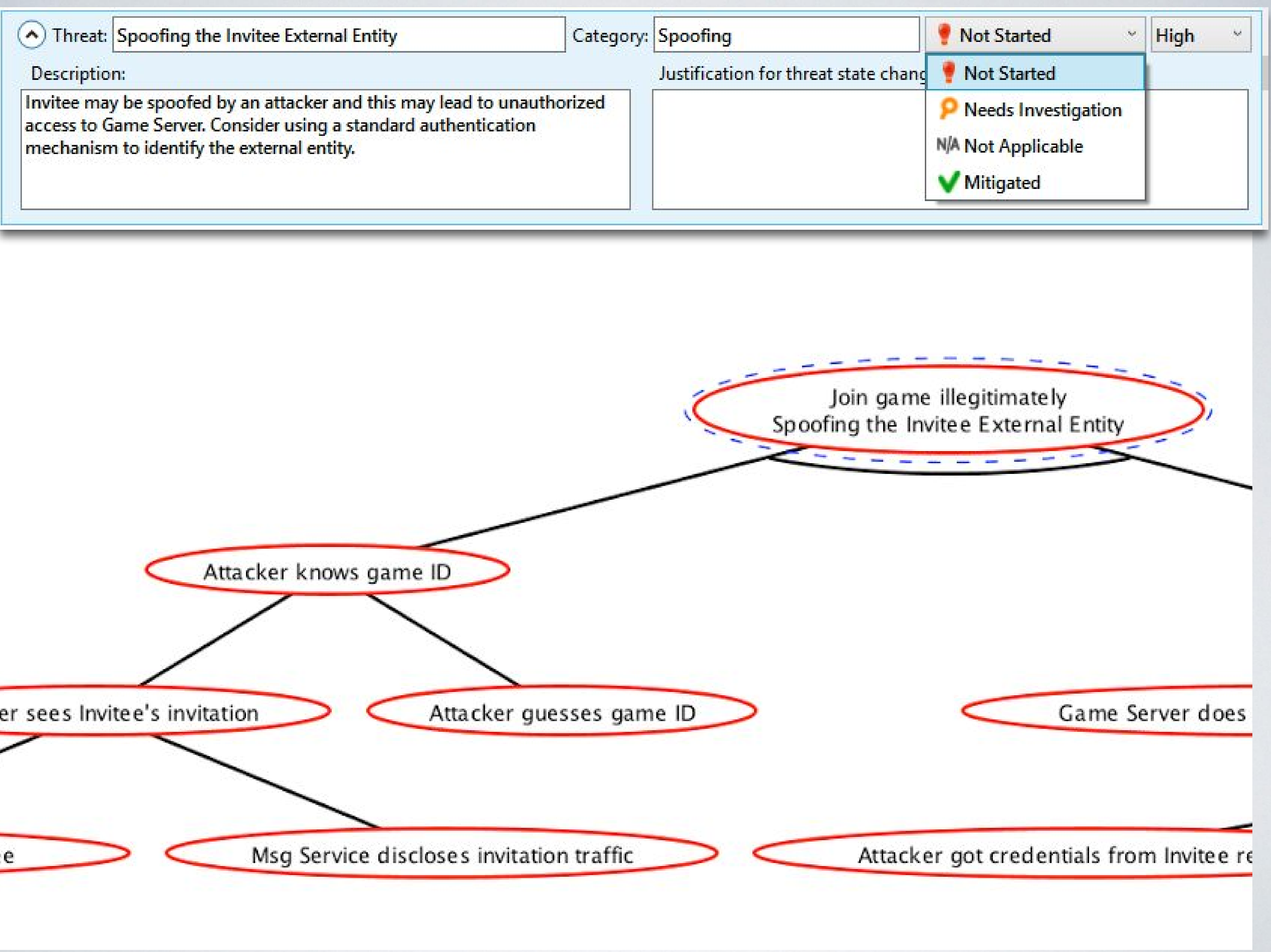
- Shown in tree form to make it easier to follow.

FORMAT

```
X || (Y && (Z || W))
```

- Root node is the attack itself
- Siblings connected with an arc must all be true (AND)
- Siblings with no arc just need one to be true (OR)





Threat: Spoofing the Invitee External Entity

Category: Spoofing

Not Started

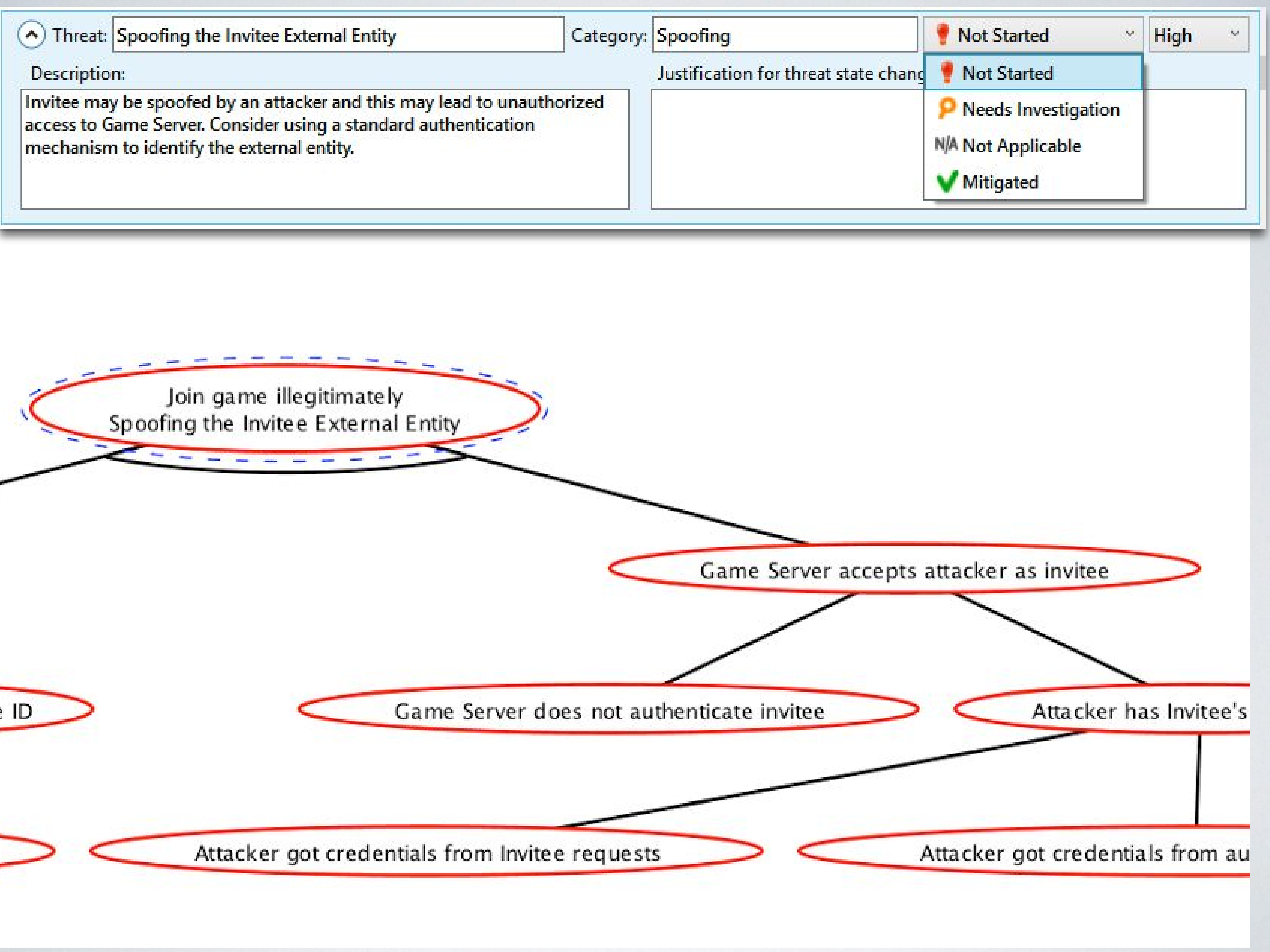
High

Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang

Not Started
Needs Investigation
Not Applicable
Mitigated
Join game illegitimately
Spoofing the Invitee External Entity
Attacker knows game ID
er sees Invitee's invitation
Attacker guesses game ID
Game Server does
e
Msg Service discloses invitation traffic
Attacker got credentials from Invitee re



Threat: Spoofing the Invitee External Entity

Category: Spoofing

Not Started

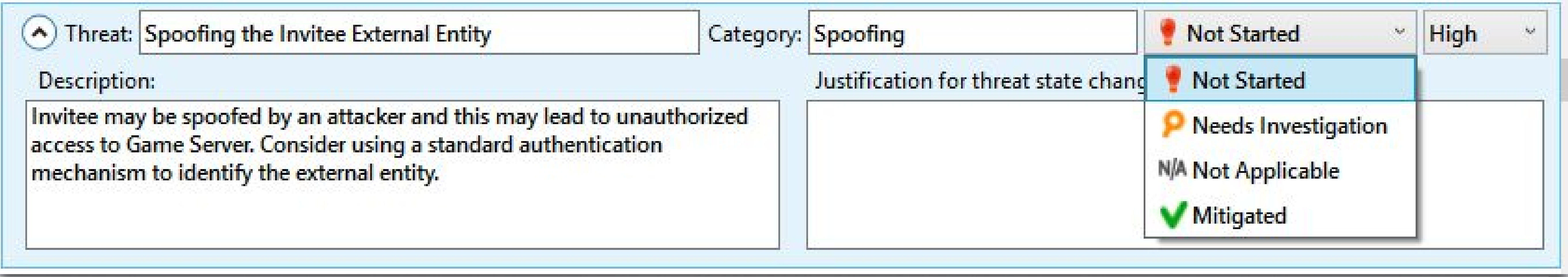
High

Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang

Not Started
Needs Investigation
N/A Not Applicable
Mitigated
Join game illegitimately
Spoofing the Invitee External Entity
Game Server accepts attacker as invitee
e ID
Game Server does not authenticate invitee
Attacker has Invitee's
Attacker got credentials from Invitee requests
Attacker got credentials from au



Threat: Spoofing the Invitee External Entity

Category: Spoofing

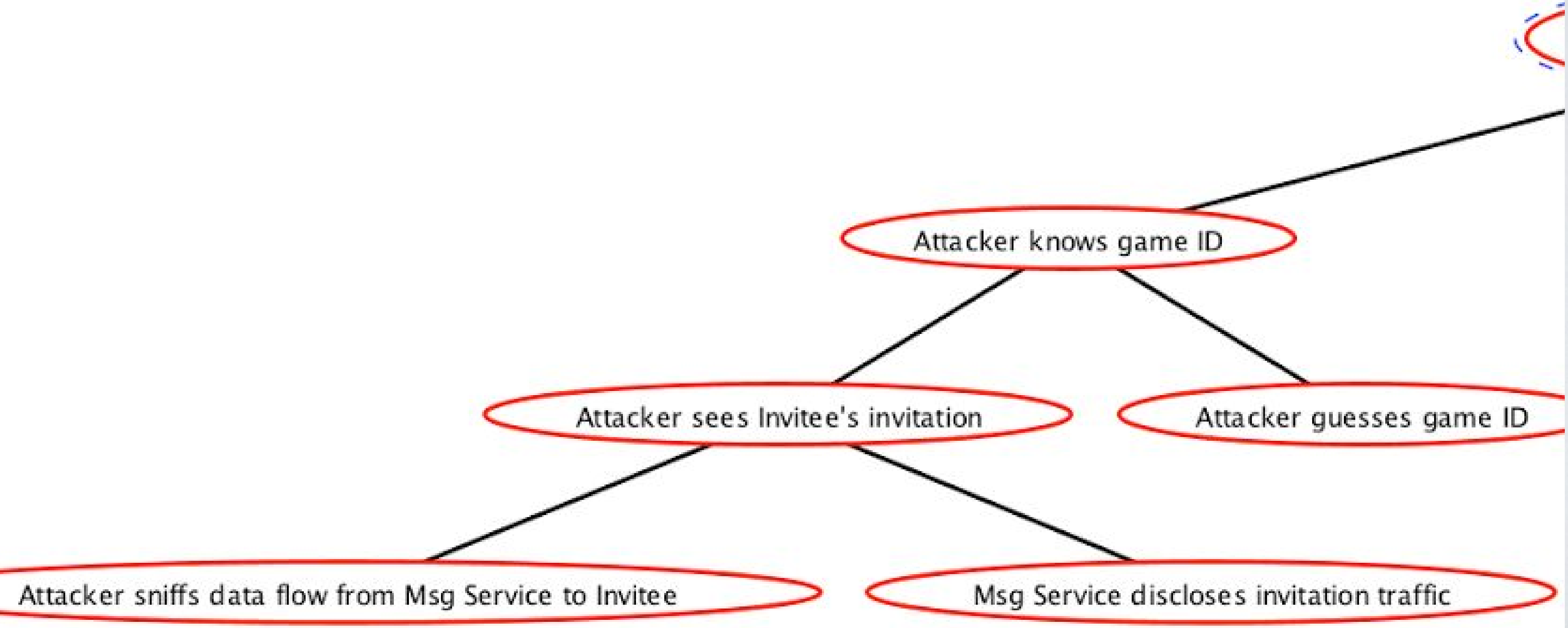
Not Started

High

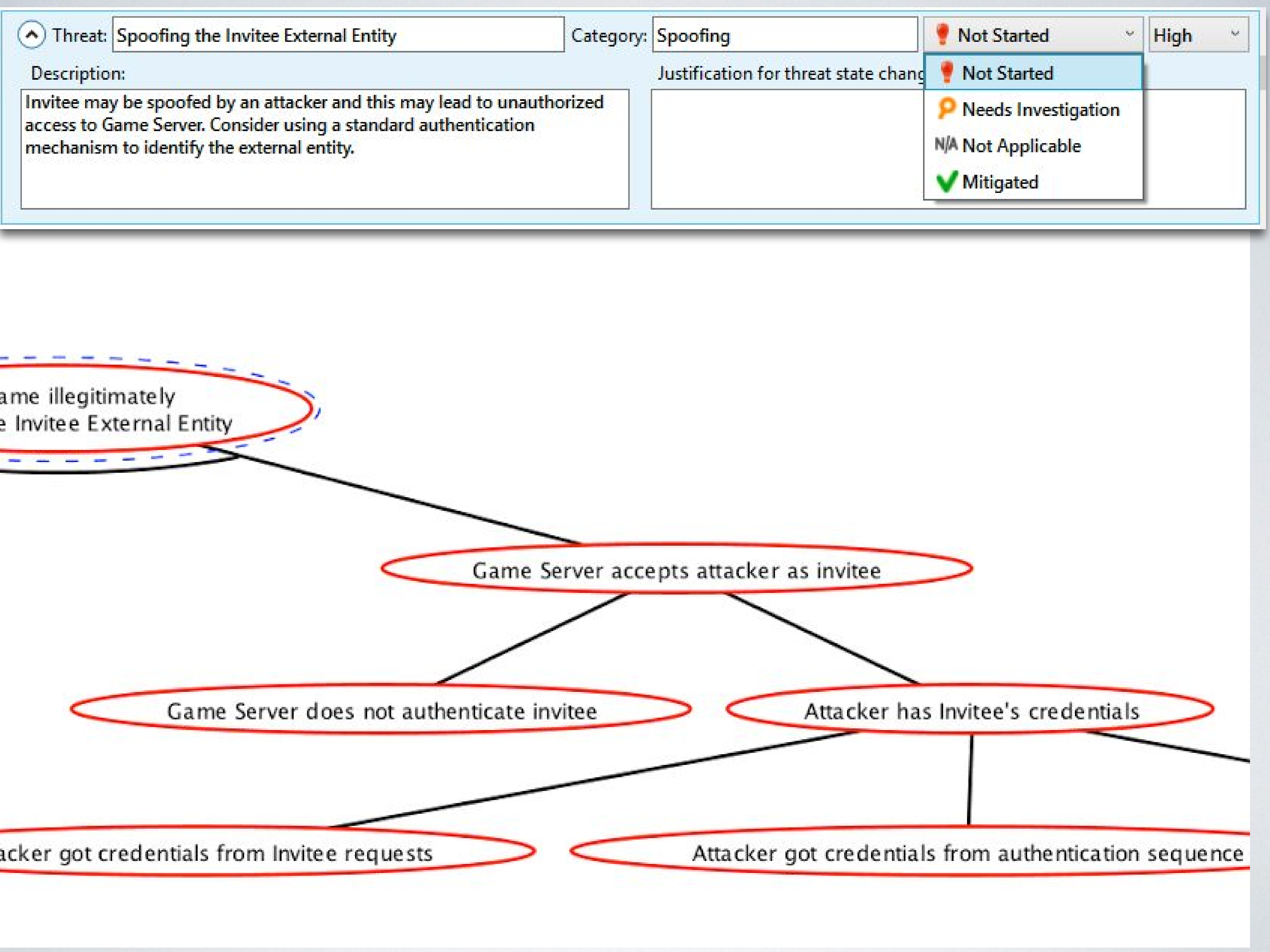
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang



Attacker knows game ID
Attacker sees Invitee's invitation
Attacker guesses game ID
Attacker sniffs data flow from Msg Service to Invitee
Msg Service discloses invitation traffic



Threat: Spoofing the Invitee External Entity

Category: Spoofing

Not Started

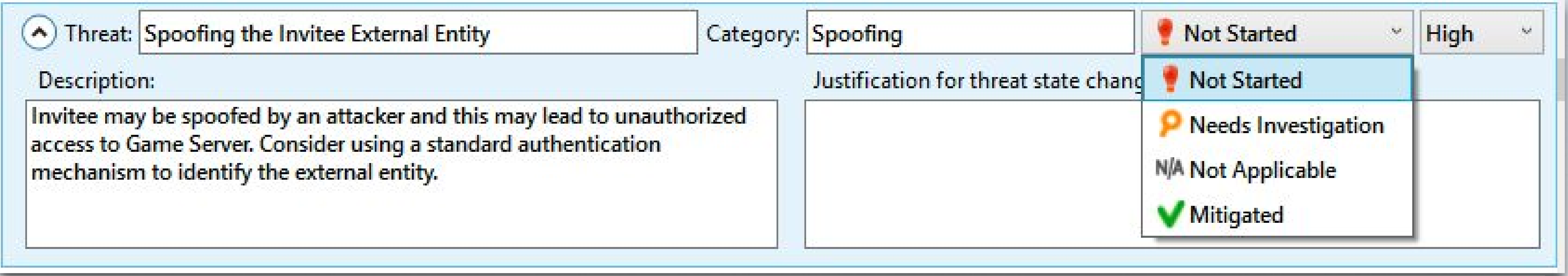
High

Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang

Not Started
Needs Investigation
N/A Not Applicable
Mitigated
ame illegitimately
e Invitee External Entity
Game Server accepts attacker as invitee
Game Server does not authenticate invitee
Attacker has Invitee's credentials
acker got credentials from Invitee requests
Attacker got credentials from authentication sequence



Threat: Spoofing the Invitee External Entity

Category: Spoofing

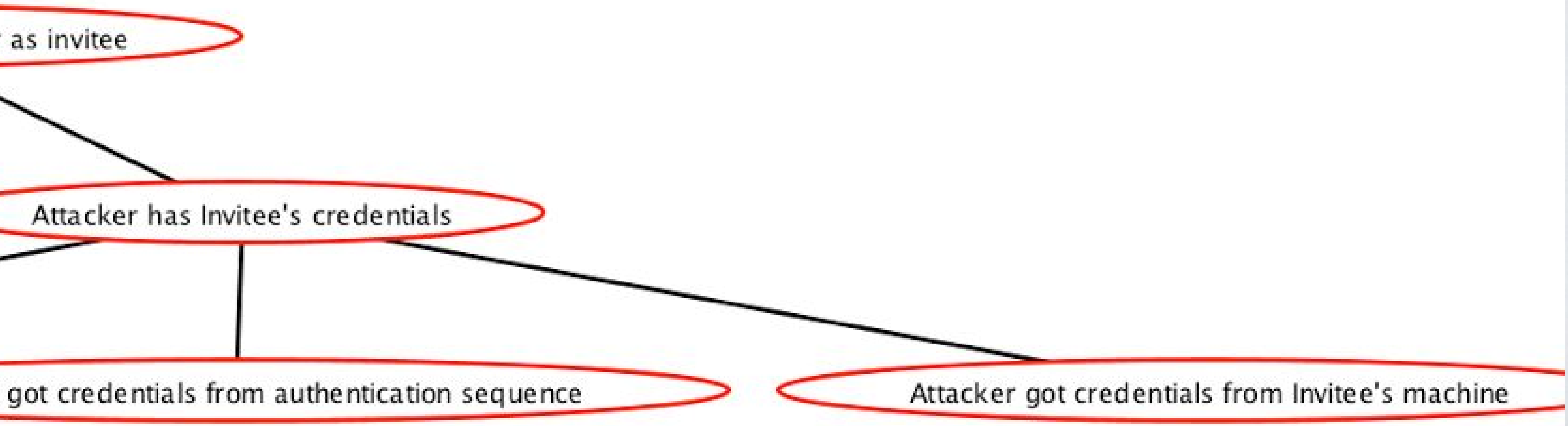
Not Started

High

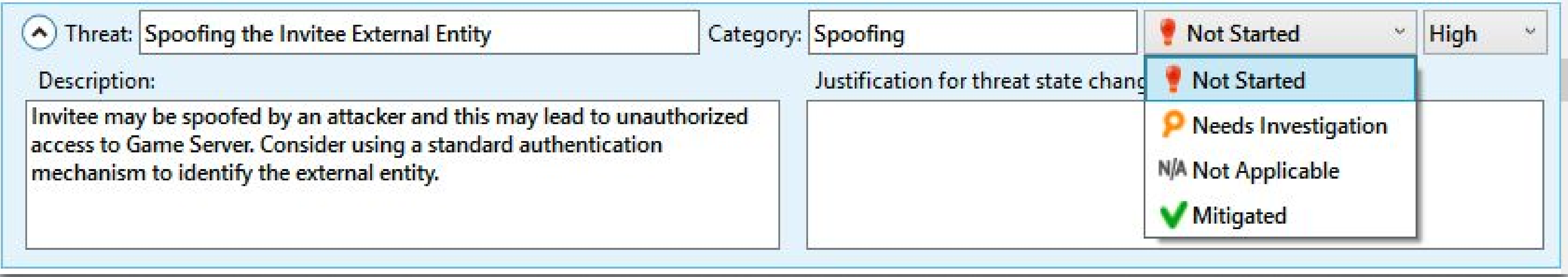
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang



as invitee
Attacker has Invitee's credentials
got credentials from authentication sequence
Attacker got credentials from Invitee's machine



Threat: Spoofing the Invitee External Entity

Category: Spoofing

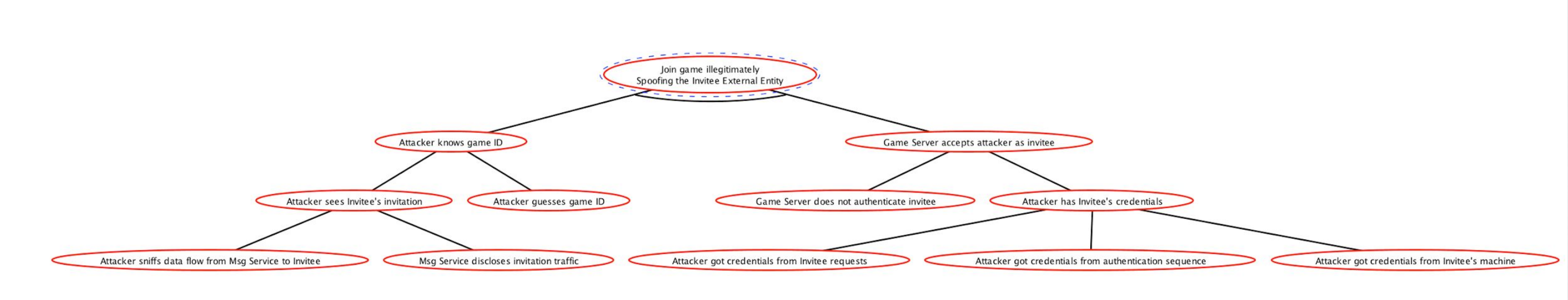
Not Started

High

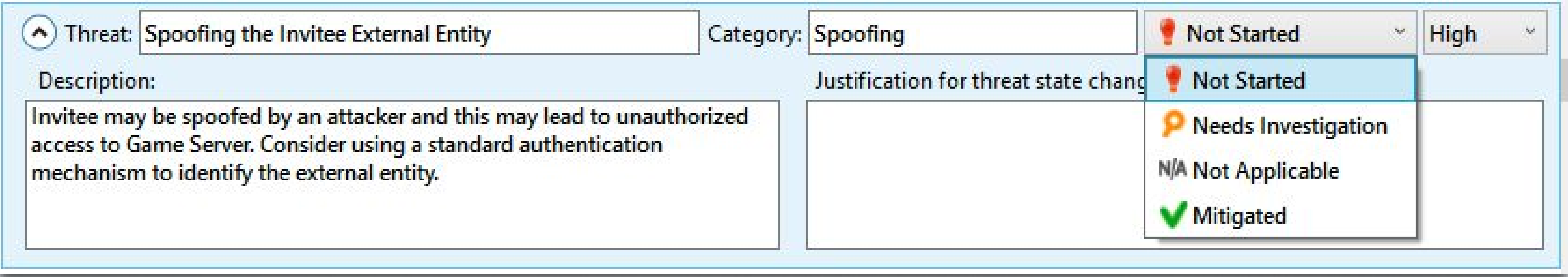
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang



Join game illegitimately
Spoofing the Invitee External Entity
Attacker knows game ID
Game Server accepts attacker as invitee
Attacker sees Invitee's invitation
Attacker guesses game ID
Game Server does not authenticate invitee
Attacker has Invitee's credentials
Attacker sniffs data flow from Msg Service to Invitee
Msg Service discloses invitation traffic
Attacker got credentials from Invitee requests
Attacker got credentials from authentication sequence
Attacker got credentials from Invitee's machine


Threat: Spoofing the Invitee External Entity

Category: Spoofing

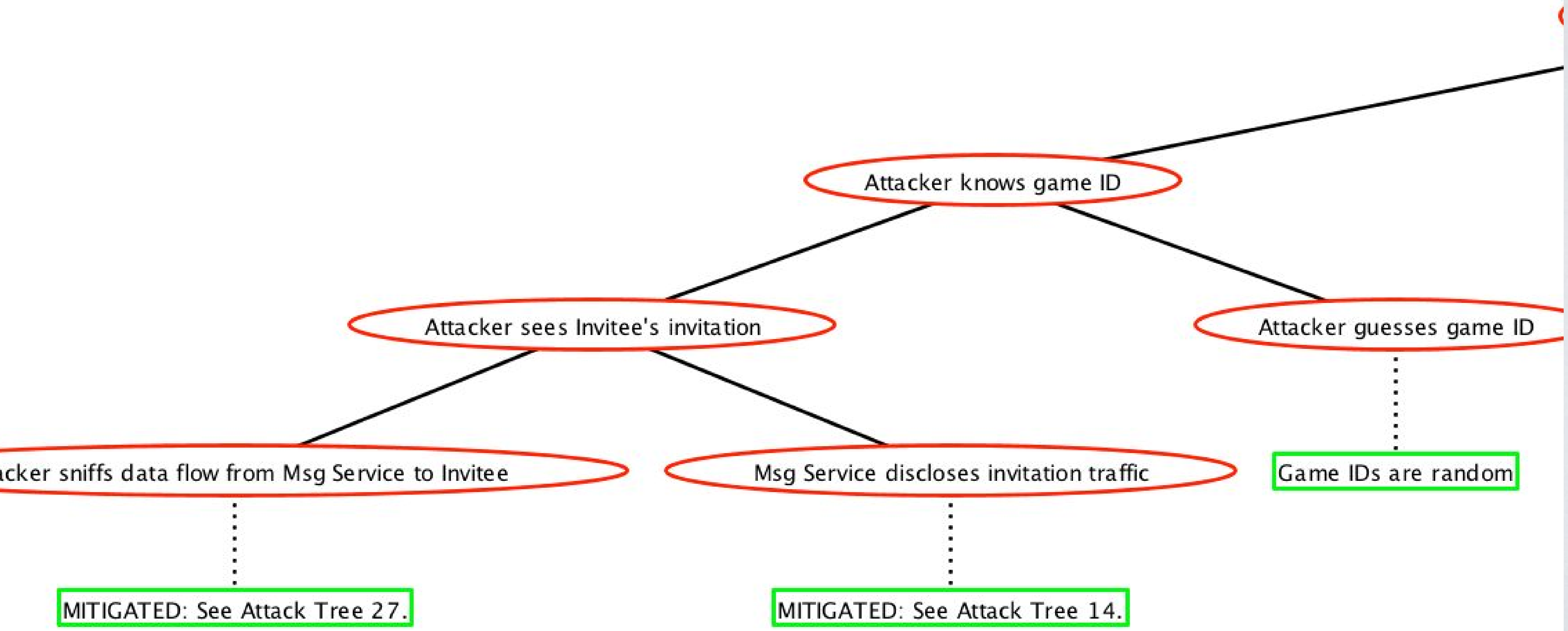
Not Started

High

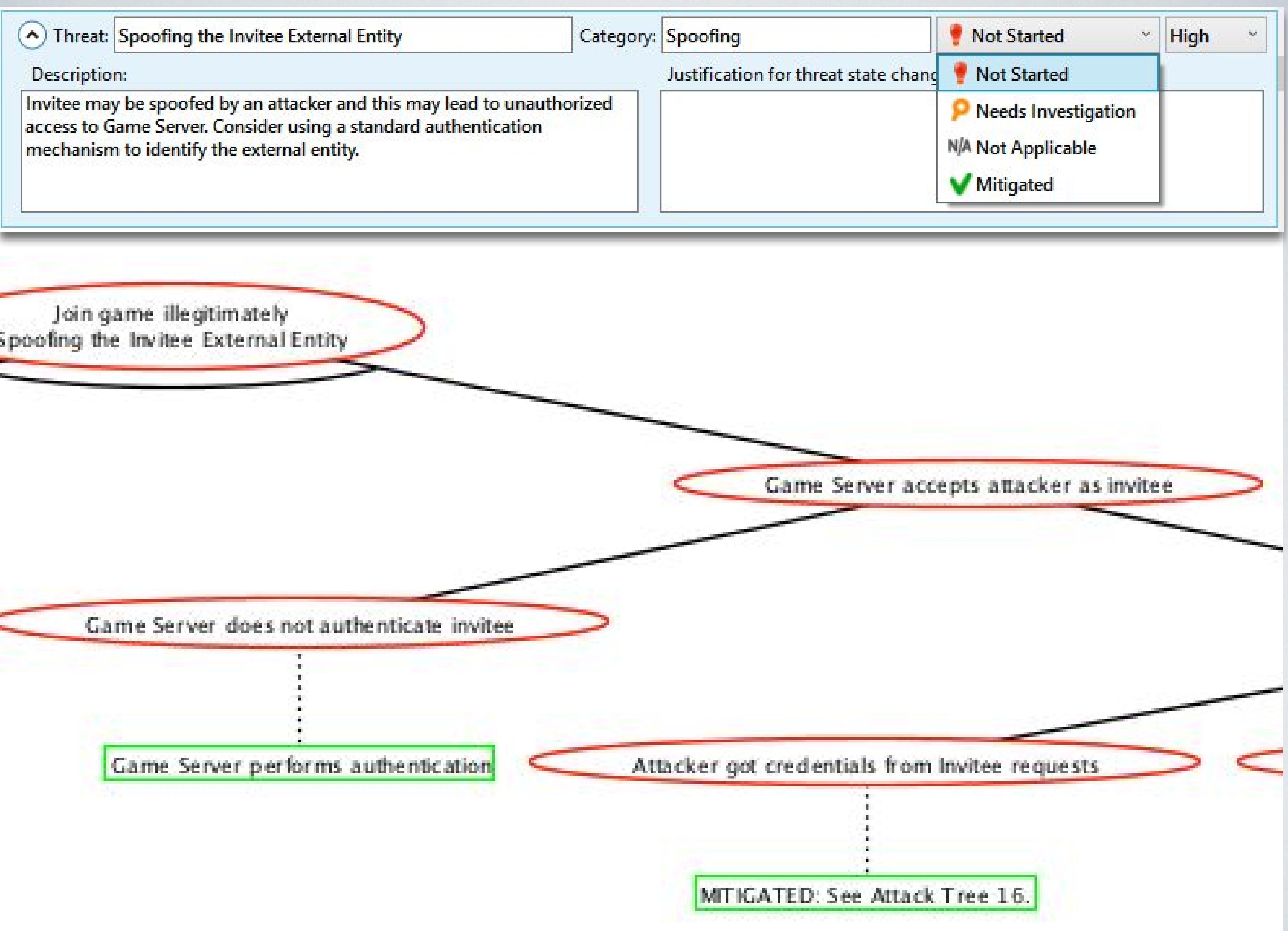
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang



Attacker knows game ID
Attacker sees Invitee's invitation
Attacker guesses game ID
cker sniffs data flow from Msg Service to Invitee
Msg Service discloses invitation traffic
Game IDs are random
MITIGATED: See Attack Tree 27.
MITIGATED: See Attack Tree 14.



Threat: Spoofing the Invitee External Entity

Category: Spoofing

Not Started

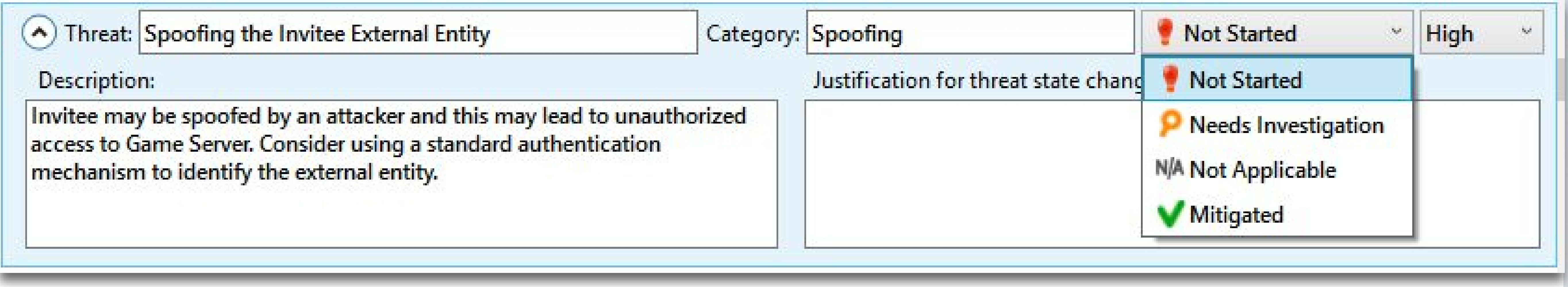
High

Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang

Not Started
Needs Investigation
N/A Not Applicable
Mitigated
Join game illegitimately
Spoofing the Invitee External Entity
Game Server accepts attacker as invitee
Game Server does not authenticate invitee
Game Server performs authentication
Attacker got credentials from Invitee requests
MITIGATED: See Attack Tree 16.



Threat: Spoofing the Invitee External Entity

Category: Spoofing

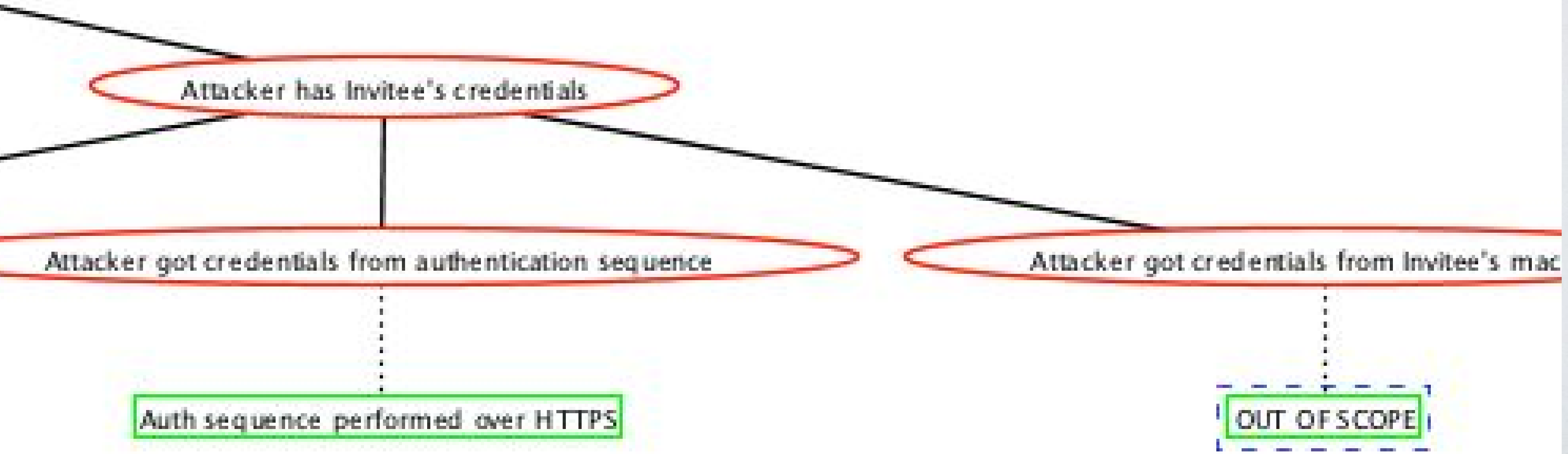
Not Started

High

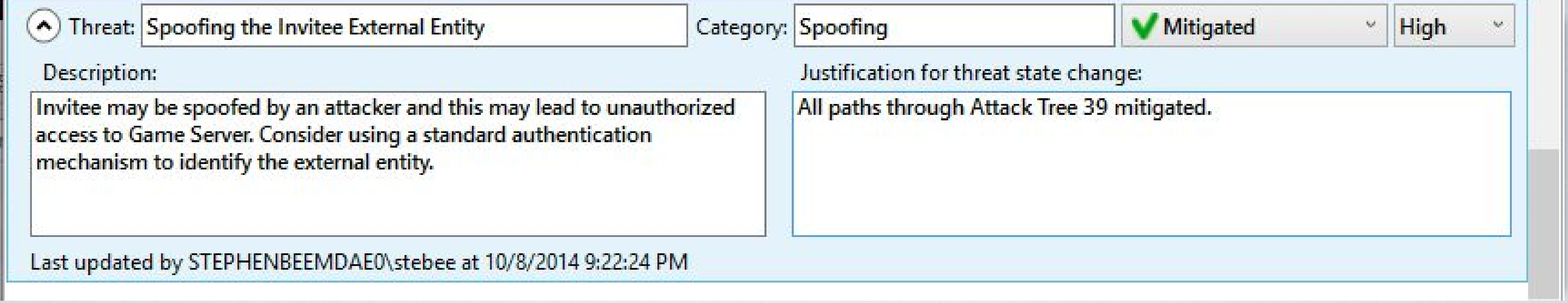
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state chang



Attacker has Invitee's credentials
Attacker got credentials from authentication sequence
Attacker got credentials from Invitee's mac
Auth sequence performed over HTTPS
OUT OF SCOPE



Threat: Spoofing the Invitee External Entity

Category: Spoofing

Mitigated

High

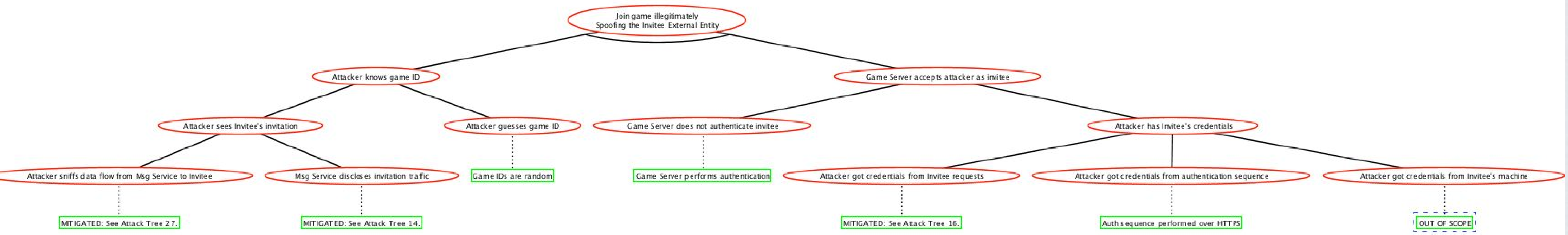
Description:

Invitee may be spoofed by an attacker and this may lead to unauthorized access to Game Server. Consider using a standard authentication mechanism to identify the external entity.

Justification for threat state change:

All paths through Attack Tree 39 mitigated.

Last updated by STEPHENBEEMDAE0\stebee at 10/8/2014 9:22:24 PM


Join game illegitimately
Spoofing the Invitee External Entity
Attacker knows game ID
Game Server accepts attacker as invitee
Attacker sees Invitee's invitation
Attacker guesses game ID
Game Server does not authenticate invitee
Attacker has Invitee's credentials
Attacker sniffs data flow from Msg Service to Invitee
Msg Service discloses invitation traffic
Game IDs are random
Game Server performs authentication
Attacker got credentials from Invitee requests
Attacker got credentials from authentication sequence
Attacker got credentials from Invitee's machine
MITIGATED: See Attack Tree 27.
MITIGATED: See Attack Tree 14.
MITIGATED: See Attack Tree 16.
Auth sequence performed over HTTPS
OUT OF SCOPE

- Take the DFD and list out all the possible intersections—STRIDE x Elements. Each of these is a “threat”.

- Some threats are impossible or out of scope. For the rest, prioritize based on potential damage, then construct attack trees to find out whether they’re mitigated or not.

- Unmitigated threats are vulnerabilities.

LIVE DEMO

MITIGATING VULNERABILITIES

Risk vs. Effort

Threat Modeling

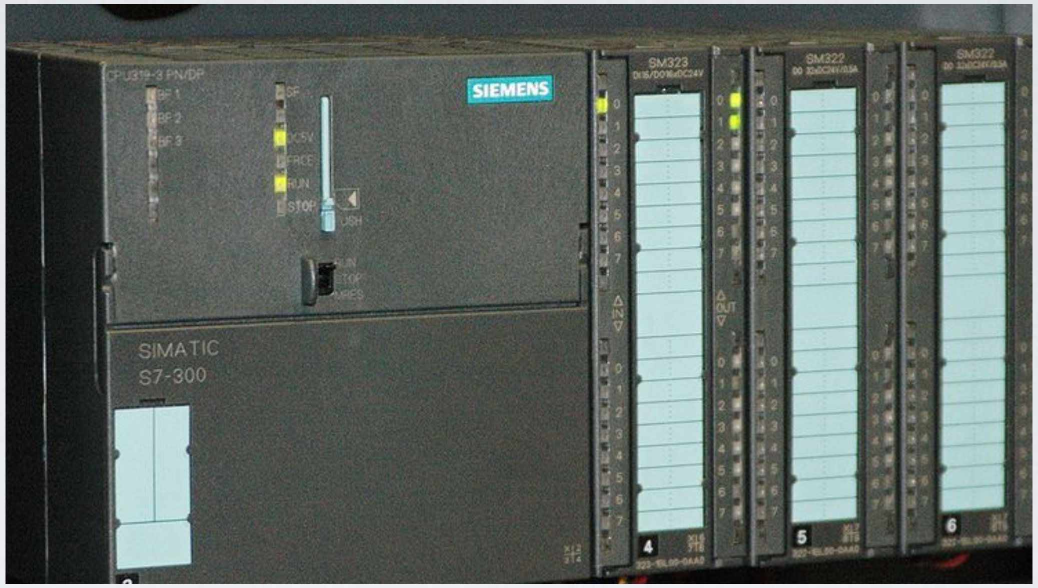
Threat modeling is a **process**
by which a **system** is **methodically analyzed**
from an **attacker's perspective**,
to **identify attack goals**,
evaluate the risks they pose
and **mitigate their vulnerabilities**.

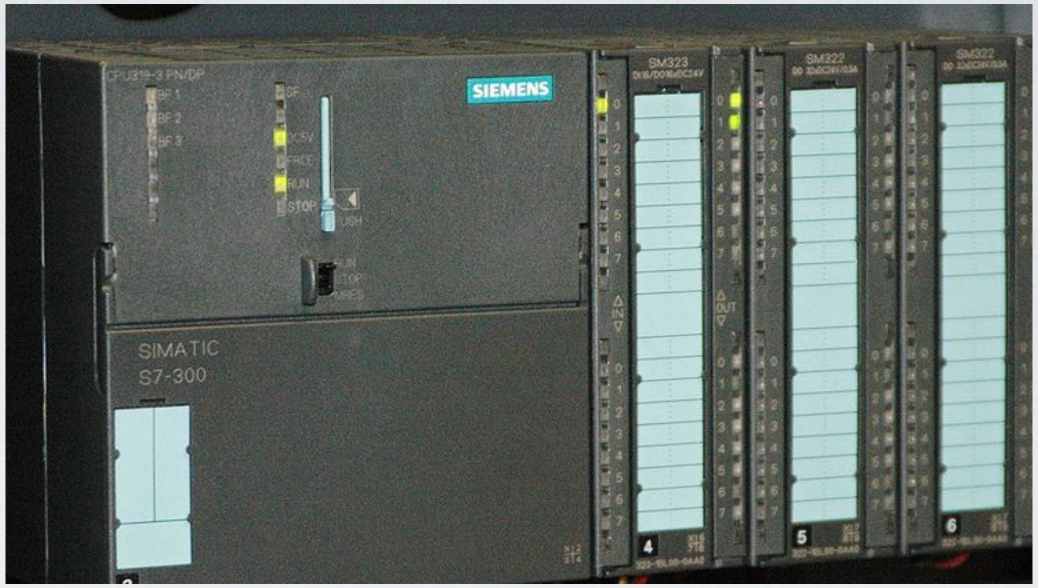
~~MITIGATE~~

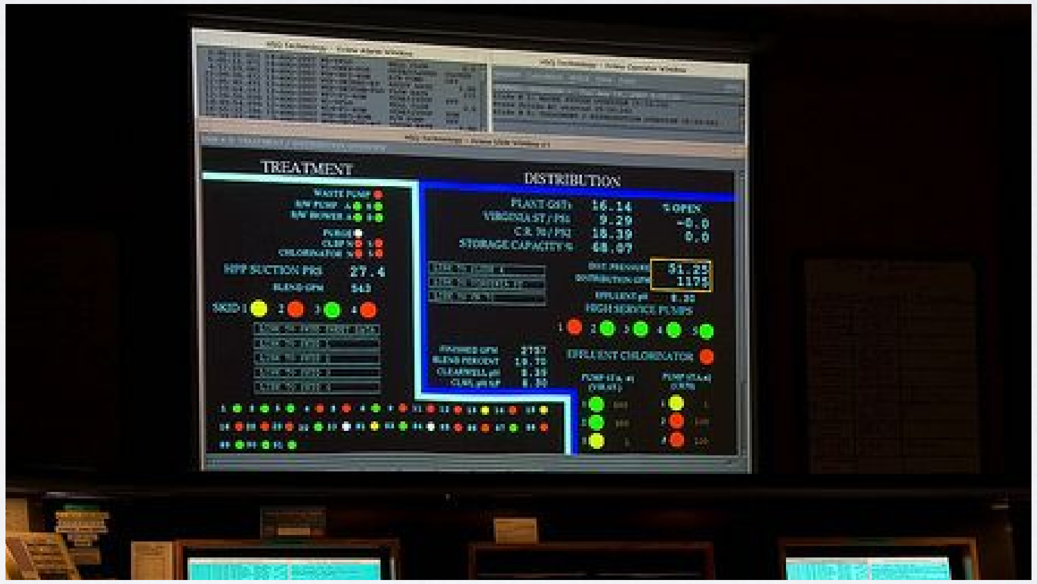
~~EVERY~~

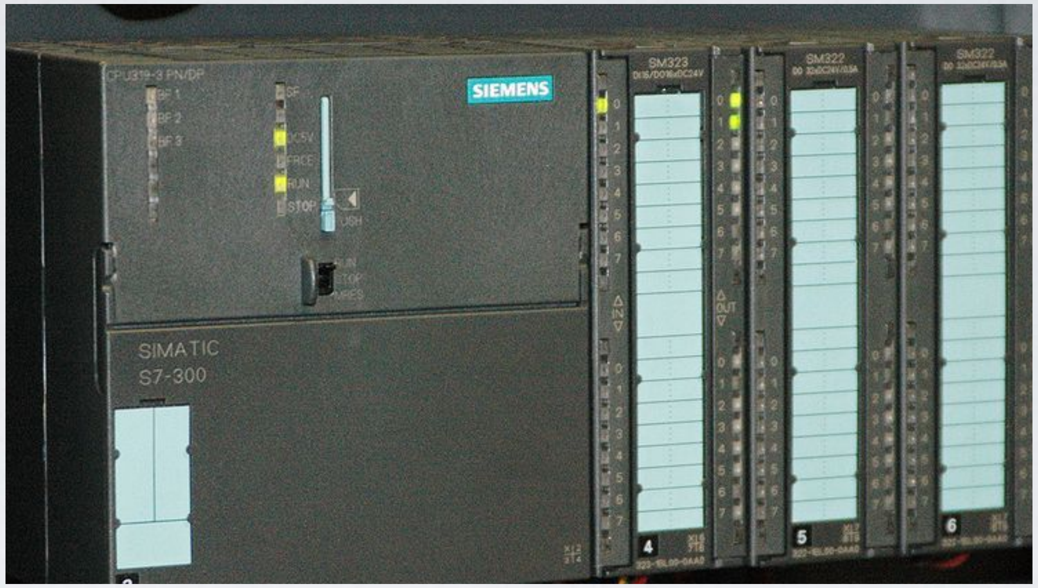
~~VULNERABILITY~~

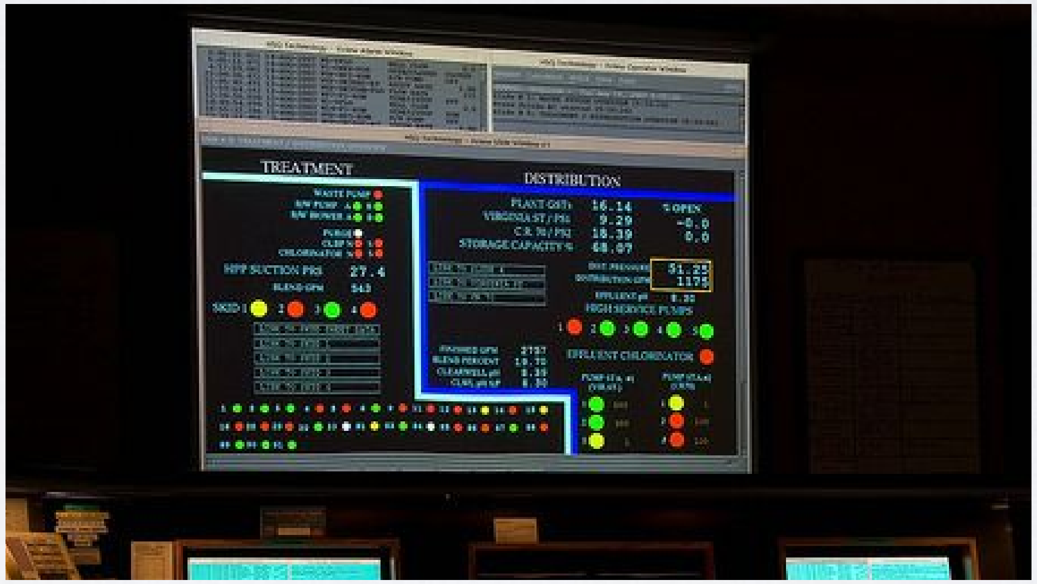
PERFECT
SECURITY
IS
IMPOSSIBLE

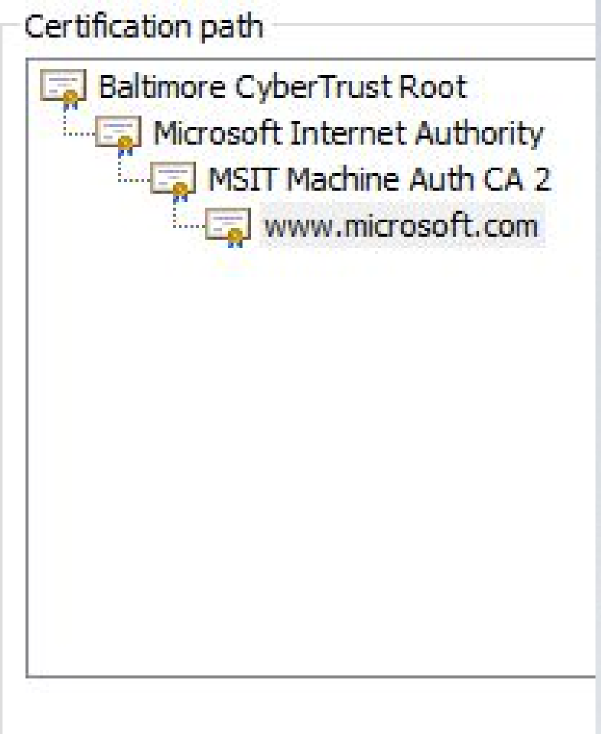

CPU319-3 PN/DP
SIEMENS
SIMATIC
S7-300
SM323
SM322
SM322
4
5
6


SIEMENS
SIMATIC S7-300
CPU319-3 PN/DP
SM323
SM322
SM322
4
5
6

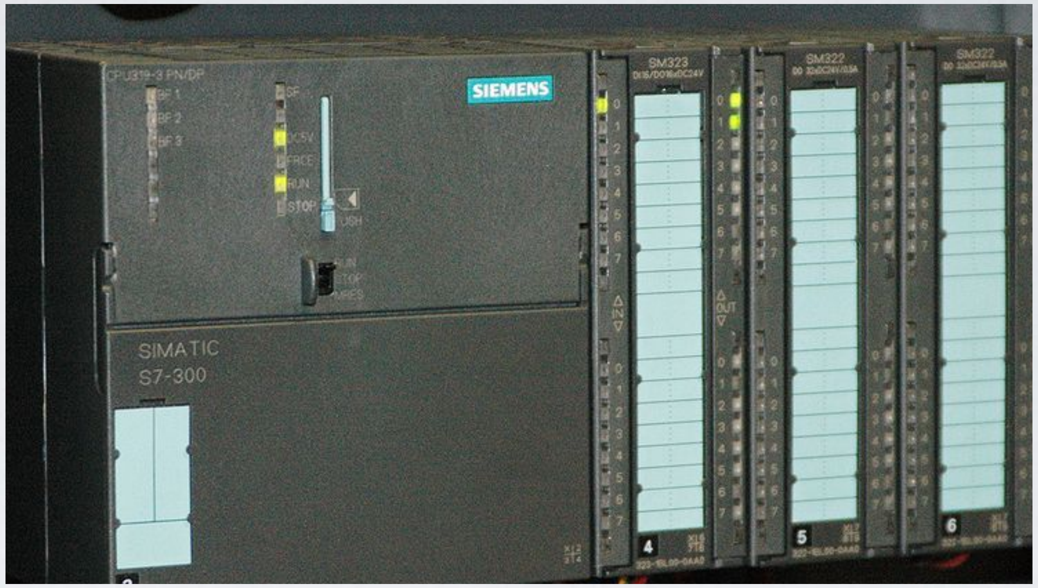

TREATMENT
DISTRIBUTION
WASTE PUMP
PLANT GST
16.14
VIRGINIA ST / PSI
9.29
STORAGE CAPACITY %
68.07
% OPEN
HPP SUCTION PSI
27.4
SKID 1
HIGH SERVICE PUMPS
EFFLUENT CHLORINATOR

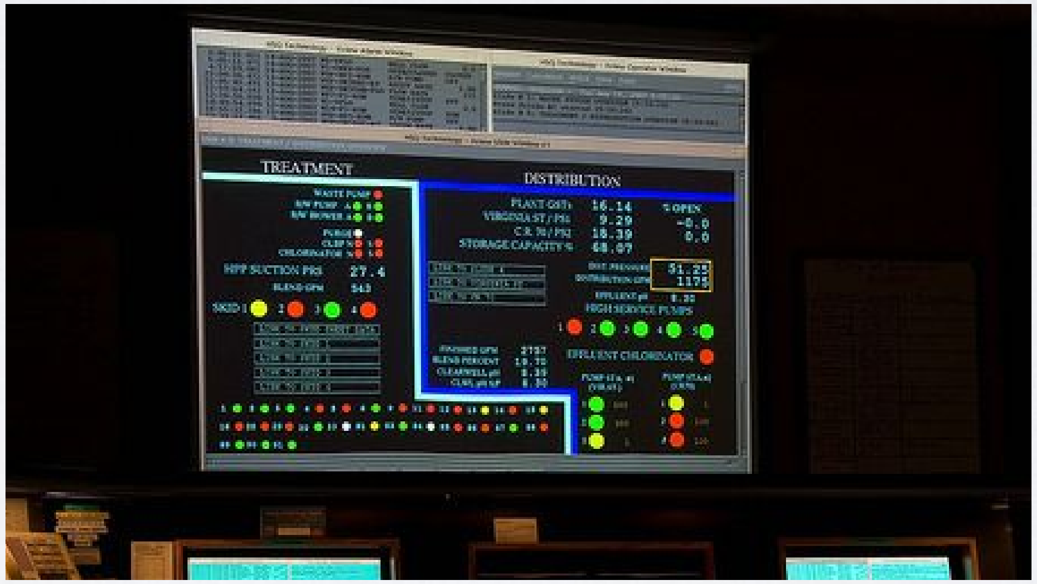


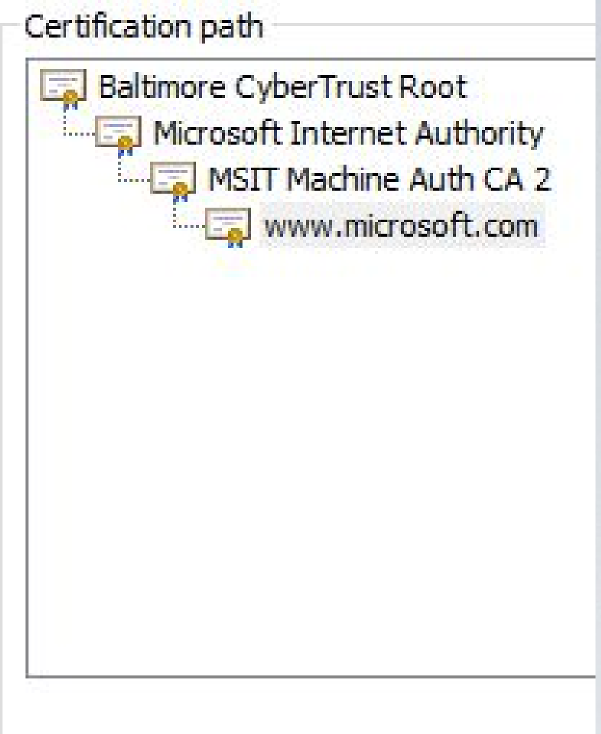



Certification path

- Baltimore CyberTrust Root
  - Microsoft Internet Authority
    - MSIT Machine Auth CA 2
      - www.microsoft.com







Certification path

- Baltimore CyberTrust Root
  - Microsoft Internet Authority
    - MSIT Machine Auth CA 2
      - www.microsoft.com

PERFECT
SECURITY
IS
IMPOSSIBLE

RISK =
LIKELIHOOD X COST

REAL

- **R**eward: What's it worth to the attacker?
- **E**ffort: How little does the attacker have to work?
- **A**udience: How many people will be affected?
- **L**evel of Skill: How many attackers have the skill required to carry out the attack.

Assign each a value from 1 to 10, multiply them all together and move the decimal two to the left, for a value from 0.01 to 100.0

THE GAME CENTER LEADERBOARD HACK

- **R**eward: 1
- **E**ffort: 10
- **A**udience: 3
- **L**evel of Skill: 9
- **Total rating: 2.7**

TAKE ACTION

- Define a “security bar”, the risk rating above which you will act on a vulnerability.

- Vulnerabilities above this bar go in your bug database.

- Vulnerabilities below this bar go in your backlog.

CREATING MITIGATIONS

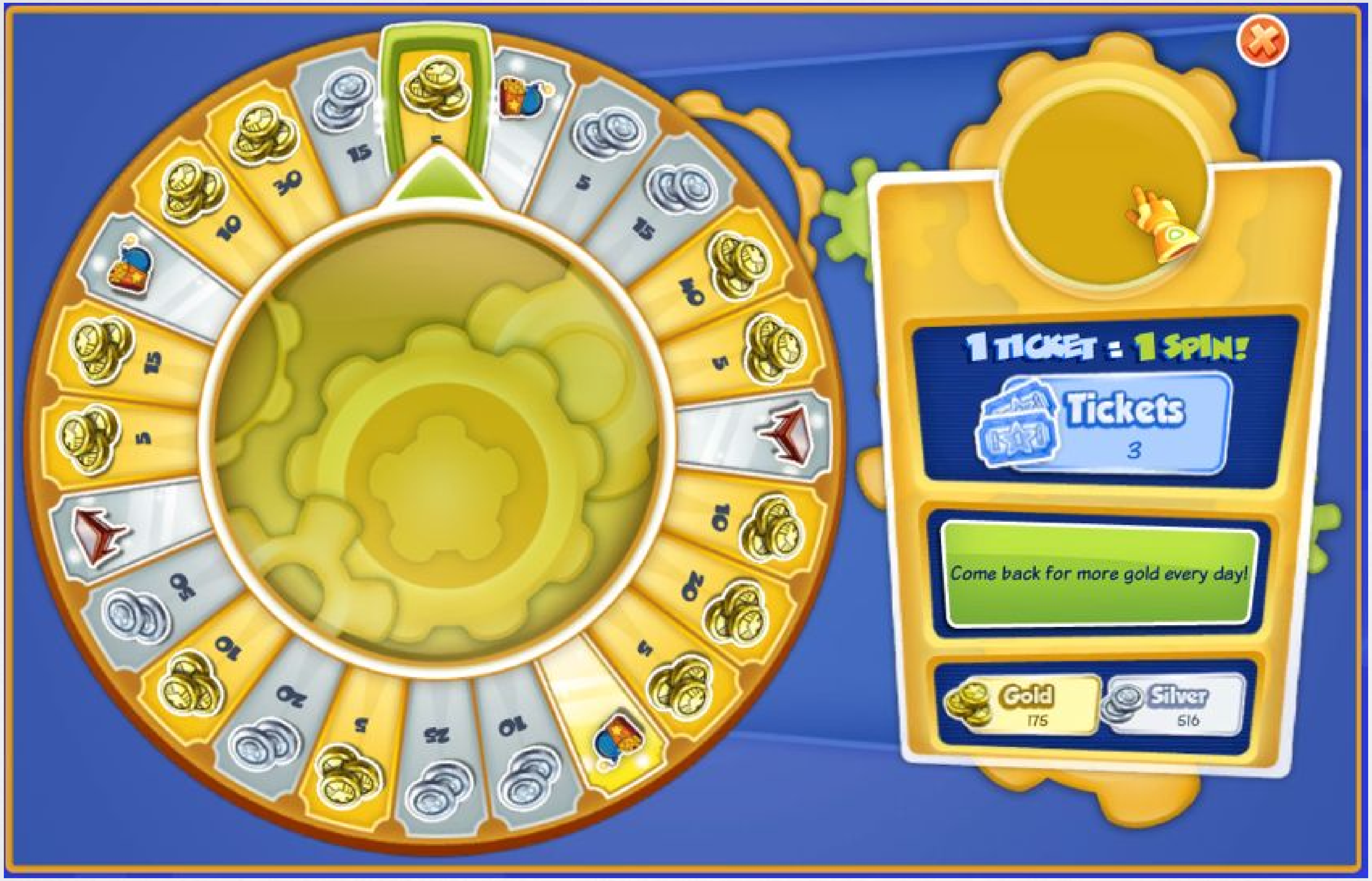
1. Change the circumstances so that paths through the attack tree are closed off.

2. Change the risk variables so that the vulnerability falls below your security bar.

CHANGE THE RISK

- Reduce the reward!
- Increase the effort!
- Limit the audience!
- Raise the skill level!

SECURITY THROUGH GAME DESIGN



1 TICKET = 1 SPIN!

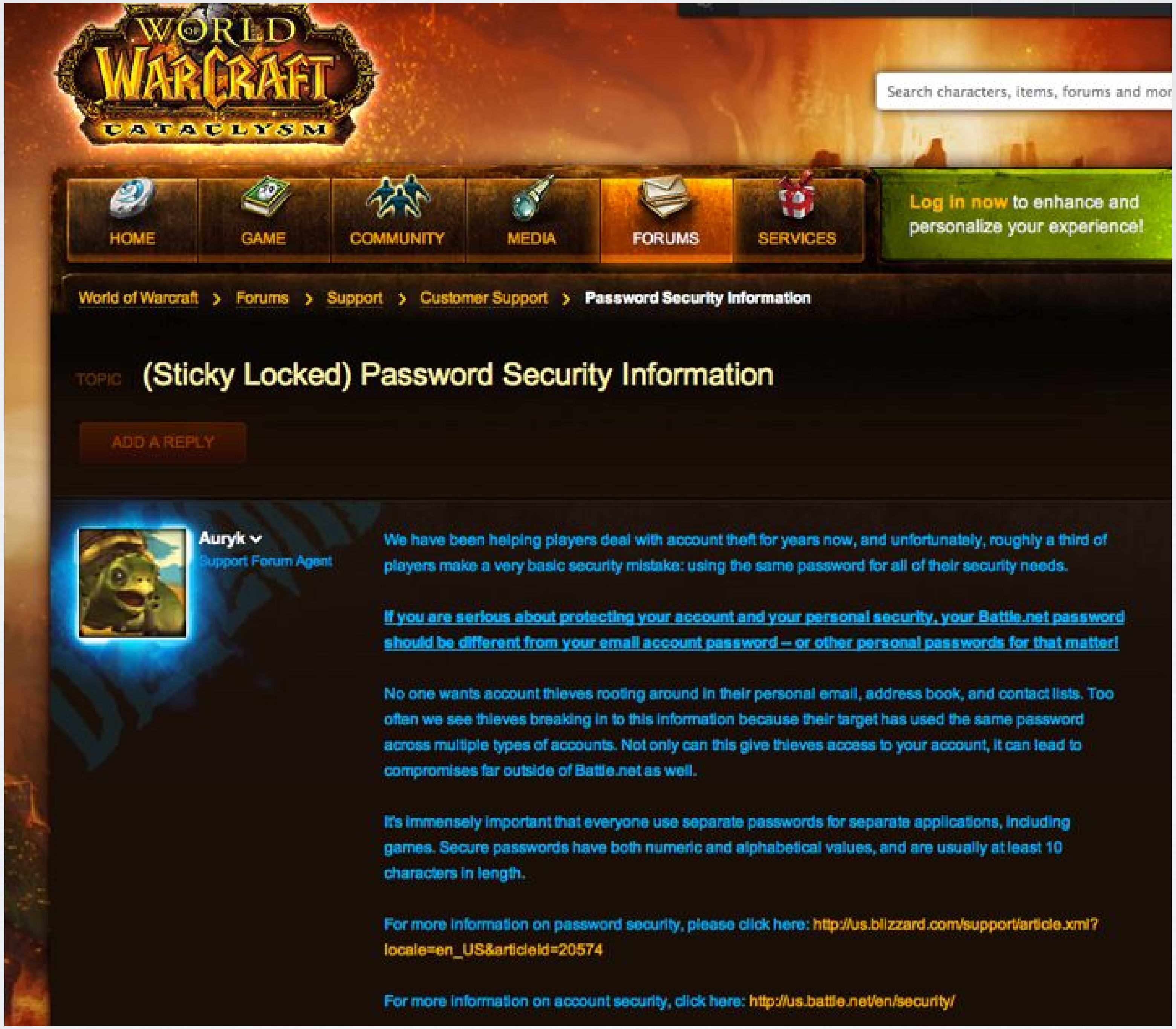
Tickets
3

Come back for more gold every day!

Gold
175

Silver
516

SECURITY THROUGH COMMUNITY MANAGEMENT



WORLD OF WARCRAFT CATACLYSM
Search characters, items, forums and mor
HOME
GAME
COMMUNITY
MEDIA
FORUMS
SERVICES
Log in now to enhance and personalize your experience!
World of Warcraft › Forums › Support › Customer Support › Password Security Information
TOPIC
ADD A REPLY

(Sticky Locked) Password Security Information

Auryk
Support Forum Agent

We have been helping players deal with account theft for years now, and unfortunately, roughly a third of players make a very basic security mistake: using the same password for all of their security needs.

If you are serious about protecting your account and your personal security, your Battle.net password should be different from your email account password – or other personal passwords for that matter!

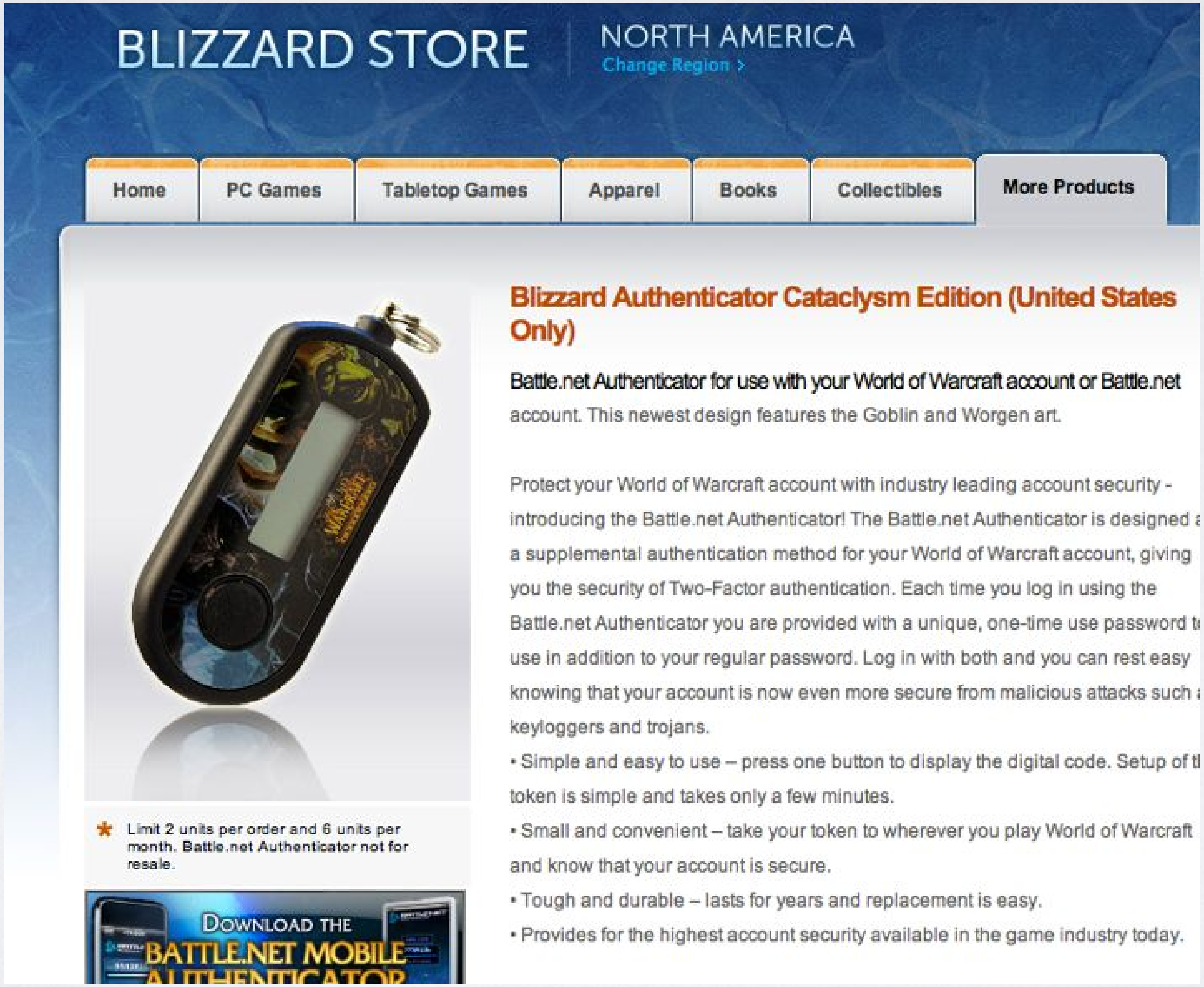
No one wants account thieves rooting around in their personal email, address book, and contact lists. Too often we see thieves breaking in to this information because their target has used the same password across multiple types of accounts. Not only can this give thieves access to your account, it can lead to compromises far outside of Battle.net as well.

It's immensely important that everyone use separate passwords for separate applications, including games. Secure passwords have both numeric and alphabetical values, and are usually at least 10 characters in length.

For more information on password security, please click here: http://us.blizzard.com/support/article.xml?locale=en_US&articleId=20574

For more information on account security, click here: http://us.battle.net/en/security/

SECURITY THROUGH BUSINESS DEVELOPMENT



Blizzard Authenticator Cataclysm Edition (United States Only)

Battle.net Authenticator for use with your World of Warcraft account or Battle.net account. This newest design features the Goblin and Worgen art.

Protect your World of Warcraft account with industry leading account security - introducing the Battle.net Authenticator! The Battle.net Authenticator is designed a a supplemental authentication method for your World of Warcraft account, giving you the security of Two-Factor authentication. Each time you log in using the Battle.net Authenticator you are provided with a unique, one-time use password t use in addition to your regular password. Log in with both and you can rest easy knowing that your account is now even more secure from malicious attacks such a keyloggers and trojans.

- Simple and easy to use – press one button to display the digital code. Setup of t token is simple and takes only a few minutes.
- Small and convenient – take your token to wherever you play World of Warcraft and know that your account is secure.
- Tough and durable – lasts for years and replacement is easy.
- Provides for the highest account security available in the game industry today.

* Limit 2 units per order and 6 units per month. Battle.net Authenticator not for resale.

LATHER
RINSE
REPEAT

- Perfect security is impossible, but zero security is unacceptable. You have to strike a smart balance.

- Risk is likelihood times cost.

- Making attacks impossible is best.

- Making attacks less likely or less costly might be just as good.