



# Designing a Simple Authentication Scheme

Game illegitimately  
Invites External Entity

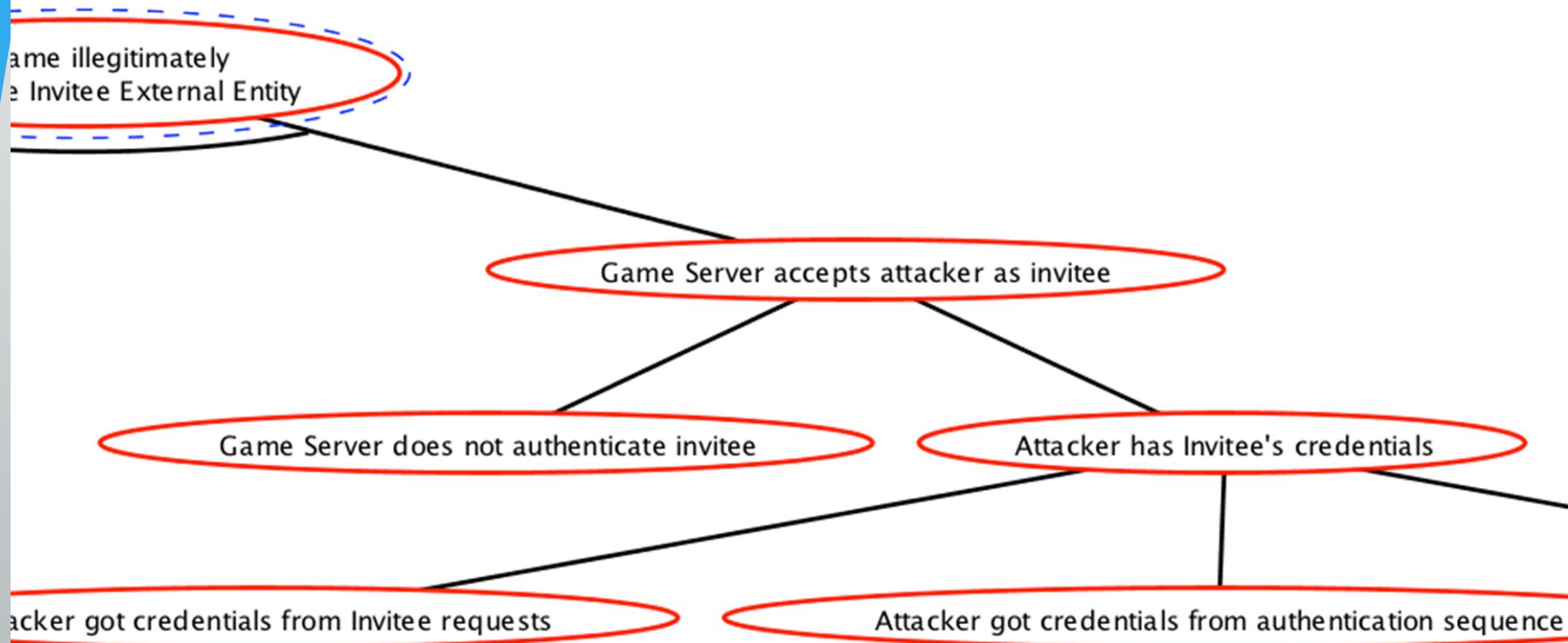
Game Server accepts attacker as invitee

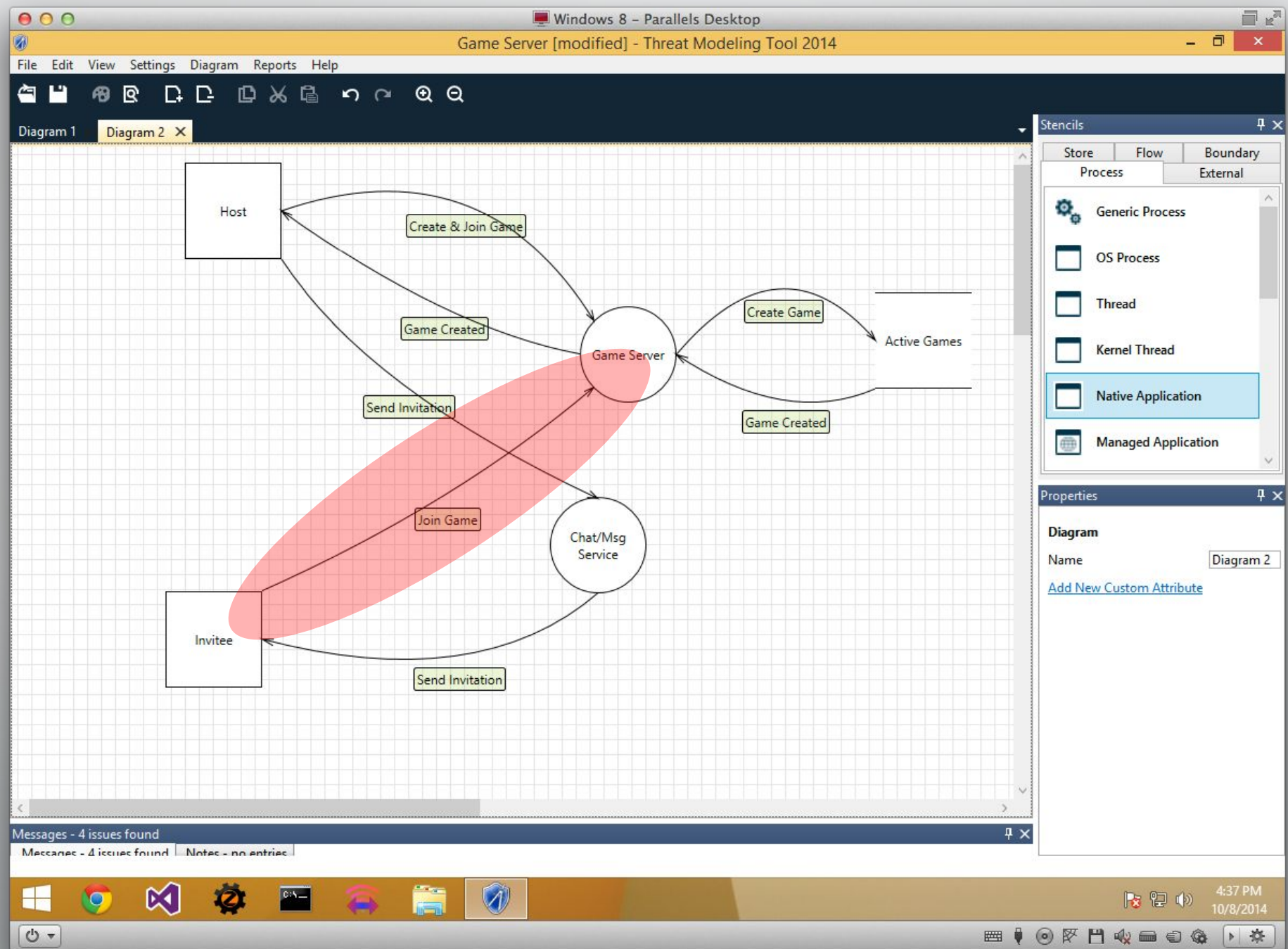
Game Server does not authenticate invitee

Attacker has Invitee's credentials

Attacker got credentials from Invitee requests

Attacker got credentials from authentication sequence

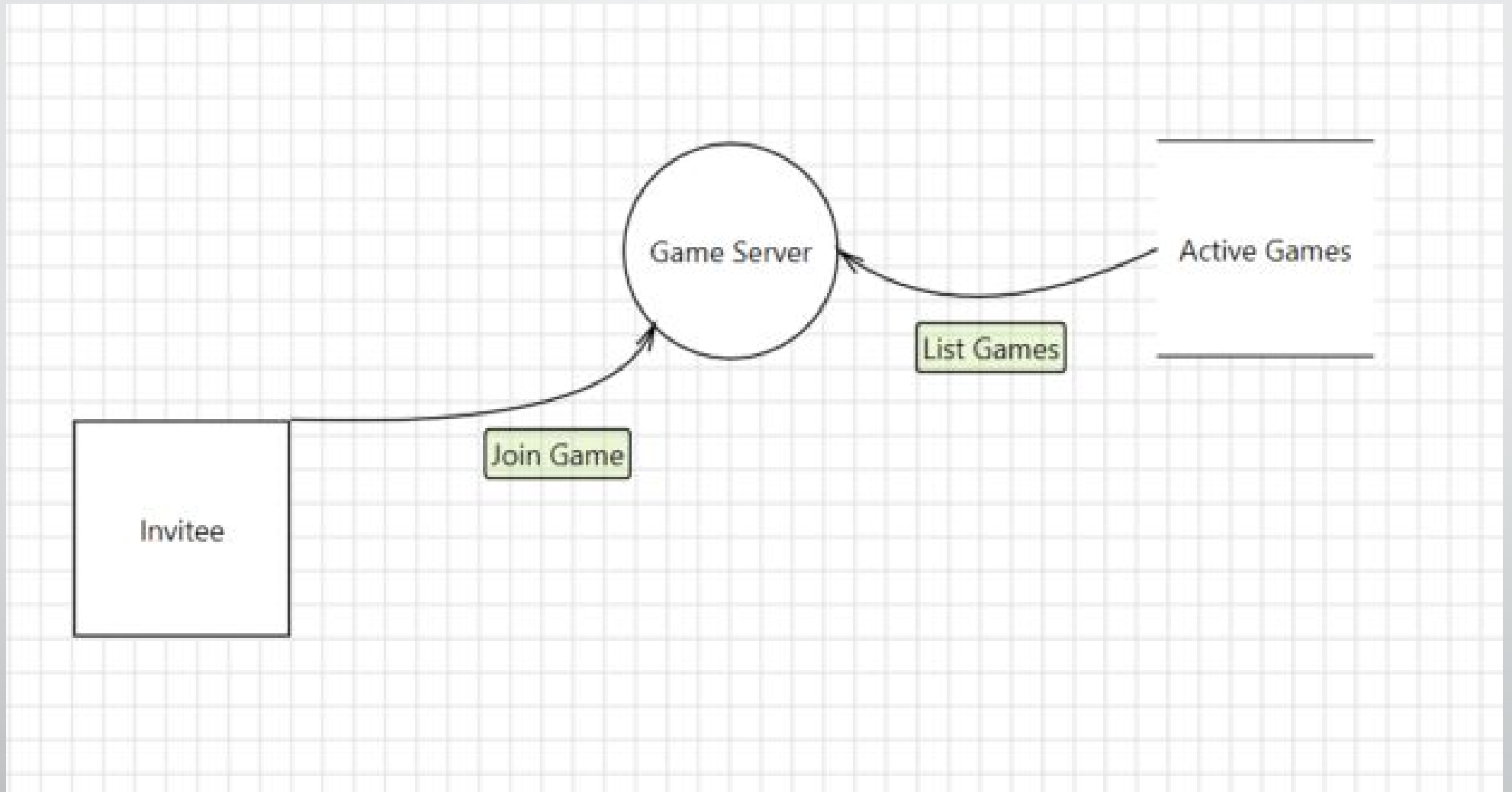


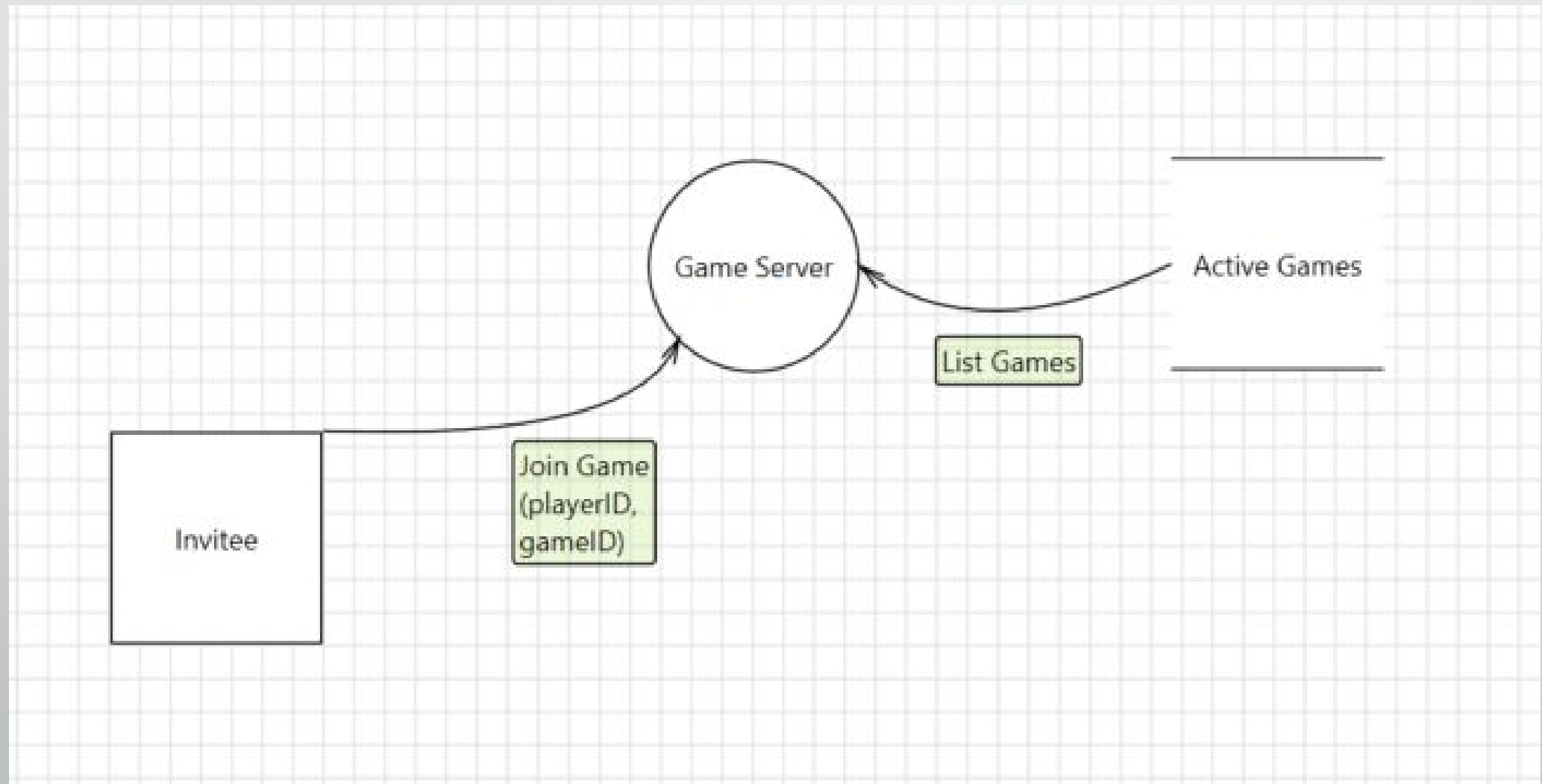


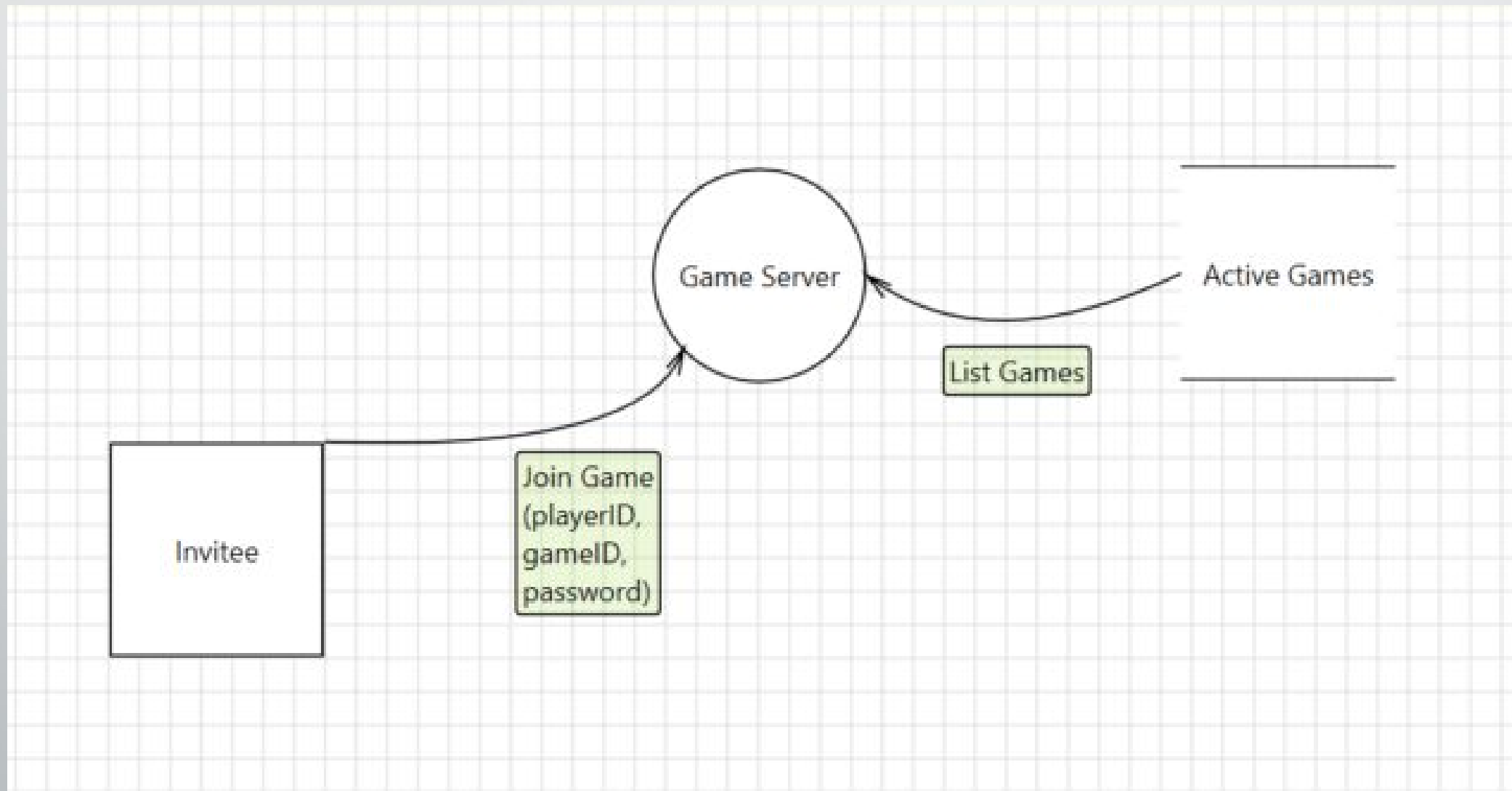


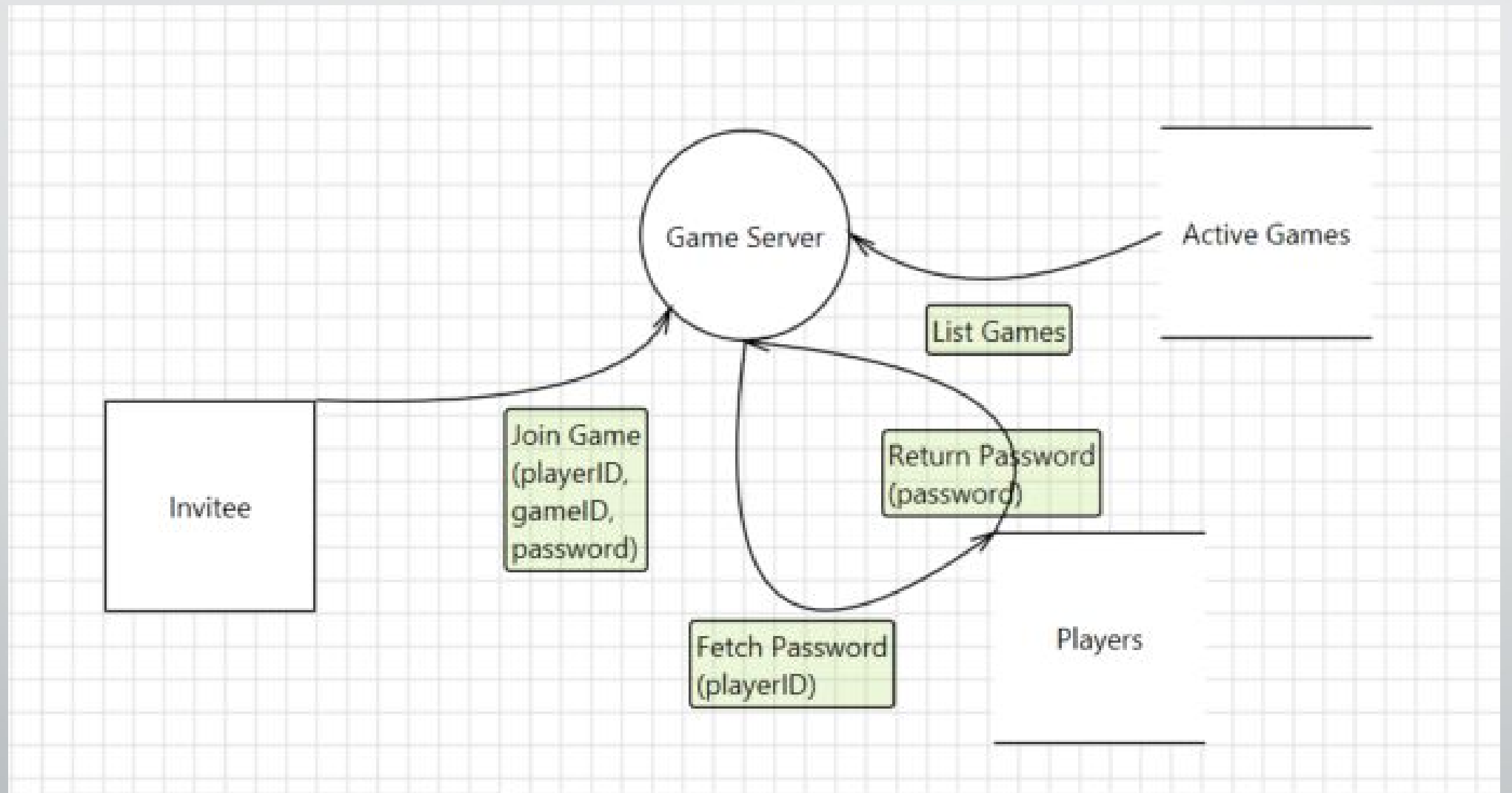
*Authentication requires us to...*

Demonstrate possession of a  
*shared secret*  
without revealing it













*Here's why that's bad...*

- Dependent on the player database
  - Time-consuming
  - Inconvenient
- Must protect request



*Authentication requires us to...*

Demonstrate possession of a  
*shared secret*  
without revealing it

## *A cryptographic hash...*

- Reduces an arbitrary document to a fixed-size representation...
- ...in a way that minimizes the chance of collisions...
- ...and is impossible to invert in less than brute-force time.

# All About Hashes





$H[x]$  = "the hash of  $x$ "

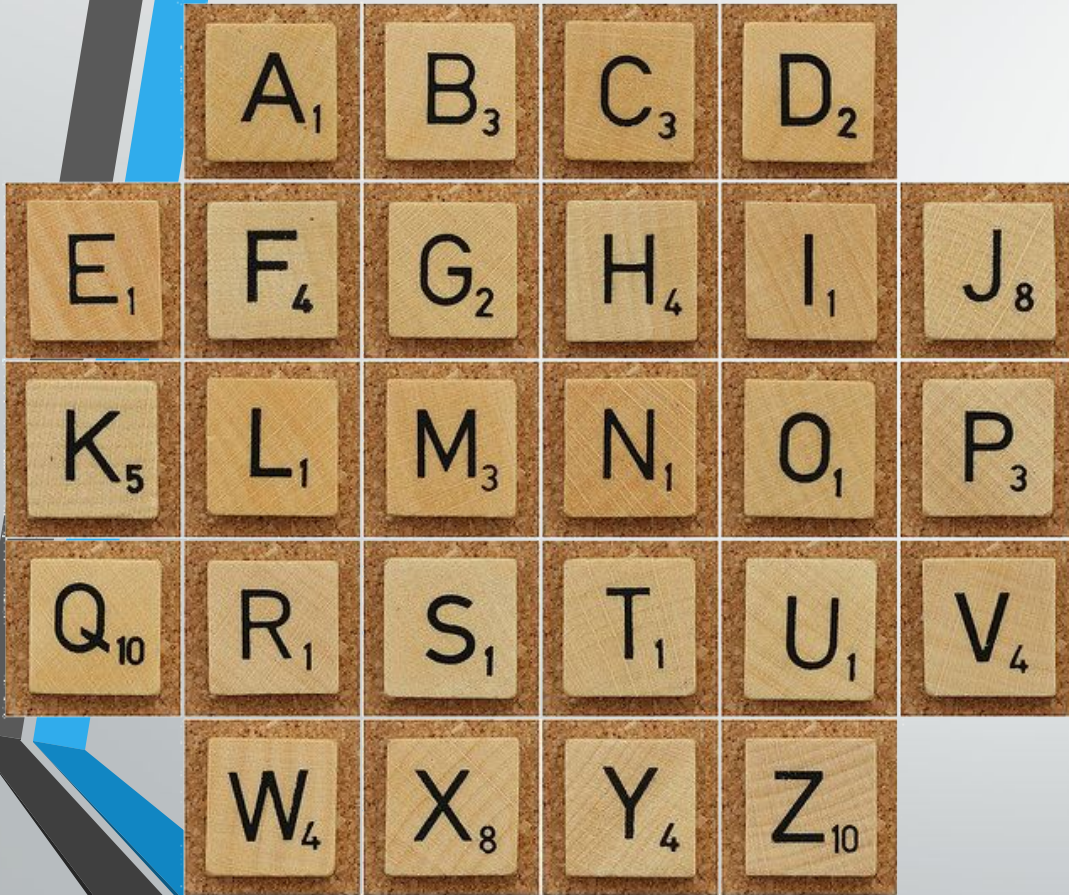
$SCR[x]$  = "how much would  $x$  score in Scrabble"



$SCR["advance"] =$   
 $1+2+4+1+1+3+1 = 13$

$SCR["advance" || "FOO"] =$   
 $19$

"advance19"

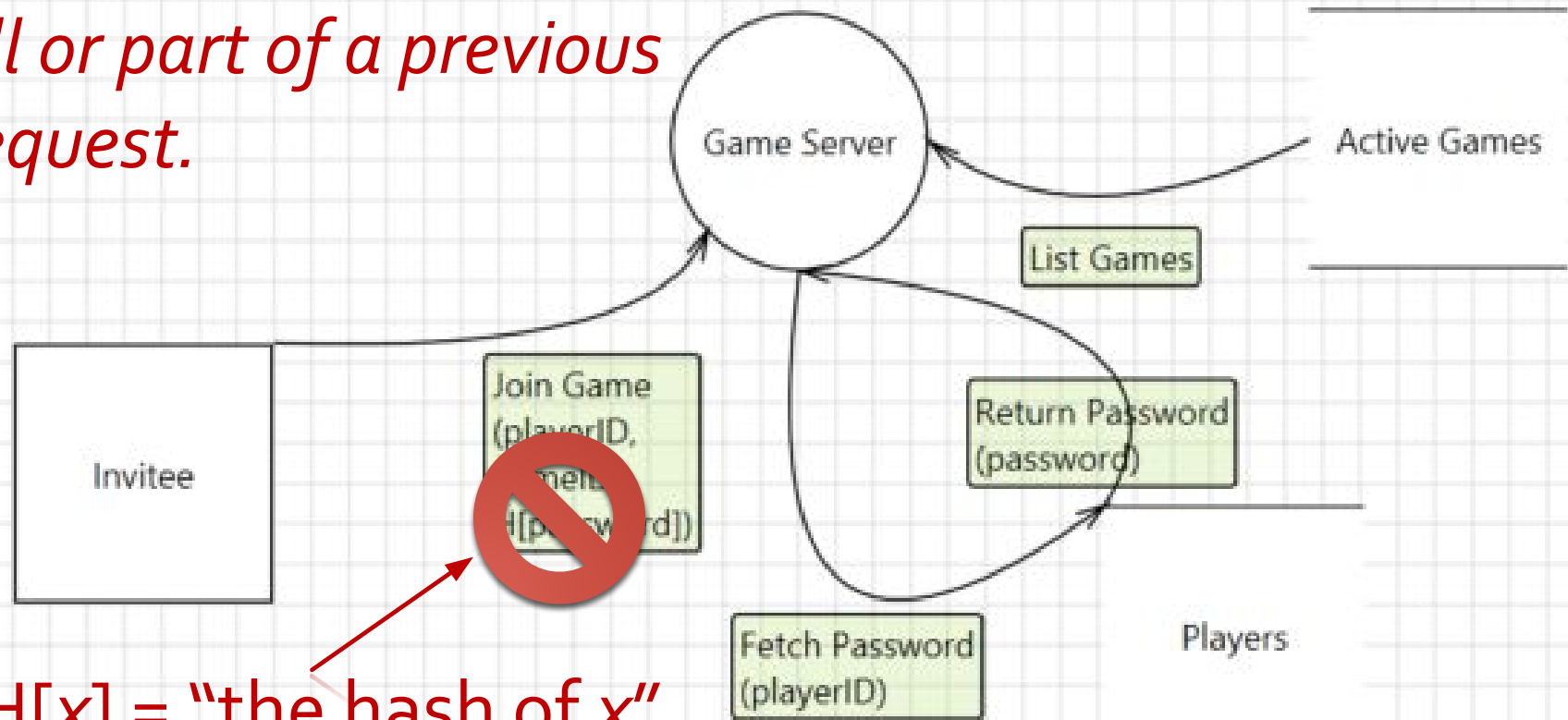


$\text{SCR}[\text{"advance"} \parallel \text{"BB"}] = 19$

$\text{SCR}[\text{"surrender"} \parallel \text{"BB"}] = 16$   
"surrender16"

$\text{SCR}[\text{"surrender"} \parallel \text{"FOO"}] = 16$

*Replay attack: Resubmitting  
all or part of a previous  
request.*



$H[x]$  = "the hash of  $x$ "

$H[x||y]$  = "the hash of  $x$  followed by  $y$ "



## *Preventing replay attacks...*

- Known precisely to both parties
- Changes over time; never reused
- Cannot be influenced by attacker
- *Secrecy not required!*

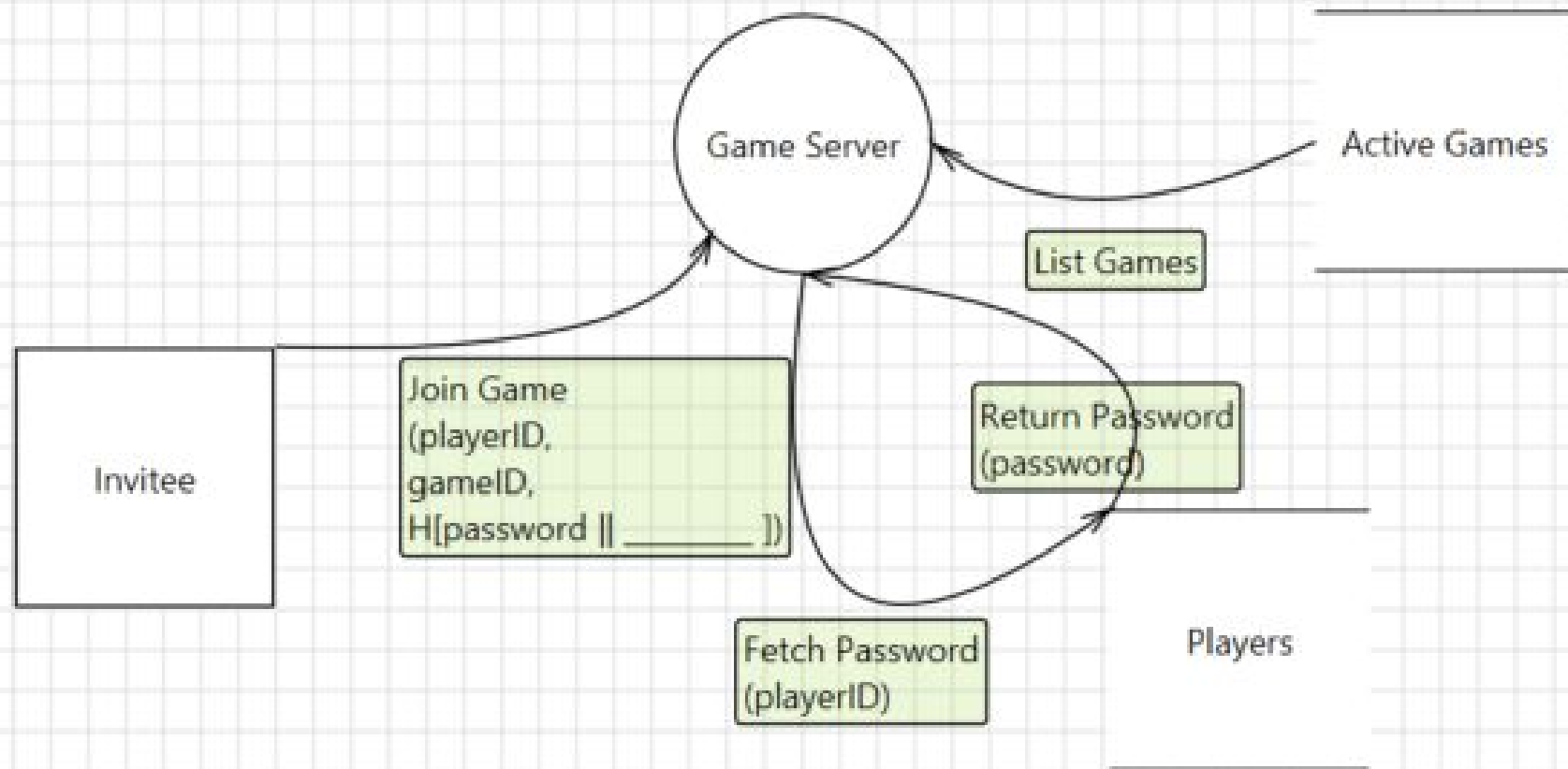
Generic term for this value is a “nonce”.

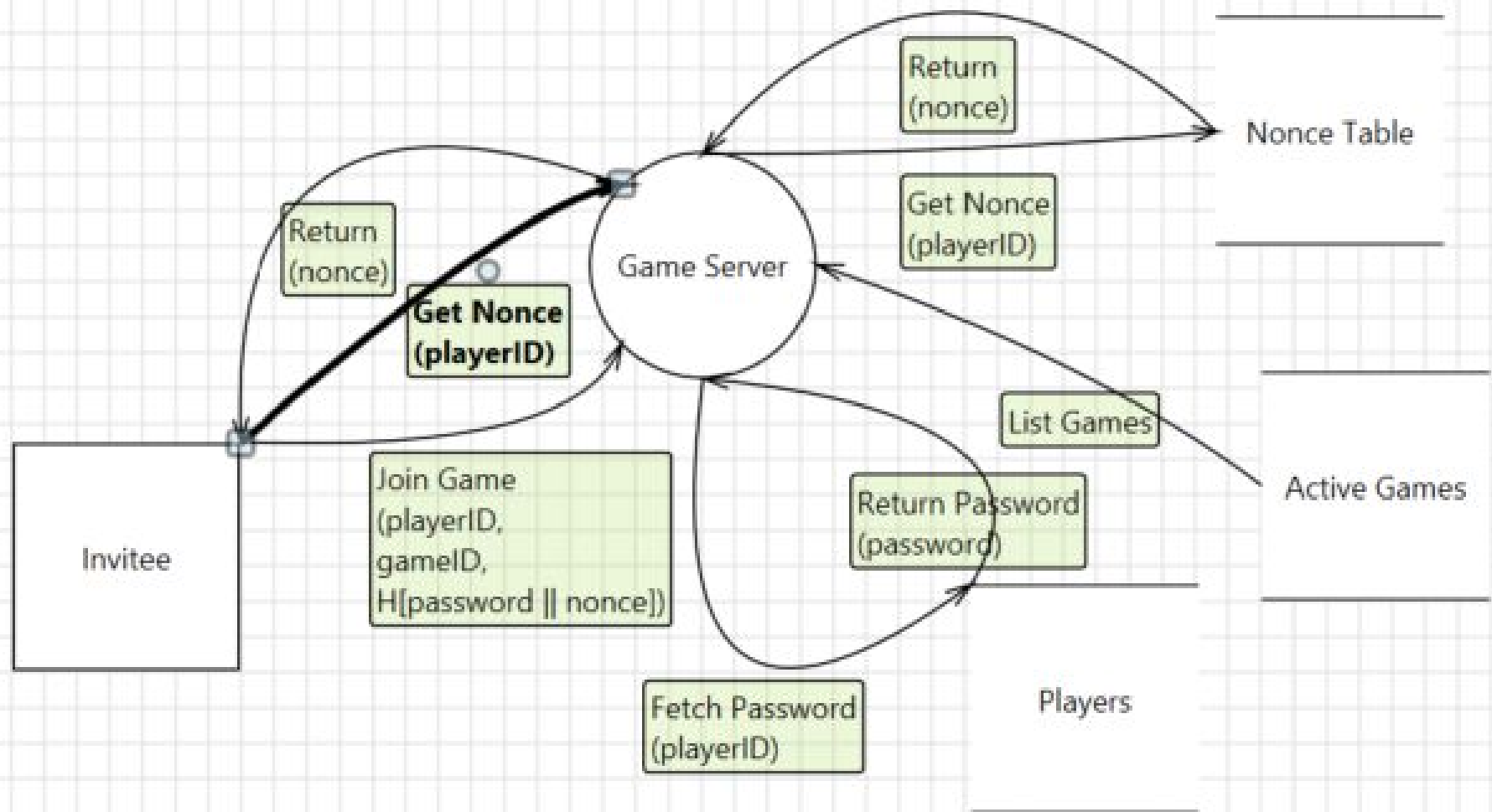


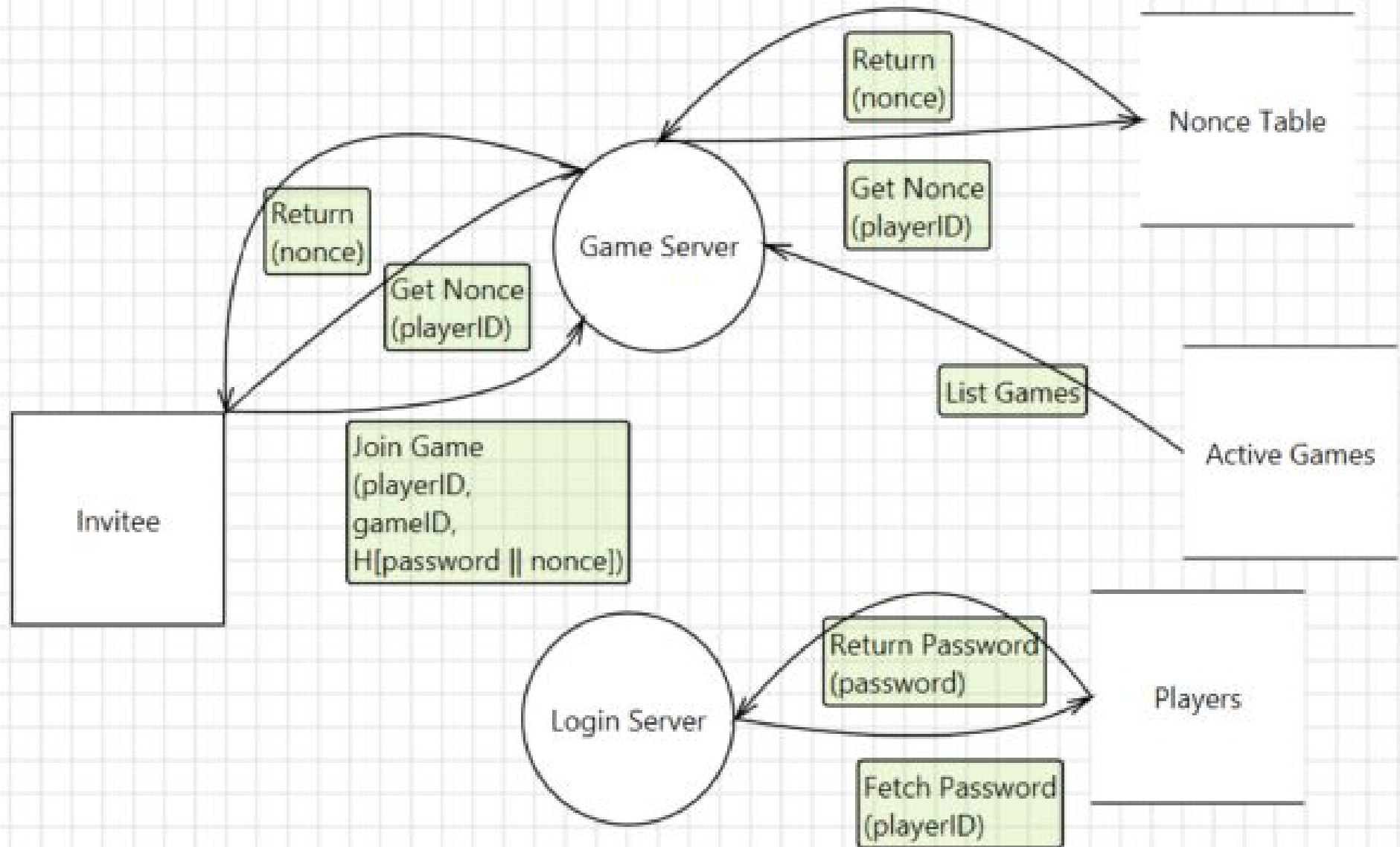


## *Nonce candidates...*

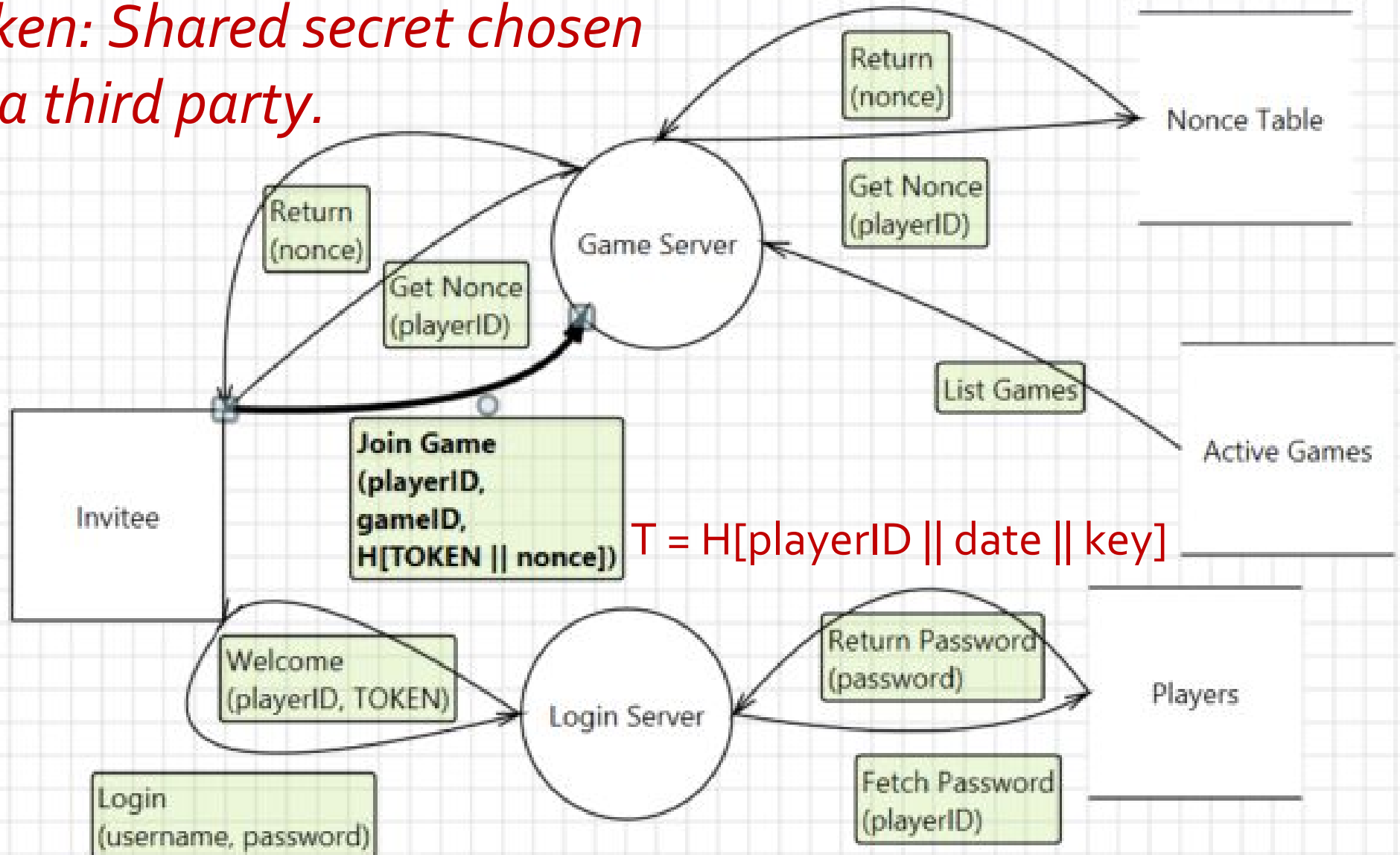
- Challenge value from server
- Time or date
- Sequence number

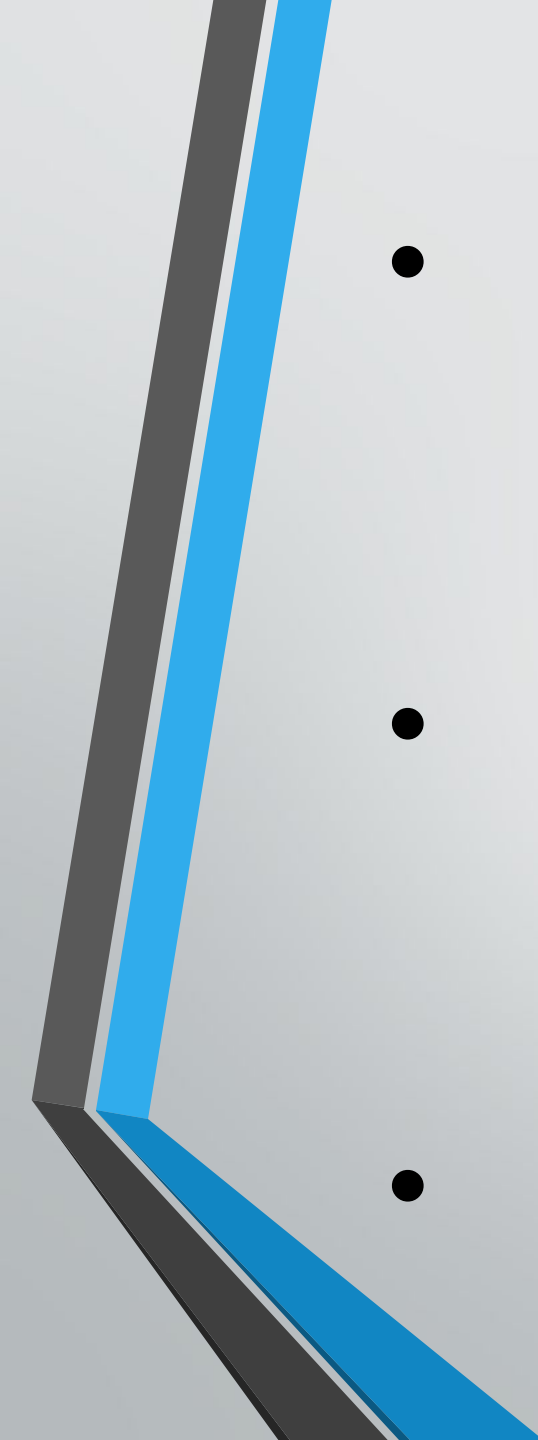






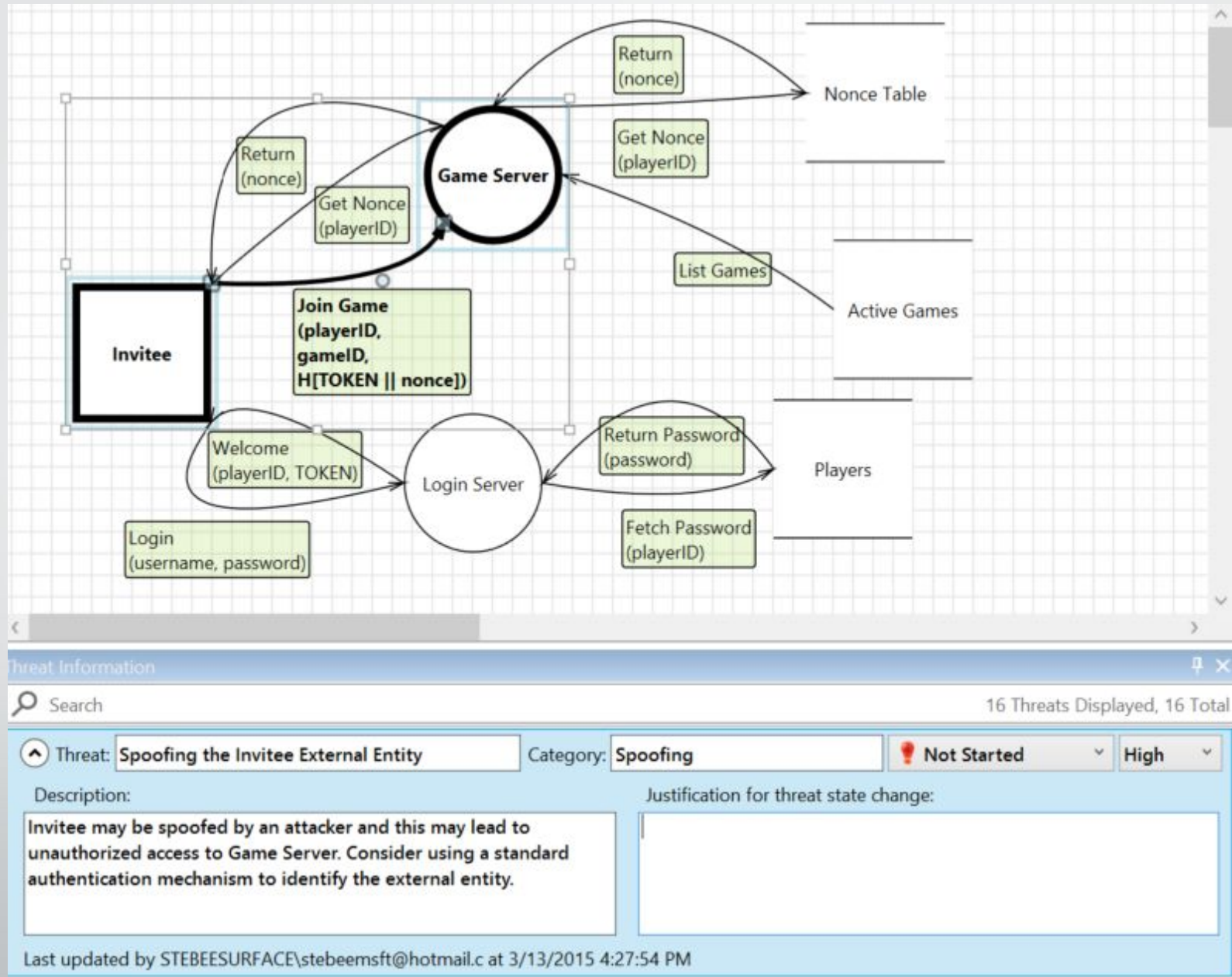
*Token: Shared secret chosen by a third party.*



- 
- No connection between Game Server and Player database/Login Server
  - Game Server requests contain no secret information and don't need SSL
  - Invitee is authenticated

▼ Threat:	Spoofing the Invitee External Entity	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	🚨 Not Started ▼	High ▼
▼ Threat:	Spoofing of Source Data Store Active Games	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Weak Access Control for a Resource	Category:	Information Disclosure	🚨 Not Started ▼	High ▼
▼ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	🚨 Not Started ▼	High ▼
▼ Threat:	Spoofing the Invitee External Entity	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Spoofing of Source Data Store Generic Data St	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Weak Access Control for a Resource	Category:	Information Disclosure	🚨 Not Started ▼	High ▼
▼ Threat:	Spoofing of Destination Data Store Generic Da	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Potential Excessive Resource Consumption for	Category:	Denial Of Service	🚨 Not Started ▼	High ▼
▼ Threat:	Spoofing the Invitee External Entity	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	🚨 Not Started ▼	High ▼
▼ Threat:	Spoofing of Destination Data Store Players	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Potential Excessive Resource Consumption for	Category:	Denial Of Service	🚨 Not Started ▼	High ▼
▼ Threat:	Spoofing of Source Data Store Players	Category:	Spoofing	🚨 Not Started ▼	High ▼
▼ Threat:	Weak Access Control for a Resource	Category:	Information Disclosure	🚨 Not Started ▼	High ▼





#### Threat Information

Search

16 Threats Displayed, 16 Total

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:


Last updated by STEBEESURFACE\stebeemsft@hotmail.c at 3/13/2015 4:27:54 PM



## Threat Information

 Search

16 Threats Displayed, 16 Total

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:

Hash of TOKEN proves possession of shared secret.

Last updated by STEBEESURFACE\stebeemsft@hotmail.c at 3/13/2015 4:29:57 PM

Threat: **Elevation Using Impersonation** Category: **Elevation Of Privilege**  **Not Started** **High**

Threat: **Spoofing of Source Data Store Active Games** Category: **Spoofing**  **Not Started** **High**

Threat: **Weak Access Control for a Resource** Category: **Information Disclosure**  **Not Started** **High**

Threat: **Elevation Using Impersonation** Category: **Elevation Of Privilege** N/A Not Applicable High

Description:

Game Server may be able to impersonate the context of Invitee in order to gain additional privilege.

Justification for threat state change:

Outside scope

Last updated by STEBEESURFACE\stebeemsft@hotmail.c at 3/13/2015 4:32:34 PM

Threat: <b>Spoofing of Source Data Store Active Games</b>	Category: <b>Spoofing</b>	Not Started	High
Threat: <b>Weak Access Control for a Resource</b>	Category: <b>Information Disclosure</b>	Not Started	High
Threat: <b>Elevation Using Impersonation</b>	Category: <b>Elevation Of Privilege</b>	N/A Not Applicable	High
Threat: <b>Spoofing the Invitee External Entity</b>	Category: <b>Spoofing</b>	Not Started	High
Threat: <b>Spoofing of Source Data Store Generic Data Store</b>	Category: <b>Spoofing</b>	Not Started	High
Threat: <b>Weak Access Control for a Resource</b>	Category: <b>Information Disclosure</b>	Not Started	High
Threat: <b>Spoofing of Destination Data Store Generic Data Store</b>	Category: <b>Spoofing</b>	Not Started	High
Threat: <b>Potential Excessive Resource Consumption for</b>	Category: <b>Denial Of Service</b>	Not Started	High
Threat: <b>Spoofing the Invitee External Entity</b>	Category: <b>Spoofing</b>	Not Started	High
Threat: <b>Elevation Using Impersonation</b>	Category: <b>Elevation Of Privilege</b>	N/A Not Applicable	High



⬆ Threat: **Spoofing of Source Data Store Generic Data Store** Category: **Spoofing** **N/A Not Applicable** **High**

Description:

Nonce Table may be spoofed by an attacker and this may lead to incorrect data delivered to Game Server. Consider using a standard authentication mechanism to identify the source data store.

Justification for threat state change:

Outside scope.

Last updated by STEBEESURFACE\stebeemsft@hotmail.c at 3/13/2015 4:37:16 PM

⬇ Threat: **Weak Access Control for a Resource** Category: **Information Disclosure** **⚠ Not Started** **High**

⬇ Threat: **Spoofing of Destination Data Store Generic Data Store** Category: **Spoofing** **N/A Not Applicable** **High**

⬇ Threat: **Potential Excessive Resource Consumption for** Category: **Denial Of Service** **⚠ Not Started** **High**

⬇ Threat: **Spoofing the Invitee External Entity** Category: **Spoofing** **⚠ Not Started** **High**

⬇ Threat: **Elevation Using Impersonation** Category: **Elevation Of Privilege** **N/A Not Applicable** **High**

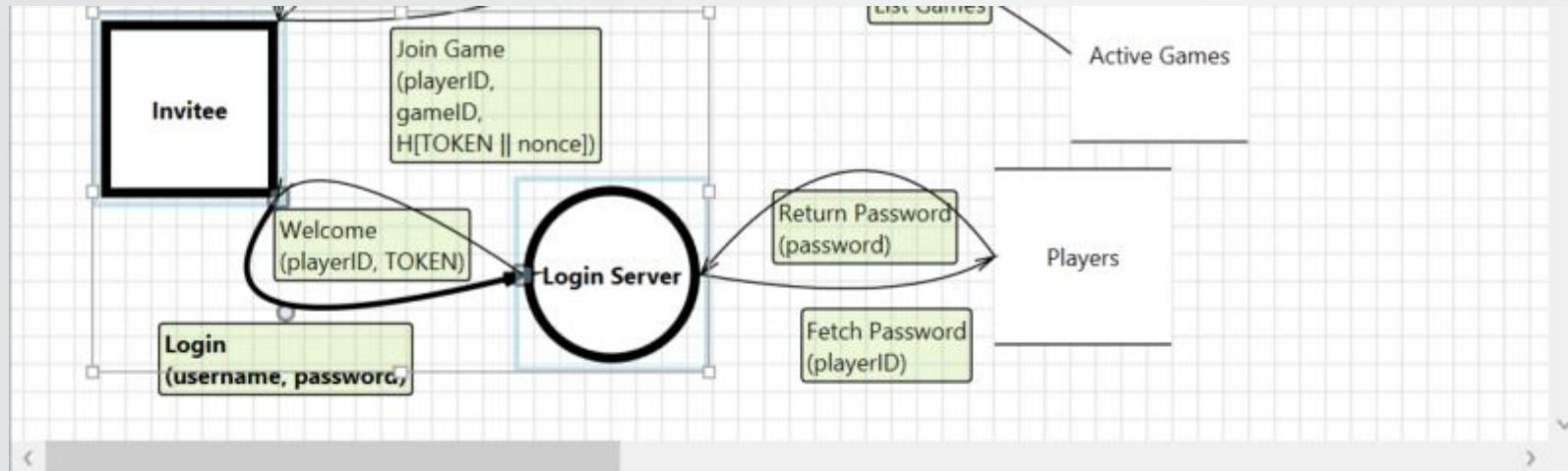
⬇ Threat: **Spoofing of Destination Data Store Players** Category: **Spoofing** **N/A Not Applicable** **High**

⬇ Threat: **Potential Excessive Resource Consumption for** Category: **Denial Of Service** **⚠ Not Started** **High**

⬇ Threat: **Spoofing of Source Data Store Players** Category: **Spoofing** **N/A Not Applicable** **High**

⬆ Threat:	Weak Access Control for a Resource	Category:	Information Disclosure	N/A Not Applicable	High
Description:		Justification for threat state change:			
Improper data protection of Active Games can allow an attacker to read information not intended for disclosure. Review authorization settings.		Outside scope.			
Last updated by STEBEESURFACE\stebeemsft@hotmail.c at 3/13/2015 4:39:41 PM					
⬇ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	N/A Not Applicable	High
⬇ Threat:	Spoofing the Invitee External Entity	Category:	Spoofing	💡 Not Started	High
⬇ Threat:	Spoofing of Source Data Store Generic Data St	Category:	Spoofing	N/A Not Applicable	High
⬇ Threat:	Weak Access Control for a Resource	Category:	Information Disclosure	N/A Not Applicable	High
⬇ Threat:	Spoofing of Destination Data Store Generic Da	Category:	Spoofing	N/A Not Applicable	High
⬇ Threat:	Potential Excessive Resource Consumption for	Category:	Denial Of Service	💡 Not Started	High
⬇ Threat:	Spoofing the Invitee External Entity	Category:	Spoofing	💡 Not Started	High
⬇ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	N/A Not Applicable	High
⬇ Threat:	Spoofing of Destination Data Store Players	Category:	Spoofing	N/A Not Applicable	High
⬇ Threat:	Potential Excessive Resource Consumption for	Category:	Denial Of Service	💡 Not Started	High
⬇ Threat:	Spoofing of Source Data Store Players	Category:	Spoofing	N/A Not Applicable	High
⬇ Threat:	Weak Access Control for a Resource	Category:	Information Disclosure	N/A Not Applicable	High





Threat Information

Search

16 Threats Displayed, 16 Total

▼ Threat:	Spoofing the Invitee External Entity	Category:	Spoofing	✔ Mitigated	High
▼ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	N/A Not Applicable	High
▼ Threat:	Spoofing of Source Data Store Active Games	Category:	Spoofing	N/A Not Applicable	High
▼ Threat:	Weak Access Control for a Resource	Category:	Information Disclosure	N/A Not Applicable	High
▼ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	N/A Not Applicable	High
▲ Threat:	Spoofing the Invitee External Entity	Category:	Spoofing	N/A Not Applicable	High

Description:

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

Justification for threat state change:

Possibility that attacker has stolen Invitee's password is outside our scope.

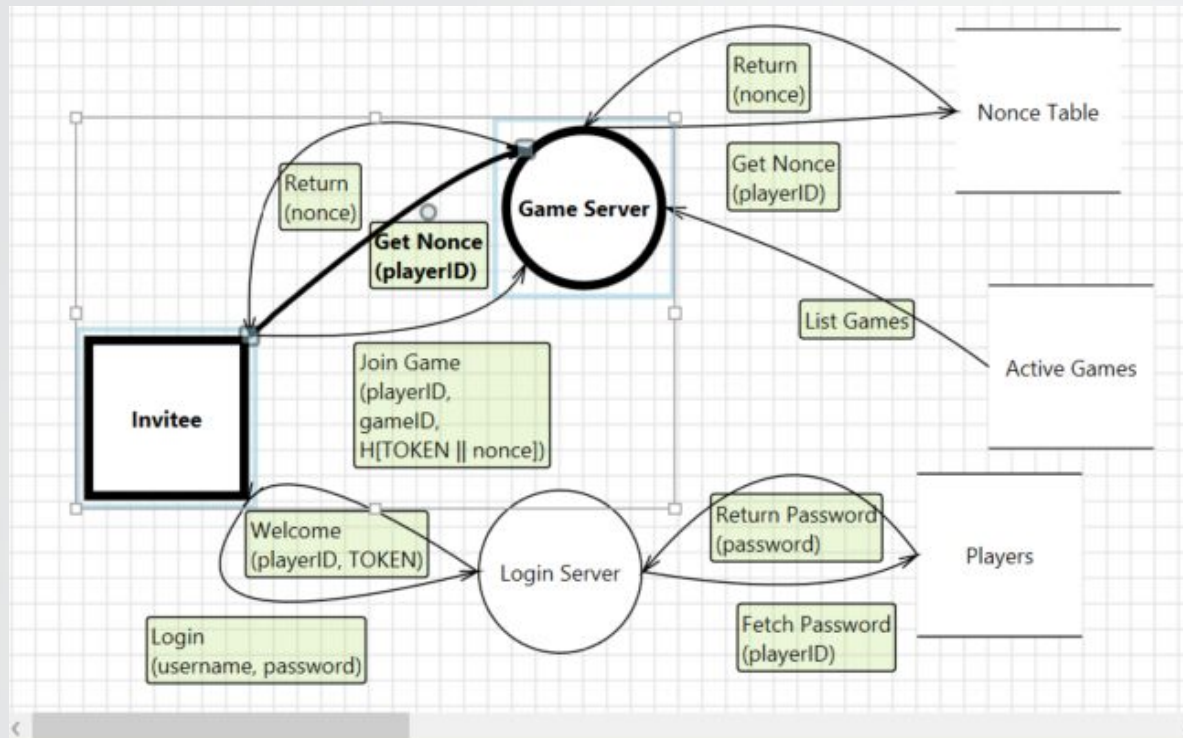
Last updated by STEBEESURFACE\stebeemsft@hotmail.c at 3/13/2015 4:41:54 PM

▼ Threat:	Potential Excessive Resource Consumption	Category:	Denial Of Service	🔍 Needs Investigation ▼	High ▼
▼ Threat:	Spoofing the Invitee Extension	Category:	Spoofing	🚫 Not Started ▼	High ▼
▼ Threat:	Elevation Using Impersonation	Category:	Elevation Of Privilege	N/A Not Applicable ▼	High ▼
▼ Threat:	Spoofing of Destination	Category:	Spoofing	N/A Not Applicable ▼	High ▼
⬆ Threat:	Potential Excessive Resource Consumption	Category:	Denial Of Service	🔍 Needs Investigation ▼	High ▼

Description:

Does Login Server or Players take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification for threat state change:



Threat Information

Search 16 Threats Displayed, 16 Total

Threat:	Weak Access Control	Category:	Information Disclosure	N/A Not Applicable	High
Threat:	Spoofing of Destination	Category:	Spoofing	N/A Not Applicable	High
Threat:	Potential Excessive Resource Consumption	Category:	Denial Of Service	Needs Investigation	High
Threat:	Spoofing the Invitee	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:



# Questions