

# Model Report

## Threat modeling report

Version 1.0 • Proposed



Date/Time  
Generated:  
Author:

5/11/2023 4:47:17 PM

{ReportAuthor}

EA Repository : C:\Users\bob\OneDrive\Documents\Sparx\Presentations\Threat modeling in EA for INCOSE  
Canada\Castle\_Threat\_model.qea

CREATED WITH  **ENTERPRISE  
ARCHITECT**

# Table of Contents

1.1	Dashboard diagram .....	4
<b>2</b>	<b>Context.....</b>	<b>5</b>
<b>3</b>	<b>Threat List Context .....</b>	<b>5</b>
3.1	THRT72 - Castle services May be Subject to Elevation of Privilege Using Remote Code Execution ( <i>Threat</i> ).....	5
3.2	THRT73 - Data Flow Generic Data Flow Is Potentially Interrupted ( <i>Threat</i> ).....	5
3.3	THRT79 - Data Flow join, leave castle Is Potentially Interrupted ( <i>Threat</i> ) .....	5
3.4	THRT75 - Data Flow Sniffing ( <i>Threat</i> ).....	6
3.5	THRT71 - Elevation by Changing the Execution Flow in Castle services ( <i>Threat</i> ).....	6
3.6	THRT66 - Elevation Using Impersonation ( <i>Threat</i> ).....	6
3.7	THRT69 - Elevation Using Impersonation ( <i>Threat</i> ).....	6
3.8	THRT80 - External Entity Remote castle Potentially Denies Receiving Data ( <i>Threat</i> ).....	6
3.9	THRT76 - Potential Data Repudiation by Castle services ( <i>Threat</i> ).....	7
3.10	THRT77 - Potential Lack of Input Validation for Castle services ( <i>Threat</i> ).....	7
3.11	THRT74 - Potential Process Crash or Stop for Castle services ( <i>Threat</i> ).....	7
3.12	THRT81 - Spoofing of the Remote castle External Destination Entity ( <i>Threat</i> ).....	7
3.13	THRT78 - Spoofing the Castle services Process ( <i>Threat</i> ).....	8
3.14	THRT67 - Spoofing the Local User External Entity ( <i>Threat</i> ) .....	8
3.15	THRT68 - Spoofing the Remote castle External Entity ( <i>Threat</i> ) .....	8
<b>4</b>	<b>Level 1.....</b>	<b>8</b>
<b>5</b>	<b>Threat List Level 1.....</b>	<b>10</b>
5.1	THRT40 - Castle service May be Subject to Elevation of Privilege Using Remote Code Execution ( <i>Threat</i> ) .....	10
5.2	THRT61 - Castle service Process Memory Tampered ( <i>Threat</i> ) .....	11
5.3	THRT48 - Data Flow Generic Data Flow Is Potentially Interrupted ( <i>Threat</i> ).....	11
5.4	THRT57 - Data Flow Generic Data Flow Is Potentially Interrupted ( <i>Threat</i> ).....	11
5.5	THRT30 - Data Flow Join, leave, Set users props Is Potentially Interrupted ( <i>Threat</i> ) .....	11
5.6	THRT39 - Data Flow Query users props Is Potentially Interrupted ( <i>Threat</i> ) .....	11
5.7	THRT28 - Data Flow Sniffing ( <i>Threat</i> ).....	12
5.8	THRT37 - Data Flow Sniffing ( <i>Threat</i> ).....	12
5.9	THRT46 - Data Flow Sniffing ( <i>Threat</i> ).....	12
5.10	THRT55 - Data Flow Sniffing ( <i>Threat</i> ).....	12
5.11	THRT41 - Elevation by Changing the Execution Flow in Castle service ( <i>Threat</i> ) .....	12
5.12	THRT59 - Elevation by Changing the Execution Flow in My castle SSDP ( <i>Threat</i> ).....	13
5.13	THRT32 - Elevation by Changing the Execution Flow in Remote Castle service ( <i>Threat</i> ) .....	13
5.14	THRT50 - Elevation by Changing the Execution Flow in Remote castle SSDP ( <i>Threat</i> ).....	13
5.15	THRT02 - Elevation Using Impersonation ( <i>Threat</i> ).....	13
5.16	THRT11 - Elevation Using Impersonation ( <i>Threat</i> ).....	13
5.17	THRT12 - Elevation Using Impersonation ( <i>Threat</i> ).....	14
5.18	THRT17 - Elevation Using Impersonation ( <i>Threat</i> ).....	14
5.19	THRT18 - Elevation Using Impersonation ( <i>Threat</i> ).....	14
5.20	THRT19 - Elevation Using Impersonation ( <i>Threat</i> ).....	14
5.21	THRT20 - Elevation Using Impersonation ( <i>Threat</i> ).....	14
5.22	THRT22 - Elevation Using Impersonation ( <i>Threat</i> ).....	14
5.23	THRT23 - Elevation Using Impersonation ( <i>Threat</i> ).....	15

5.24	THRT24 - Elevation Using Impersonation ( <i>Threat</i> ).....	15
5.25	THRT25 - Elevation Using Impersonation ( <i>Threat</i> ).....	15
5.26	THRT60 - Elevation Using Impersonation ( <i>Threat</i> ).....	15
5.27	THRT62 - Elevation Using Impersonation ( <i>Threat</i> ).....	15
5.28	THRT58 - My castle SSDP May be Subject to Elevation of Privilege Using Remote Code Execution ( <i>Threat</i> ).....	16
5.29	THRT36 - Potential Data Repudiation by Castle service ( <i>Threat</i> ) .....	16
5.30	THRT54 - Potential Data Repudiation by My castle SSDP ( <i>Threat</i> ) .....	16
5.31	THRT28 - Potential Data Repudiation by Remote Castle service ( <i>Threat</i> ).....	16
5.32	THRT45 - Potential Data Repudiation by Remote castle SSDP ( <i>Threat</i> ).....	16
5.33	THRT09 - Potential Excessive Resource Consumption for Castle service or LSA ( <i>Threat</i> ).....	17
5.34	THRT14 - Potential Excessive Resource Consumption for Castle service or Registry ( <i>Threat</i> )	17
5.35	THRT06 - Potential Excessive Resource Consumption for Shacct or SAM ( <i>Threat</i> ) .....	17
5.36	THRT35 - Potential Lack of Input Validation for Castle service ( <i>Threat</i> ) .....	17
5.37	THRT53 - Potential Lack of Input Validation for My castle SSDP ( <i>Threat</i> ) .....	17
5.38	THRT27 - Potential Lack of Input Validation for Remote Castle service ( <i>Threat</i> ).....	18
5.39	THRT44 - Potential Lack of Input Validation for Remote castle SSDP ( <i>Threat</i> ) .....	18
5.40	THRT38 - Potential Process Crash or Stop for Castle service ( <i>Threat</i> ).....	18
5.41	THRT56 - Potential Process Crash or Stop for My castle SSDP ( <i>Threat</i> ).....	18
5.42	THRT29 - Potential Process Crash or Stop for Remote Castle service ( <i>Threat</i> ) .....	19
5.43	THRT47 - Potential Process Crash or Stop for Remote castle SSDP ( <i>Threat</i> ).....	19
5.44	THRT31 - Remote Castle service May be Subject to Elevation of Privilege Using Remote Code Execution ( <i>Threat</i> ).....	19
5.45	THRT49 - Remote castle SSDP May be Subject to Elevation of Privilege Using Remote Code Execution ( <i>Threat</i> ).....	19
5.46	THRT10 - Spoofing of Destination Data Store LSA ( <i>Threat</i> ).....	19
5.47	THRT13 - Spoofing of Destination Data Store Registry ( <i>Threat</i> ).....	20
5.48	THRT05 - Spoofing of Destination Data Store SAM ( <i>Threat</i> ).....	20
5.49	THRT07 - Spoofing of Source Data Store LSA ( <i>Threat</i> ).....	20
5.50	THRT15 - Spoofing of Source Data Store Registry ( <i>Threat</i> ) .....	20
5.51	THRT04 - Spoofing of Source Data Store SAM ( <i>Threat</i> ).....	20
5.52	THRT25 - Spoofing the Castle service Process ( <i>Threat</i> ).....	21
5.53	THRT34 - Spoofing the Castle service Process ( <i>Threat</i> ).....	21
5.54	THRT01 - Spoofing the Local User External Entity ( <i>Threat</i> ) .....	21
5.55	THRT42 - Spoofing the My castle SSDP Process ( <i>Threat</i> ).....	21
5.56	THRT52 - Spoofing the My castle SSDP Process ( <i>Threat</i> ).....	21
5.57	THRT26 - Spoofing the Remote Castle service Process ( <i>Threat</i> ) .....	21
5.58	THRT33 - Spoofing the Remote Castle service Process ( <i>Threat</i> ) .....	22
5.59	THRT43 - Spoofing the Remote castle SSDP Process ( <i>Threat</i> ).....	22
5.60	THRT51 - Spoofing the Remote castle SSDP Process ( <i>Threat</i> ).....	22
5.61	THRT03 - Weak Access Control for a Resource ( <i>Threat</i> ).....	22
5.62	THRT08 - Weak Access Control for a Resource ( <i>Threat</i> ).....	22
5.63	THRT16 - Weak Access Control for a Resource ( <i>Threat</i> ).....	22

# 1.1 Dashboard diagram

Dashboard diagram in package 'Dashboard'

Dashboard  
Version 1.0  
Bob Hruska created on 2/24/2020. Last modified 2/24/2020

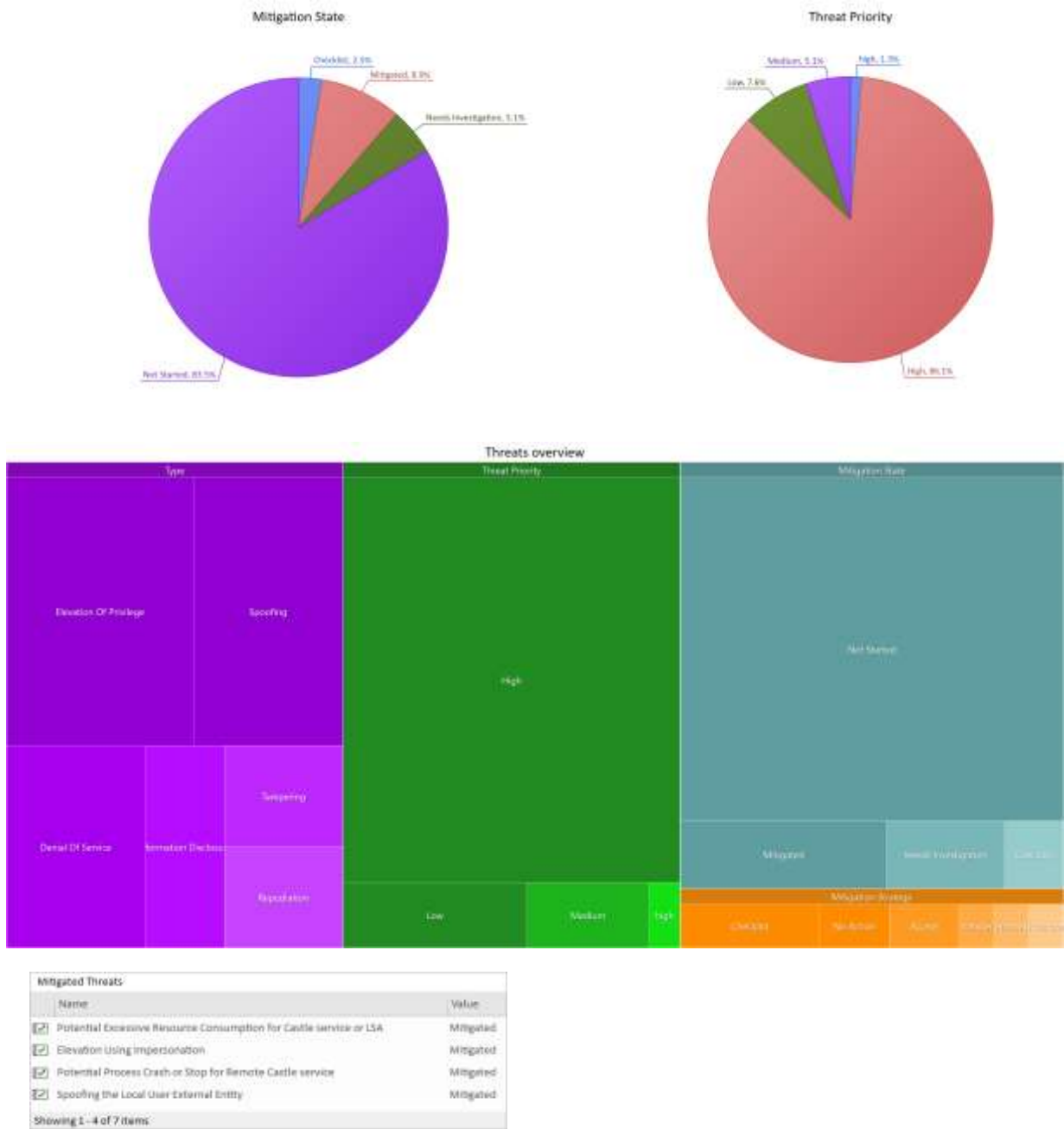


Figure 1: Dashboard

## 2 Context

Very high-level; entire component / product / system

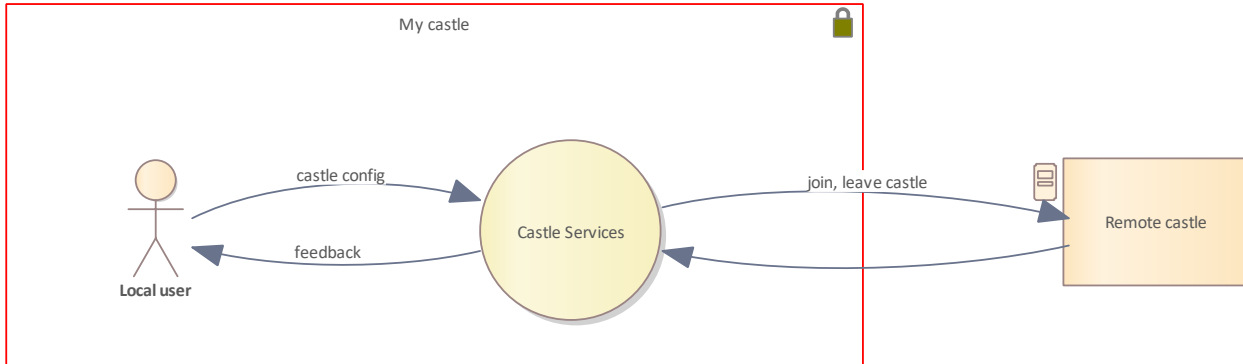


Figure 1: Diagram "Context"

Name	Description
Castle Services	Services provided by my castle to the others.
Local user	Is one whose username and encrypted password are stored on the computer itself. When you log in as a local user, the computer checks its own list of users and its own password file to see if you are allowed to log into the computer.
Remote castle	The other castle
My castle	

Table 1: List of diagram elements of Context diagram

## 3 Threat List Context

### 3.1 THRT72 - Castle services May be Subject to Elevation of Privilege Using Remote Code Execution (Threat)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Needs Investigation

Remote castle may be able to remotely execute code for Castle services.

- > Threatens Castle Services (Process)
- > Threatens (Association)
- > Threatens Remote castle (External System)

### 3.2 THRT73 - Data Flow Generic Data Flow Is Potentially Interrupted (Threat)

- ◆ **Type:** Denial Of Service
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Checklist

An external agent interrupts data flowing across a trust boundary in either direction.

- > Threatens Castle Services (Process)
- > Threatens Remote castle (External System)
- > Threatens Denial of Service (Mitigation Checklist)
- > Threatens (Association)

### 3.3 THRT79 - Data Flow join, leave castle Is Potentially Interrupted (Threat)

- ◆ **Type:** Denial Of Service
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started

*An external agent interrupts data flowing across a trust boundary in either direction.*

- > Threatens Remote castle (External System)
- > Threatens join, leave castle (Association)
- > Threatens Castle Services (Process)

### 3.4 THRT75 - Data Flow Sniffing (Threat)

- ◆ **Type:** Information Disclosure
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started
- ◆ **Mitigation Strategy:** Accept

*Data flowing across Generic Data Flow may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.*

- > Threatens (Association)
- > Threatens Remote castle (External System)
- > Threatens Castle Services (Process)

### 3.5 THRT71 - Elevation by Changing the Execution Flow in Castle services (Threat)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started

*An attacker may pass data into Castle services in order to change the flow of program execution within Castle services to the attacker's choosing.*

- > Threatens Castle Services (Process)
- > Threatens Remote castle (External System)
- > Threatens (Association)

### 3.6 THRT66 - Elevation Using Impersonation (Threat)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started

*Castle services may be able to impersonate the context of Local User in order to gain additional privilege.*

- > Threatens castle config (Association)
- > Threatens Local user (Human Actor)
- > Threatens Castle Services (Process)

### 3.7 THRT69 - Elevation Using Impersonation (Threat)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started

*Castle services may be able to impersonate the context of Remote castle in order to gain additional privilege.*

- > Threatens Castle Services (Process)
- > Threatens Remote castle (External System)
- > Threatens (Association)

### 3.8 THRT80 - External Entity Remote castle Potentially Denies Receiving Data (Threat)

- Type: Repudiation
- Threat Priority: High
- Mitigation State: Mitigated
- Mitigation Strategy: Checklist

Remote castle claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

- Threatens Remote castle (External System)
- Threatens Repudiation (Mitigation Checklist)
- Threatens join, leave castle (Association)
- Threatens Castle Services (Process)

### 3.9 THRT76 - Potential Data Repudiation by Castle services (Threat)

- Type: Repudiation
- Threat Priority: High
- Mitigation State: Not Started

Castle services claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

- Threatens (Association)
- Threatens Castle Services (Process)
- Threatens Remote castle (External System)

### 3.10 THRT77 - Potential Lack of Input Validation for Castle services (Threat)

- Type: Tampering
- Threat Priority: High
- Mitigation State: Not Started

Data flowing across Generic Data Flow may be tampered with by an attacker. This may lead to a denial of service attack against Castle services or an elevation of privilege attack against Castle services or an information disclosure by Castle services. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

- Threatens Remote castle (External System)
- Threatens Castle Services (Process)
- Threatens (Association)

### 3.11 THRT74 - Potential Process Crash or Stop for Castle services (Threat)

- Type: Denial Of Service
- Threat Priority: High
- Mitigation State: Not Started

Castle services crashes, halts, stops or runs slowly; in all cases violating an availability metric.

- Threatens (Association)
- Threatens Remote castle (External System)
- Threatens Castle Services (Process)

### 3.12 THRT81 - Spoofing of the Remote castle External Destination Entity (Threat)

- Type: Spoofing
- Threat Priority: High

🔑 **Mitigation State:** Needs Investigation

*Remote castle may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Remote castle. Consider using a standard authentication mechanism to identify the external entity.*

- > Threatens join, leave castle (*Association*)
- > Threatens Castle Services (*Process*)
- > Threatens Remote castle (*External System*)

### 3.13 THRT78 - Spoofing the Castle services Process (*Threat*)

- 🔑 **Type:** Spoofing
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Mitigated
- 🔑 **Mitigation Strategy:** Transfer

*Castle services may be spoofed by an attacker and this may lead to information disclosure by Remote castle. Consider using a standard authentication mechanism to identify the destination process.*

- > Threatens Castle Services (*Process*)
- > Threatens (*Association*)
- > Threatens Remote castle (*External System*)

### 3.14 THRT67 - Spoofing the Local User External Entity (*Threat*)

- 🔑 **Type:** Spoofing
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Mitigated
- 🔑 **Mitigation Strategy:** Accept

*Local User may be spoofed by an attacker and this may lead to unauthorized access to Castle services. Consider using a standard authentication mechanism to identify the external entity.*

- > Threatens castle config (*Association*)
- > Threatens Castle Services (*Process*)
- > Threatens Local user (*Human Actor*)

### 3.15 THRT68 - Spoofing the Remote castle External Entity (*Threat*)

- 🔑 **Type:** Spoofing
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Mitigated
- 🔑 **Mitigation Strategy:** No Action

*Remote castle may be spoofed by an attacker and this may lead to unauthorized access to Castle services. Consider using a standard authentication mechanism to identify the external entity.*

- > Threatens Remote castle (*External System*)
- > Threatens Castle Services (*Process*)
- > Threatens (*Association*)

## 4 Level 1

*High level; single feature / scenario*



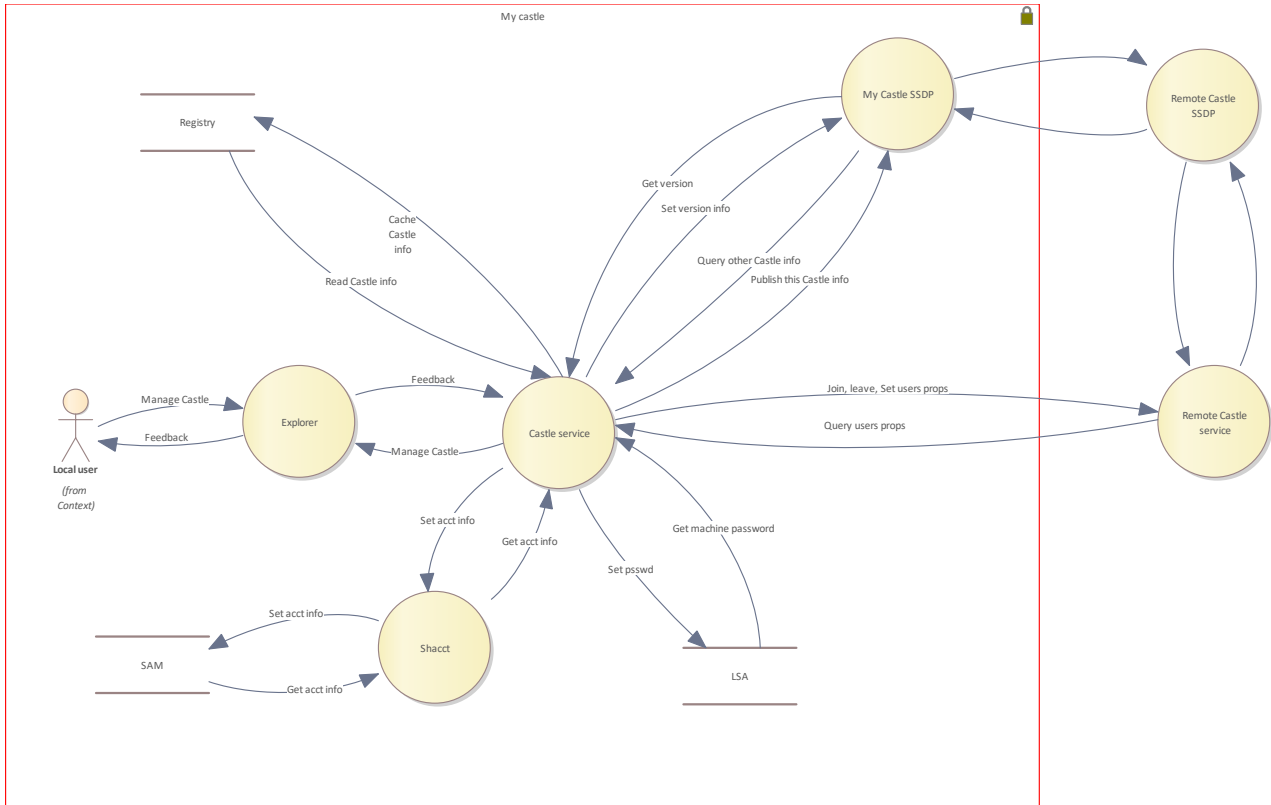


Figure 2: Diagram "Level 1"

Name	Description
Local user	Is one whose username and encrypted password are stored on the computer itself. When you log in as a local user, the computer checks its own list of users and its own password file to see if you are allowed to log into the computer.
My castle	
Castle service	My castle service
Explorer	Windows Program Manager or Windows Explorer. It manages the Windows Graphical Shell including the Start menu, taskbar, desktop, and File Manager.
My Castle SSDP	SSDP Discovery access and hosts messages for the SSDP Discovery Tool, which is part of Microsoft Windows operating systems. It listens for and discovers devices on a network that utilize SSDP discovery protocol.
Remote Castle service	The external service
Remote Castle SSDP	SSDP Discovery access and hosts messages for the SSDP Discovery Tool, which is part of Microsoft Windows operating systems. It listens for and discovers devices on a network that utilize SSDP discovery protocol.
Shacct	shacct.dll is a module belonging to Microsoft® Windows® Operating System from Microsoft Corporation.
LSA	The LSA stores local security policy information in a set of objects. Your application can query or edit the local security policy by accessing these objects.
Registry	The Windows Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry. The kernel, device drivers, services, Security Accounts Manager, and user interface can all use the registry. The registry also allows access to counters for profiling system performance.
SAM	The Security Account Manager (SAM) is a database file in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users.

Table 2: List of diagram elements of Level 1 diagram

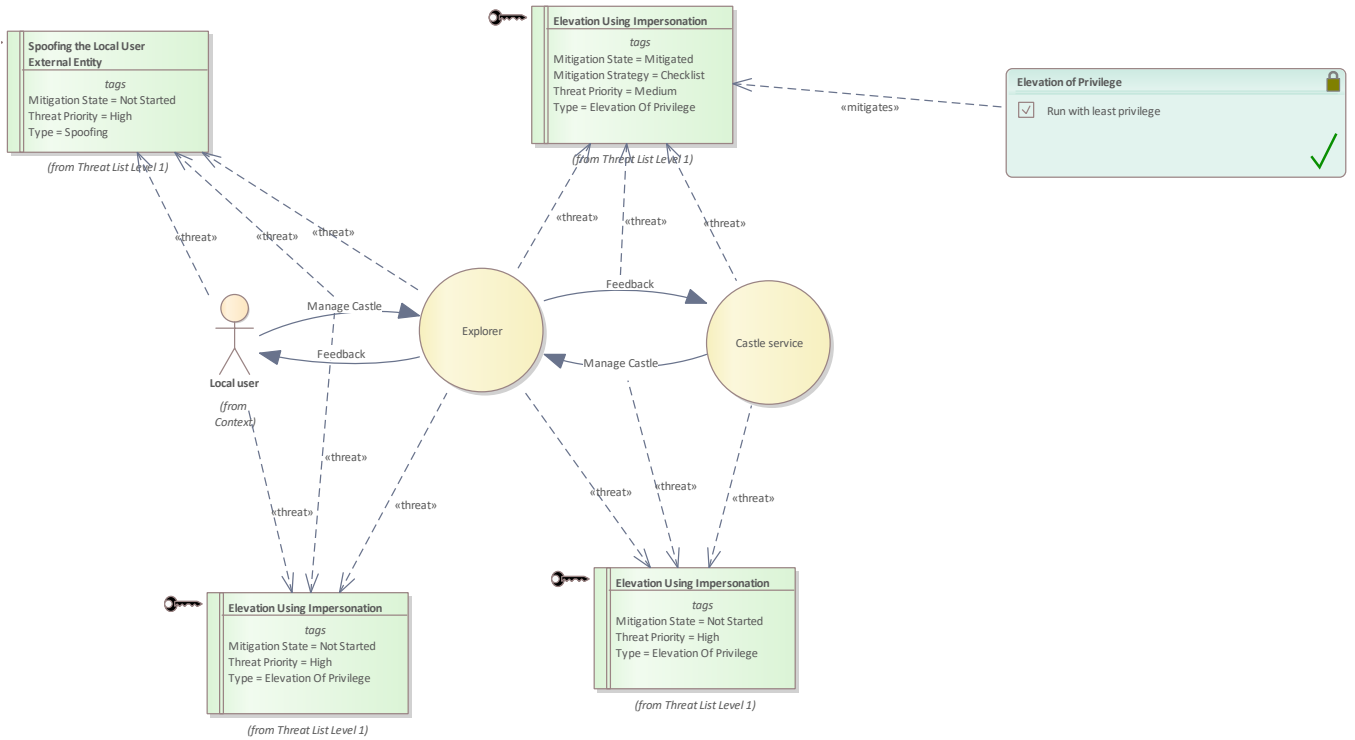


Figure 3: Diagram "Manage castle"

Name	Description
Local user	Is one whose username and encrypted password are stored on the computer itself. When you log in as a local user, the computer checks its own list of users and its own password file to see if you are allowed to log into the computer.
Castle service	My castle service
Explorer	Windows Program Manager or Windows Explorer. It manages the Windows Graphical Shell including the Start menu, taskbar, desktop, and File Manager.
Elevation of Privilege	
Manage Castle	
Manage Castle	
Manage Castle	
Feedback	
Elevation Using Impersonation	Explorer may be able to impersonate the context of Local User in order to gain additional privilege.
Elevation Using Impersonation	Explorer may be able to impersonate the context of Castle service in order to gain additional privilege.
Elevation Using Impersonation	Castle service may be able to impersonate the context of Explorer in order to gain additional privilege.
Spoofing the Local User External Entity	Local User may be spoofed by an attacker and this may lead to unauthorized access to Explorer. Consider using a standard authentication mechanism to identify the external entity.

Table 3: List of diagram elements of Manage castle diagram

## 5 Threat List Level 1

### 5.1 THRT40 - Castle service May be Subject to Elevation of Privilege Using Remote Code Execution (Threat)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Needs Investigation

*Remote Castle service may be able to remotely execute code for Castle service.*

- > Threatens Castle service (Process)
- > Threatens Remote Castle service (Process)
- > Threatens Query users props (Association)




## 5.2 THRT61 - Castle service Process Memory Tampered (Threat)

-  **Type:** Tampering
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*If Castle service is given access to memory, such as shared memory or pointers, or is given the ability to control what Shacct executes (for example, passing back a function pointer.), then Castle service can tamper with Shacct. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.*

- > Threatens Shacct (Process)
- > Threatens Castle service (Process)
- > Threatens Set acct info (Association)

## 5.3 THRT48 - Data Flow Generic Data Flow Is Potentially Interrupted (Threat)

-  **Type:** Denial Of Service
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*An external agent interrupts data flowing across a trust boundary in either direction.*

- > Threatens (Association)
- > Threatens My Castle SSDP (Process)
- > Threatens Remote Castle SSDP (Process)

## 5.4 THRT57 - Data Flow Generic Data Flow Is Potentially Interrupted (Threat)

-  **Type:** Denial Of Service
-  **Threat Priority:** Low
-  **Mitigation State:** Not Started

*An external agent interrupts data flowing across a trust boundary in either direction.*

- > Threatens Remote Castle SSDP (Process)
- > Threatens (Association)
- > Threatens My Castle SSDP (Process)




## 5.5 THRT30 - Data Flow Join, leave, Set users props Is Potentially Interrupted (Threat)

-  **Type:** Denial Of Service
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*An external agent interrupts data flowing across a trust boundary in either direction.*

- > Threatens Join, leave, Set users props (Association)
- > Threatens Castle service (Process)
- > Threatens Remote Castle service (Process)




## 5.6 THRT39 - Data Flow Query users props Is Potentially Interrupted (Threat)

-  **Type:** Denial Of Service
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*An external agent interrupts data flowing across a trust boundary in either direction.*

- > Threatens Castle service (Process)
- > Threatens Query users props (Association)
- > Threatens Remote Castle service (Process)




## 5.7 THRT28 - Data Flow Sniffing (Threat)

-  **Type:** Information Disclosure
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*Data flowing across Join, leave, Set users props may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.*

- > Threatens Join, leave, Set users props (Association)
- > Threatens Remote Castle service (Process)
- > Threatens Castle service (Process)




## 5.8 THRT37 - Data Flow Sniffing (Threat)

-  **Type:** Information Disclosure
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*Data flowing across Query users props may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.*

- > Threatens Castle service (Process)
- > Threatens Remote Castle service (Process)
- > Threatens Query users props (Association)




## 5.9 THRT46 - Data Flow Sniffing (Threat)

-  **Type:** Information Disclosure
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*Data flowing across Generic Data Flow may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.*

- > Threatens Remote Castle SSDP (Process)
- > Threatens My Castle SSDP (Process)
- > Threatens (Association)




## 5.10 THRT55 - Data Flow Sniffing (Threat)

-  **Type:** Information Disclosure
-  **Threat Priority:** Medium
-  **Mitigation State:** Not Started

*Data flowing across Generic Data Flow may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.*

- > Threatens (Association)
- > Threatens My Castle SSDP (Process)
- > Threatens Remote Castle SSDP (Process)




## 5.11 THRT41 - Elevation by Changing the Execution Flow in Castle service (Threat)

-  **Type:** Elevation Of Privilege
-  **Threat Priority:** Low
-  **Mitigation State:** Not Started

*An attacker may pass data into Castle service in order to change the flow of program execution within Castle service to the attacker's choosing.*

- > Threatens Query users props (Association)
- > Threatens Remote Castle service (Process)
- > Threatens Castle service (Process)




## 5.12 THRT59 - Elevation by Changing the Execution Flow in My castle SSDP (Threat)

-  **Type:** Elevation Of Privilege
-  **Threat Priority:** Low
-  **Mitigation State:** Checklist

*An attacker may pass data into My castle SSDP in order to change the flow of program execution within My castle SSDP to the attacker's choosing.*

- > Threatens Remote Castle SSDP (Process)
- > Threatens (Association)
- > Threatens My Castle SSDP (Process)




## 5.13 THRT32 - Elevation by Changing the Execution Flow in Remote Castle service (Threat)

-  **Type:** Elevation Of Privilege
-  **Threat Priority:** Low
-  **Mitigation State:** Not Started

*An attacker may pass data into Remote Castle service in order to change the flow of program execution within Remote Castle service to the attacker's choosing.*

- > Threatens Join, leave, Set users props (Association)
- > Threatens Castle service (Process)
- > Threatens Remote Castle service (Process)




## 5.14 THRT50 - Elevation by Changing the Execution Flow in Remote castle SSDP (Threat)

-  **Type:** Elevation Of Privilege
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*An attacker may pass data into Remote castle SSDP in order to change the flow of program execution within Remote castle SSDP to the attacker's choosing.*

- > Threatens Remote Castle SSDP (Process)
- > Threatens (Association)
- > Threatens My Castle SSDP (Process)



## 5.15 THRT02 - Elevation Using Impersonation (Threat)

-  **Type:** Elevation Of Privilege
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*Explorer may be able to impersonate the context of Local User in order to gain additional privilege.*

- > Threatens Explorer (Process)
- > Threatens Manage Castle (Association)
- > Threatens Local user (Human Actor)

## 5.16 THRT11 - Elevation Using Impersonation (Threat)

-  **Type:** Elevation Of Privilege
-  **Threat Priority:** High
-  **Mitigation State:** Not Started

*Explorer may be able to impersonate the context of Castle service in order to gain additional privilege.*

- > Threatens Castle service (Process)
- > Threatens Manage Castle (Association)
- > Threatens Explorer (Process)

## 5.17 THRT12 - Elevation Using Impersonation (*Threat*)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** Medium
- ◆ **Mitigation State:** Mitigated
- ◆ **Mitigation Strategy:** Checklist

*Castle service may be able to impersonate the context of Explorer in order to gain additional privilege.*

- > Threatens Elevation of Privilege (*Mitigation Checklist*)
- > Threatens Explorer (*Process*)
- > Threatens Castle service (*Process*)
- > Threatens Feedback (*Association*)

## 5.18 THRT17 - Elevation Using Impersonation (*Threat*)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started

*My castle SSDP may be able to impersonate the context of Castle service in order to gain additional privilege.*

- > Threatens My Castle SSDP (*Process*)
- > Threatens Castle service (*Process*)
- > Threatens Publish this Castle info (*Association*)

## 5.19 THRT18 - Elevation Using Impersonation (*Threat*)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started

*My castle SSDP may be able to impersonate the context of Castle service in order to gain additional privilege.*

- > Threatens Set version info (*Association*)
- > Threatens Castle service (*Process*)
- > Threatens My Castle SSDP (*Process*)

## 5.20 THRT19 - Elevation Using Impersonation (*Threat*)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** Low
- ◆ **Mitigation State:** Not Started

*Castle service may be able to impersonate the context of My castle SSDP in order to gain additional privilege.*

- > Threatens Castle service (*Process*)
- > Threatens My Castle SSDP (*Process*)
- > Threatens Query other Castle info (*Association*)

## 5.21 THRT20 - Elevation Using Impersonation (*Threat*)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started

*Castle service may be able to impersonate the context of My castle SSDP in order to gain additional privilege.*

- > Threatens My Castle SSDP (*Process*)
- > Threatens Set version info (*Association*)
- > Threatens Castle service (*Process*)

## 5.22 THRT22 - Elevation Using Impersonation (*Threat*)

- ◆ **Type:** Elevation Of Privilege
- ◆ **Threat Priority:** High
- ◆ **Mitigation State:** Not Started



*Remote Castle service may be able to impersonate the context of Castle service in order to gain additional privilege.*

- > Threatens Castle service (Process)
- > Threatens Join, leave, Set users props (Association)
- > Threatens Remote Castle service (Process)

## 5.23 THRT23 - Elevation Using Impersonation (Threat)

- 🔑 **Type:** Elevation Of Privilege
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

*Castle service may be able to impersonate the context of Remote Castle service in order to gain additional privilege.*

- > Threatens Castle service (Process)
- > Threatens Remote Castle service (Process)
- > Threatens Query users props (Association)

## 5.24 THRT24 - Elevation Using Impersonation (Threat)

- 🔑 **Type:** Elevation Of Privilege
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

*Remote castle SSDP may be able to impersonate the context of My castle SSDP in order to gain additional privilege.*

- > Threatens Remote Castle SSDP (Process)
- > Threatens My Castle SSDP (Process)
- > Threatens (Association)

## 5.25 THRT25 - Elevation Using Impersonation (Threat)

- 🔑 **Type:** Elevation Of Privilege
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

*My castle SSDP may be able to impersonate the context of Remote castle SSDP in order to gain additional privilege.*

- > Threatens My Castle SSDP (Process)
- > Threatens Remote Castle SSDP (Process)
- > Threatens (Association)

## 5.26 THRT60 - Elevation Using Impersonation (Threat)

- 🔑 **Type:** Elevation Of Privilege
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started
- 🔑 **Mitigation Strategy:** Publicise

*Shacct may be able to impersonate the context of Castle service in order to gain additional privilege.*

- > Threatens Shacct (Process)
- > Threatens Castle service (Process)
- > Threatens Set acct info (Association)

## 5.27 THRT62 - Elevation Using Impersonation (Threat)

- 🔑 **Type:** Elevation Of Privilege
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

*Castle service may be able to impersonate the context of Shacct in order to gain additional privilege.*

- > Threatens Get acct info (Association)
- > Threatens Shacct (Process)
- > Threatens Castle service (Process)

## 5.28 THRT58 - My castle SSDP May be Subject to Elevation of Privilege Using Remote Code Execution (*Threat*)

- 🔗 **Type:** Elevation Of Privilege
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*Remote castle SSDP may be able to remotely execute code for My castle SSDP.*

- > Threatens (*Association*)
- > Threatens My Castle SSDP (*Process*)
- > Threatens Remote Castle SSDP (*Process*)

## 5.29 THRT36 - Potential Data Repudiation by Castle service (*Threat*)

- 🔗 **Type:** Repudiation
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*Castle service claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.*

- > Threatens Remote Castle service (*Process*)
- > Threatens Query users props (*Association*)
- > Threatens Castle service (*Process*)

## 5.30 THRT54 - Potential Data Repudiation by My castle SSDP (*Threat*)

- 🔗 **Type:** Repudiation
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*My castle SSDP claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.*

- > Threatens Remote Castle SSDP (*Process*)
- > Threatens (*Association*)
- > Threatens My Castle SSDP (*Process*)

## 5.31 THRT28 - Potential Data Repudiation by Remote Castle service (*Threat*)

- 🔗 **Type:** Repudiation
- 🔗 **Threat Priority:** Low
- 🔗 **Mitigation State:** Not Started

*Remote Castle service claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.*

- > Threatens Castle service (*Process*)
- > Threatens Remote Castle service (*Process*)
- > Threatens Join, leave, Set users props (*Association*)

## 5.32 THRT45 - Potential Data Repudiation by Remote castle SSDP (*Threat*)

- 🔗 **Type:** Repudiation
- 🔗 **Threat Priority:** Medium
- 🔗 **Mitigation State:** Not Started

*Remote castle SSDP claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.*

- > Threatens Remote Castle SSDP (*Process*)
- > Threatens (*Association*)
- > Threatens My Castle SSDP (*Process*)



## 5.33 THRT09 - Potential Excessive Resource Consumption for Castle service or LSA (Threat)

- 🔗 **Type:** Denial Of Service
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Mitigated

*Does Castle service or LSA 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.*

- > Threatens LSA (Data Store)
- > Threatens Castle service (Process)
- > Threatens Set psswd (Association)

## 5.34 THRT14 - Potential Excessive Resource Consumption for Castle service or Registry (Threat)

- 🔗 **Type:** Denial Of Service
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started
- 🔗 **Mitigation Strategy:** Terminate

*Does Castle service or Registry 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.*

- > Threatens Registry (Data Store)
- > Threatens Cache Castle info (Association)
- > Threatens Castle service (Process)

## 5.35 THRT06 - Potential Excessive Resource Consumption for Shacct or SAM (Threat)

- 🔗 **Type:** Denial Of Service
- 🔗 **Threat Priority:** Medium
- 🔗 **Mitigation State:** Not Started

*Does Shacct or SAM 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.*

- > Threatens Shacct (Process)
- > Threatens Set acct info (Association)
- > Threatens SAM (Data Store)

## 5.36 THRT35 - Potential Lack of Input Validation for Castle service (Threat)

- 🔗 **Type:** Tampering
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*Data flowing across Query users props may be tampered with by an attacker. This may lead to a denial of service attack against Castle service or an elevation of privilege attack against Castle service or an information disclosure by Castle service. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.*

- > Threatens Remote Castle service (Process)
- > Threatens Query users props (Association)
- > Threatens Castle service (Process)

## 5.37 THRT53 - Potential Lack of Input Validation for My castle SSDP (Threat)

- 🔗 **Type:** Tampering
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

Data flowing across Generic Data Flow may be tampered with by an attacker. This may lead to a denial of service attack against My castle SSDP or an elevation of privilege attack against My castle SSDP or an information disclosure by My castle SSDP. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

- > Threatens My Castle SSDP (Process)
- > Threatens (Association)
- > Threatens Remote Castle SSDP (Process)

## 5.38 THRT27 - Potential Lack of Input Validation for Remote Castle service (Threat)

- 🔗 **Type:** Tampering
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

Data flowing across Join, leave, Set users props may be tampered with by an attacker. This may lead to a denial of service attack against Remote Castle service or an elevation of privilege attack against Remote Castle service or an information disclosure by Remote Castle service. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

- > Threatens Remote Castle service (Process)
- > Threatens Join, leave, Set users props (Association)
- > Threatens Castle service (Process)

## 5.39 THRT44 - Potential Lack of Input Validation for Remote castle SSDP (Threat)

- 🔗 **Type:** Tampering
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started
- 🔗 **Mitigation Strategy:** Checklist

Data flowing across Generic Data Flow may be tampered with by an attacker. This may lead to a denial of service attack against Remote castle SSDP or an elevation of privilege attack against Remote castle SSDP or an information disclosure by Remote castle SSDP. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

- > Threatens Remote Castle SSDP (Process)
- > Threatens My Castle SSDP (Process)
- > Threatens (Association)

## 5.40 THRT38 - Potential Process Crash or Stop for Castle service (Threat)

- 🔗 **Type:** Denial Of Service
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

Castle service crashes, halts, stops or runs slowly; in all cases violating an availability metric.

- > Threatens Remote Castle service (Process)
- > Threatens Castle service (Process)

--> Threatens Query users props (Association)

## 5.41 THRT56 - Potential Process Crash or Stop for My castle SSDP (Threat)

- Type: Denial Of Service
- Threat Priority: High
- Mitigation State: Not Started

*My castle SSDP crashes, halts, stops or runs slowly; in all cases violating an availability metric.*

--> Threatens (Association)  
--> Threatens Remote Castle SSDP (Process)  
--> Threatens My Castle SSDP (Process)

## 5.42 THRT29 - Potential Process Crash or Stop for Remote Castle service (Threat)

- Type: Denial Of Service
- Threat Priority: High
- Mitigation State: Mitigated
- Mitigation Strategy: No Action

*Remote Castle service crashes, halts, stops or runs slowly; in all cases violating an availability metric.*

--> Threatens Castle service (Process)  
--> Threatens Join, leave, Set users props (Association)  
--> Threatens Remote Castle service (Process)

## 5.43 THRT47 - Potential Process Crash or Stop for Remote castle SSDP (Threat)

- Type: Denial Of Service
- Threat Priority: High
- Mitigation State: Not Started

*Remote castle SSDP crashes, halts, stops or runs slowly; in all cases violating an availability metric.*

--> Threatens Remote Castle SSDP (Process)  
--> Threatens (Association)  
--> Threatens My Castle SSDP (Process)

## 5.44 THRT31 - Remote Castle service May be Subject to Elevation of Privilege Using Remote Code Execution (Threat)

- Type: Elevation Of Privilege
- Threat Priority: High
- Mitigation State: Not Started

*Castle service may be able to remotely execute code for Remote Castle service.*

--> Threatens Castle service (Process)  
--> Threatens Remote Castle service (Process)  
--> Threatens Join, leave, Set users props (Association)

## 5.45 THRT49 - Remote castle SSDP May be Subject to Elevation of Privilege Using Remote Code Execution (Threat)

- Type: Elevation Of Privilege
- Threat Priority: High
- Mitigation State: Not Started

*My castle SSDP may be able to remotely execute code for Remote castle SSDP.*

--> Threatens My Castle SSDP (Process)  
--> Threatens Remote Castle SSDP (Process)  
--> Threatens (Association)

## 5.46 THRT10 - Spoofing of Destination Data Store LSA (Threat)

- Type: Spoofing
- Threat Priority: High
- Mitigation State: Not Started

LSA may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of LSA. Consider using a standard authentication mechanism to identify the destination data store.

- Threatens Set psswd (Association)
- Threatens Castle service (Process)
- Threatens LSA (Data Store)

## 5.47 THRT13 - Spoofing of Destination Data Store Registry (Threat)

- Type: Spoofing
- Threat Priority: High
- Mitigation State: Not Started

Registry may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Registry. Consider using a standard authentication mechanism to identify the destination data store.

- Threatens Castle service (Process)
- Threatens Cache Castle info (Association)
- Threatens Registry (Data Store)

## 5.48 THRT05 - Spoofing of Destination Data Store SAM (Threat)

- Type: Spoofing
- Threat Priority: High
- Mitigation State: Not Started

SAM may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SAM. Consider using a standard authentication mechanism to identify the destination data store.

- Threatens Set acct info (Association)
- Threatens SAM (Data Store)
- Threatens Shacct (Process)

## 5.49 THRT07 - Spoofing of Source Data Store LSA (Threat)

- Type: Spoofing
- Threat Priority: High
- Mitigation State: Not Started

LSA may be spoofed by an attacker and this may lead to incorrect data delivered to Castle service. Consider using a standard authentication mechanism to identify the source data store.

- Threatens Castle service (Process)
- Threatens Get machine password (Association)
- Threatens LSA (Data Store)

## 5.50 THRT15 - Spoofing of Source Data Store Registry (Threat)

- Type: Spoofing
- Threat Priority: High
- Mitigation State: Not Started

Registry may be spoofed by an attacker and this may lead to incorrect data delivered to Castle service. Consider using a standard authentication mechanism to identify the source data store.

- Threatens Castle service (Process)
- Threatens Read Castle info (Association)
- Threatens Registry (Data Store)

## 5.51 THRT04 - Spoofing of Source Data Store SAM (Threat)

- Type: Spoofing

- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*SAM may be spoofed by an attacker and this may lead to incorrect data delivered to Shacct. Consider using a standard authentication mechanism to identify the source data store.*

- > Threatens SAM (Data Store)
- > Threatens Shacct (Process)
- > Threatens Get acct info (Association)

## 5.52 THRT25 - Spoofing the Castle service Process (Threat)

- 🔗 **Type:** Spoofing
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*Castle service may be spoofed by an attacker and this may lead to unauthorized access to Remote Castle service. Consider using a standard authentication mechanism to identify the source process.*

- > Threatens Castle service (Process)
- > Threatens Join, leave, Set users props (Association)
- > Threatens Remote Castle service (Process)

## 5.53 THRT34 - Spoofing the Castle service Process (Threat)

- 🔗 **Type:** Spoofing
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*Castle service may be spoofed by an attacker and this may lead to information disclosure by Remote Castle service. Consider using a standard authentication mechanism to identify the destination process.*

- > Threatens Remote Castle service (Process)
- > Threatens Query users props (Association)
- > Threatens Castle service (Process)

## 5.54 THRT01 - Spoofing the Local User External Entity (Threat)

- 🔗 **Type:** Spoofing
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*Local User may be spoofed by an attacker and this may lead to unauthorized access to Explorer. Consider using a standard authentication mechanism to identify the external entity.*

- > Threatens Manage Castle (Association)
- > Threatens Explorer (Process)
- > Threatens Local user (Human Actor)

## 5.55 THRT42 - Spoofing the My castle SSDP Process (Threat)

- 🔗 **Type:** Spoofing
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*My castle SSDP may be spoofed by an attacker and this may lead to unauthorized access to Remote castle SSDP. Consider using a standard authentication mechanism to identify the source process.*

- > Threatens My Castle SSDP (Process)
- > Threatens (Association)
- > Threatens Remote Castle SSDP (Process)

## 5.56 THRT52 - Spoofing the My castle SSDP Process (Threat)

- 🔗 **Type:** Spoofing
- 🔗 **Threat Priority:** High
- 🔗 **Mitigation State:** Not Started

*My castle SSDP may be spoofed by an attacker and this may lead to information disclosure by Remote castle SSDP. Consider using a standard authentication mechanism to identify the destination process.*

- > Threatens My Castle SSDP (Process)



- > Threatens Remote Castle SSDP (Process)
- > Threatens (Association)

## 5.57 THRT26 - Spoofing the Remote Castle service Process (Threat)

- 🔑 **Type:** Spoofing
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

Remote Castle service may be spoofed by an attacker and this may lead to information disclosure by Castle service. Consider using a standard authentication mechanism to identify the destination process.

- > Threatens Remote Castle service (Process)
- > Threatens Query users props (Association)
- > Threatens Castle service (Process)

## 5.58 THRT33 - Spoofing the Remote Castle service Process (Threat)

- 🔑 **Type:** Spoofing
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

Remote Castle service may be spoofed by an attacker and this may lead to unauthorized access to Castle service. Consider using a standard authentication mechanism to identify the source process.

- > Threatens Join, leave, Set users props (Association)
- > Threatens Remote Castle service (Process)
- > Threatens Castle service (Process)

## 5.59 THRT43 - Spoofing the Remote castle SSDP Process (Threat)

- 🔑 **Type:** Spoofing
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

Remote castle SSDP may be spoofed by an attacker and this may lead to information disclosure by My castle SSDP. Consider using a standard authentication mechanism to identify the destination process.

- > Threatens Remote Castle SSDP (Process)
- > Threatens (Association)
- > Threatens My Castle SSDP (Process)

## 5.60 THRT51 - Spoofing the Remote castle SSDP Process (Threat)

- 🔑 **Type:** Spoofing
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

Remote castle SSDP may be spoofed by an attacker and this may lead to unauthorized access to My castle SSDP. Consider using a standard authentication mechanism to identify the source process.

- > Threatens My Castle SSDP (Process)
- > Threatens (Association)
- > Threatens Remote Castle SSDP (Process)

## 5.61 THRT03 - Weak Access Control for a Resource (Threat)

- 🔑 **Type:** Information Disclosure
- 🔑 **Threat Priority:** High
- 🔑 **Mitigation State:** Not Started

Improper data protection of SAM can allow an attacker to read information not intended for disclosure. Review authorization settings.

- > Threatens Shacct (Process)
- > Threatens SAM (Data Store)
- > Threatens Get acct info (Association)

## 5.62 THRT08 - Weak Access Control for a Resource (Threat)

- 🔑 **Type:** Information Disclosure
- 🔑 **Threat Priority:** High

🔑 **Mitigation State:** Not Started

*Improper data protection of LSA can allow an attacker to read information not intended for disclosure. Review authorization settings.*

--> Threatens Castle service (Process)

--> Threatens LSA (Data Store)

## 5.63 THRT16 - Weak Access Control for a Resource (Threat)

🔑 **Type:** Information Disclosure

🔑 **Threat Priority:** High

🔑 **Mitigation State:** Not Started

*Improper data protection of Registry can allow an attacker to read information not intended for disclosure. Review authorization settings.*

--> Threatens Read Castle info (Association)

--> Threatens Registry (Data Store)

--> Threatens Castle service (Process)