# Windows Registry

# Windows Registry

Hierarchical database containing system and per-user settings

Tree structure in memory

Data saved in various files on disk

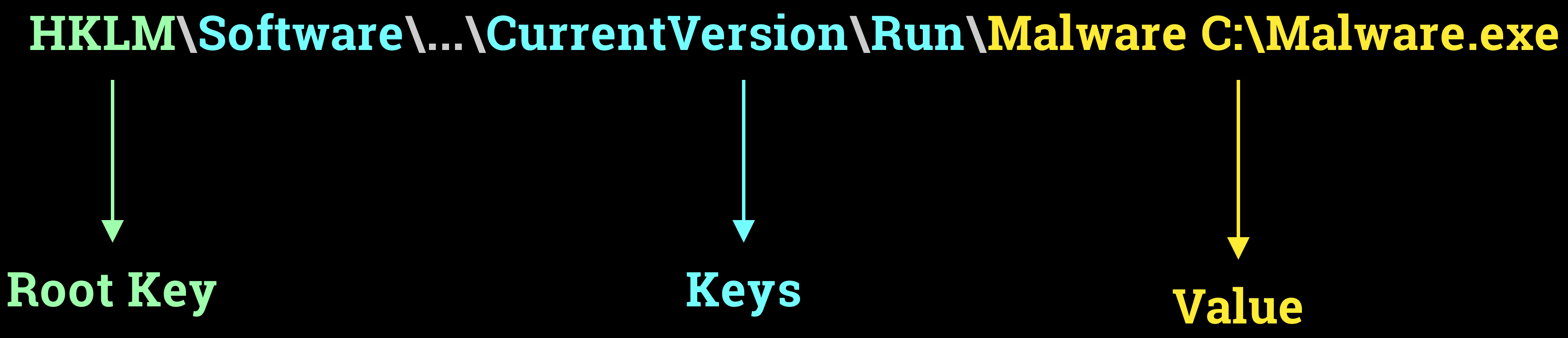
# Windows Registry

place for malware persistence

some malware lives in it

malware may modify it to reduce security

# General Structure



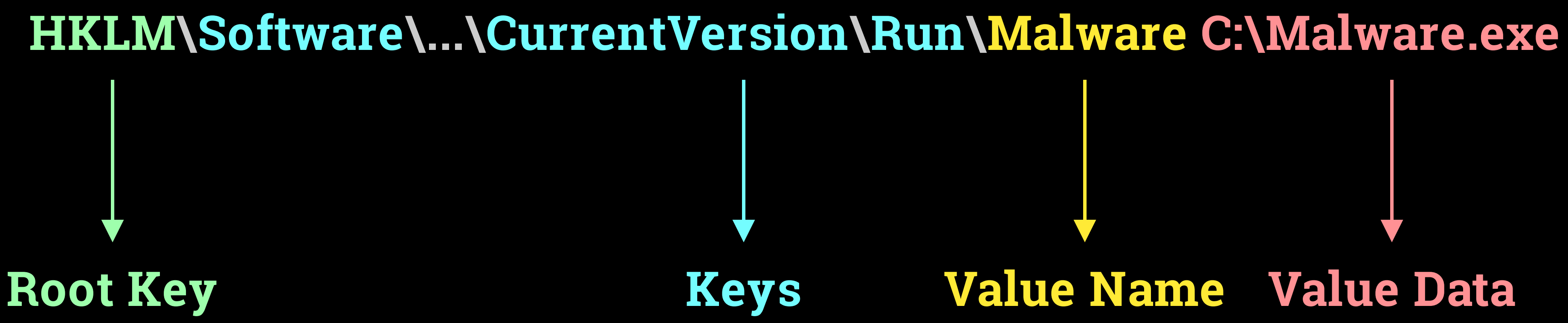
HKLM\Software\...\CurrentVersion\Run\Malware C:\Malware.exe

Root Key

Keys

Value

# General Structure



HKLM\Software\...\CurrentVersion\Run\Malware C:\Malware.exe

Root Key

Keys

Value Name

Value Data

# Value Data Types 1

| Data type | Description |
|---|---|
| REG_SZ | fixed-length Unicode string |
| REG_EXPAND_SZ | variable-length Unicode string |
| REG_DWORD | 32-bit number |
| REG_DWORD_BIG_ENDIAN | 32- bit number, with high byte first |
| REG_QWORD | 64-bit number |
| REG_BINARY | binary data of arbitrary length |

# Value Data Types 2

| Data type | Description |
|---|---|
| REG_RESOURCE_LIST | Hardware resource description |
| REG_FULL_RESOURCE_DESCRIPTOR | Hardware resource description |
| REG_RESOURCE_REQUIREMENTS_LIST | Resource requirements |
| REG_LINK | Unicode symbol link |
| REG_MULTI_SZ | Array of Unicode strings |
| REG_NONE | No value type |

# Value Data Types to Remember

## REG_SZ

can represent filenames, paths, types, names

## REG_DWORD

often represent true(1)/false(0)

## REG_BINARY

can store numbers larger than 32 bits

can store encrypted malware binaries

# Registry Root Keys 1

### HKEY_LOCAL_MACHINE (HKLM)

local computer and OS configuration info

### HKEY_CLASSES_ROOT (HKCR)

file associations, COM object registration

merged view of HKLM and HKCU

### HKEY_USERS (HKU)

subkeys for each user profile that is actively loaded

### HKEY_CURRENT_USER (HKCU)

data of the currently logged-on user (functions like symbolic link)

### HKEY_CURRENT_USER-_LOCAL_SETTINGS (HKCULS)

points to local settings of currently logged-on user

# Registry Root Keys 2

### HKEY_PERFORMANCE_TEXT (HKPT)

performance counters text strings

### HKEY_PERFORMANCE_DATA (HKPD)

runtime and performance data

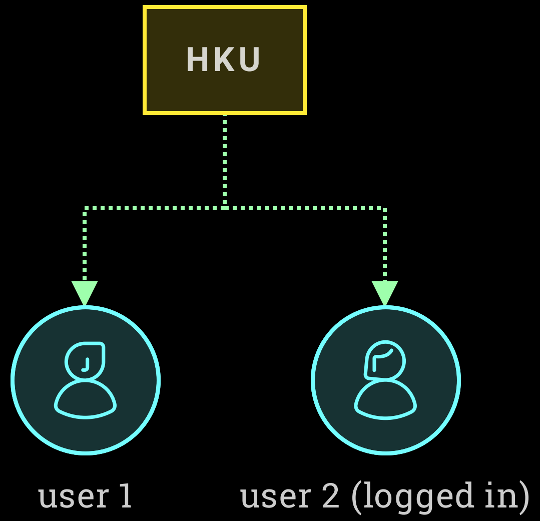
### HKEY_PERFORMANCE_NLSTEXT (HKPNT)

performance counters text strings in US English

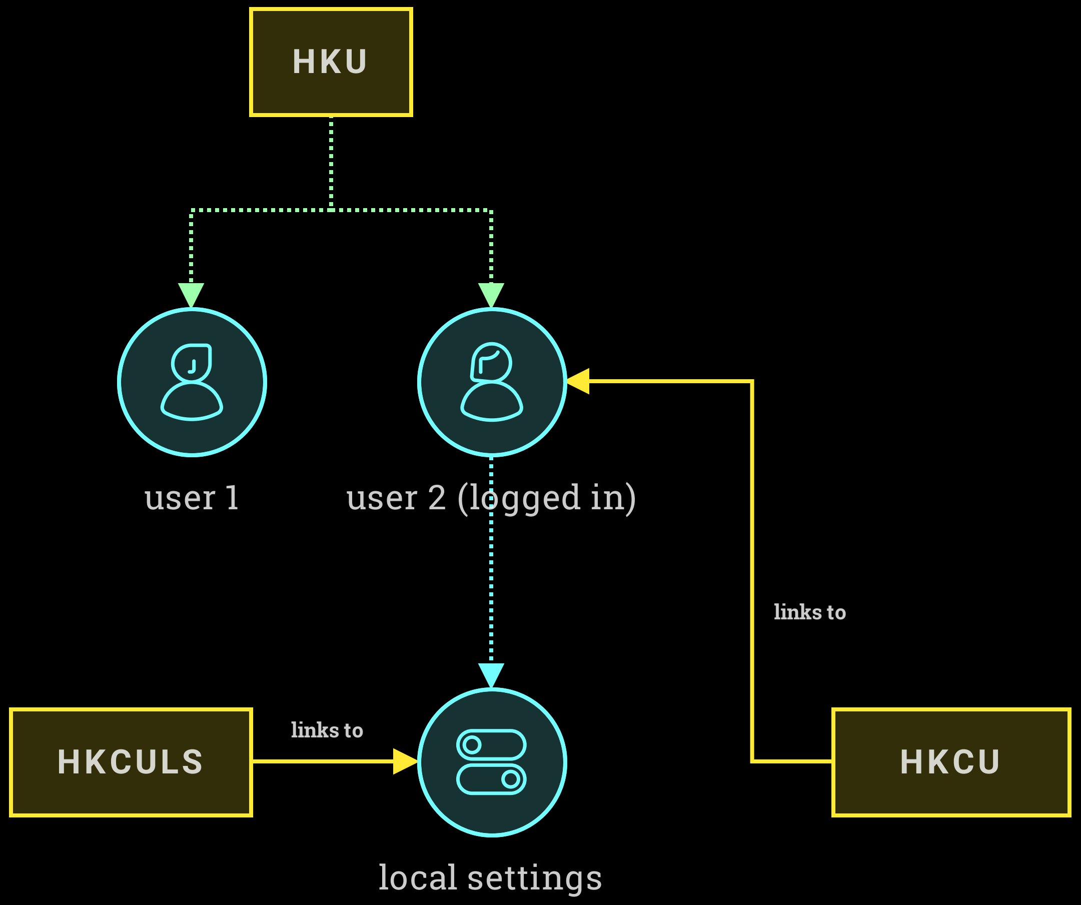
### HKEY_CURRENT_CONFIG (HKCC)

points to HKLM entry for  hardware profile

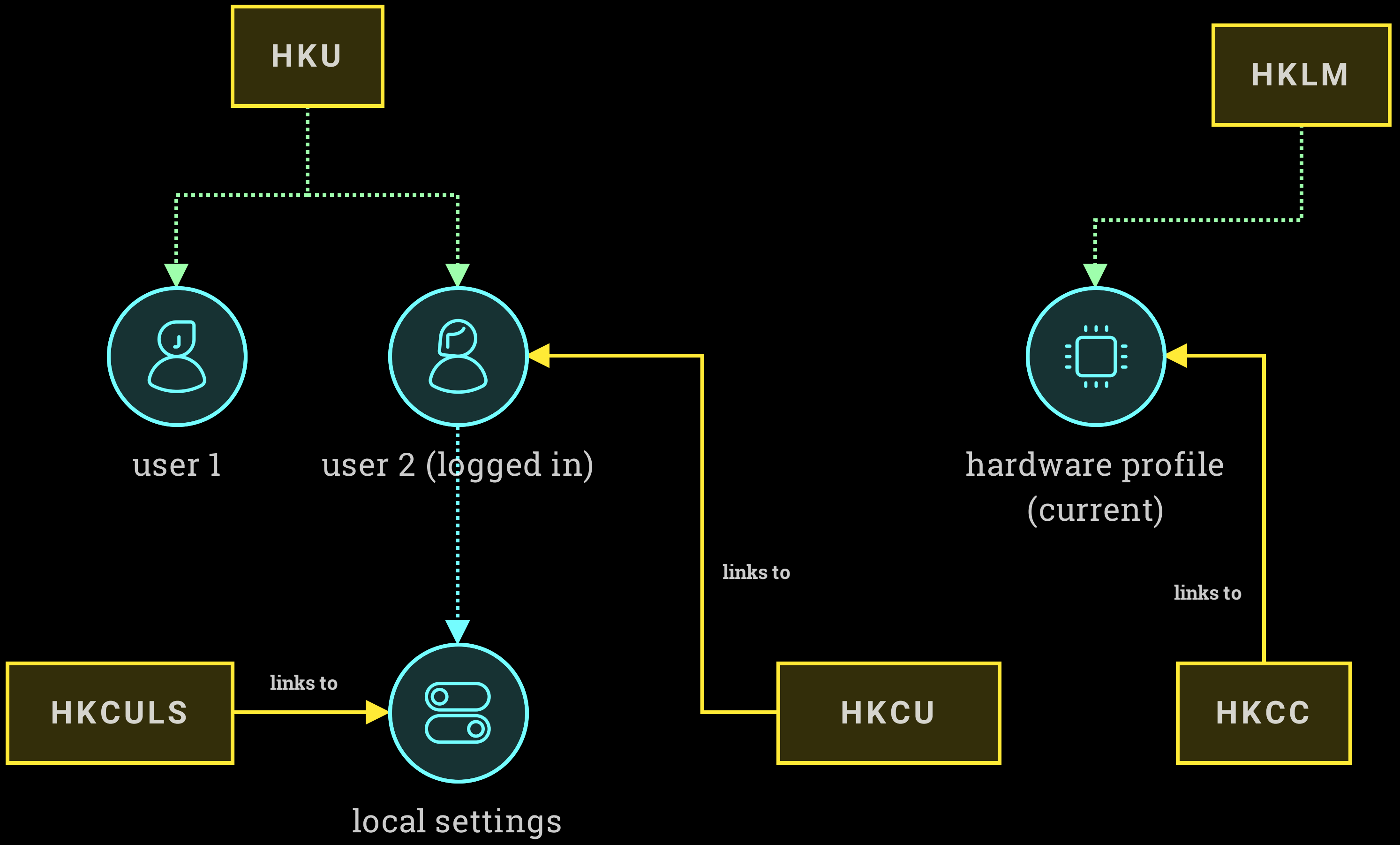
# Links between Registry Root Keys



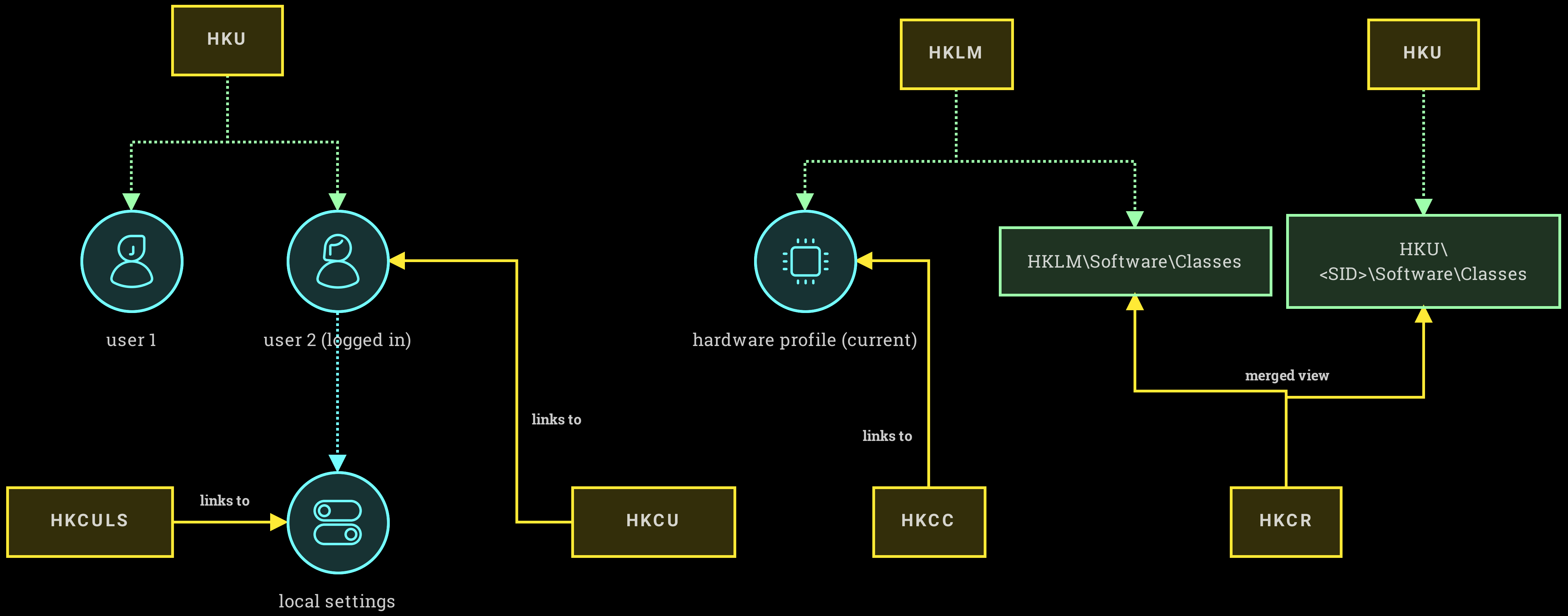
# Links between Registry Root Keys



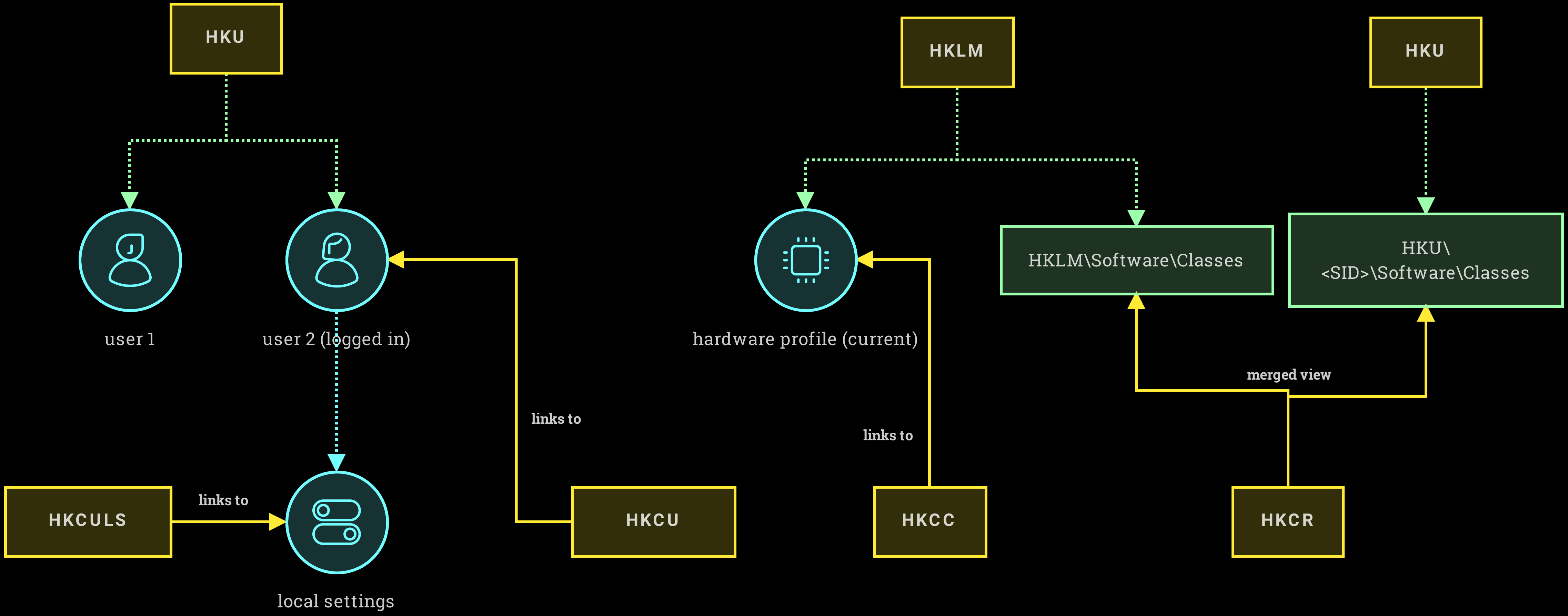
# Links between Registry Root Keys



# Links between Registry Root Keys



# Links between Registry Root Keys



# Registry Hives

A hive is a logical group of keys, subkeys, and values in the registry that has a set of supporting files loaded into memory when the operating system is started or a user logs in.

Reference: https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-hives

# Registry Hives

| Hive | Supporting Files |
|---|---|
| HKCC | System, System.alt, System.log, System.sav |
| HKCU | Ntuser.dat, Ntuser.dat.log |
| HKLM\SAM | Sam, Sam.log, Sam.sav |
| HKLM\Security | Security, Security.log, Security.sav |
| HKLM\Software | Software, Software.log, Software.sav |
| HKLM\System | System, System.alt, System.log, System.sav |
| HKU\.DEFAULT | Default, Default.log, Default.sav |

Reference: https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-hives

# Myth

## ~~REGISTRY ROOT KEYS ARE THE SAME AS HIVES~~

They are not the same. Hives always have corresponding files on disk.

Some root keys are links to other parts of the registry and do not have corresponding files.

Four of the hives are subkeys of HKLM

# Examples: Registry and ASEPs

| ASEP | Registry |
|---|---|
| Run keys | HKLM\Software\Microsoft\Windows\CurrentVersion\Run<br>HKCU\Software\Microsoft\Windows\CurrentVersion\Run |
| RunOnce keys | HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce<br>HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce |
| IFEO | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options |
| Winlogon | HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon |

# Examples: Registry and ASEPs

| ASEP | Registry |
|---|---|
| AppInit DLLs | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs |
| Active Setup | HKLM\|HKCU\SOFTWARE\Microsoft\Active Setup\Installed Components |
| Shim Databases | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ with subkeys InstalledSDB and Custom |
| Browser Helper Objects | HKLM\SOFTWARE\Windows\CurrentVersion\Explorer\Browser Helper Objects |