

Exclusively made for



Fachhochschule
Münster University of
Applied Sciences



VIRTUALFORGE
run your business safer

Damian Poddebniak, Sebastian Schinzel, Andreas Wiegenstein
Patch me if you can

Troopers16 (SAP Security Track) March 16, 2016

© 2016, Virtual Forge GmbH & FH Münster.
Alle Rechte vorbehalten.

Damian Poddebniak

Research assistant at Münster University of applied sciences
Focus on IT Security and cryptography

Prof. Dr. Sebastian Schinzel

Professor for computer security at Muenster University of applied sciences
CTO of CycleSEC GmbH

#SAP
#Security
#Research

Andreas Wiegenstein

CTO of Virtual Forge GmbH
SAP Security Researcher, active since 2003
Received credit from SAP for > **80** reported 0-day vulnerabilities
Speaker at international Conferences
Troopers, BlackHat, DeepSec, Hack in the Box, IT Defense, RSA, ...

Agenda

1. When I grow up, I want to be a Man-in-the-Middle!
2. Integrity and authenticity of software packages
3. SAP Basics
4. Introduction SAP Patches, SMP & Download Manager
5. Security Issues
6. Conclusions

When I grow up, I want to
be a Man-in-the-Middle!

When I grow up, I want to be a Man-in-the-Middle!

You want to be a Man-in-the-Middle? Anyone can be a Man-in-the-Middle!

- You like coffee? Starbucks has free Wifi.
- The hotel you are (briefly) staying this night has Wifi?
- You can setup a TOR exit node

But who would download SAP software over those?

When I grow up, I want to be a Man-in-the-Middle!

More involved ways to become a MitM

- Use one of those Cisco/Juniper/Huawei/etc. exploits to compromise router
- BGP hijacking
- DNS Spoofing, DNS Poisoning
- Man-in-the-Middle-as-a-Service, Hacking Team

→ Target: Administrators

[Integrity and authenticity of software packages

Integrity and authenticity of software packages

HTTP/FTP download **Trust maintainer + download server + network**

HTTPS/SSH download **Trust maintainer + download server**

Digitally signed package **Trust maintainer**

Integrity and authenticity of software packages

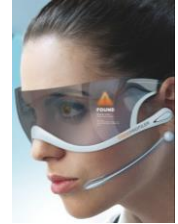
Digitally signed package

- Proof that package wasn't changed since the maintainer signed it



Software package m

Customer:
public key e_a



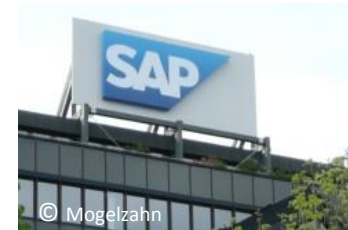
Signature check: $s' \stackrel{?}{=} \text{hash}(m')^e$

m', s'

m, s

Signature creation: $s = \text{hash}(m)^d$

SAP:
public key: e_a
private key: d_a



Integrity and authenticity of software packages

Unsigned packages over HTTP

- “Dilettante is a man in the middle proxy that injects malicious codes into JARs served by Maven Central.”

<https://github.com/mveytsman/dilettante>

- Buffer Overflow in HTTP parser of Debian’s APT package manager

<https://lists.debian.org/debian-security-announce/2014/msg00219.html>

[SAP Basics

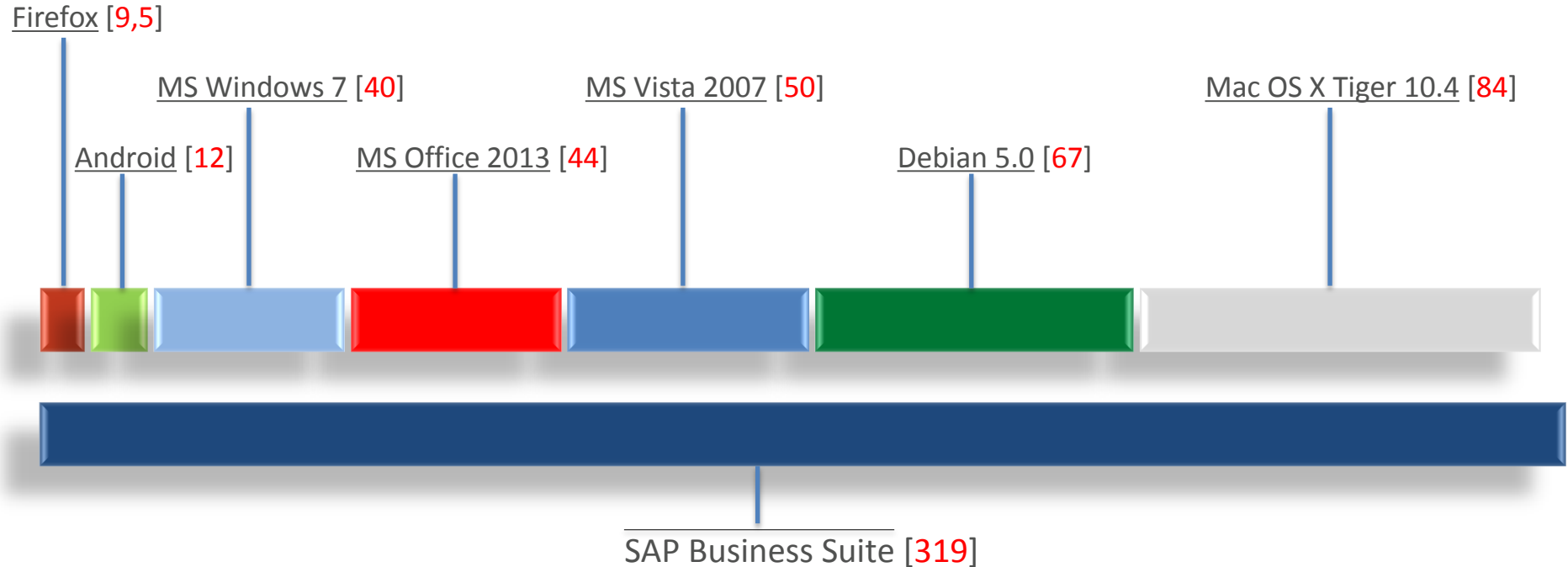
SAP matters

Why protect SAP systems?

- **More than 300,000 companies run SAP**
- **SAP customers ...**
 - Transport > 1.1 billion flight passengers per year
 - Produce 78% of the world's food
 - Produce 82 % of the world's medical devices
- **74% of the world's transaction revenue touches an SAP system**
- **... and ...**
 - **72% of the world-wide beer production depends on companies that run SAP !!!**

IT Complexity vs. ERP Complexity

Sizes of major Applications in Million Lines of Code



[Introduction SAP Patches, SMP & Download Manager

SAP Patches

There are two main ways to obtain and install SAP patches

1. SAP Service Marketplace


- Download new products
- Download new versions of products
- Download support packages (collection of one or more patches)
- Download patches

2. Transaction SNOTE

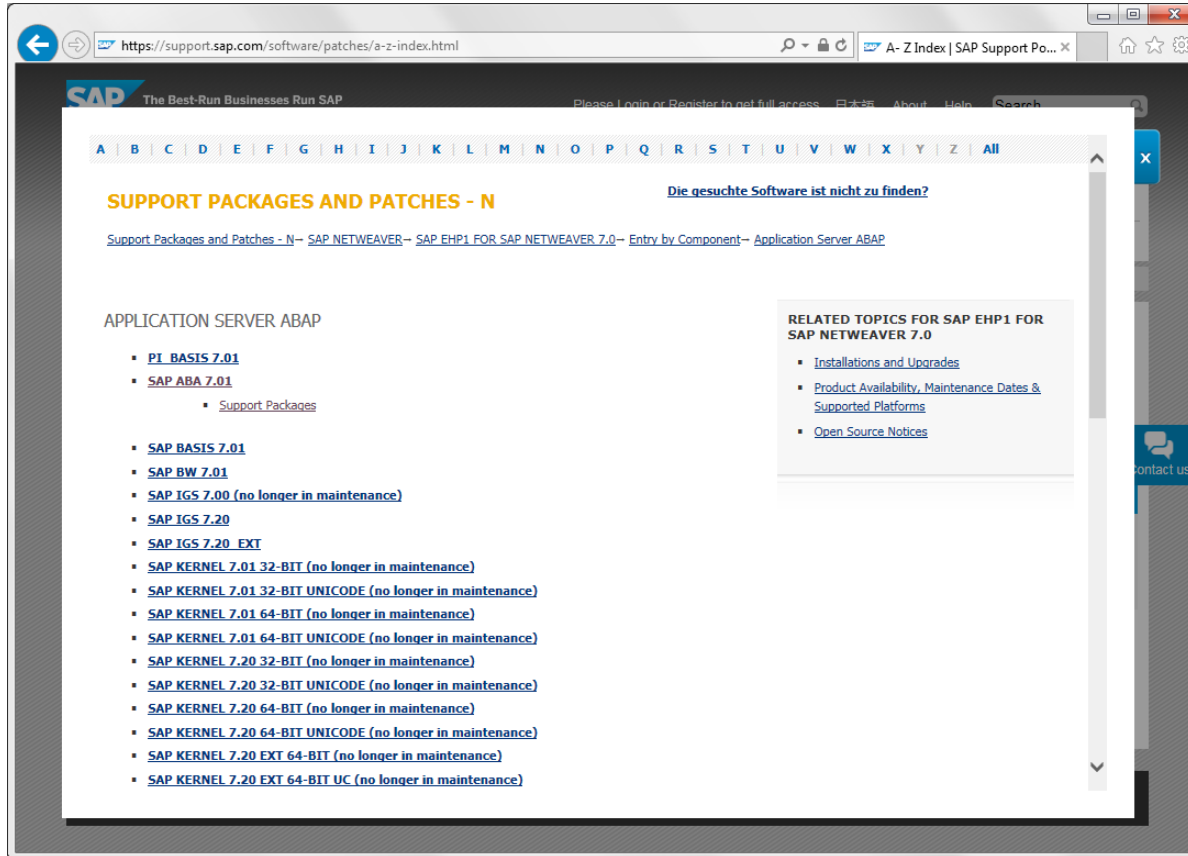
- Download SAP OSS Notes (minor patches)
- Implement corrections automatically / correction instructions manually

SAP Service Marketplace

The screenshot shows the SAP Software Download Center interface. At the top, there's a navigation bar with the SAP logo, a search bar, and links for 'Please Login or Register to get full access', '日本語', 'About', and 'Help'. Below this is a 'Support Portal' section with a grid of links: 'Knowledge Base & Incidents', 'Release, Upgrade & Maintenance Info', 'Software Downloads' (highlighted), 'Keys, Systems & Installations', 'Support Programs & Services', 'Remote Support', 'Users & Authorizations', 'Documentation', and 'SAP Solution Manager'. The main content area is titled 'SAP Software Download Center' and includes a welcome message: 'Download SAP products that are associated with your S-User ID. You will require the Download Software authorization, which you can request via your company's SAP user administrator.' Below this is a section 'What would you like to download today?' with three icons: 'Installations & Upgrades', 'Support Packages & Patches', and 'Files for your Databases'. To the right of this section is a 'Useful Links' box with a 'Contact us' button and three links: 'Top Downloads' (lists the most searched for download files), 'Ramp-Up software' (lists all Ramp-Up products you have signed up for), and 'Customer Validation' (lists all products if you are participating in the Customer Validation initiative). At the bottom, there's a footer with links for 'Terms of Use', 'Copyright', 'Privacy', 'Impressum', and 'Contact Us', along with social media icons for YouTube, Twitter, and Facebook.

 Search for Software
 my Download Basket

SAP Service Marketplace



The screenshot shows a web browser window with the URL <https://support.sap.com/software/patches/a-z-index.html>. The page is titled "SUPPORT PACKAGES AND PATCHES - N" and includes a search bar at the top. Below the title, there is a navigation bar with letters A through Z and "All". The main content area lists various support packages and patches for Application Server ABAP, including:

- PI BASIS 7.01
- SAP ABA 7.01
 - Support Packages
- SAP BASIS 7.01
- SAP BW 7.01
- SAP IGS 7.00 (no longer in maintenance)
- SAP IGS 7.20
- SAP IGS 7.20_EXT
- SAP KERNEL 7.01 32-BIT (no longer in maintenance)
- SAP KERNEL 7.01 32-BIT UNICODE (no longer in maintenance)
- SAP KERNEL 7.01 64-BIT (no longer in maintenance)
- SAP KERNEL 7.01 64-BIT UNICODE (no longer in maintenance)
- SAP KERNEL 7.20 32-BIT (no longer in maintenance)
- SAP KERNEL 7.20 32-BIT UNICODE (no longer in maintenance)
- SAP KERNEL 7.20 64-BIT (no longer in maintenance)
- SAP KERNEL 7.20 64-BIT UNICODE (no longer in maintenance)
- SAP KERNEL 7.20 EXT 64-BIT (no longer in maintenance)
- SAP KERNEL 7.20 EXT 64-BIT UC (no longer in maintenance)

On the right side, there is a section titled "RELATED TOPICS FOR SAP EHP1 FOR SAP NETWEAVER 7.0" with links to:

- Installations and Upgrades
- Product Availability, Maintenance Dates & Supported Platforms
- Open Source Notices

The browser window also shows a "contact us" button on the right side.

SAP Service Marketplace

Download Objekte

SAP ABA 7.01

Markieren Sie ein oder mehrere Objekte und drücken Sie die Schaltfläche "Zum Download Basket hinzufügen". Wir empfehlen die Verwendung des [SAP Download Manager](#) — insbesondere für Downloads großer Objekte oder für auf einen späteren Zeitpunkt terminierte Downloads. Mehr Information [über Multispinning und das Entpacken mehrteiliger Archive](#), finden Sie hier. Klicken Sie die -Ikone, um die [Generierung einer Liste der Nebeneffekte](#) zu beantragen.

[Zum Download Basket hinzufügen](#) [Download Basket verwalten](#) [Alle auswählen](#) [Auswahl zurücknehmen](#)

Die folgenden Objekte können heruntergeladen werden:

	Dateityp	Download Objekt	Titel	Infodatei	Dateigröße [kb]	Freigegeben am	Geändert am
<input type="checkbox"/>	SAR	SAPKA70117	ABA Support Package 0017 for 7.01	Info	14273	25.03.2015	25.03.2015
<input type="checkbox"/>	SAR	SAPKA70116	ABA Support Package 0016 for 7.01	Info	10170	27.06.2014	27.06.2014
<input type="checkbox"/>	SAR	SAPKA70115	ABA Support Package 0015 for 7.01	Info	10389	27.01.2014	27.01.2014
<input type="checkbox"/>	SAR	SAPKA70114	ABA Support Package 0014 for 7.01	Info	14251	01.08.2013	01.08.2013
<input type="checkbox"/>	SAR	SAPKA70113	ABA Support Package 0013 for 7.01	Info	13225	18.02.2013	18.02.2013
<input type="checkbox"/>	SAR	SAPKA70112	ABA Support Package 0012 for 7.01	Info	14636	13.08.2012	13.08.2012
<input type="checkbox"/>	SAR	SAPKA70111	ABA Support Package 0011 for 7.01	Info	13478	07.03.2012	07.03.2012
<input type="checkbox"/>	SAR	SAPKA70110	ABA Support Package 0010 for 7.01	Info	13088	25.08.2011	25.08.2011
<input type="checkbox"/>	SAR	SAPKA70109	ABA Support Package 0009 for 7.01	Info	12220	20.05.2011	20.05.2011
<input type="checkbox"/>	SAR	SAPKA70108	ABA Support Package 0008 for 7.01	Info	17587	13.12.2010	13.12.2010
<input type="checkbox"/>	CAD	SAPKA70107	ABA Support Package 0007 for 7.01	Info	17776	12.07.2010	12.07.2010

SAP Service Marketplace

SAP Download Area - Internet Explorer

https://websmp230.sap-ag.de/sap(bD1kZSZjPTAwMQ==)/bc/bsp/spn/download_basket/main.htm?smp-webas=

Download Basket Download-Historie

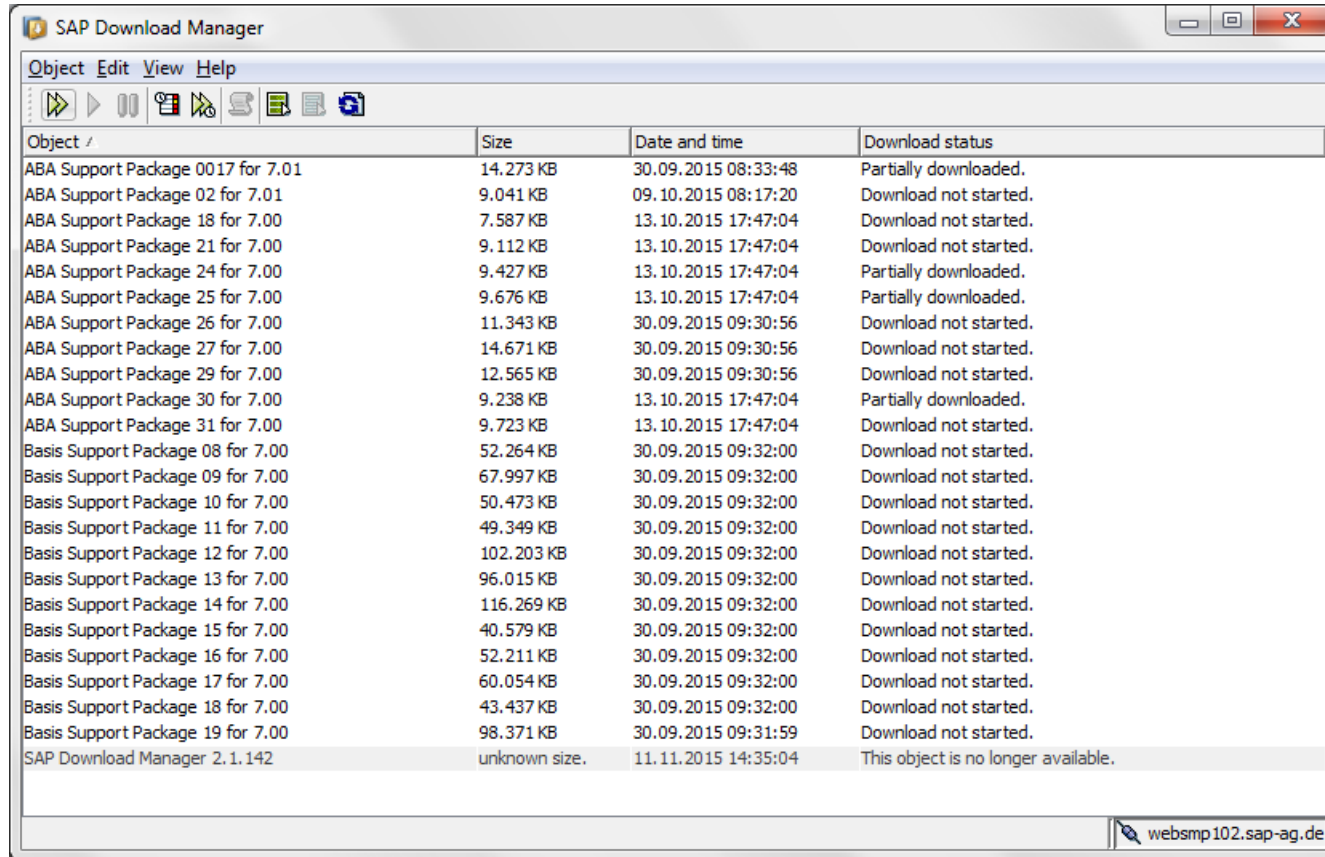
Löschen Download Manager holen

Im Rahmen unserer Verpflichtung, eine stabile und effiziente Performance der Download-Infrastruktur für SAP-Kunden sicherzustellen, wurde der Download von SAP-Hinweisen auf derzeit 1.000 Hinweise pro Tag beschränkt. Wenn Sie weitere Unterstützung benötigen, nutzen Sie bitte Ihre vorhandenen Kommunikationskanäle.

Beschreibung	Dateiname	Status	Größe [KB]	Verfallsdatum	Beantragt am
(Alle)					
ABA Support Package 02 for 7.01	SAPKA70102	Verfügbar für Download	9.041		09.10.2015 08:17:20
Basis Support Package 15 for 7.00	SAPKB70015	Verfügbar für Download	40.579		30.09.2015 09:32:00
Basis Support Package 12 for 7.00	SAPKB70012	Verfügbar für Download	102.203		30.09.2015 09:32:00
Basis Support Package 16 for 7.00	SAPKB70016	Verfügbar für Download	52.211		30.09.2015 09:32:00
Basis Support Package 11 for 7.00	SAPKB70011	Verfügbar für Download	49.349		30.09.2015 09:32:00
Basis Support Package 13 for 7.00	SAPKB70013	Verfügbar für Download	96.015		30.09.2015 09:32:00
Basis Support Package 14 for 7.00	SAPKB70014	Verfügbar für Download	116.269		30.09.2015 09:32:00
Basis Support Package 17 for 7.00	SAPKB70017	Verfügbar für Download	60.054		30.09.2015 09:32:00
Basis Support Package 18 for 7.00	SAPKB70018	Verfügbar für Download	43.437		30.09.2015 09:32:00
Basis Support Package 08 for 7.00	SAPKB70008	Verfügbar für Download	52.264		30.09.2015 09:32:00
Basis Support Package 09 for 7.00	SAPKB70009	Verfügbar für Download	67.997		30.09.2015 09:32:00
Basis Support Package 10 for 7.00	SAPKB70010	Verfügbar für Download	50.473		30.09.2015 09:32:00
Basis Support Package 19 for 7.00	SAPKB70019	Verfügbar für Download	98.371		30.09.2015 09:31:59
ABA Support Package 24 for 7.00	SAPKA70024	Teilweise heruntergeladen	9.427		30.09.2015 09:30:56
ABA Support Package 25 for 7.00	SAPKA70025	Teilweise heruntergeladen	9.676		30.09.2015 09:30:56
ABA Support Package 29 for 7.00	SAPKA70029	Verfügbar für Download	12.565		30.09.2015 09:30:56
ABA Support Package 27 for 7.00	SAPKA70027	Verfügbar für Download	14.671		30.09.2015 09:30:56
ABA Support Package 26 for 7.00	SAPKA70026	Verfügbar für Download	11.343		30.09.2015 09:30:56

100%

SAP Download Manager



The screenshot shows the SAP Download Manager application window. It has a menu bar with 'Object', 'Edit', 'View', and 'Help'. Below the menu is a toolbar with various icons. The main area contains a table with four columns: 'Object /', 'Size', 'Date and time', and 'Download status'. The table lists various support packages for SAP 7.01, including ABA and Basis packages. The download status for most packages is 'Download not started', while some are 'Partially downloaded'. The last entry, 'SAP Download Manager 2.1.142', has a status of 'This object is no longer available.' The bottom right corner of the window shows the URL 'websmp102.sap-ag.de'.

Object /	Size	Date and time	Download status
ABA Support Package 0017 for 7.01	14.273 KB	30.09.2015 08:33:48	Partially downloaded.
ABA Support Package 02 for 7.01	9.041 KB	09.10.2015 08:17:20	Download not started.
ABA Support Package 18 for 7.00	7.587 KB	13.10.2015 17:47:04	Download not started.
ABA Support Package 21 for 7.00	9.112 KB	13.10.2015 17:47:04	Download not started.
ABA Support Package 24 for 7.00	9.427 KB	13.10.2015 17:47:04	Partially downloaded.
ABA Support Package 25 for 7.00	9.676 KB	13.10.2015 17:47:04	Partially downloaded.
ABA Support Package 26 for 7.00	11.343 KB	30.09.2015 09:30:56	Download not started.
ABA Support Package 27 for 7.00	14.671 KB	30.09.2015 09:30:56	Download not started.
ABA Support Package 29 for 7.00	12.565 KB	30.09.2015 09:30:56	Download not started.
ABA Support Package 30 for 7.00	9.238 KB	13.10.2015 17:47:04	Partially downloaded.
ABA Support Package 31 for 7.00	9.723 KB	13.10.2015 17:47:04	Download not started.
Basis Support Package 08 for 7.00	52.264 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 09 for 7.00	67.997 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 10 for 7.00	50.473 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 11 for 7.00	49.349 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 12 for 7.00	102.203 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 13 for 7.00	96.015 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 14 for 7.00	116.269 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 15 for 7.00	40.579 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 16 for 7.00	52.211 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 17 for 7.00	60.054 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 18 for 7.00	43.437 KB	30.09.2015 09:32:00	Download not started.
Basis Support Package 19 for 7.00	98.371 KB	30.09.2015 09:31:59	Download not started.
SAP Download Manager 2.1.142	unknown size.	11.11.2015 14:35:04	This object is no longer available.

SAP Software Archives

File types in the Download Basket

- **CAR** Archives (older format)
- **SAR** Archives (since R/3 Release 4.6C)
 - May contain signatures : File SIGNATURE . SMF

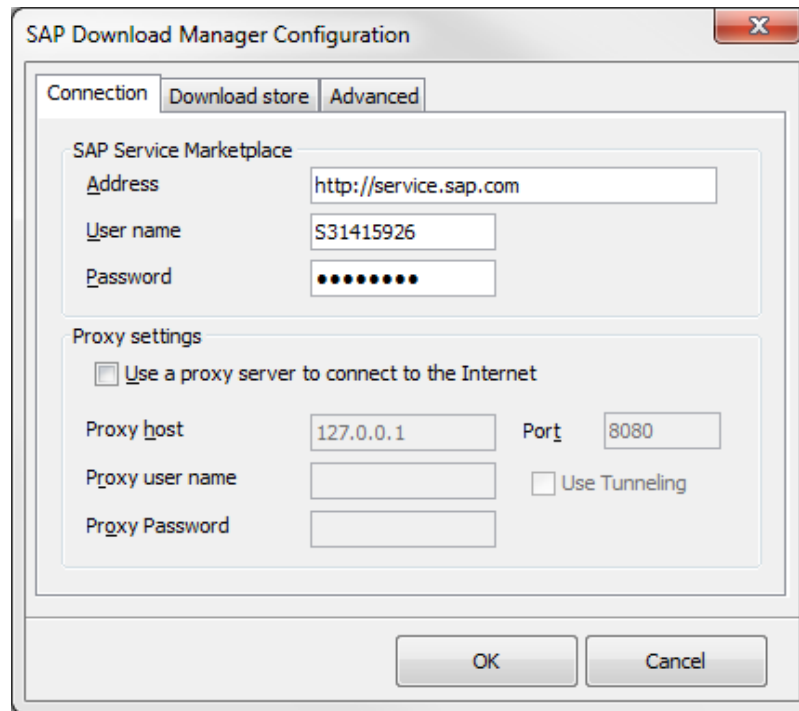
Archives are extracted with a proprietary compression utility: SAPCAR

- Command-line tool
- Available since R/3 Release 4.6C
- See SAP Note 212876

[Security Issues

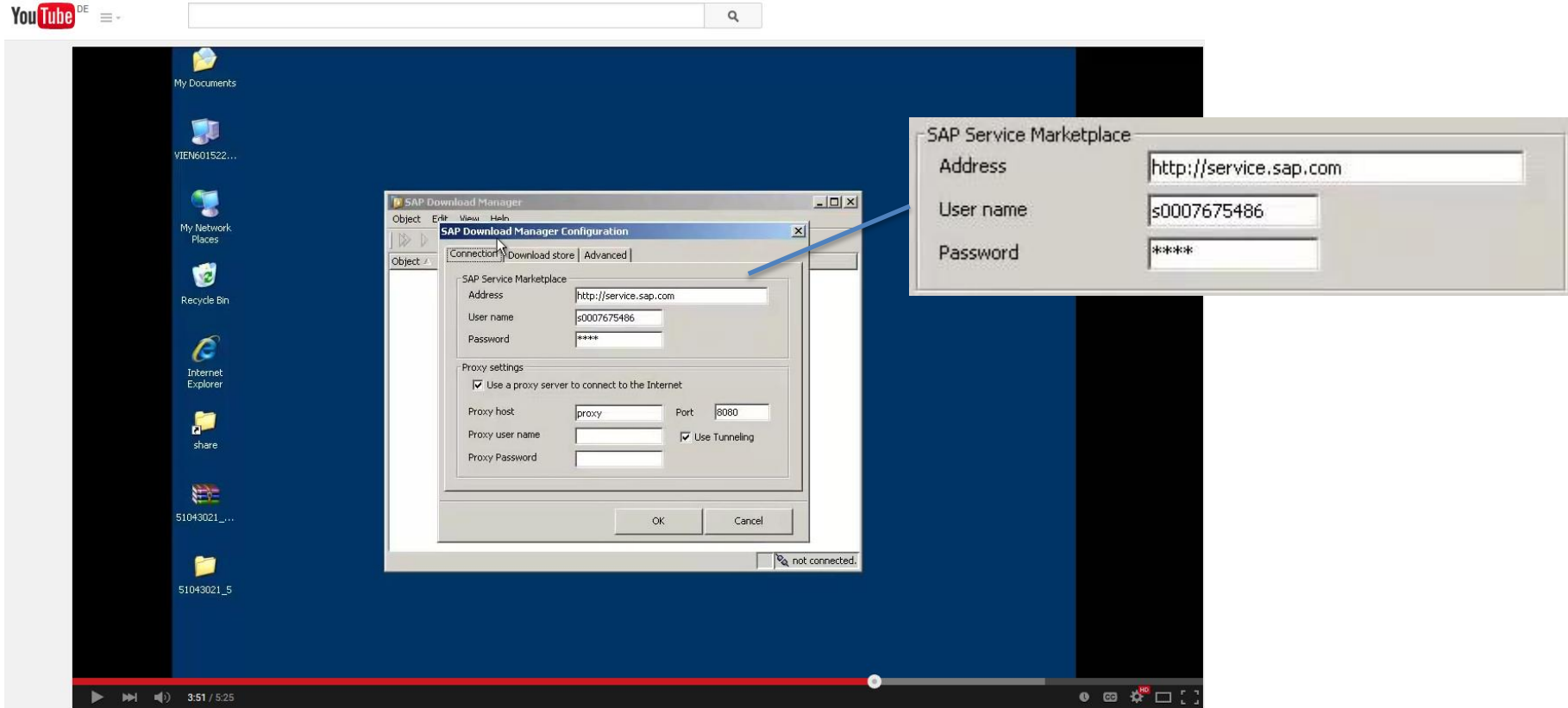
1. Insecure Default (HTTP Connection)

Download Manager is installed with a default HTTP connection to Walldorf



SAP Patch: Note 2235412, Oct 2015

Insecure Training (Installation guide on YouTube)



Insecure Advice (Discussion on SCN)

Download manager settings

This question is **Assumed Answered**.

I am trying to configure Download manager, i setup with username and password, with proxy settings of my internet but I cant connect. My question is what would be the path to connect to put under settings. I am putting "<https://websmp105.sap-ag.de/notes>" Is this correct?

Another question is how do i create RFC connection to SAPnet. i know the transaction is SM59. What do I need to configure this connection?

Any help will be appreciated.



Re: Download manager settings

Hi Bill,

- 1) use <http://service.sap.com> instead of <https://websmp105.sap-ag.de/notes>
- 2) for RFC to SAPnet check this http://help.sap.com/erp2005_ehp_03/helpdata/EN/6a/15ef3957fd0a1be10000000a114084/frameset.htm

2. Insecure Password Storage (XOR)

Download Manager uses a trivial algorithm to obfuscate the SMP password

PW: @@@@

```
270: 7E 00 0E 00 00 03 F9 74 00 0C 53 4D 50 5F 50 41 ~ .. ut SMP_PA
280: 53 53 57 4F 52 44 73 71 00 7E 00 05 00 00 00 06 SSWORDsq.~ ..
290: 75 72 00 02 5B 49 4D BA 60 26 76 EA B2 A5 02 00 ur.. [IM²`&vé²#..
2A0: 00 78 70 00 00 00 06 00 00 00 72 00 00 00 71 00 xp.....r...q
2B0: 00 00 70 00 00 00 6F 00 00 00 6E 00 00 00 6D 74 p...o...n...nt
2C0: 00 07 57 4E 44 5F 54 4F 50 73 71 00 7E 00 0E 00 WND_TOPsq.~ ..
2D0: 00 00 D7 74 00 0D 55 53 45 5F 54 55 4E 4E 45 4C ..xt..USE_TUNNEL
```

PW: AAAAAA

```
270: 7E 00 0E 00 00 03 F9 74 00 0C 53 4D 50 5F 50 41 ~ .. ut SMP_PA
280: 53 53 57 4F 52 44 73 71 00 7E 00 05 00 00 00 06 SSWORDsq.~ ..
290: 75 72 00 02 5B 49 4D BA 60 26 76 EA B2 A5 02 00 ur.. [IM²`&vé²#..
2A0: 00 78 70 00 00 00 06 00 00 00 73 00 00 00 72 00 xp.....s...r
2B0: 00 00 71 00 00 00 70 00 00 00 6F 00 00 00 6E 74 q...p...o...nt
2C0: 00 07 57 4E 44 5F 54 4F 50 73 71 00 7E 00 0E 00 WND_TOPsq.~ ..
2D0: 00 00 D7 74 00 0D 55 53 45 5F 54 55 4E 4E 45 4C ..xt..USE_TUNNEL
```

2. Mitigation

SAP Patch: Notes 2074276, 2282338

SAP Download Manager - Help

The current version of the SAP Download Manager is 2.1.142, status November 2015.

Please note

For security reasons, unlike previous versions of the SAP Download Manager, the current one **no longer stores your portal password** in the tool's settings. So whenever you use the SAP Download Manager, you have to enter your password manually.

3. HTTP Basic Authentication used

Download Manager uses Basic Authentication, i.e. passwords can be stolen by MITM attacks

Fake Response ...

Response from http://service.sap.com:80/~form/download_basket?_MODE=BASKET_CONTENT&J_VER

Forward

Drop

Intercept is on

Action

Raw

Headers

Hex

HTML

Render

```
HTTP/1.1 401 Unauthorized
Cache-Control: no-cache
Connection: close
Content-Length: 1
Content-Type: text/html
Date: Tue, 34 Feb 2019 25:30:35 GMT
Pragma: no-cache
Server: Microsoft-IIS/7.0
Via: websmp208
WWW-Authenticate: Basic realm="SAP Service Marketplace"
```

... leaks Credentials

```
Host: service.sap.com:80
Proxy-Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.0 (java 1.5)
Authorization: Basic QmVhbSBtZSB1cDpTY290dHkh
```

4. How about using HTTPS?

Welcome to the SAP Download Manager

Connection Information
Enter parameters to connect to the SAP Service Marketplace

SAP Service Marketplace

Address:

User name:

Password:

Proxy Settings

☐ Use a proxy server to connect to the Internet

Proxy host: Port:

Proxy user name: ☐ Use Tunneling

Proxy Password:

< Back Next > Cancel

Welcome to the SAP Download Manager

Connection Information
Enter parameters to connect to the SAP Service Marketplace

SAP Service Marketplace

Address:

User name:

Password:

Proxy Settings

☐ Use a proxy server to connect to the Internet

Proxy host: Port:

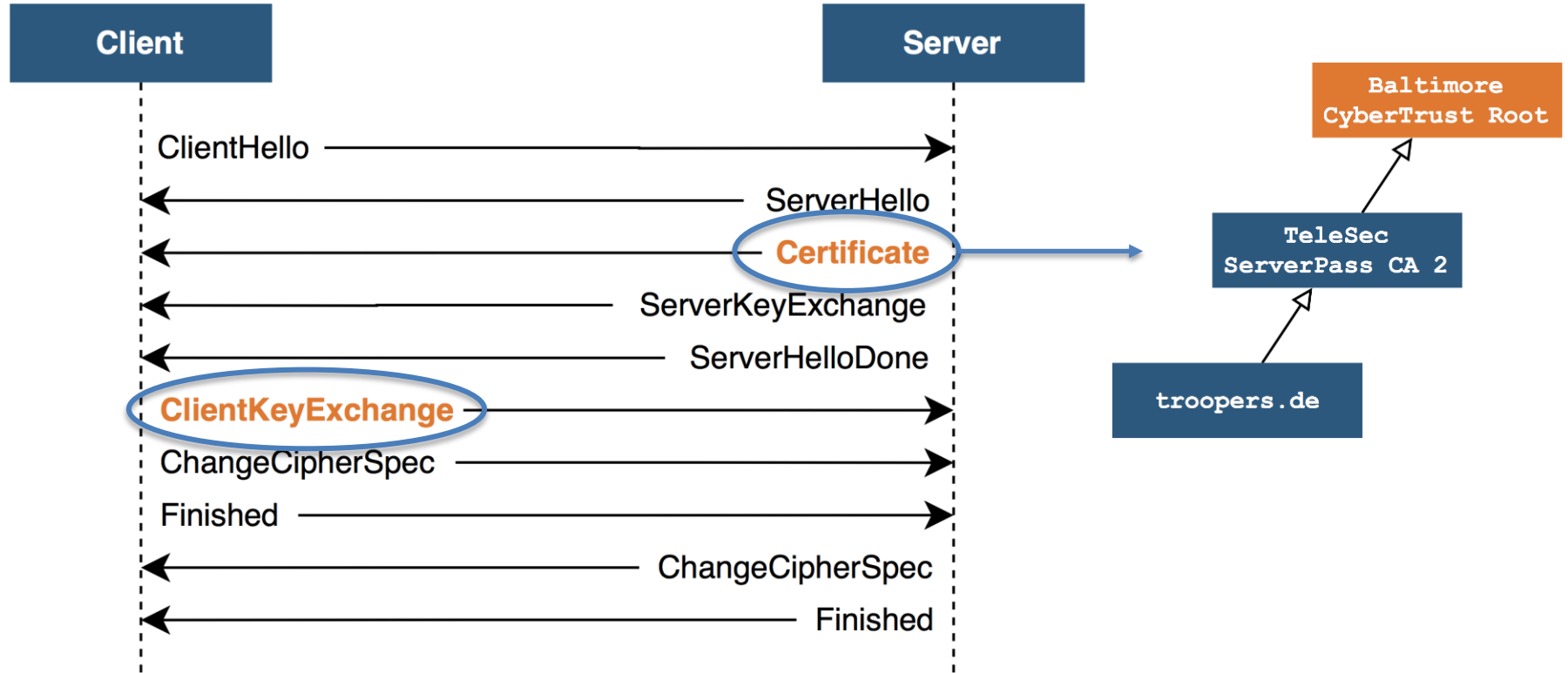
Proxy user name: ☐ Use Tunneling

Proxy Password:

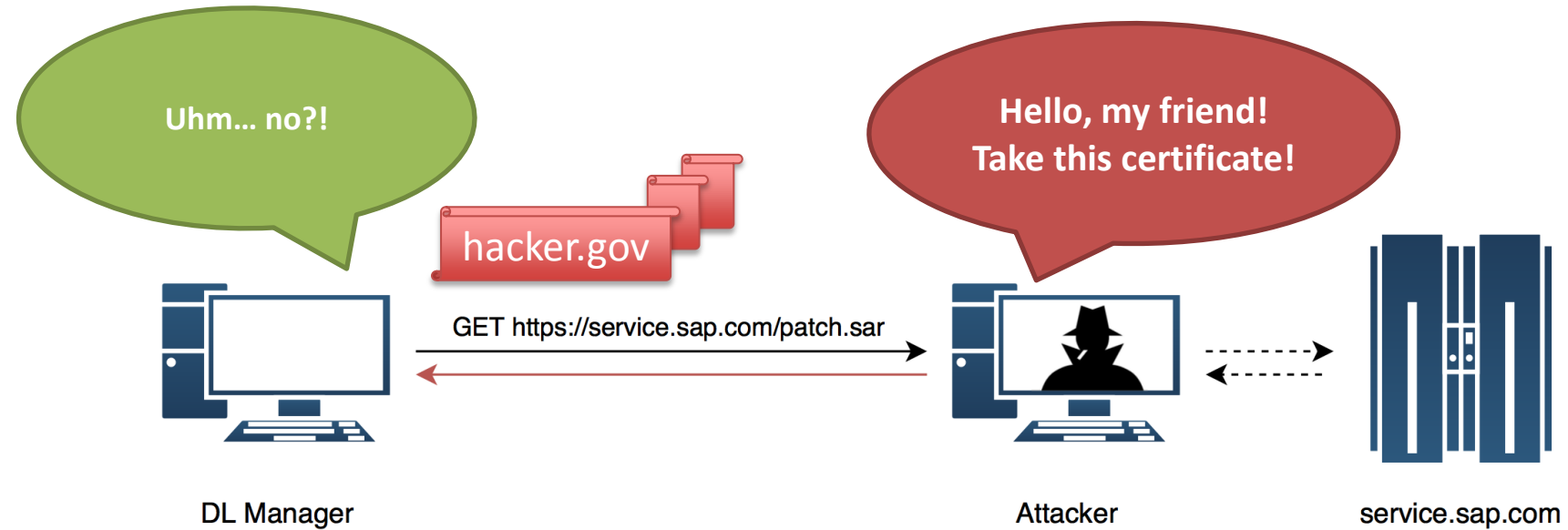
< Back Next > Cancel

SAP Patch : Note 2235412, Oct 2015

TLS in a Nutshell



TLS in a Nutshell



CVE-2014-3577

Vulnerability Details : [CVE-2014-3577](#)

org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.0.2 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "CN=" string in a field in the distinguished name (DN) of a certificate, as demonstrated by the "foo,CN=www.apache.org" string in the O field.

Publish Date : 2014-08-21 Last Update Date : 2015-10-28

DEMO

How does it work?

- String representation of distinguished name (RFC4514):

O=**SAP**,
OU=ABAP Security Unit,
CN=**service.sap.com**,
...

- You are not the owner of **service.sap.com**
 - A CA **won't issue** such a certificate for you!

How does it work?

■ What about this one?

O=**Hacker Inc.**,
OU=**CN=service.sap.com, Code network**,
CN=**hacker.gov**,
...

■ You are the owner of **hacker.gov**...

→ A CA **will issue** such a certificate for you!

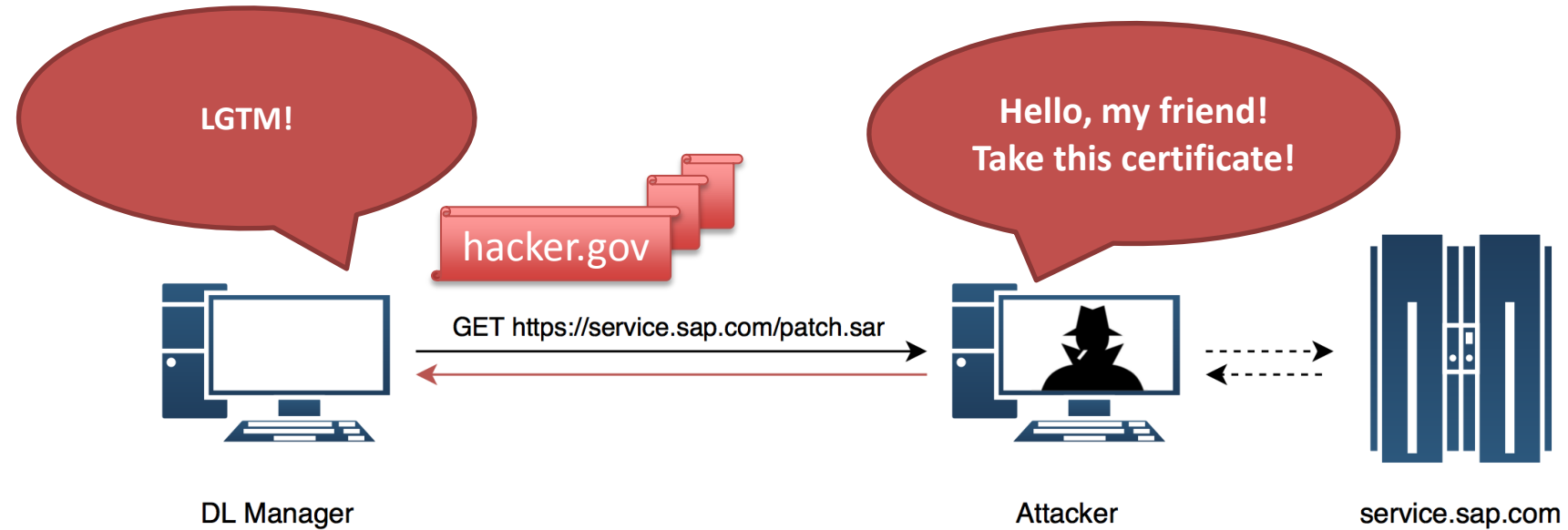
How does it work?

„O=Hacker Inc., OU=CN=service.sap.com, Code Network, CN=hacker.gov, ...“

- 1) Find „CN=“ and extract Value:
 - Value ← „service.sap.com“

- 2) Validate common name against domain name
 - Configured Value matches extracted Value!

TLS in a Nutshell



There is a Catch...

■ Preliminaries:

- Basic understanding of *ASN.1 (DER)* and *X.509* required

■ Constraints:

- Suitable CA*...
- Some cash required...

*issuing such certificates is not really a CA's fault!

Presence of the Vulnerability

- SAP Download Manager used *HttpClient* v4.0 since **08.2009**
- *CVE-2014-3577* was released **08.2014**
 - Apache HttpComponents HttpClient < 4.3.5
 - HttpAsyncClient < 4.0.2
- Vulnerability in SAP Download Manager was patched **11.2015**
- → Vulnerability **existed over 6 years...**
- → ...and **over 15 months after CVE release**

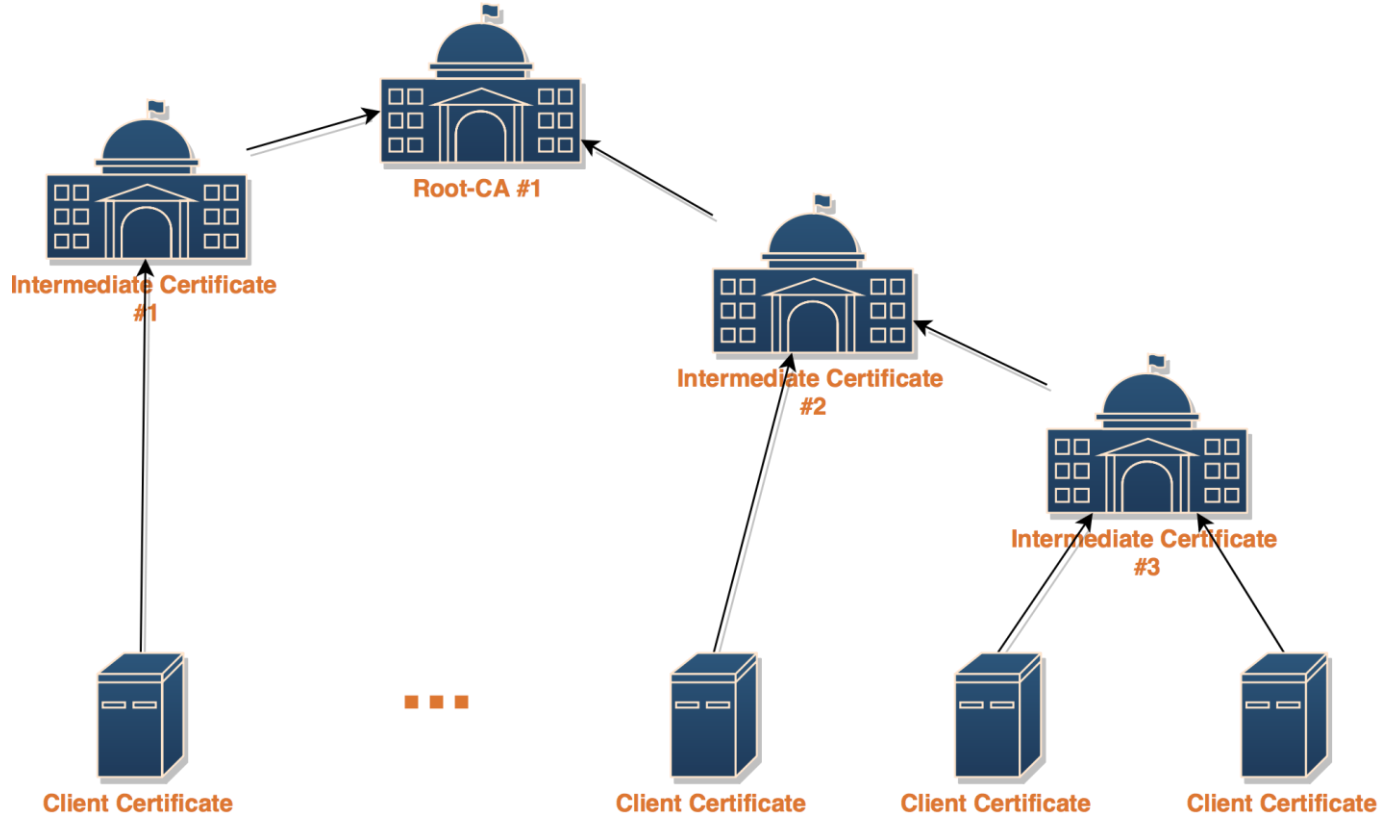
SAP Patch: Notes 2235412, 2282338

A Note on PKIs

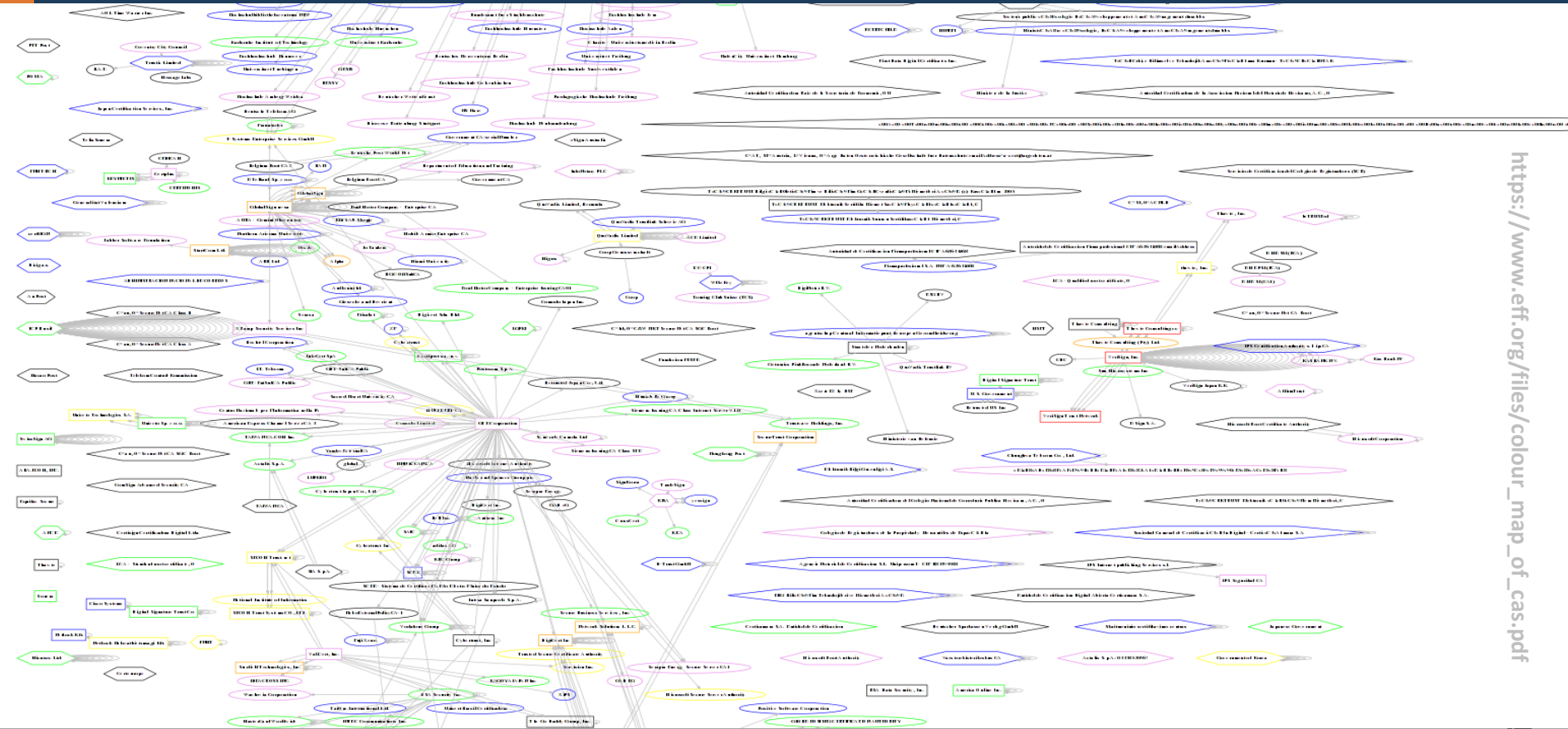
TLS is awesome, but...

...it may not solve all your problems!

A Note on PKIs - Imagination...



A Note on PKIs - Reality...



https://www.eff.org/files/colour_map_of_cas.pdf

A Note on PKIs



Look for: „Certificate Authority Collapse“

We **DO NOT SAY** that **any CA** might be vulnerable!

We **JUST SAY** that there are **over 650 of them*...**

*<https://www.eff.org/de/observatory>

Signatures to the Rescue

■ Usage of signatures

- Each SAP download package should be signed
- Signature must be validated with public key in application

■ Transmitting signed packages over TLS even better!

- Authentication*2 + Integrity*2 + Confidentiality

Signature Validation with SAPCAR

■ We took a quick look on *SAPCAR*, too

→ Signature checking „looks good“

■ How to invoke:

→ `.\sapcar.exe -tVvf <package.sar>`

■ Caution:

→ Not every package has a signature...

See SAP Note 2178665

Insecure Default (before September 2015)

Product	Download over HTTP?	Download over HTTPS (TLS)?	Packages digitally signed?
Microsoft Windows	No	Yes (Mandatory)	Yes (check mandatory)
Apple OS X	No	Yes (Mandatory)	Yes (check mandatory)
Ubuntu	Yes (Standard)	Yes (Optional)	Yes (check mandatory)
SAP	Yes (Standard)	Yes (Optional)	Yes (check <u>optional</u>)

checked 2015-03-03

State after September 2015

Product	Download over HTTP?	Download over HTTPS (TLS)?	Packages digitally signed?
Microsoft Windows	No	Yes (Mandatory)	Yes (check mandatory)
Apple OS X	No	Yes (Mandatory)	Yes (check mandatory)
Ubuntu	Yes (Standard)	Yes (Optional)	Yes (check mandatory)
SAP	No	Yes (Mandatory)	Yes (check <u>optional</u>)

checked 2015-03-03

5. Protocol downgrade // Arbitrary redirects (1)

Download Manager falls down to HTTP in case of insecure download locations

5	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401
6	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200
7	http://service.sap.com	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301
8	https://websmp101.sap-ag...	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401

HTTP/1.1 200 OK
Via: websmp110
Content-Length: 277
Content-Type: text/html
Server: Microsoft-IIS/7.0
Date: Wed, 07 Oct 2015 15:15:02 GMT

OBJID=011000358700000734382011E
DOWNLOAD_KA70025.SAR=http://service.sap.com/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT
SIZE=0000009676
TEXT=ABA Support Package 25 for 7.00
CLASSIFICATION=01100035870000000022
DESCRIPTION=ABA Support Package 25 for 7.00

5. Protocol downgrade // Arbitrary redirects (2)

The actual SAR packet (= the patch) is downloaded via HTTP !

5	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401
6	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200
7	http://service.sap.com	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301
8	https://websmp101.sap-ag...	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401

```
GET /~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT HTTP/1.1
Host: service.sap.com:80
Proxy-Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.0 (java 1.5)
```

5. Protocol downgrade → Visibility

Everyone sniffing web traffic will notice protocol downgrades

1	https://service.sap.com	GET	/~form/download_basket?_MODE=OBJECT_VERSION&OBJID=011000358700000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301	521	HTML	
2	https://websmp201.sap-ag...	GET	/~form/download_basket?_MODE=OBJECT_VERSION&OBJID=011000358700000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401	4237	HTML	
3	https://websmp201.sap-ag...	GET	/~form/download_basket?_MODE=OBJECT_VERSION&OBJID=011000358700000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	189	script	
4	https://service.sap.com	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301	557	HTML	
5	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401	4237	HTML	
6	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	422	script	
7	http://service.sap.com	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301	493	HTML	SAR
8	https://websmp101.sap-ag...	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401	4237	HTML	SAR
9	https://websmp101.sap-ag...	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	9909...		SAR
10	https://service.sap.com	GET	/~form/download_basket?_MODE=OBJECT_VERSION&OBJID=011000358700000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301	521	HTML	
11	https://websmp106.sap-ag...	GET	/~form/download_basket?_MODE=OBJECT_VERSION&OBJID=011000358700000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401	4237	HTML	
12	https://websmp106.sap-ag...	GET	/~form/download_basket?_MODE=OBJECT_VERSION&OBJID=011000358700000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	189	script	
13	https://service.sap.com	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301	557	HTML	
14	https://websmp207.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401	4237	HTML	
15	https://websmp207.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	422	script	

SAP Patch: Note 2235412, Oct 2015

6. Directory Traversal & extension control

Download Manager accepts filename + extension for local storage of downloaded package

5	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401
6	https://websmp110.sap-ag...	GET	/~form/download_basket?_MODE=DOWNLOAD_START2&OBJID=0110003587000...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200
7	http://service.sap.com	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	301
8	https://websmp101.sap-ag...	GET	/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	401

HTTP/1.1 200 OK

Via: websmp110

Content-Length: 277

Content-Type: text/html

Server: Microsoft-IIS/7.0

Date: Wed, 07 Oct 2015 15:15:02 GMT

OBJID=011000358700000734382011E

DOWNLOAD_KA70025.SAR=http://service.sap.com/~swdc/011000358700000734382011E/KA70025.SAR?_ACTION=DL_DIRECT

SIZE=0000009676

TEXT=ABA Support Package 25 for 7.00

CLASSIFICATION=01100035870000000022

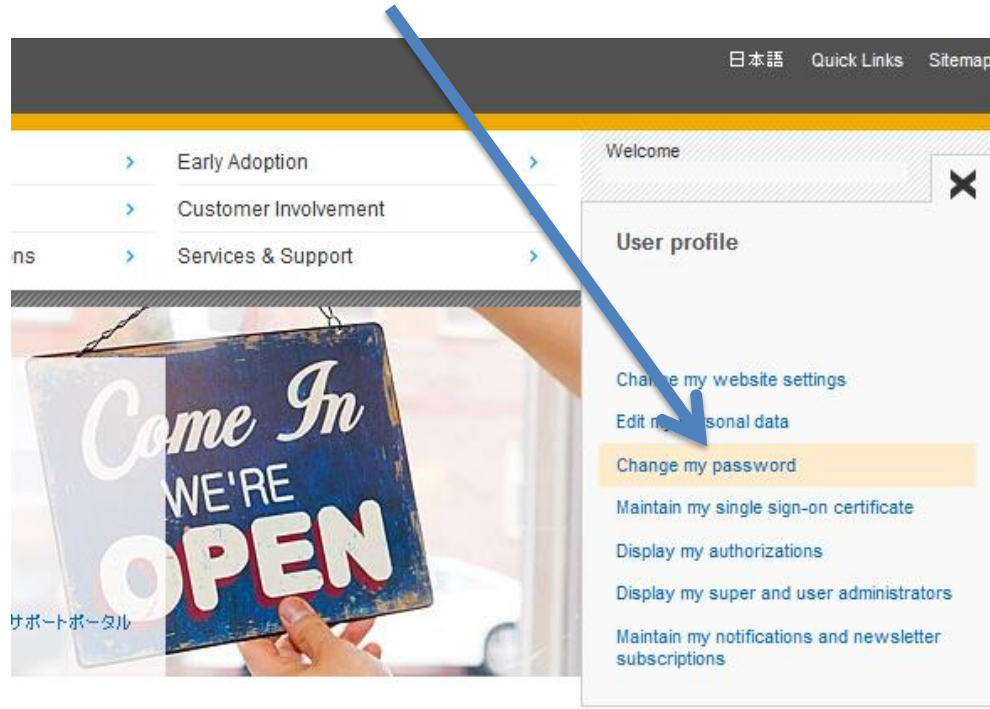
DESCRIPTION=ABA Support Package 25 for 7.00

SAP Patch: Note 2235412, Oct 2015

[Conclusions

Conclusion #1 - SMP Passwords

SAP Customers: Reset the password of your SAP SMP accounts used in Download Manager



Conclusion #2 - SMP Authorizations

SAP customers: Reduce the authorization objects of SMP accounts used in Download Manager

Authorization objects	
<input checked="" type="checkbox"/>	Close incidents
<input type="checkbox"/>	Display System Data
<input checked="" type="checkbox"/>	Display all incidents
<input checked="" type="checkbox"/>	Display incidents
<input type="checkbox"/>	Edit Authorizations
<input type="checkbox"/>	Edit System Data
<input type="checkbox"/>	Edit User Data
<input checked="" type="checkbox"/>	Edit all Login Data
<input type="checkbox"/>	Edit my Login Data
<input type="checkbox"/>	Manage Installations
<input type="checkbox"/>	Open Remote Connections
<input type="checkbox"/>	Register Object Keys
<input type="checkbox"/>	Register Object and Developer Keys
<input checked="" type="checkbox"/>	Report an incident
<input type="checkbox"/>	Request License Keys
<input type="checkbox"/>	Request License Keys (Partner)
<input type="checkbox"/>	Reserve Namespaces
<input type="checkbox"/>	SSL Certificate Administrator (Ordering and Renewing)
<input checked="" type="checkbox"/>	Send incidents to SAP
<input type="checkbox"/>	Service Reports and Feedback
<input checked="" type="checkbox"/>	Software download
<input type="checkbox"/>	Support Desk Evaluation

Save Cancel Reset

Only select „Software Download“

<input type="checkbox"/>	Service Reports and Feedback
<input checked="" type="checkbox"/>	Software download
<input type="checkbox"/>	Support Desk Evaluation

Conclusion

Transport security for software package distribution channels

- Costs next to nothing, easy to deploy (Let's encrypt)
- So many ways to make attacker's live hard:
certificate pinning, HSTS, TLS 1.2, PFS, ...
- Must be default if not mandatory

Digital signatures for software packages

- Adds trust to software packages
- Must be mandatory, especially for critical software as SAP

[BIZEC.org Joint SAP Security Research

Thank you for your attention.

Questions Now or later ?



Andreas Wiegenstein
@codeprofiler



Sebastian Schinzel
@seecurity

Damian Poddebniak
duesee_2x4e@mailbox.org

Disclaimer

© 2016 Virtual Forge GmbH and FH Münster. All rights reserved.

Information contained in this publication is subject to change without prior notice.

These materials are provided by Virtual Forge and FH Münster and serve only as information.

SAP, ABAP and other named SAP products and services as well as their respective logos are trademarks or registered trademarks of SAP SE in Germany and other countries worldwide.

All other names of products and services are trademarks of their respective companies.

Virtual Forge and FH Münster accept no liability or responsibility for errors or omissions in this publication. From the information contained in this publication, no further liability is assumed. No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Virtual Forge GmbH, Germany or FH Münster. The General Terms and Conditions of Virtual Forge apply.