Removing complexity layers in the UNICORE installation

Timo Strunk
Nanomatch GmbH

UNICORE Summit 2018
21.09.18

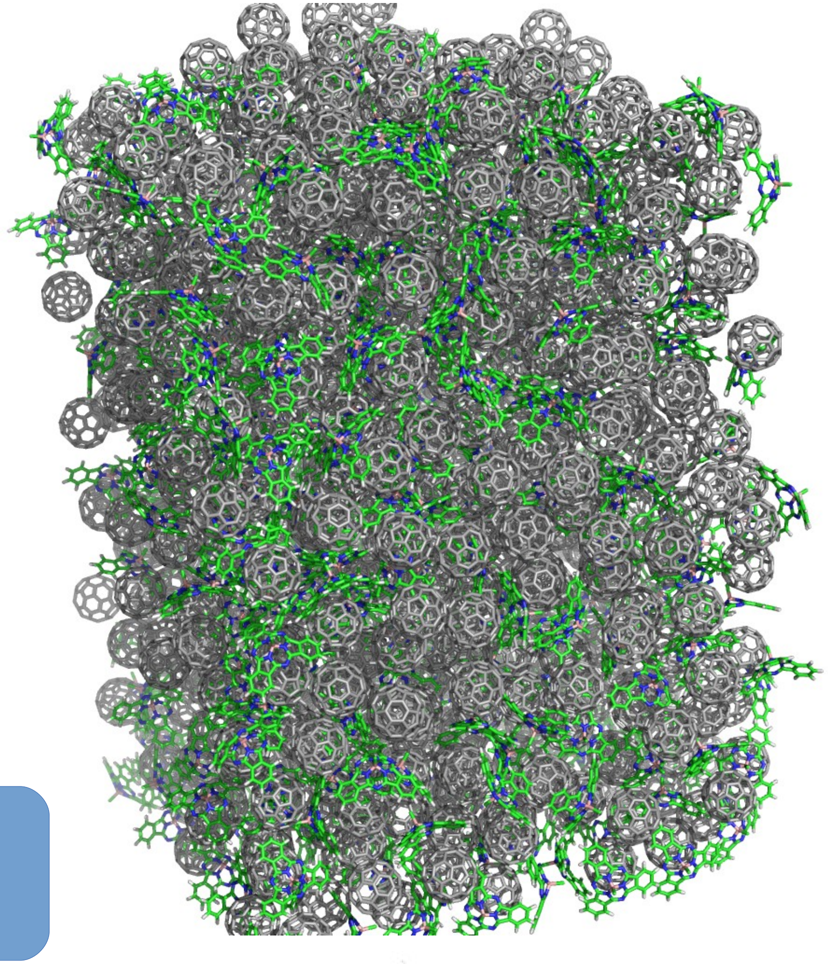
Removing complexity layers in the UNICORE installation

- Nanomatch GmbH
- Experience with UNICORE installations at our customers’ sites
- Goal of our installer
- UNICORE install complexity layers
- Demo

Nanomatch GmbH

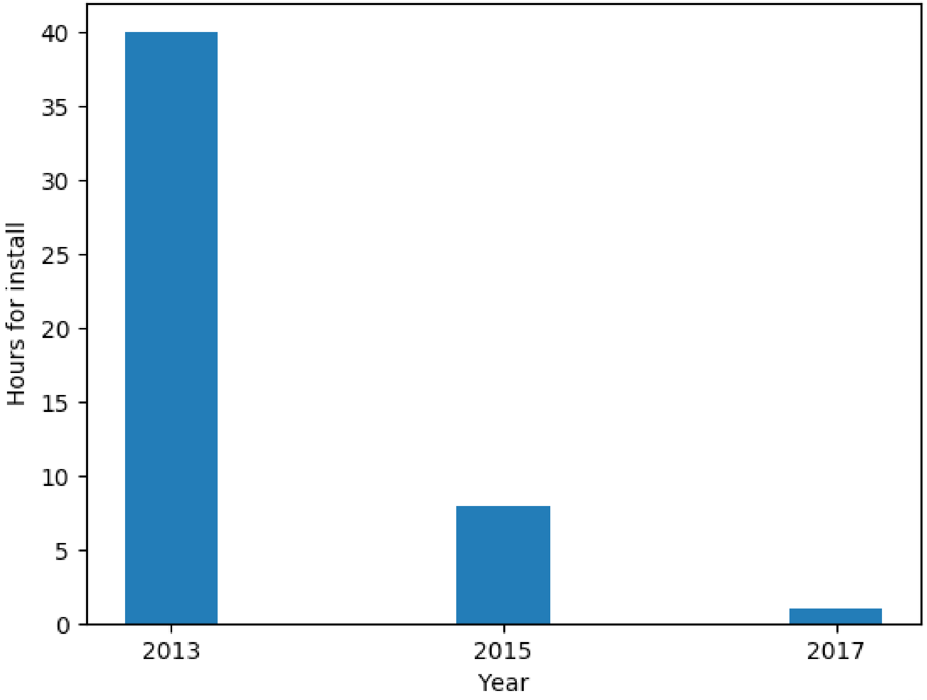
- We develop programs for the simulation of organic thin-films
  - OLED, OPV, OFET
- Our tools require a HPC architecture
  - 1 – 1000 cpus per job
  - 1 – 7 days runtime (of complete workflows)
  - In-House at the customers site

No cloud service possible
We have to release our software



Nanomatch GmbH

- UNICORE install was a big support burden
  - Nanomatch needs to be able to scale
  - Customers need to be able to install our software on their own
- We require a Grid API
  - Solutions of competitors:
    - Comsol targets all different queuing systems directly via ssh
    - Other software delivers their own workflow engine / middleware



Our goal in this talk

- We will tackle the easiest possible UNICORE installation.
  - Single Cluster, everything running on the headnode
  - REST API enabled
  - However:
    - No security issues allowed
    - No warnings allowed
- Before installing UNICORE a cluster operator knows
  - The hostname
  - The cluster’s authentication system (LDAP, Kerberos, Local)
  - The batch system (Torque, Slurm)
  - The file system layout / strategy

Our goal in this talk (2)

- We will tackle the easiest possible UNICORE installation.
  - Single Cluster, everything running on the headnode
  - REST API enabled
  - However:
    - No security issues allowed
    - No warnings allowed

Every security issue is a potential lawsuit

Every warning equals a support email

- Before installing UNICORE a cluster operator knows
  - The hostname
  - The cluster’s authentication system (LDAP, Kerberos, Local)
  - The batch system (Torque, Slurm)
  - The file system layout / strategy

Our goal in this talk (3)

- We will tackle the easiest possible UNICORE installation.
  - Single Cluster, everything running on the headnode
  - REST API enabled
  - However:
    - No security issues allowed
    - No warnings allowed

Every security issue is a potential lawsuit

Every warning equals a support email

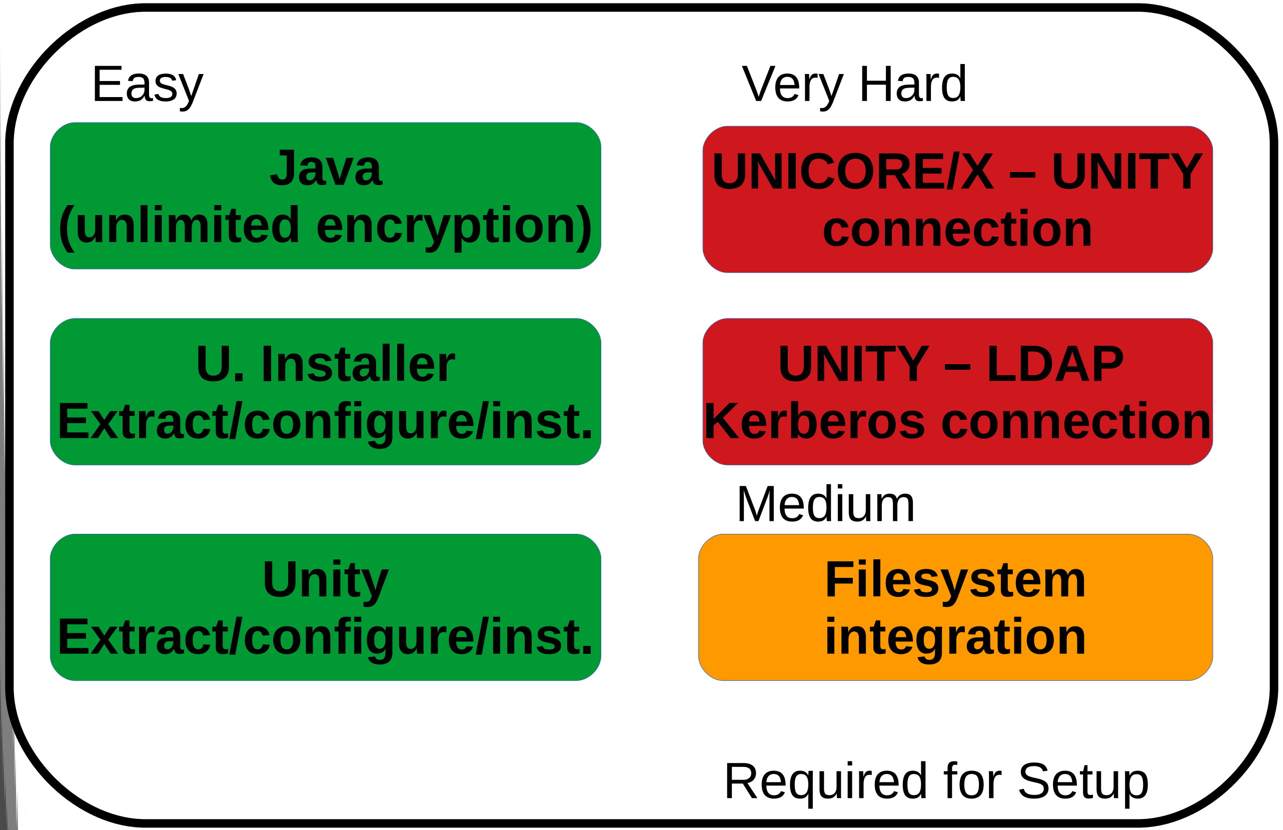
- Before installing UNICORE a cluster operator knows
  - The hostname
  - The cluster’s authentication system (LDAP, Kerberos, Local)
  - The batch system (Torque, Slurm)
  - The file system layout / strategy

Complexity Layers

- We will tackle the easiest possible UNICORE installation.
  - Single Cluster, everything running on the headnode
  - REST API enabled
  - However:
    - No security issues allowed
    - No warnings allowed
- Before installing UNICORE a cluster operator knows
  - The hostname
  - The cluster’s authentication system (LDAP, Kerberos, Local)
  - The batch system (Torque, Slurm)
  - The file system layout / strategy

- Convincing a cluster operator to actually install UNICORE is an uphill battle
  - Performance concerns
  - Security concerns
  - Learning a lot of new techniques required

Complexity Layers



Easy

Java (unlimited encryption)

U. Installer Extract/configure/inst.

Unity Extract/configure/inst.

Very Hard

UNICORE/X – UNITY connection

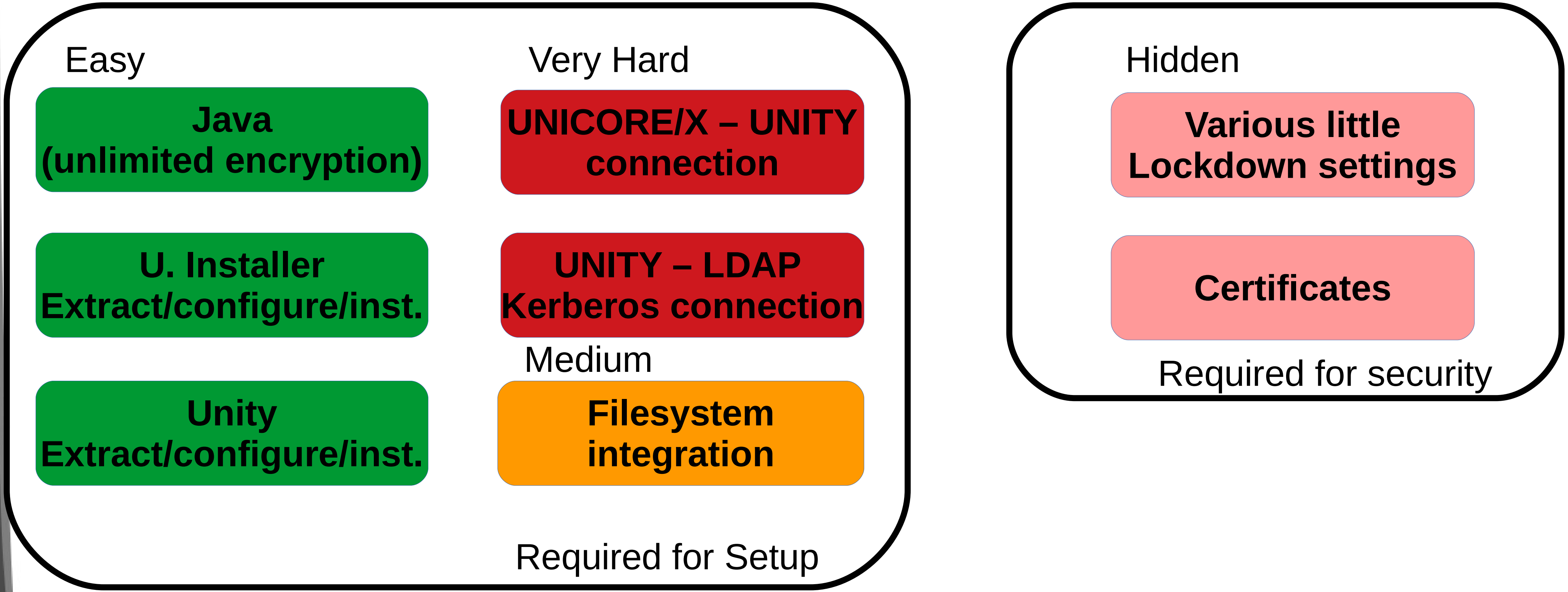
UNITY – LDAP Kerberos connection

Medium

Filesystem integration

Required for Setup

Complexity Layers



Easy

Java (unlimited encryption)

U. Installer Extract/configure/inst.

Unity Extract/configure/inst.

Very Hard

UNICORE/X – UNITY connection

UNITY – LDAP Kerberos connection

Medium

Filesystem integration

Required for Setup

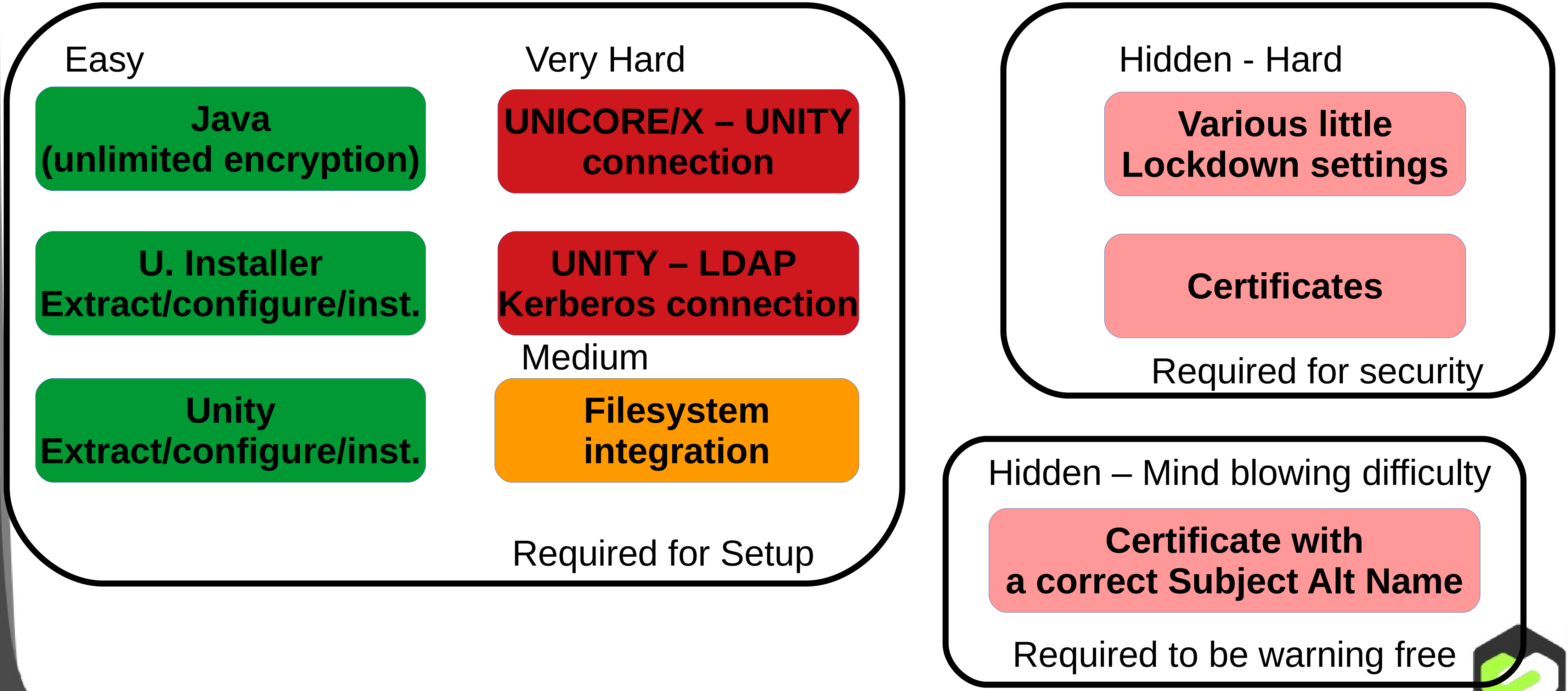
Hidden

Various little Lockdown settings

Certificates

Required for security

Complexity Layers



Easy

Java (unlimited encryption)

U. Installer Extract/configure/inst.

Unity Extract/configure/inst.

Very Hard

UNICORE/X – UNITY connection

UNITY – LDAP Kerberos connection

Medium

Filesystem integration

Required for Setup

Hidden - Hard

Various little Lockdown settings

Certificates

Required for security

Hidden – Mind blowing difficulty

Certificate with a correct Subject Alt Name

Required to be warning free

Complexity Layers

Very Hard

UNICORE/X – UNITY connection

You need to write two new VO config files and understand the architecture of Unity and its users and groups
Thx @ Krzysztof Benedyczak for writing this for me

You need to generate a new separate truststore for unity and give it to UNICORE/X.

UNITY – LDAP Kerberos connection

Quite involved and requires lots of knowledge of Unity if users should be transparently authenticated against LDAP.

Not required anymore if authentication should be done against local Linux users thanks to Krzysztof

Complexity Layers

Certificates

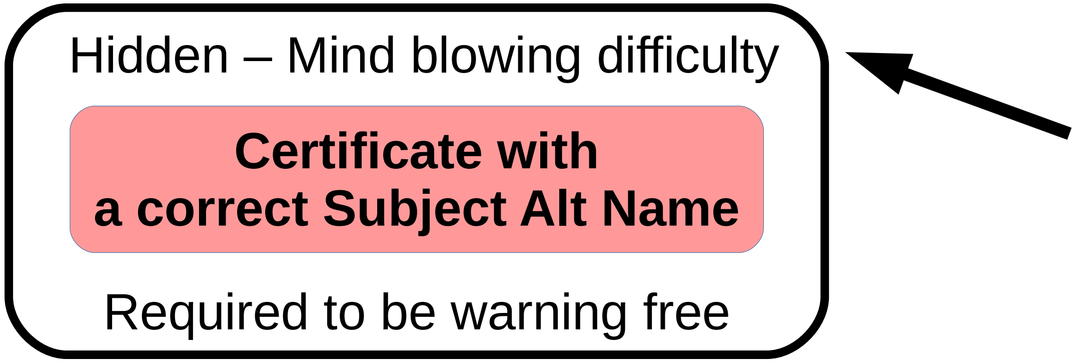
- You need to learn
  - How does a ‘good’ DN look for UNICORE?
  - Java keytool
  - Openssl
- Change all configuration files in the right places
  - Remember to turn on SSL in the TSI
- Demo certs and demo user have to be removed

Complexity Layers

Various little Lockdown settings

- A default jmxremote port is open and a default static password is set
  - This is a root exploit
  - Nobody I know closed these ports ever
  - Neither did we
- It's written in the hardening guide

Complexity Layers



Hidden – Mind blowing difficulty

Certificate with a correct Subject Alt Name

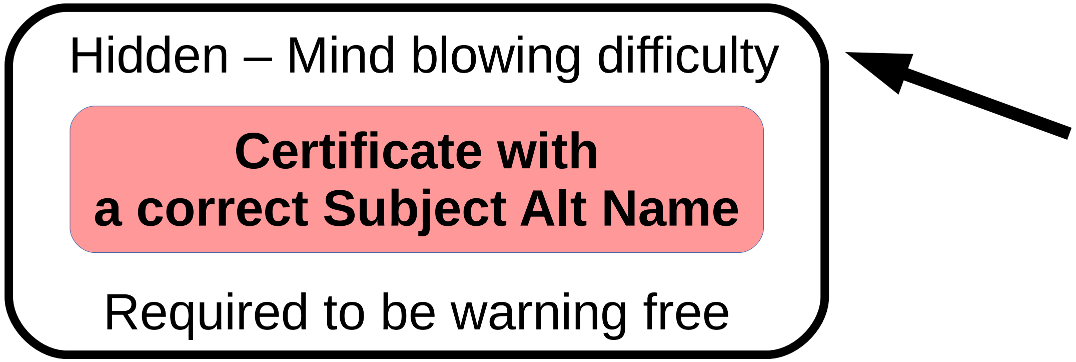
Required to be warning free

I had to read the official RFC document for X.509 certificates to get the correct version field in my certificates for Java to parse it correctly.

RFC 5280 - Excerpt

“This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2). If no extensions are present, but a UniqueIdentifier is present, the version SHOULD be 2 (value is 1); however, the version MAY be 3. If only basic fields are present, the version SHOULD be 1 (the value is omitted from the certificate as the default value); however, the version MAY be 2 or 3.”

Complexity Layers



Hidden – Mind blowing difficulty

Certificate with a correct Subject Alt Name

Required to be warning free

I had to read the official RFC document for X.509v3 certificates to get the correct version field in my certificates for Java to parse it correctly.

RFC 5280 – Excerpt – Translation:
The value of the version number of version 3 of X.509 certificates is 2
If you set a value of 3, Java will interpret it as version 1 and fail

The domain name should be encoded in the Subject Alt Name Extension of the certificate. It is not parsed anymore, if it is in a normal DN field.

Summary

- Change all configuration files in roughly 115 places
- Write two vo.config files
- Create 5-8 certificates

- We cannot expect our customers to do this on their own.

  → Installation has to be automated

Installer / Configurator

- BSD license
https://github.com/timostrunk/UNICOREDaemonCerts
- Generates all certificates with correct subject alt names
- Configures Unity to use PAM, i.e. the configured linux login to authenticate users without any additional configuration
- Can also use an existing CA by only generating certificate requests
- Number of warnings generated currently: Roughly 5
  - 2 deprecation warnings, 3 Unity default password warnings (which can be dismissed, because the default password is random)

Check

- Before installing UNICORE a cluster operator knows
  - The hostname
  - The cluster’s authentication system (LDAP, Kerberos, Local)
  - The batch system (Torque, Slurm)
  - The file system layout / strategy
- This is now actually sufficient to install UNICORE
  - You still have to spend some time configuring simpleidb though, but it contains only available limited information.

Conclusion

- With an introduction video it is now possible to install UNICORE on a single host in under 20 minutes
  - Secure for deployment and not only for development
  - Seamless authentication using PAM module (by Krzysztof)
- Outlook
  - We will integrate our installer in a CI system, which installs UNICORE multiple times a day
  - We will stress this installation with a perpetual workload

Acknowledgements

- Bernd Schuller & Björn Hagemeier & everybody in Jülich
  - An amazing amount of support and development
- Krzysztof Benedyczak
  - His excellent PAM integration
- You for listening