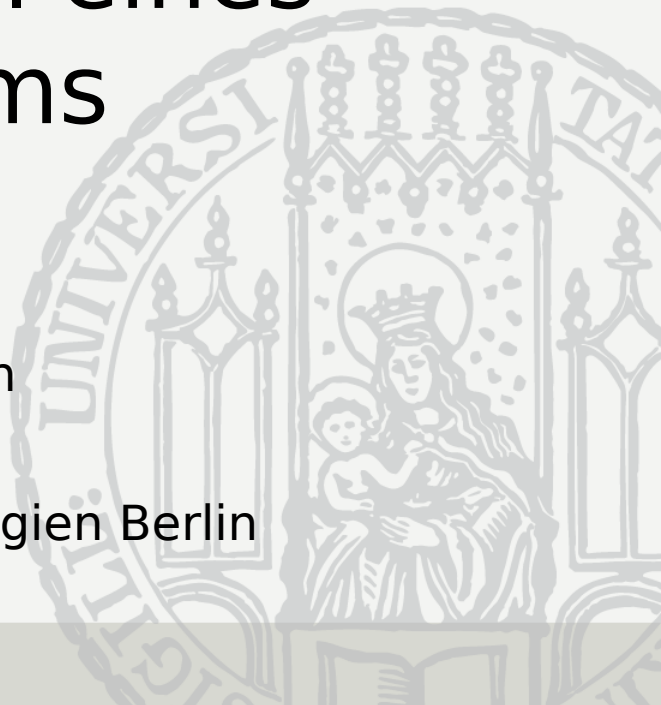
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Vollautomatisierte e-Learning Plattform am Beispiel eines Universitätspraktikums

- **Jan Schmidt**, Nils gentschen Felde
- MNM-Team
- Ludwig-Maximilians-Universität München

10. DFN-Forum Kommunikationstechnologien Berlin

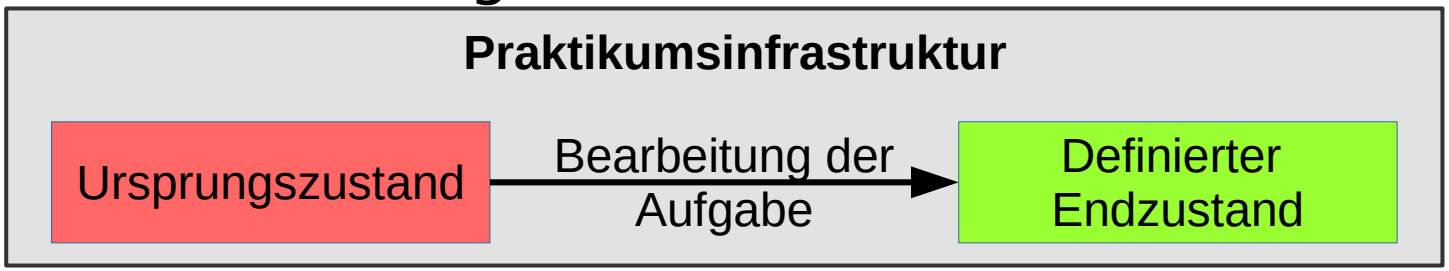


Themenverwandte Arbeiten

- Automated Grading
  - Automatische Korrektur von Programmieraufgaben
  - Input-Output überprüfuen
  - Code-Analyse
  - Abstract Syntax Tree (AST)
  - Unit-Testing
- Hacking Labs
  - Bereitstellung einer Infrastruktur
  - Challenges: Finden und Beheben von Sicherheitslücken
  - Zur Überprüfung der Lösungen aber Humaninteraktion notwendig
- Keine Automatismen zur automatisierten Überprüfung systemnaher Aufgaben

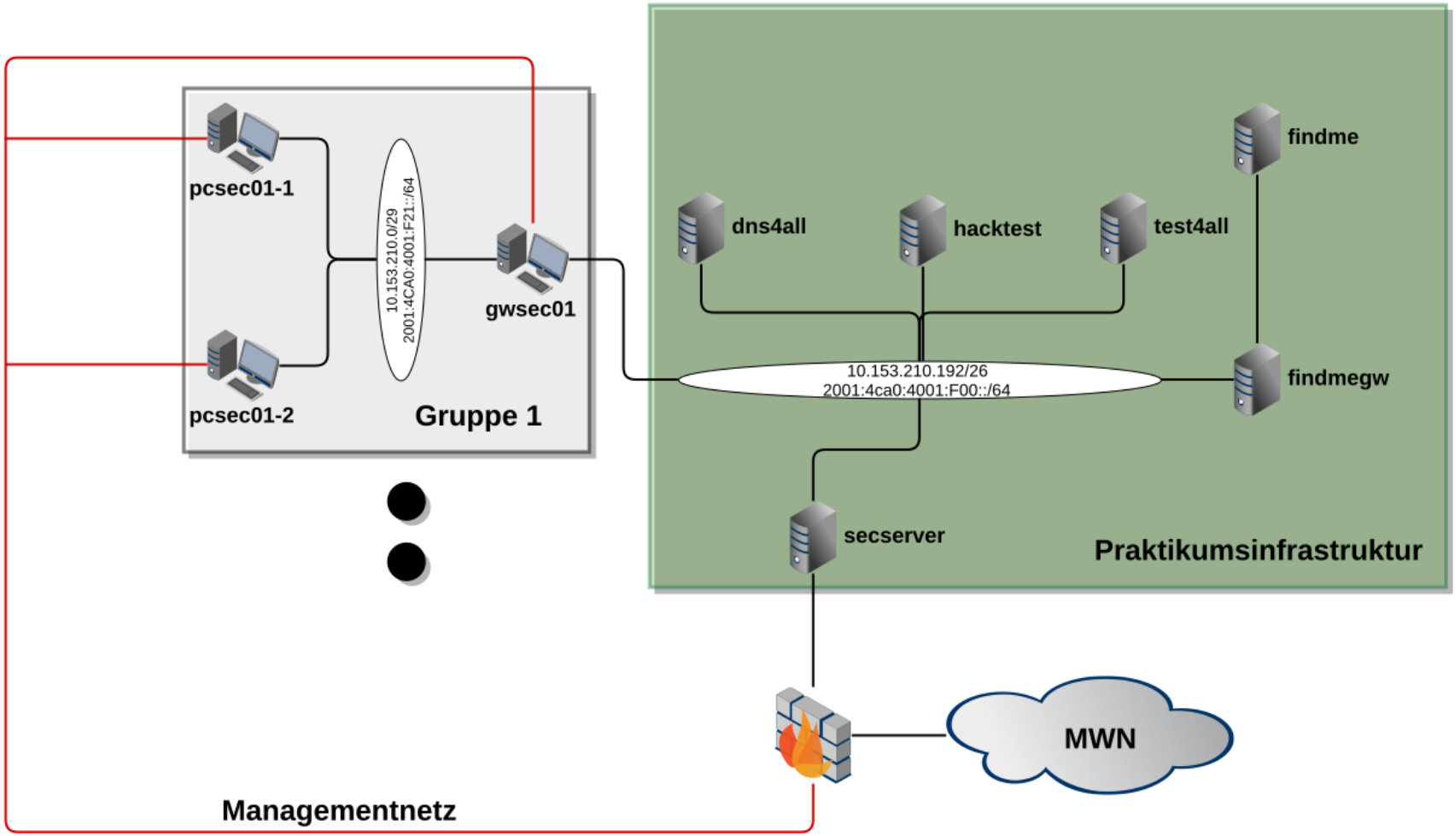
Problemstellung

- Im Gegensatz zu Programmieraufgaben kein AST o.Ä. für Systemzustand
- Überprüfung von Config-Files: nur syntaktische Korrektheit
- Praktikumsaufgabe als Zustandsautomat



- Überprüfung des Endzustands, nicht des Lösungswegs
- Endzustand muss zur Laufzeit überprüft werden

Praktikum IT-Sicherheit

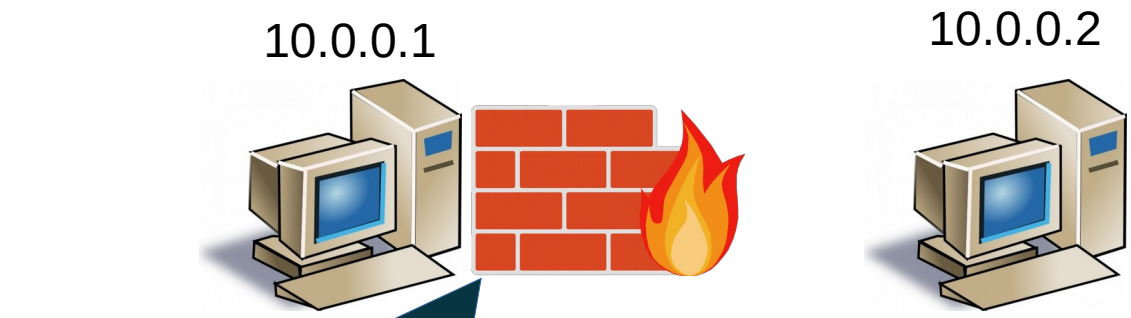


Beispielaufgabe

- Konfiguration einer statischen Firewall
- Whitelist
- Genaue Spezifikation der zu öffnenden Ports
- Mögliche Lösungswege:
  - Ferm
  - Iptables

Testroutine

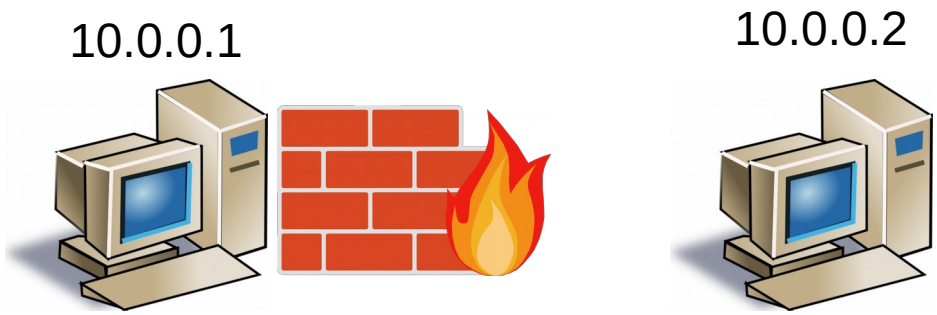
Ist UDP-Port 123 erreichbar?




```
-A INPUT     -p udp -m udp --sport 123 -j ACCEPT
-A INPUT     -p udp -m udp --dport 123 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 123 -j ACCEPT
-A OUTPUT -p udp -m udp --sport 123 -j ACCEPT
```

Testroutine

Ist UDP-Port 123 erreichbar?

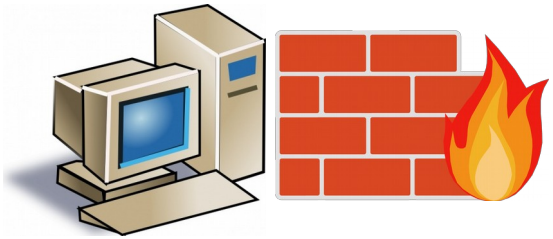



```
$ nc -lu -p 123
```

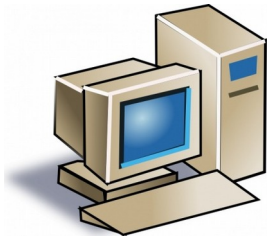
Testroutine

Ist UDP-Port 123 erreichbar?

10.0.0.1



10.0.0.2



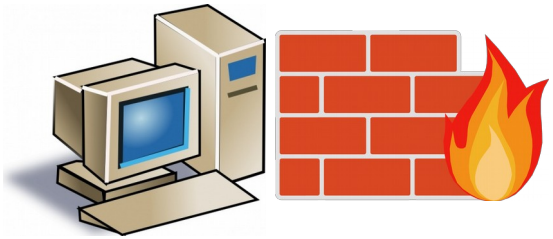
```
$ nc -lu -p 123
```

```
$ nc -u 10.0.0.1 -p 123
>> Hello World!
```

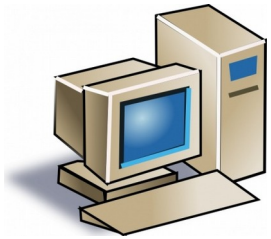
Testroutine

Ist UDP-Port 123 erreichbar?

10.0.0.1



10.0.0.2

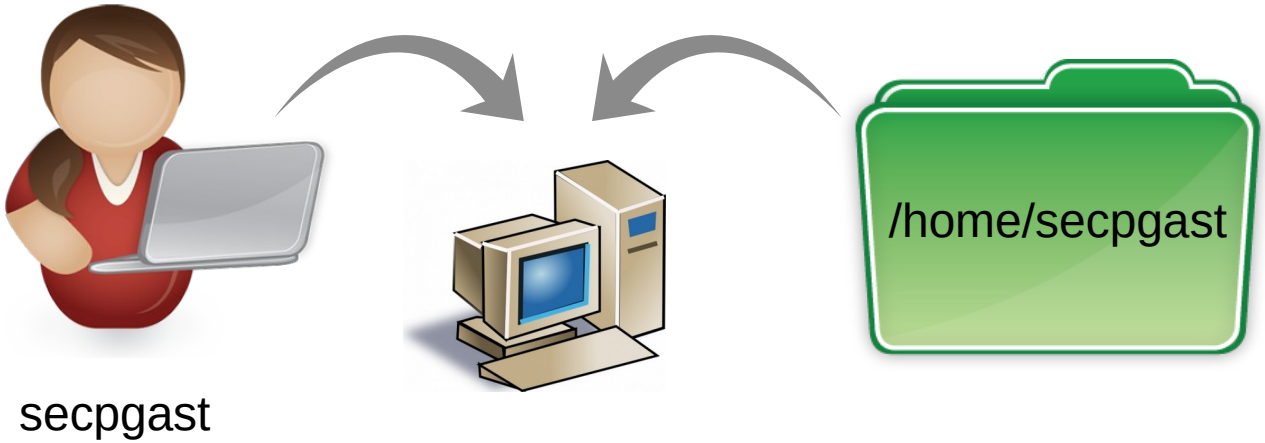


```
$ nc -lu -p 123
<< Hello World!
```

```
$ nc -u 10.0.0.1 -p 123
>> Hello World!
```

Beispielaufgabe

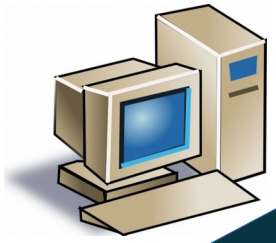
- Anlegen eines Nutzers
- Erstellen des entsprechenden Home-Verzeichnisses



Testroutine

Existiert der Nutzer?

10.0.0.1

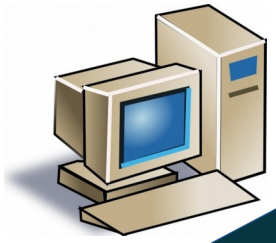


```
$ cat /etc/passwd | grep secpgast
```

Testroutine

Existiert der Nutzer?

10.0.0.1



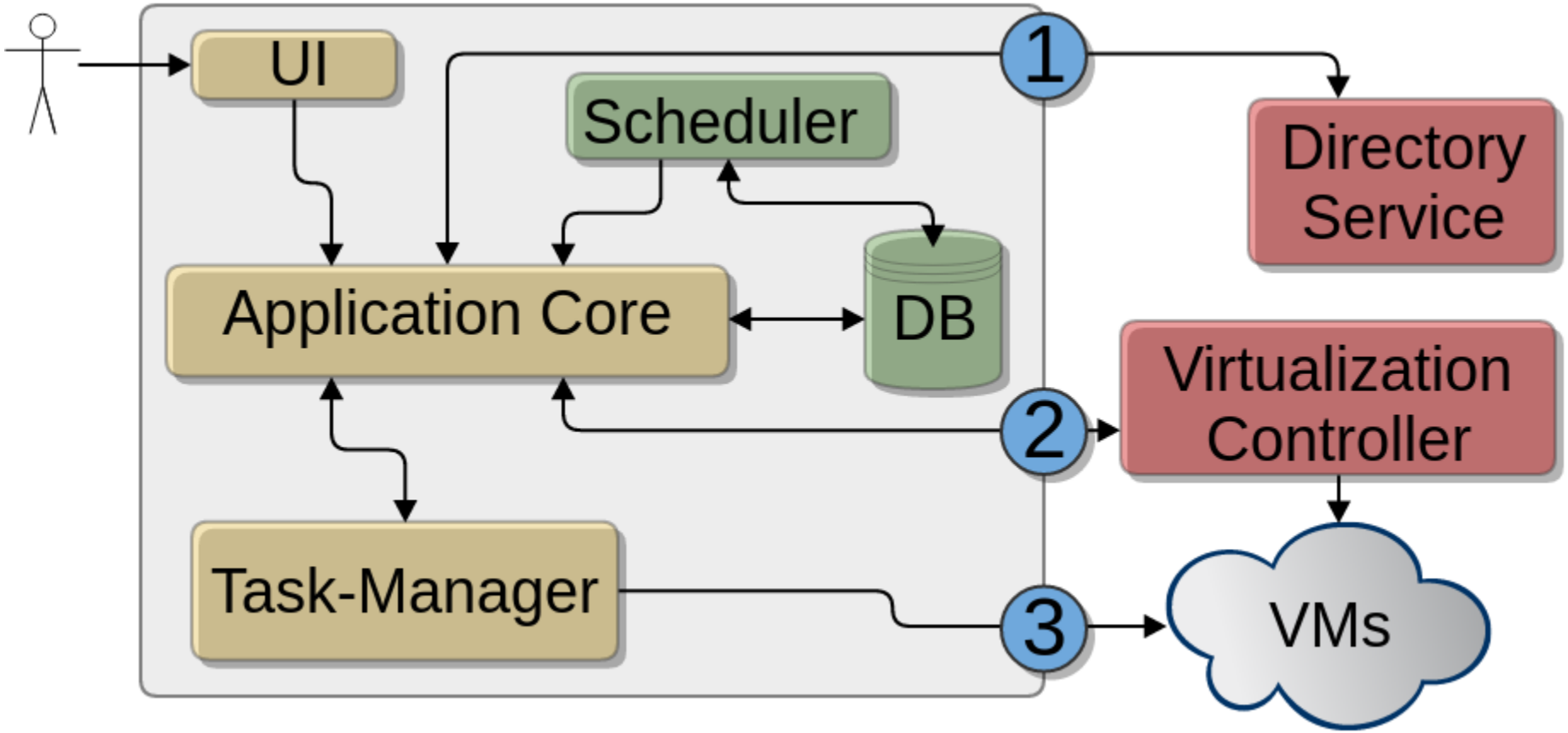
```
$ cat /etc/passwd | grep secpgast
secpgast:x:1000:1000:secpgast:/home/secpgast:/bin/bash
```

secpgast

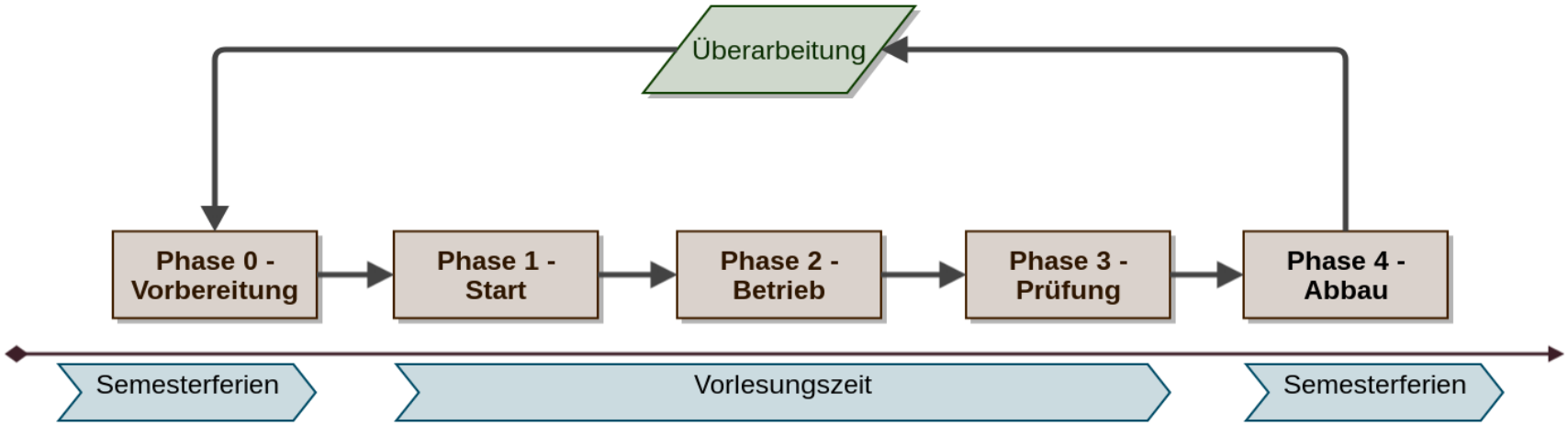
Aufgabenkategorisierung

- Komplexität der Testroutine abhängig vom Aufgabentyp
- Resultat
  - Interne Konfiguration
    - → Direkter Zugriff auf das zu testende System
  - Konfiguration eines externen Diensts
    - → Erreichbarkeit des zu testenden Systems
  - Programmieraufgaben
    - → Sichere Ausführungsumgebung, Spezifikation
  - Standardisierte Abgaben
  - Freie Abgabe

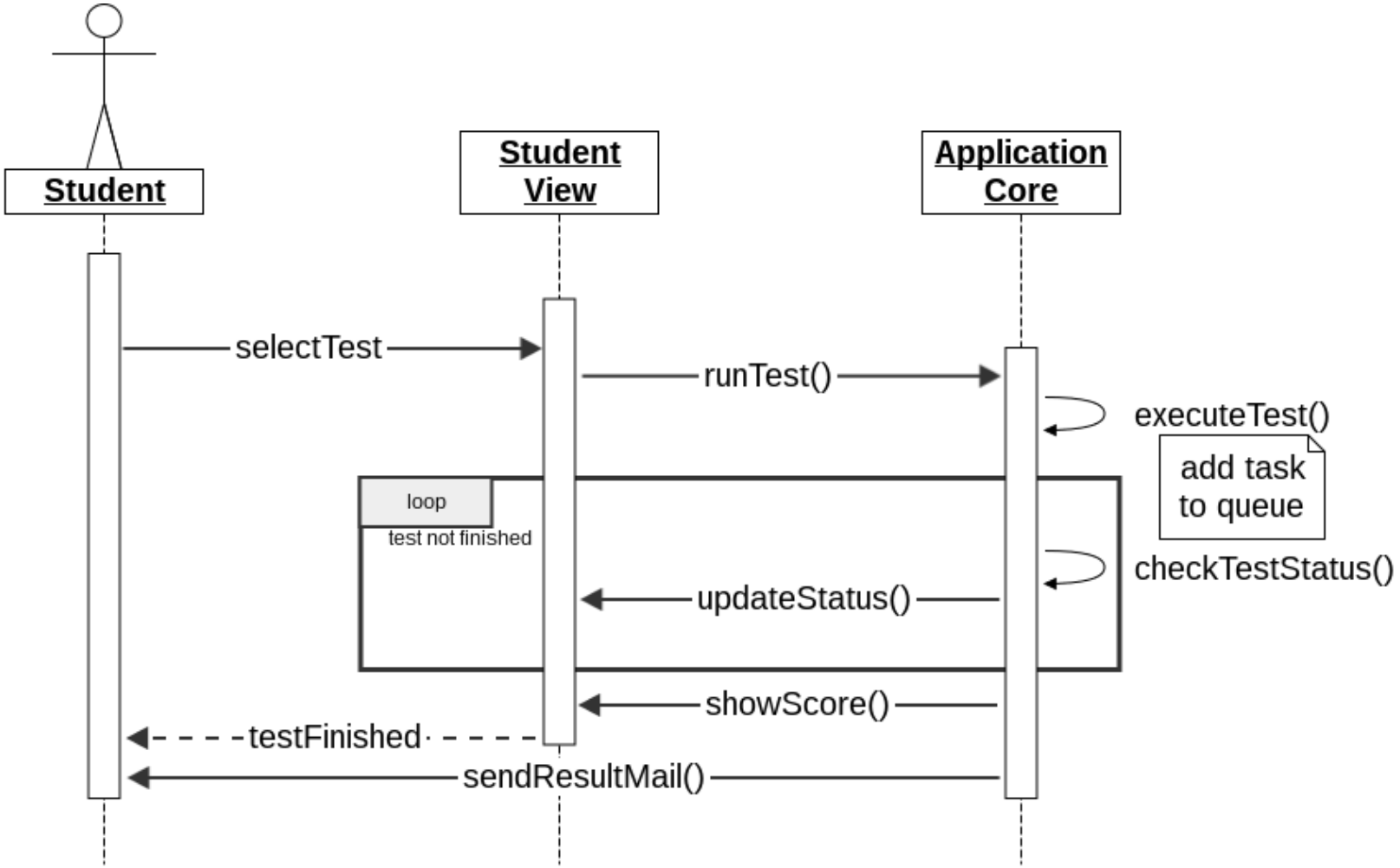
Erster Systementwurf



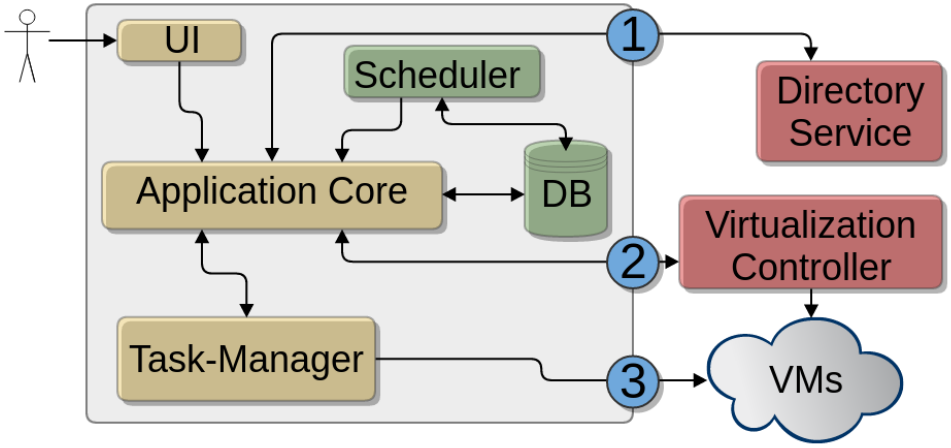
Praktikumslebenszyklus

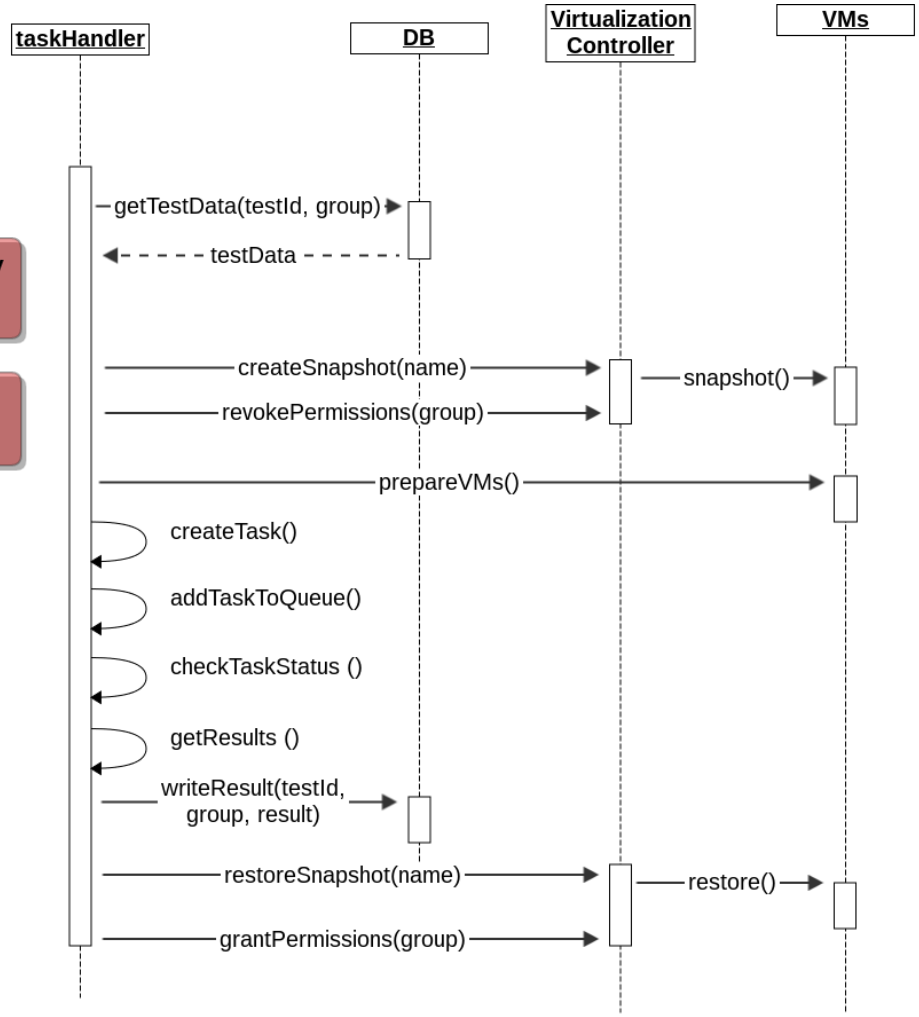


Ausführung eines Tests durch einen Studenten



Vorbereitung und Wiederherstellung der VMs

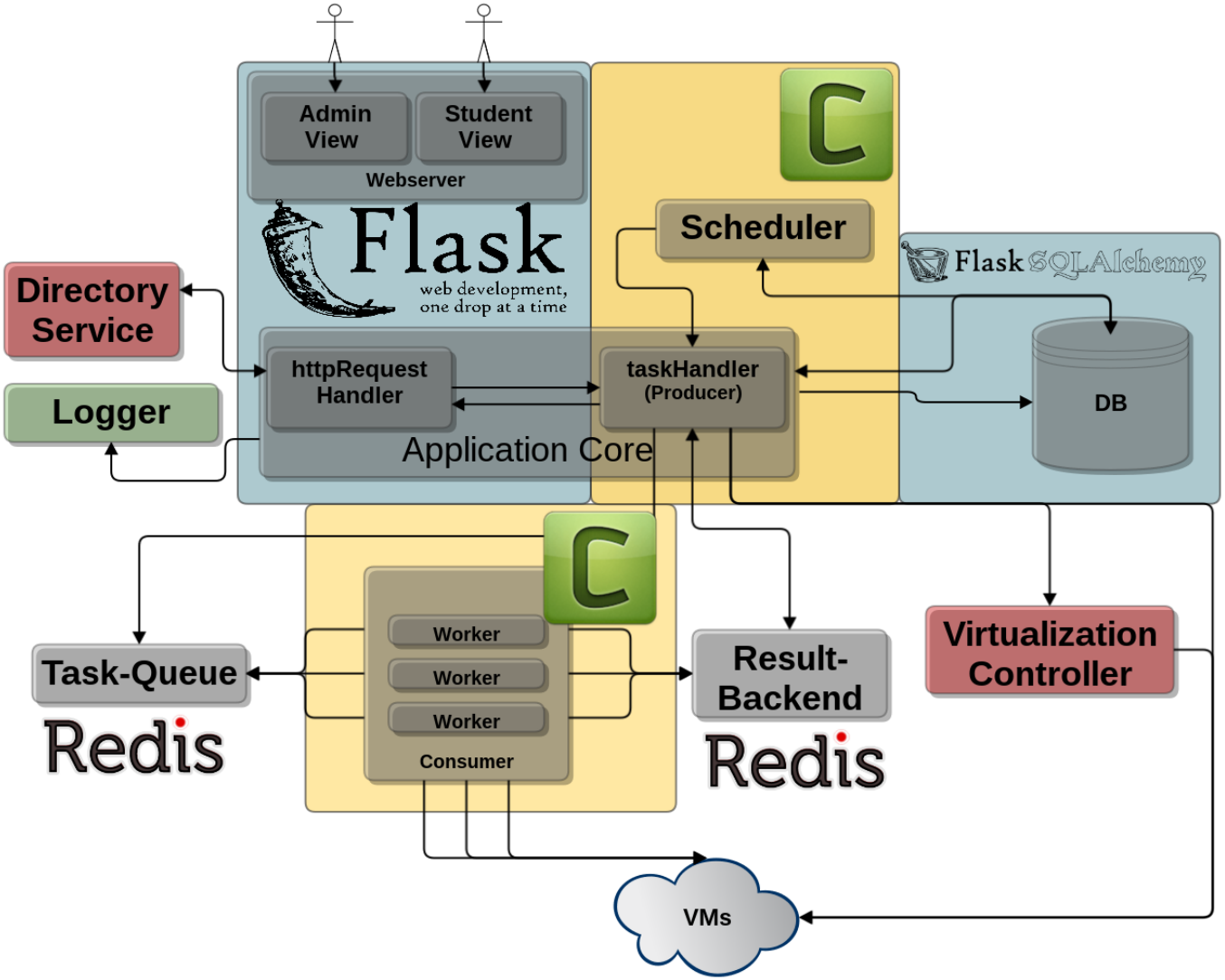




Implementierung

- Implementierung in Python
- Web-Anwendung mit Task-Management
- Verwendete Frameworks
  - Flask zur Entwicklung der Web-Anwendung
  - Objektorientierte Umsetzung des Datenmodells in SQLAlchemy (*Object Relational Mapper*)
  - Celery Task-Queue für Task-Management

Übersicht über die Implementierung



Status der Testausführung

Home - SecP-Unit ×

Willkommen Gruppe11

Blatt 4 Deadline: 2016-05-26 04:00:00

Run all Tests

Name	Beschreibung	Punkte
11g-OpenSSL	Erstellen Sie eine CRL unter /home/secpgast/Abgaben/11/crl.pem und Widerrufen Sie Ihr Zertifikat aus 11(c) und lasssen Sie sich den CRL Eintrag anzeigen.	3.0
11f-OpenSSL	Entfernen Sie das Passwort aus Ihrem Schlüssel und Speichern Sie ihn unter /home/secpgast/Abgaben/11/keys/11c.key.insecure.	1.0
11b-OpenSSL	Generieren Sie ein CSR für Ihren bestehenden CA-Schlüssel und speichern Sie das File auf dem Rechner pcsecXX-1 unter /home/secpgast/Abgaben/11/careq.csr. Lassen Sie sich sowohl die MD5, als auch die SHA1-Fingerprints Ihres Antrags ausgeben und speichern Sie diese Informationen unter /home/secpgast/Abgaben/11/private als cakey.md5 bzw. cakey.sha1.	3.0
11c-OpenSSL	Erstellen sie eine selbstsignierte X.509 Certificate Authority auf Ihrem Rechner pcsecXX-1. Beachten Sie die Hinweise auf dem Übungsblatt.	3.0
12b-Sichere-Webserver	Aktivieren Sie den Webserver auf dem Port 443/https. Stellen Sie dem Webserver ein Maschinen-Zertifikat signiert von Ihrer eigenen CA aus, damit diser sich autentisieren kann! Dieses Zertifikat sollte auf den Namen pcsecXX-2.secp.lab.nm.ifi.lmu.de ausgestellt sein, wobei Ihre IPv4- und IPv6-Adresse (eth1) ebenfalls im Zertifikat enthalten sein sollen.	3.0
11e-OpenSSL	Konvertieren Sie Ihr Zertifikat in das PKCS#12 Format und speichern Sie es als /home/secpgast/Abgaben/11/newcerts/11c.pkcs12. Verwenden sie 'SecPCert' als Passwort für das neue Zertifikat.	1.0
11a-OpenSSL	Erstellen sie eine selbstsignierte X.509 Certificate Authority auf Ihrem Rechner pcsecXX-1. Beachten Sie die Hinweise auf dem Übungsblatt.	3.0

30%
Creating snapshots...

https://secserver.secp-int.lab.nm.ifi.lmu.de/index <[1/1] 2%

Ergebnisse der Testausführung

Home - SecP-Unit ×

11c-OpenSSL	Erstellen sie eine selbstsignierte X.509 Certificate Authority auf Ihrem Rechner pcsecXX-1. Beachten Sie die Hinweise auf dem Übungsblatt.	3.0
12b-Sichere-Webserver	Aktivieren Sie den Webserver auf dem Port 443/https. Stellen Sie dem Webserver ein Maschinen-Zertifikat signiert von Ihrer eigenen CA aus, damit diser sich autentisieren kann! Dieses Zertifikat sollte auf den Namen pcsecXX-2.secp.lab.nm.ifi.lmu.de ausgestellt sein, wobei Ihre IPv4- und IPv6-Adresse (eth1) ebenfalls im Zertifikat enthalten sein sollen.	3.0
11e-OpenSSL	Konvertieren Sie Ihr Zertifikat in das PKCS#12 Format und speichern Sie es als /home/secpgast/Abgaben/11/newcerts/11c.pkcs12. Verwenden sie 'SecPCert' als Passwort für das neue Zertifikat.	1.0
11a-OpenSSL	Erstellen sie eine selbstsignierte X.509 Certificate Authority auf Ihrem Rechner pcsecXX-1. Beachten Sie die Hinweise auf dem Übungsblatt.	3.0

100%
Finished

Ergebnisse

Name	Erreicht	Fehlermeldung
11g-OpenSSL	3.0	**pcsec11-1**: 1.0
11f-OpenSSL	1.0	**pcsec11-1**: 1.0
11b-OpenSSL	3.0	**pcsec11-1**: 1.0
11c-OpenSSL	3.0	**pcsec11-1**: 1.0
12b-Sichere-Webserver	3.0	**pcsec11-1**: 1.0
11e-OpenSSL	1.0	**pcsec11-1**: 1.0
11a-OpenSSL	3.0	**pcsec11-1**: 1.0

https://secserver.secp-int.lab.nm.ifi.lmu.de/index <[1/1] 12%

Ergebnisse der Testausführung

Run all Tests

Name	Beschreibung	Punkte
1d-secpgast	Fügen Sie einen neuen Unix-Benutzer namens 'secpgast' hinzu. Achten sie darauf, dass auch ein entsprechendes Home-Verzeichnis angelegt wird.	2.0
1c-Root-Passwort	Ändern Sie das Root-Passwort all ihrer Rechner.	1.0

100%
Finished

Ergebnisse

Name	Erreicht	Fehlermeldung
1d-secpgast	0.0	**gwsec01**: No user named secpgast found! No home-dir found for secpgast. 0 **pcsec01-1**: No user named secpgast found! No home-dir found for secpgast. 0 **pcsec01-2**: No user named secpgast found! No home-dir found for secpgast. 0
1c-Root-Passwort	0.0	**gwsec01**: Login with [redacted] still possible! 0 **pcsec01-1**: Login with [redacted] still possible! 0 **pcsec01-2**: Login with [redacted] still possible! 0

Bewertung

- Herausforderung: hinreichende Fehlermeldungen
- Positives Feedback durch Studenten
- Verringerter Korrekturaufwand
- Automatisierung von 80% der Aufgaben im Praktikum IT-Sicherheit

Ausblick

- „Praktikum as a Service“
- Zeitraum frei wählbar
- Mehr Praktikumsplätze

Quelle: http://thoughtblender.blogspot.de/2011/02/thinking-as-service.html

Jan Schmidt
MNM-Team
Ludwig-Maximilians-Universität München
http://www.mnm-team.org/~schmidtja