TOWARDS DISTRIBUTED EVENT-DRIVEN MONITORING ARCHITECTURE

TEZE DISERTAČNÍ PRÁCE

Daniel Tovarňák

LABORATOŘ SOFTWAROVÝCH ARCHITEKTUR A INFORMAČNÍCH SYSTÉMŮ (LASARIS)

Monitoring (distrib. infrastruktury)

- *Průběžný a systematický sběr, analýza a vyhodnocení dat souvisejících se stavem a **chováním** jednotlivých komponent dané infrastruktury.*

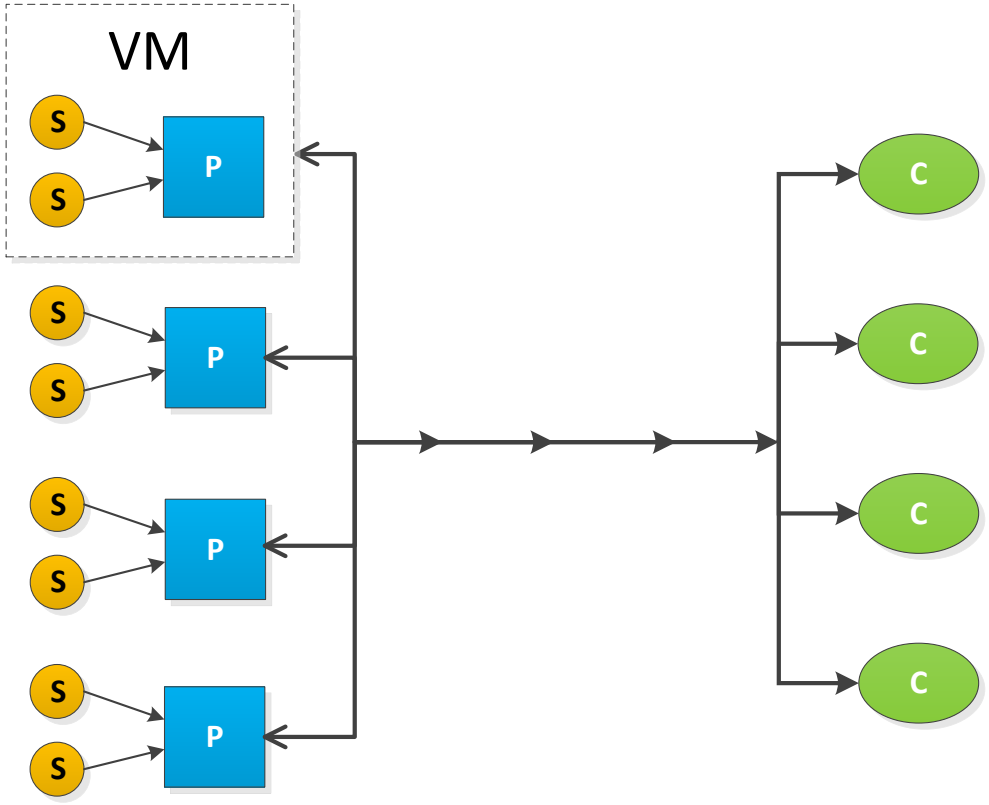
- **Cloud computing**
- Podnikové (univerzitní) sítě
- Internet of Things
- Smart Grid

- Obrovské množství aplikací (Audit – Job Scheduling)

Monitoring (distrib. infrastruktury)

- Až 1MB/s z jednoho virtuálního stroje (řád 10-100)

- *Generování*
- *Produkce*
- *Distribuce*
- *Konzumace*
- *Zpracování*



Cíl – monitoring chování

- (Automatizovaný) sběr, zpracování a analýza monitorovacích dat o chování **obrovského množství** distribuovaných entit
  - Operační systém, Aplikace, Web server, Dávkový úkol (job)
- Detekce vzorů chování v **reálném čase**
- **Nízké zatížení** monitorovaných strojů
- Nízké zatížení sítě
- Podpora **více konzumentů** současně

Vzor chování – příklad

- generate alert **if:** password-cracking-attack on 10+ hosts in 5 minutes

- password-cracking-attack: 100+ login-attempts in 30 secs

- Detekce DDoS
- Sledování SW aktualizací
- Výkonnostní špičky

Logování

- *Logy jsou typicky jediný způsob jak získat informace o chování monitorovaného zdroje [Stearley].* **Jsou ovšem krajně nevhodné pro automatizované zpracování.**

- Jsou generovány nekonzistentně, postrádají sémantiku, a především používají nestrukturovaný datový formát s informacemi **v přirozeném jazyce**.

- **REGULÁRNÍ VÝRAZY** představují **neúměrné zatížení** při použití pro velké objemy vysoce proměnlivých logů.

- **Interoperabilita** je výrazně omezena

Sběr a zpracování

- Centralizovaně (např. periodické dotazování)
  - Omezená škálovatelnost, neúměrné zatížení
- Selektivně (např. Publish-subscribe)
  - Zpracování je stále centralizované
- Distribuovaně (např. Hadoop Distributed File System)
  - Vysoká latence (~5 minut)

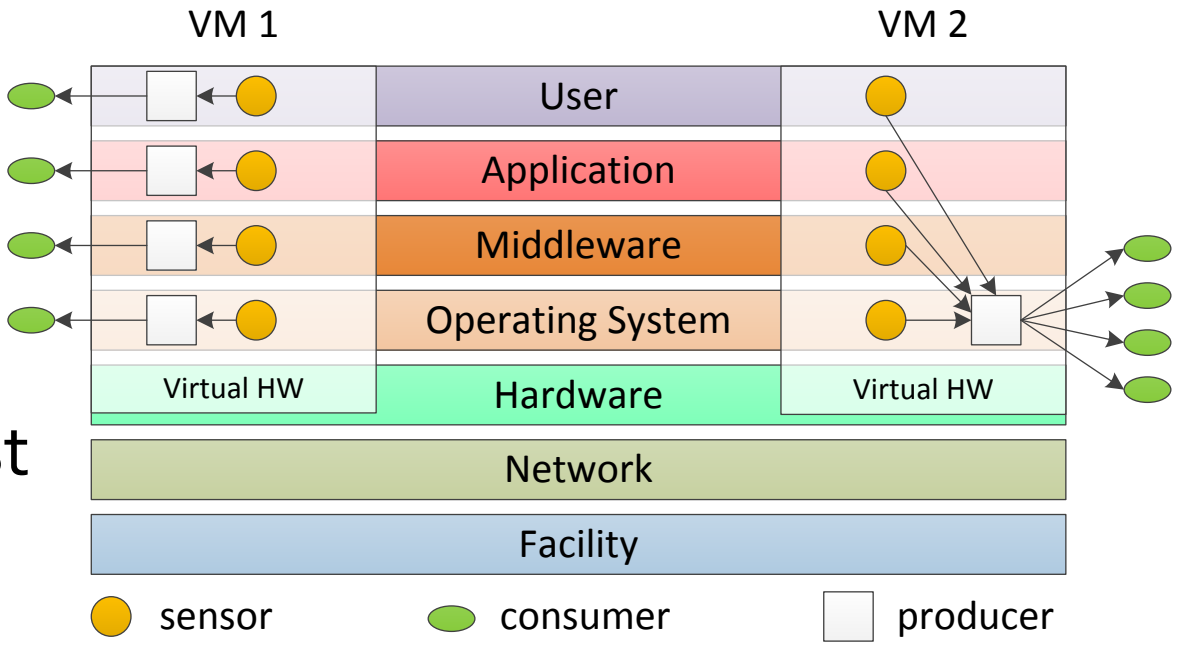
Distribuovaný sběr a zpracování

- Tradiční databázové systémy jsou nevhodné pro **trvalé dotazy** (continuous queries)
- Systémy pro zpravování proudů dat (DSMS) nepodporují **detekci vzorů**
- Techniky a algoritmy pro **zpracování komplexních událostí** (CEP) můžou být řešením.
- Distribuované varianty potřebují vylepšit pro potřeby inteligentního **monitoringu chování.** (kombinace s publish-subscribe)

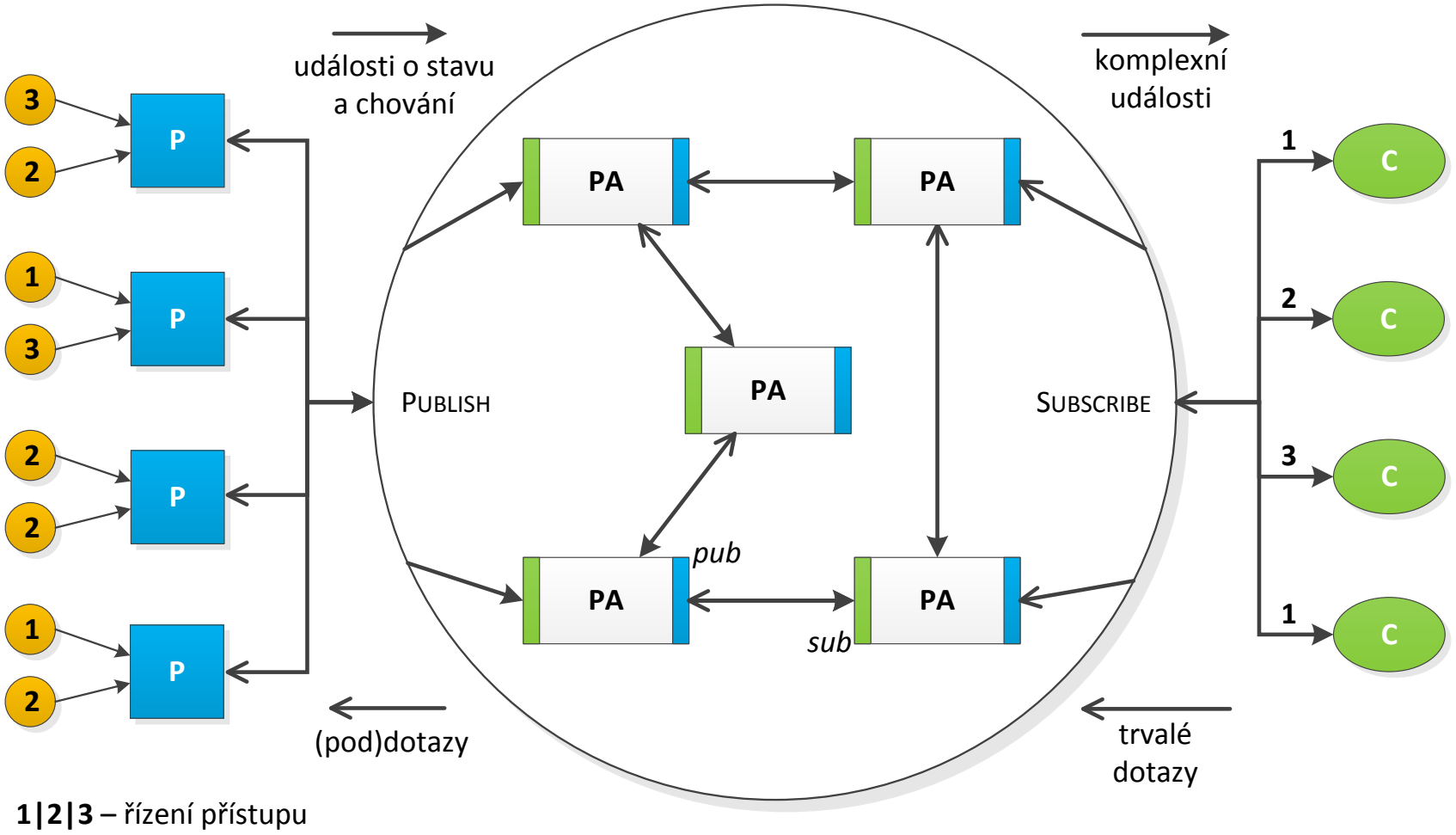
Podpora více konzumentů

- *Možnosti pro detekci incidentů a jejich následnou analýzu jsou pro uživatele cloud služeb extrémně omezené [Grobauer and Schreck]*

- Souběžnost
- Izolace
- Integrita
- Nepopiratelnost

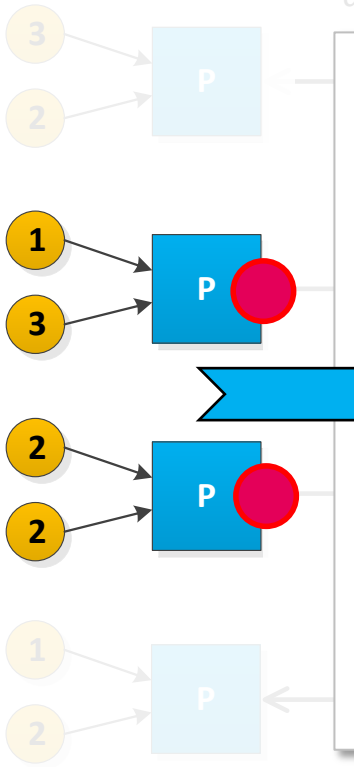


Navrhované řešení – nový mon. model



1|2|3 – řízení přístupu

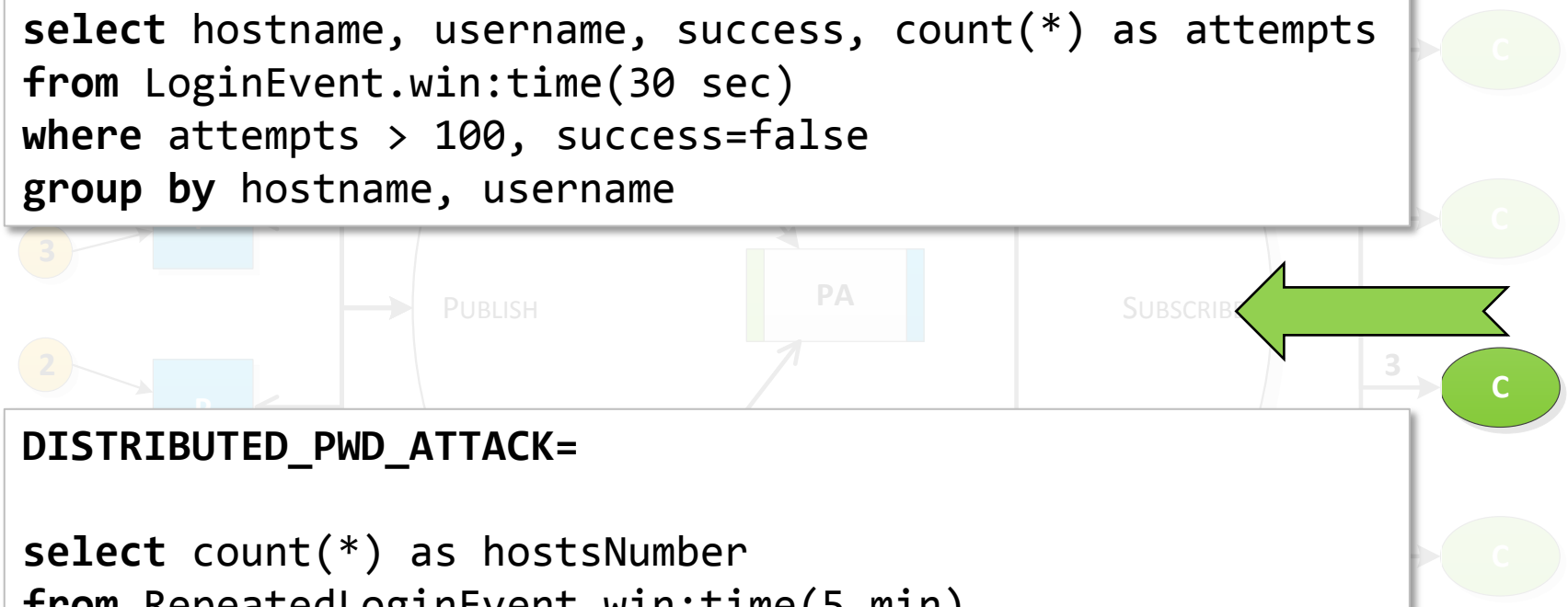
Navrhované řešení – nový mon. model




```
{'SimpleEvent':{
        'occurrenceTime':'2012-04-11T08:25:13.129Z',
        'hostname':'lykomedes.fi.muni.cz',
        'entity':'org.openssh.sshd.SERVER',
        'type':'org.openssh.LOGIN_EVENT',
        'http://openssh.com/v6.1/events.jsch':{
                'user':'xtovarn',
                'success':'false'
                'sourceIP': 147.165.0.86
                'port':22
        }
}}
```

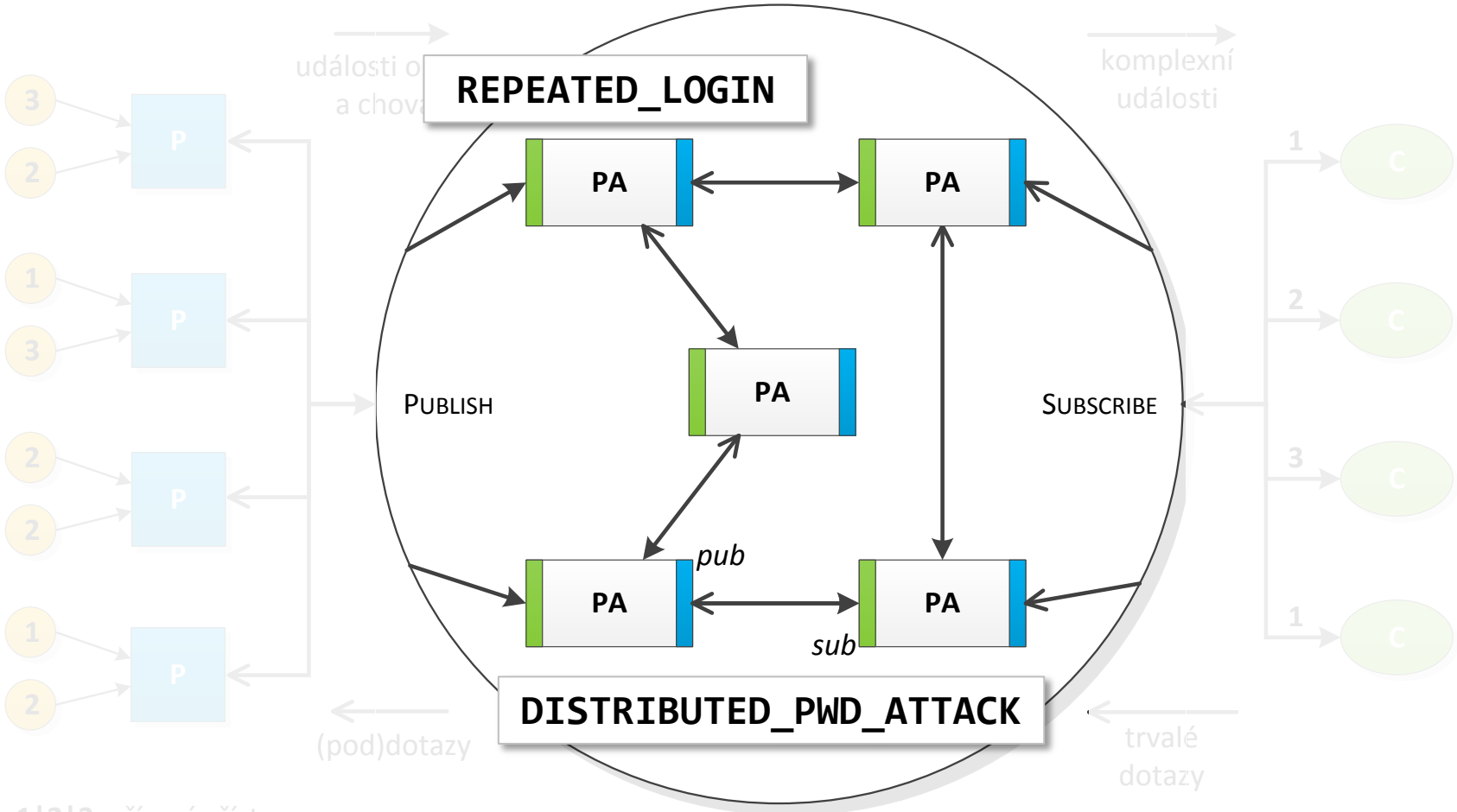
Navrhované řešení – nový mon. model

```
REPEATED_LOGIN=

select hostname, username, success, count(*) as attempts
from LoginEvent.win:time(30 sec)
where attempts > 100, success=false
group by hostname, username
```

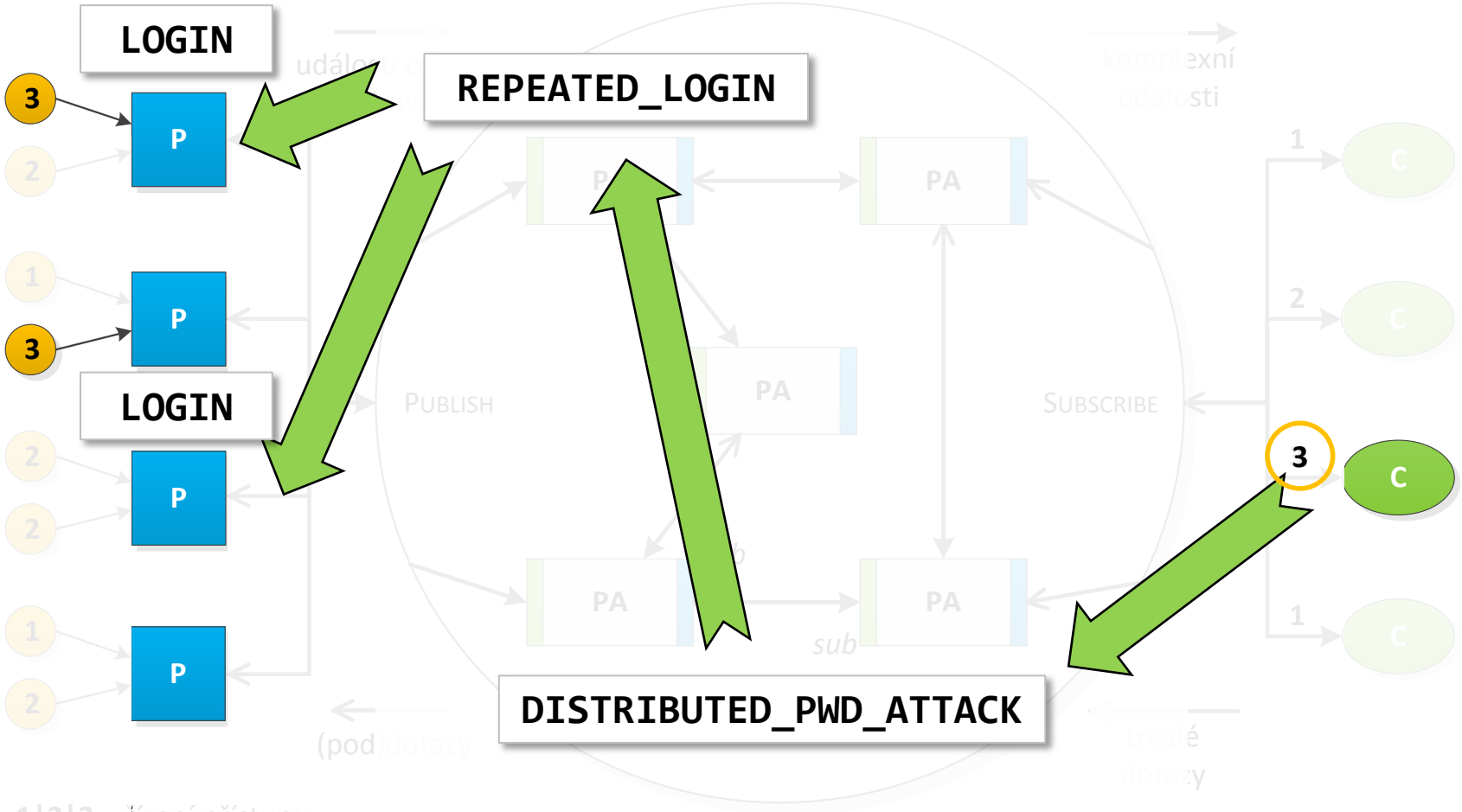



```
DISTRIBUTED_PWD_ATTACK=

select count(*) as hostsNumber
from RepeatedLoginEvent.win:time(5 min)
where hostsNumber > 10
group by hostname
```

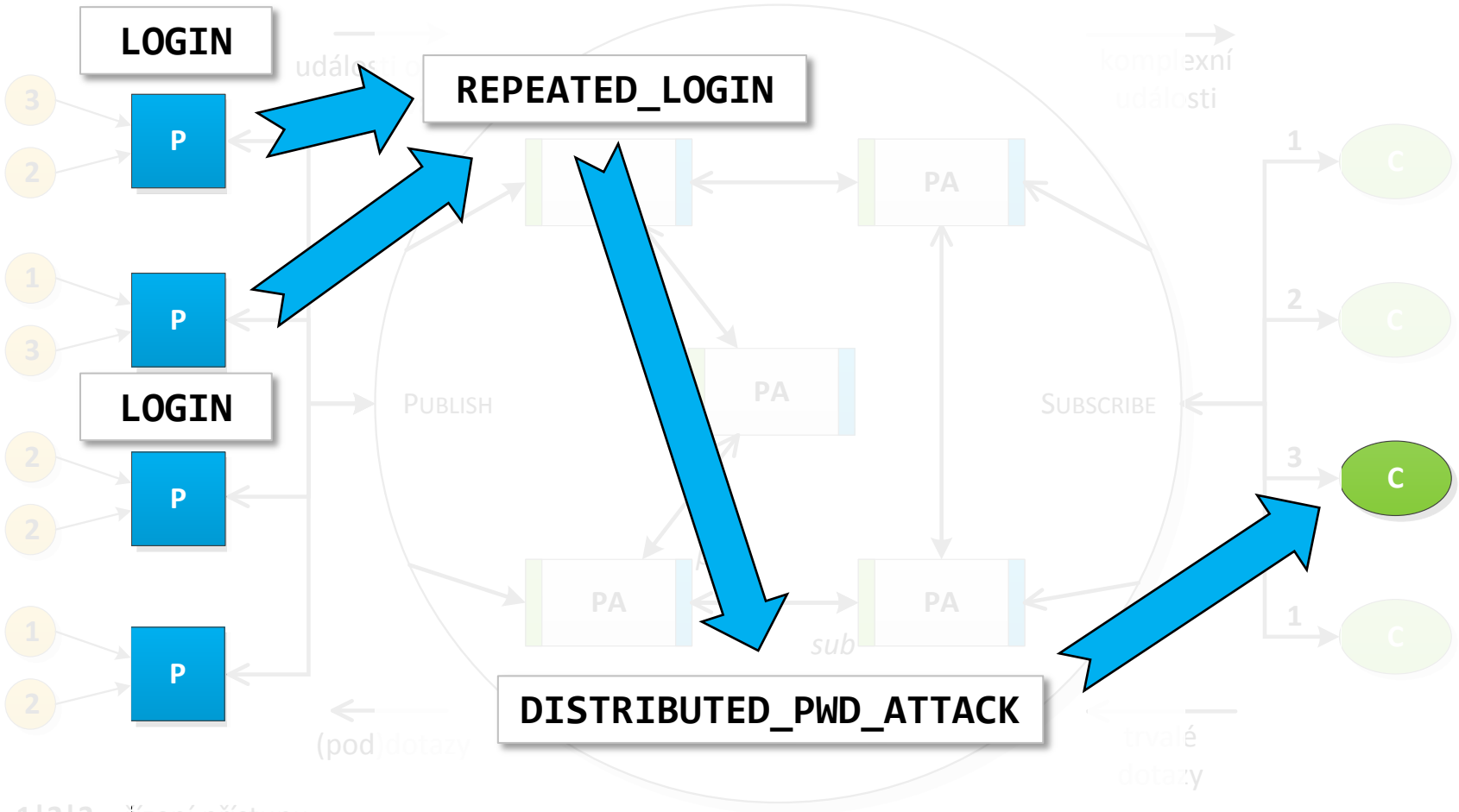
Navrhované řešení – nový mon. model



Navrhované řešení – nový mon. model

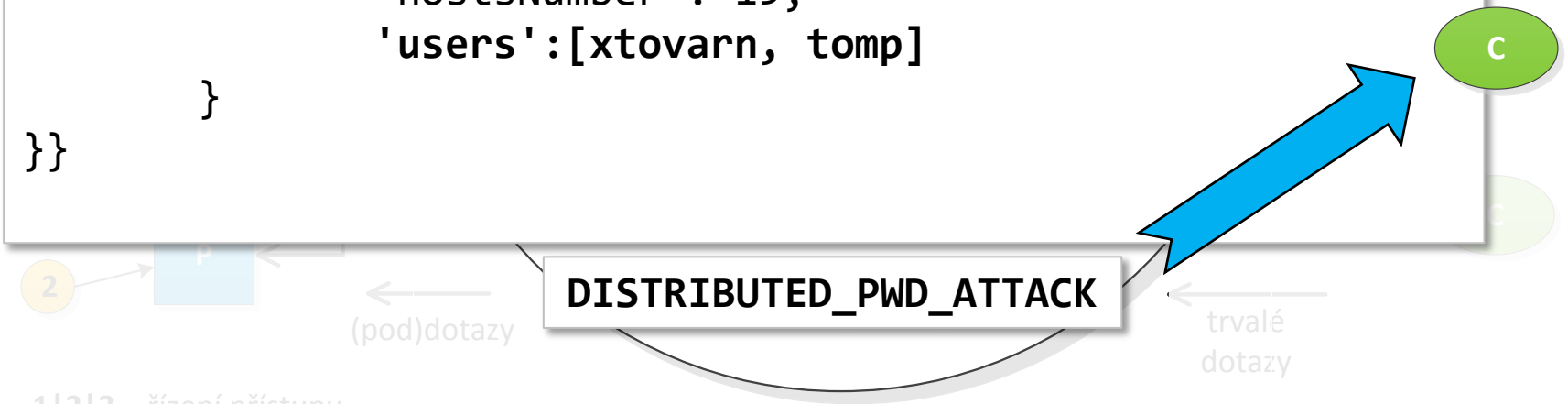


Navrhované řešení – nový mon. model



Navrhované řešení – nový mon. model

```
{'ComplexEvent':{
        'id':19058906,
        'occurrenceTime':'2012-04-11T08:25:13.129Z',
        'hostname':'processing-agent-14.fi.muni.cz',
        'entity':‘cloud1-group',
        'type':'cz.muni.fi.ngmon.DISTRIBUTED_PWD_ATTACK',
        'http://ngmon.fi.muni.cz/v1.0/complexevents.jsch':{
                'hostnames':[aisa.fi, ... , lykomedes.fi]
                ‘hostsNumber': 19,
                'users':[xtovarn, tomp]
        }
}}
```



Výzkumný záměr

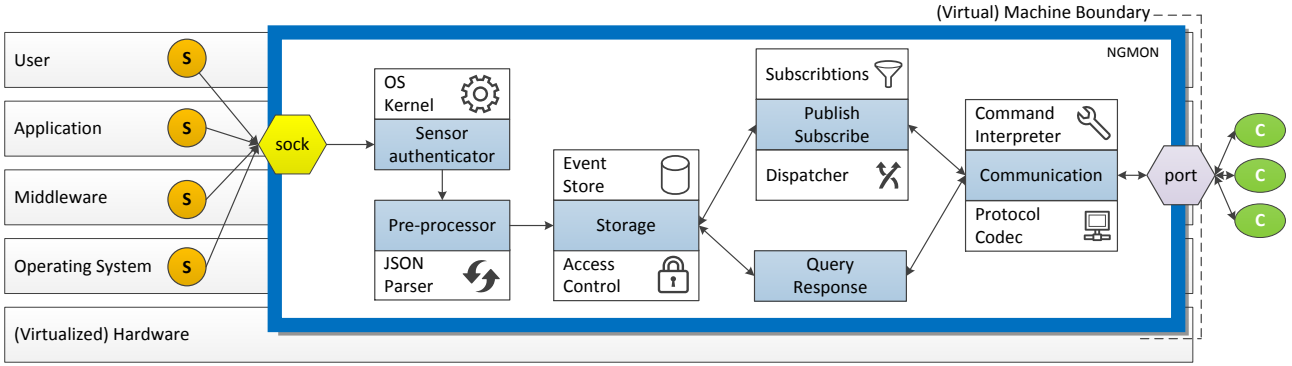
- Navrhnout příslušný logovací mechanismus (formáty, protokoly)
  - Téměř hotovo
- Navrhnout architekturu pro distribuované zpracování komplexních monitorovacích událostí
  - Topologie agentů
  - Alg. pro distribuci dotazů mezi agenty
  - Alg. pro rekurzivní dělení dotazů mezi dostupné agenty
  - Alg. pro distribuci událostí
- Mechanismy a algoritmy pro podporu více konzumentů
  - Publish-subscribe je v tomto ohledu velmi výhodné
  - Bezpečnost → SSL? Bude únosné ve smyslu zátěže?

Evaluace

- **Logování:** (neg.) zatížení a rychlost zpracování
- **Distr. zpracování:** výkon, latence, (neg.) zatížení a rychlost zpracování dotazů
- **Více uživatelů:** (neg.) zatížení
- Očekáváme **lepší** výkon, latenci a expresivitu dotazů než jakékoliv existující řešení či jejich kombinace
- To vše při **srovnatelném, či nižším** zatížení sítě a výpočetních kapacit

Dosažené výsledky

- Tovarňák, D., and Pitner, T. **Towards Multi-Tenant and Interoperable Monitoring of Virtual Machines in Cloud**, *Proceedings of 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, 2012
- **Ngmon** (ngmon.org) – producent monitorovacích dat založený na událostech
- **Logovací mechanismus** pro jazyk Java (bez přirozeného jazyka)



Shrnutí – cíle

- detekce vzorů chování **velkého množství** distribuovaných producentů v **reálném čase**
- podpora **mnoha konzumentů** při zachování **rozumného zatížení**
  - Posun k paradigmatu událostí, Návrh vhodného logovacího mechanismu
  - Návrh algoritmů a mechanismů pro distribuovanou detekci komplexních událostí
  - Mechanismy a algoritmy pro podporu více konzumentů

- Publikační cesty: ICPE , IDEAS, DEBS, Euro-Par, **FGCS**