Revize 2

C2115 Praktický úvod do superpočítání

V. lekce / Modul 1

Petr Kulhánek

kulhanek@chemi.muni.cz

Národní centrum pro výzkum biomolekul, Přírodovědecká fakulta
Masarykova univerzita, Kamenice 5, CZ-62500 Brno

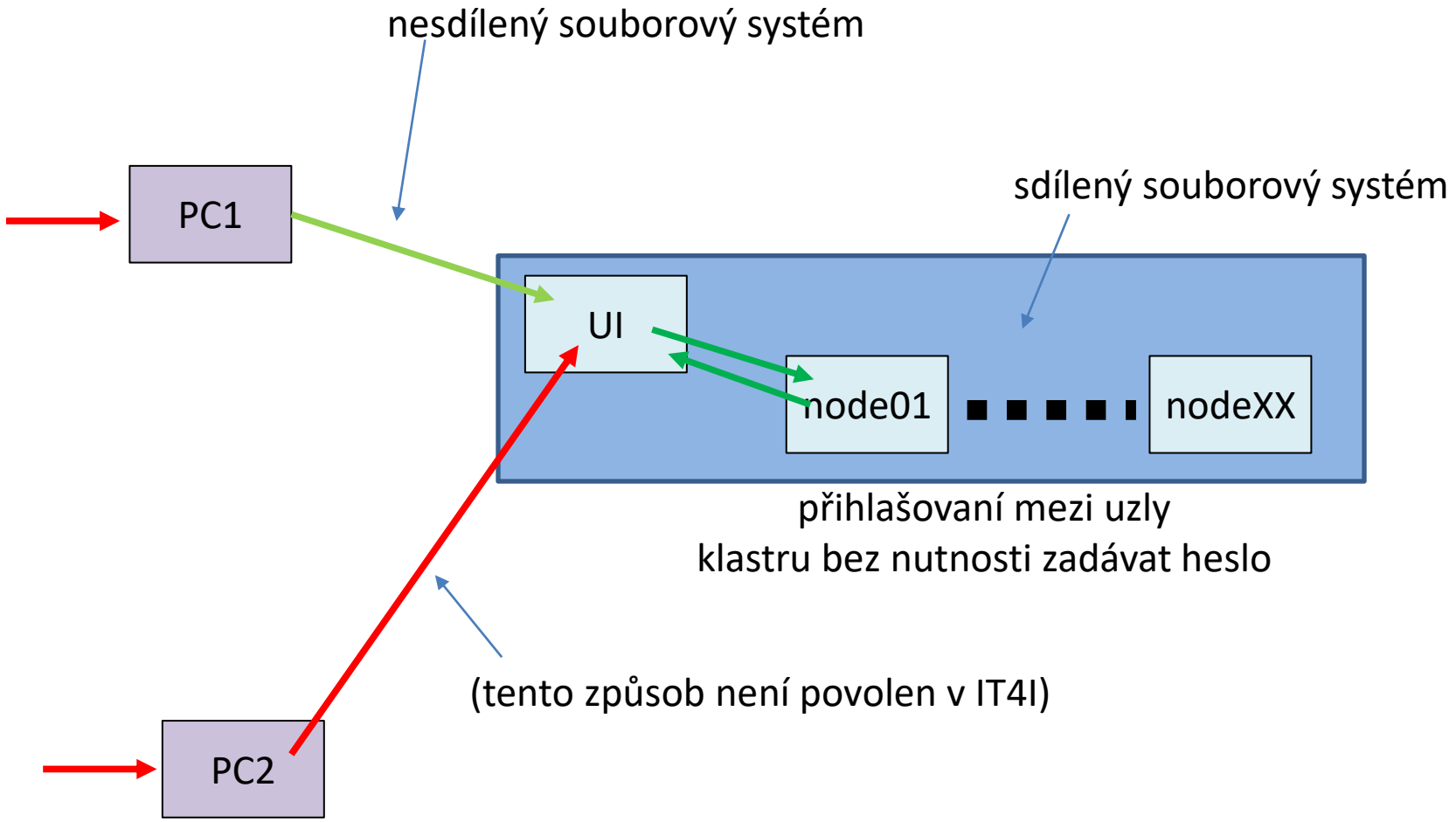
SSH klíče

man ssh

Vhodné pouze pro práci v **IT4I** nebo individuálními linuxovými stroji.

SSH klíče zásadně nepoužívejte pro přihlašování do MetaCentra nebo na klastech NCBR či CEITEC MU. Nevytvoří se během něj kerberovské lístky, bez kterých je prostředí těchto klastrů nepoužitelné!!!

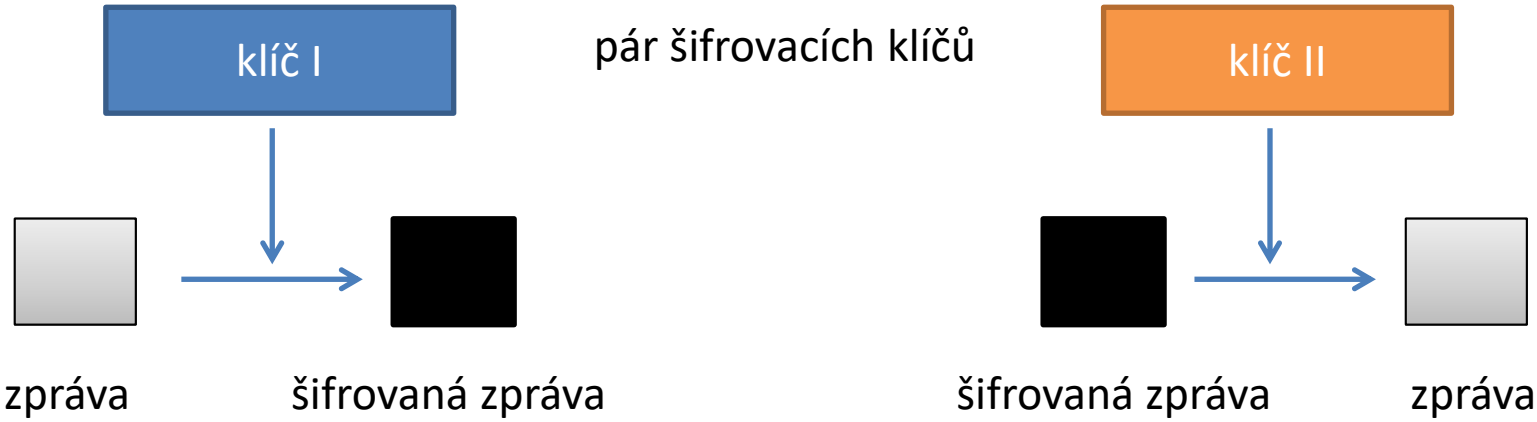
Workflow



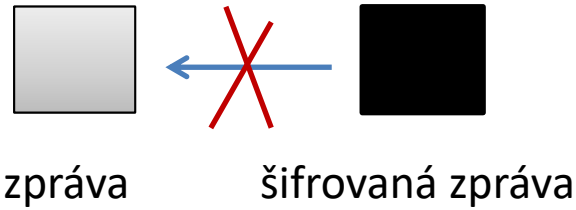
Autentizace pomocí ssh klíčů je založena na asymetrickém šifrování využívající pár šifrovacích klíčů (veřejný a soukromý klíč).

- s heslem
- bez hesla s ssh klíčem #1
- bez hesla s ssh klíčem #2

Asymetrické šifrování



Dešifrování zprávy klíčem použitým pro šifrování **není prakticky proveditelné**.

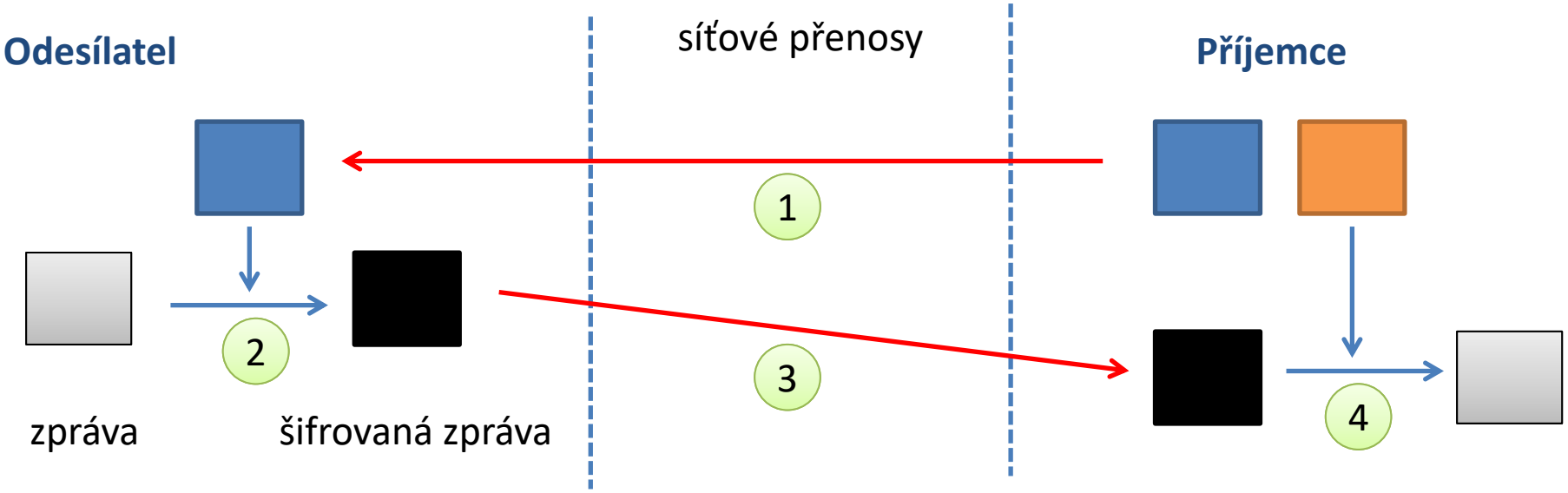


Asymetrické šifrování, použití I

veřejný klíč | soukromý klíč — pár šifrovacích klíčů

Utajený přenos zprávy:

1. získání veřejného klíče příjemce
2. šifrování zprávy odesílatele veřejným klíčem příjemce
3. odeslání šifrované zprávy přes nezabezpečenou síť
4. příjemce dešifruje zprávu svým soukromým klíčem



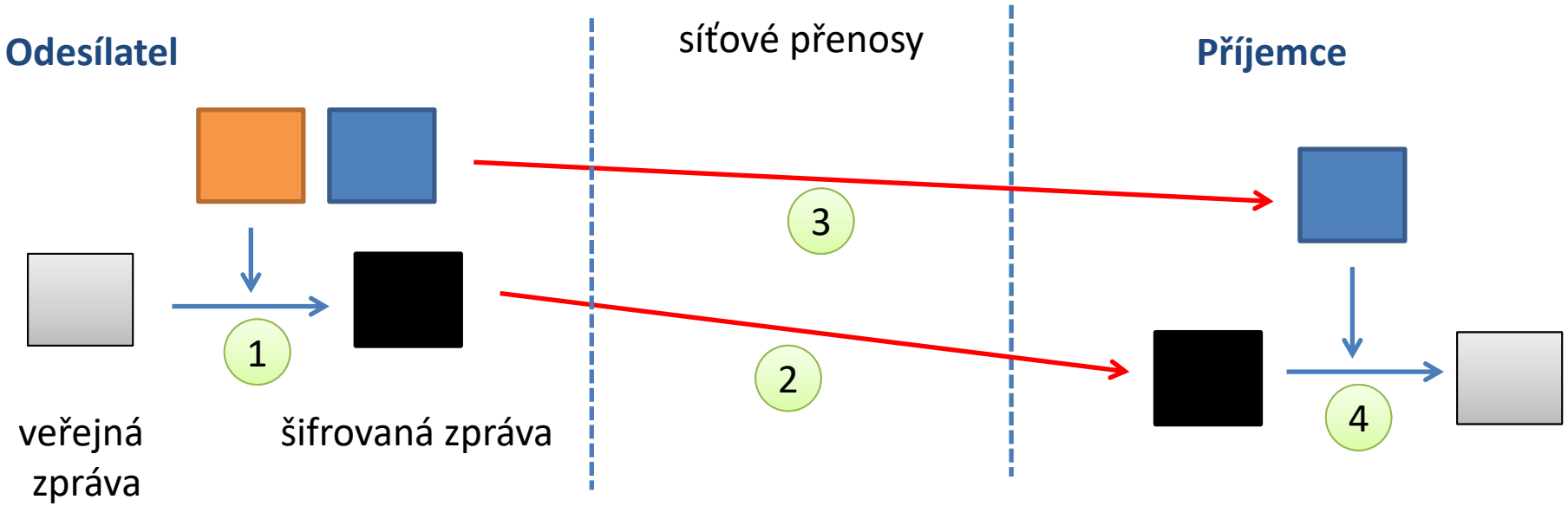
Kdokoliv, kdo zcizí soukromý klíč příjemce, muže dešifrovat přenášené zprávy!

Asymetrické šifrování, použití II

veřejný klíč | soukromý klíč — pár šifrovacích klíčů

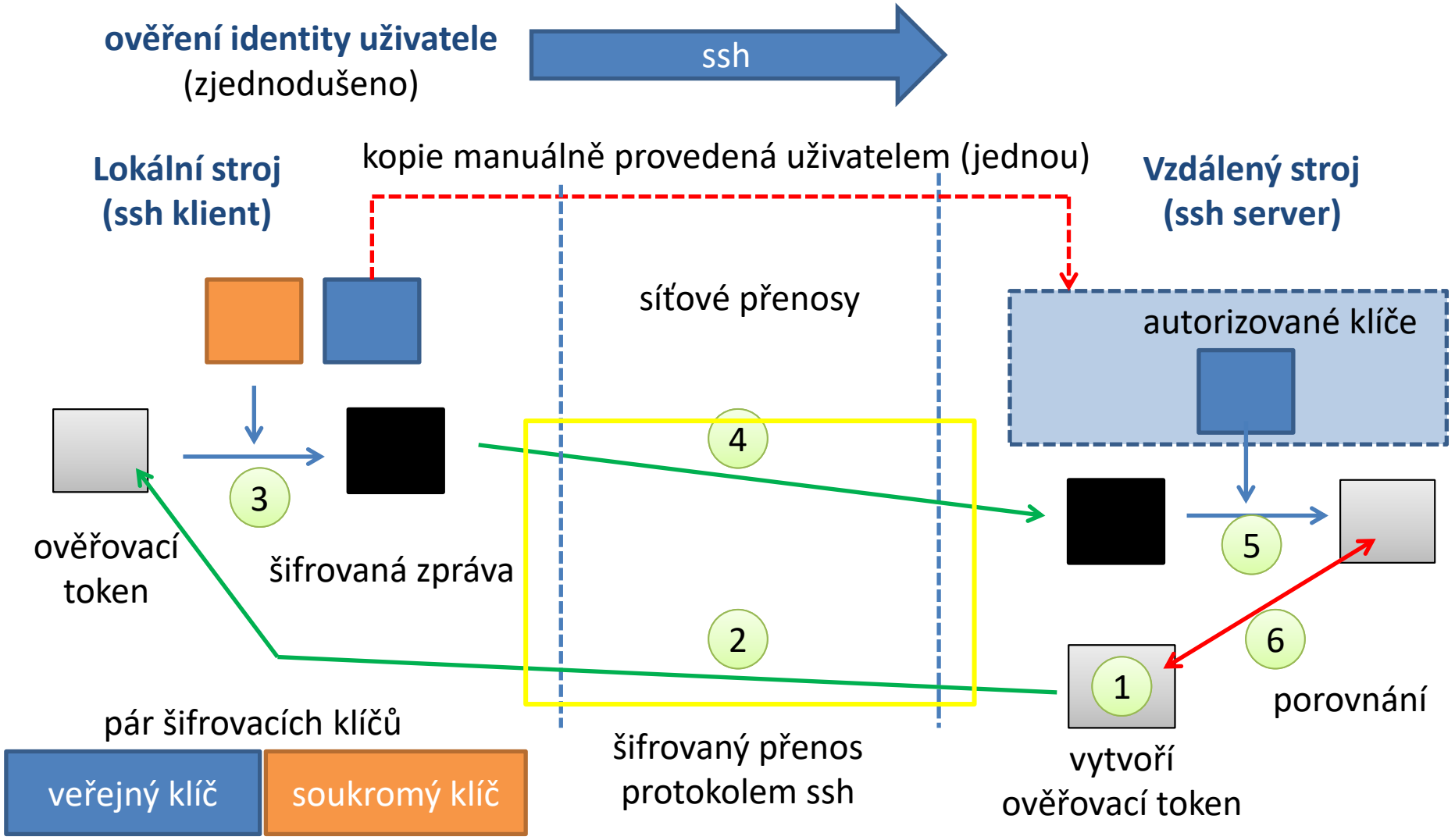
Ověření odesílatele veřejné zprávy:

1. zašifrování zprávy soukromým klíčem odesílatele
2. příjemce získá zašifrovanou zprávu a veřejný klíč odesílatele
3. příjemce dešifruje zprávu veřejným klíčem odesílatele



Kdokoliv, kdo zcizí soukromý klíč odesílatele, se za něj může vydávat!

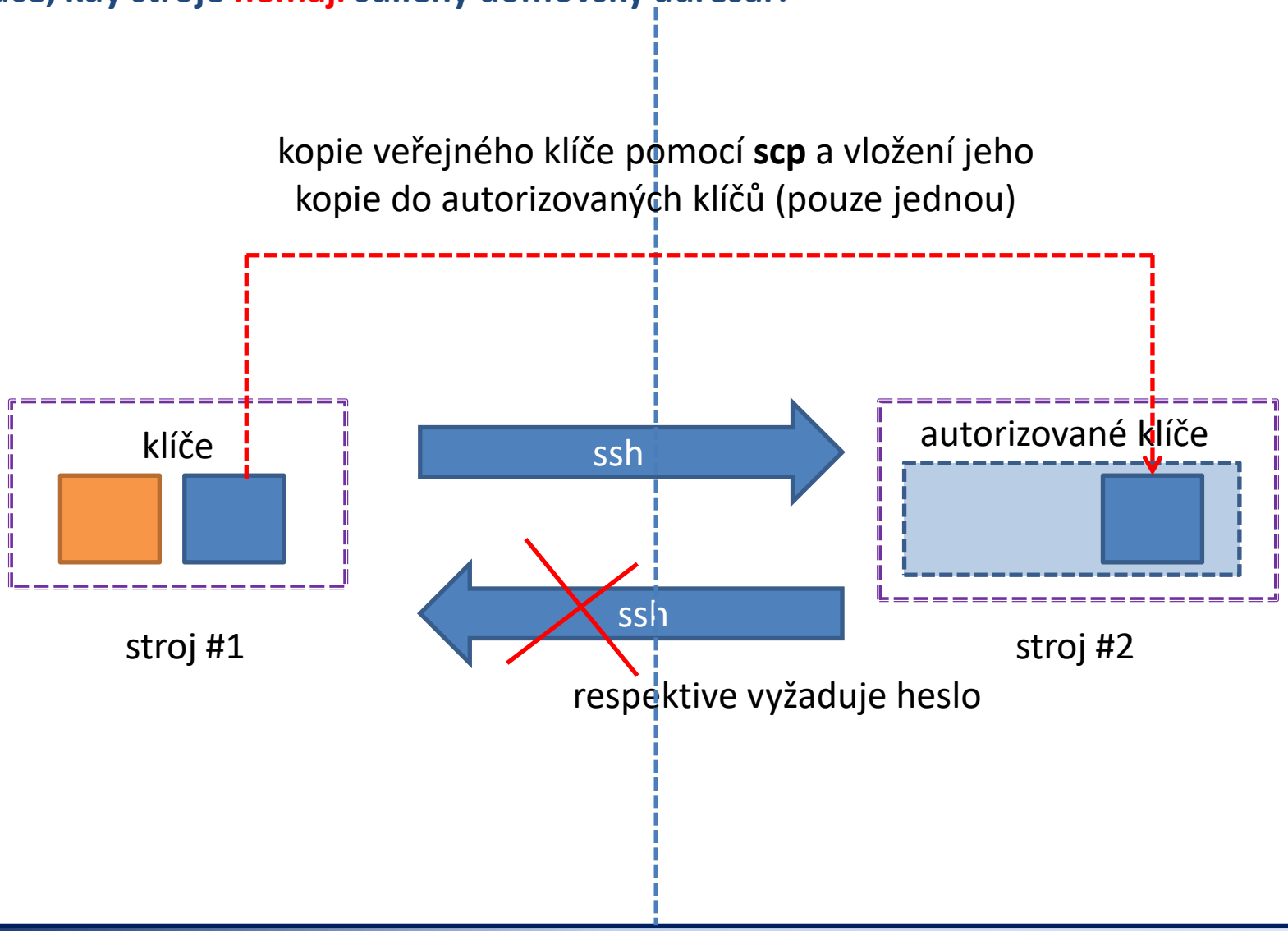
Autorizovaný veřejný ssh klíč



Kdokoliv, kdo zcizí soukromý klíč uživatele, se může přihlásit na vzdálený stroj!

Nesdílený souborový systém

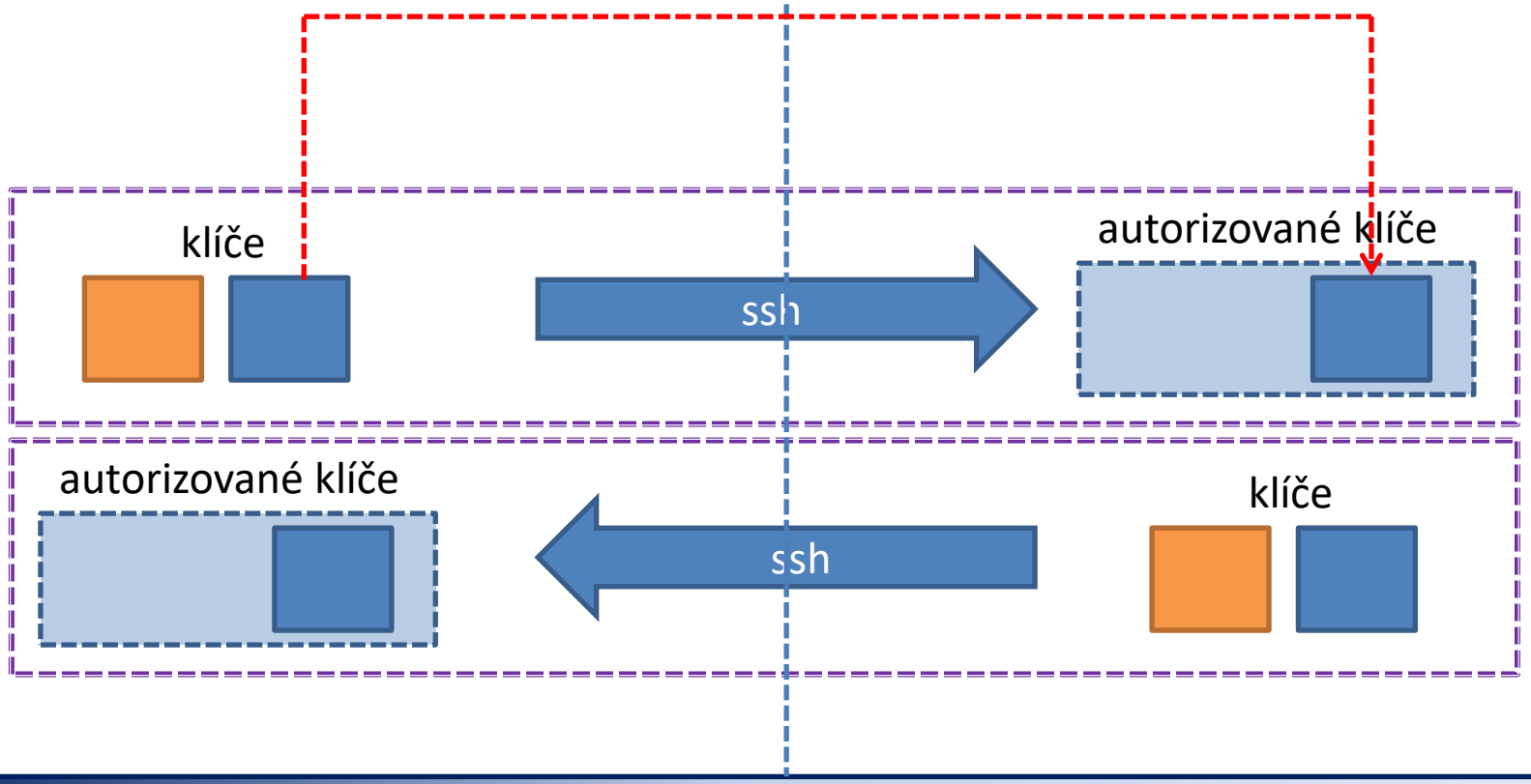
Situace, kdy stroje nemají sdílený domovský adresář:



Sdílený souborový systém

Situace, kdy stroje mají sdílený domovský adresář:

oba soubory jsou na sdíleném souborovém systému
je možné použít (pouze jednou)
cat id_rsa.pub >> authorized_kyes



Vytvoření páru v/s klíče

Pár veřejného a soukromého klíče se vytváří na daném stroji nebo skupině strojů, které mají sdílený adresář, POUZE jednou.

```
[kulhanek@wolf01 ~]$ cd .ssh

[kulhanek@wolf01 .ssh]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kulhanek/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kulhanek/.ssh/id_rsa.
Your public key has been saved in /home/kulhanek/.ssh/id_rsa.pub.
The key fingerprint is:
e9:07:0b:fc:17:23:b3:c5:1a:8a:0c:1a:98:8f:fe:28 kulhanek@wolf01.wolf.inet

[kulhanek@wolf01 .ssh]$ ls -l
-rw------- 1 kulhanek lcc  1675 Mar 21  2012 id_rsa
-rw-r--r-- 1 kulhanek lcc   395 Mar 21  2012 id_rsa.pub
-rw------- 1 kulhanek lcc 13380 Sep  4 15:55 known_hosts
```

Passphrase se nezadává!

soukromý klíč NESMÍ být čitelný pro skupinu a svět

seznam otisků palců strojů, na které jste se přihlásili pomocí příkazu ssh

Podrobnější popis: man ssh

Vytvoření autorizovaných klíčů - I

sdílený souborový systém

Vložení veřejného klíče do seznamu autorizovaných klíčů:

```
[kulhanek@node ~]$ cd .ssh
[kulhanek@node ~]$ cat id_rsa.pub >> .ssh/authorized_keys

[kulhanek@node .ssh]$ ls -l
-rw-r--r-- 1 kulhanek lcc   395 Sep 25  2012 authorized_keys
```

přístupová práva pro soubor authorized_keys, **pro skupinu a jiné - maximálně právo pro čtení**

Soubor *authorized_keys* může obsahovat více veřejných klíčů, každý je pak na jedné řádce.

Pokud přihlašování pomocí autorizovaných veřejných klíčů nebude fungovat :

- ověřte přístupová práva jednotlivých souborů (písmenka r, w (eventuálně x) ve výpisu příkazu ls -l)
- pokud běží ssh agent, odstraňte klíče, které má ve správě:

```
$ ssh-add -D
```

- znovu se přihlaste

Podrobnější popis: man ssh

Vytvoření autorizovaných klíčů - II

nesdílený souborový systém

Veřejný klíč je nutné překopírovat na vzdálený klastr. Ke vzdálenému kopírovaní slouží příkaz **scp**.

Syntaxe:

[] - možno vynechat

```
$ scp [-r] zdroj cil
```

Zdroj a cíl může být soubor nebo adresář. V případě kopírovaní adresářů je nutno použít volbu **–r** (recursive).

Vzdálený cíl nebo host se identifikuje názvem stroje odděleného od jména souboru či adresáře **dvojtečkou**.

```
[user@]hostname:[cesta/]soubor
```

Vytvoření autorizovaných klíčů - II

nesdílený souborový systém

Vložení veřejného klíče do seznamu autorizovaných klíčů :

Získání veřejného klíče ze stroje, který bude mít roli klienta (chceme z něj spouštět příkaz ssh):

```
[kulhanek@ui ~]$ scp wolf.ncbr.muni.cz:.ssh/id_rsa.pub wolf.pub
```

Zapsání veřejného klíče do seznamu autorizovaných klíčů:

dvojtečka tečka

```
[kulhanek@ui ~]$ cat wolf.pub >> .ssh/authorized_keys
[kulhanek@ui ~]$ rm wolf.pub
[kulhanek@ui ~]$ ls -l .ssh
-rw-r--r-- 1 kulhanek lcc   395 Sep 25  2012 authorized_keys
-rw------- 1 kulhanek lcc  1675 Mar 21  2012 id_rsa
-rw-r--r-- 1 kulhanek lcc   395 Mar 21  2012 id_rsa.pub
-rw------- 1 kulhanek lcc 13380 Sep  4 15:55 known_hosts
```

přístupová práva pro soubor authorized_kyes,
pro skupinu a jiné – maximálně jen právo pro čtení

Podrobnější popis: man ssh

Pro a proti

Výhody:

- nemusí se neustále zadávat heslo
- bezpečnější použití příkazů ssh a scp ve skriptech
- urychlení práce

Nevýhody:

- v případě kompromitace jednoho počítače, jsou kompromitovány všechny počítače se vzájemně autorizovanými veřejnými klíči

SSH klíče zásadně nepoužívejte pro přihlašování do MetaCentra nebo na klastech NCBR či CEITEC MU. Nevytvoří se během něj kerberovské lístky, bez kterých je prostředí těchto klastrů nepoužitelné!!!

Cvičení M1.C1

1. Nastavte vaši instanci virtuálního stroje s Ubuntu tak, abyste se do něj mohli přihlásit pomocí ssh klíčů z hostitelského stroje (použijte návod pro nesdílený souborový systém).
2. Můžete se do virtuálního stroje přihlásit bez hesla ze stroje wolf01? Chování vysvětlete.
3. Zrušte autentizaci pomocí veřejného klíče ve vaší instanci virtuálního stroje s Ubuntu.