Zneužití Asterisku pro podvodná volání

CZ.NIC, z.s.p.o.
Petr Hruška
petr.hruska@nic.cz
07.06.2010

cz nic
správce domény cz

- VoIP, výzvy minulé a budoucí
- telefonní ústředna Asterisk
- SQL injection pro Asterisk

VoIP

- první průkopníci v roce 2002
- dnes statisíce linek
- převrat v telefonii

VoIP

- běžná součást infrastruktury
- lákadlo pro útočníky
- další výzva pro VoIP, ale zdaleka ne jen pro operátory

Útoky na voip infrastrukturu

- volání na zahraniční linky, často Ukrajina, Bělorusko, Kuba a Haiti
- škody bývají ve statisících


Asterisk™

Asterisk

- Asterisk se při zpracování hovoru řídí speciálním skriptem, tzv. *dialplanem*
- dialplan obsahuje pravidla s příkazy
- o provedení pravidla rozhoduje číslo pravidla a šablona

extensions.conf

```
exten =>231,1,Ringing()
exten =>231,2,Wait(2)
exten =>231,3,Playback(hello-world)
exten =>231,4,Hangup()

exten =>230,1,Dial(SIP/franta)
```

extensions.conf

```
exten=>231,1,Ringing()
exten=>231,2,Wait(2)
exten=>231,3,Playback(hello-world)
exten=>231,4,Hangup()

exten =>230,1,Dial(SIP/franta)
```

- místo jmen typu *franta* se pro pojmenování často použije telefonní číslo

```
exten=>230,1,Dial(SIP/franta)
exten=>231,1,Dial(SIP/231)
exten=>232,1,Dial(SIP/232)
exten=>233,1,Dial(SIP/233)
```

Využití proměnné

- v proměnné ${EXTEN} je uloženo volané telefonní číslo

```
exten=>230,1,Dial(SIP/franta)
exten=>231,1,Dial(SIP/${EXTEN})
exten=>232,1,Dial(SIP/${EXTEN})
exten=>233,1,Dial(SIP/${EXTEN})
```

Využití šablony

```
exten=>230,1,Dial(SIP/franta)
exten=>_23[1-3],1,Dial(SIP/${EXTEN})
```

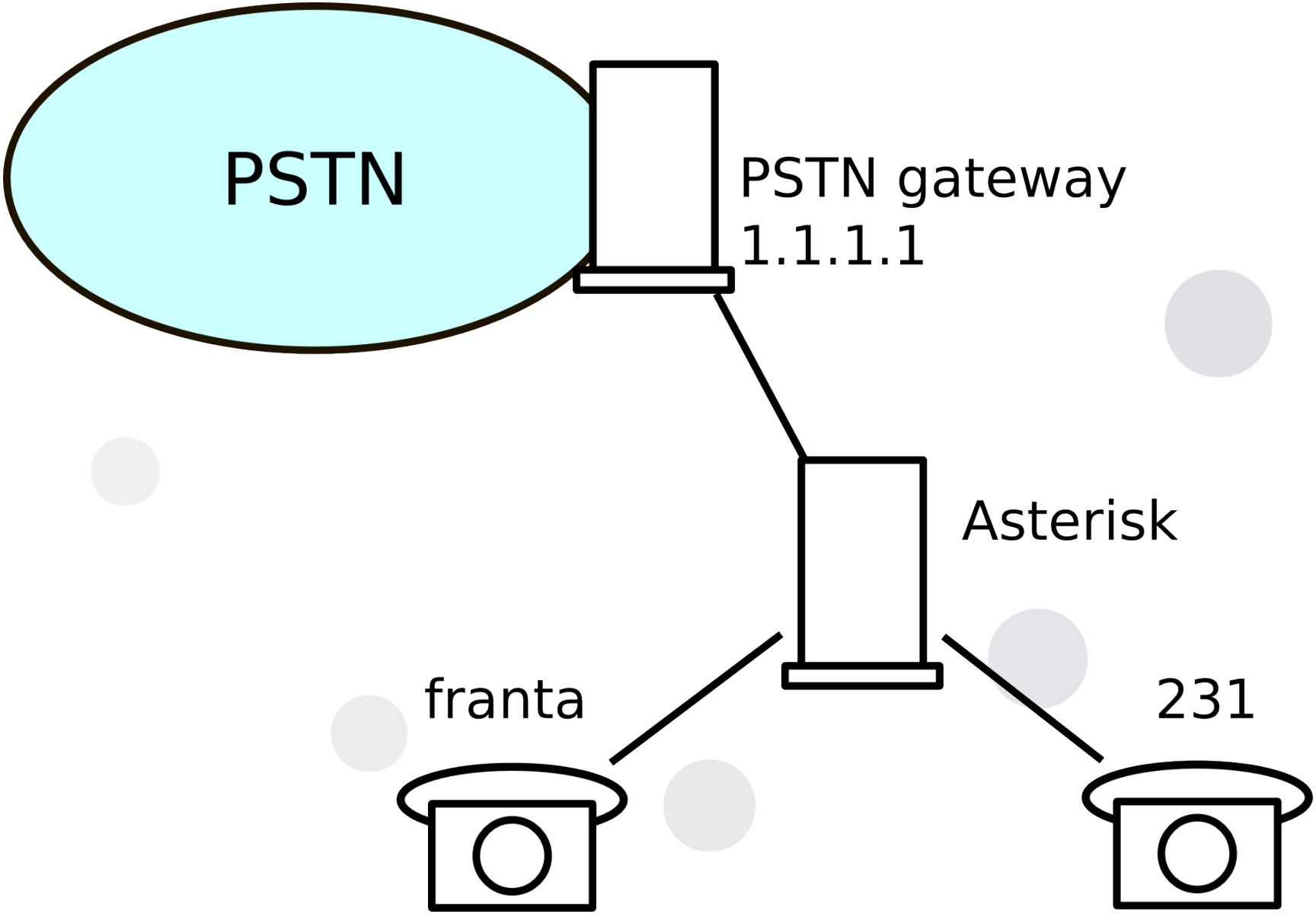
Nejen čísla

- Asterisk umožňuje volat nejen telefonní čísla, ale i obecnější identifikátory

```
exten=>franta,1,Dial(SIP/franta)
```

Využití šablony

```
exten=>230,1,Dial(SIP/franta)
exten=>_[0-9a-z][0-9a-z].,1,
    Dial(SIP/${EXTEN})
```


PSTN
PSTN gateway
1.1.1.1
Asterisk
franta
231

Konfigurace pro volání dovnitř a ven

```
[incoming]
exten=>230,1,Dial(SIP/franta)
exten=>_[0-9a-z][0-9a-z].,1,
    Dial(SIP/${EXTEN})

[internal]
exten=>_0X.,1,Dial(SIP/1.1.1.1/${EXTEN:1})
```

Větvení hovorů

```
exten=>230,1,Dial(SIP/franta&SIP/pepa)
```

Dialstring injection

Co se stane při volání na `00&SIP/1.1.1.1/222745120`?

```
exten=>_[0-9a-z][0-9a-z].,1,
    Dial(SIP/${EXTEN})

exten=>_[0-9a-z][0-9a-z].,1,
    Dial(SIP/00&SIP/1.1.1.1/222745120)
```

Dialstring injection

- obdoba SQL injection
- podobné vlastnosti, nikoliv bug ale fíčura
- nejde jen o funkci Dial

Jak se bránit

- používejte co nejpřesnější šablony
- zkontrolujte `${EXTEN}` na přítomnost speciálních znaků

`http://www.voip-forum.com/asterisk/2010-02/securityalert-asterisk-dialstring-injections/`

Jak se bránit

- nastavte si limit na placené hlasové služby
- monitorujte a vyhodnocujte logy

?