POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY
FAKULTA BEZPEČNOSTNÍHO MANAGEMENTU

Modelování kybernetických útoků

Doc. RNDr. Josef POŽÁR, CSc. - děkan

4. 4. 2012

Tato prezentace byla zpracována v rámci Projektu vědeckovýzkumného úkolu č. 4/4 „Informační bezpečnost a kybernetická kriminalita v organizaci“, který je součástí Integrovaného výzkumného úkolu na léta 2010-2015, realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.


Pasivní útoky
Odposlech
analýza provozu

Aktivní útoky

fyzické

-Destrukce

-EPM

-manipulace

maškaráda

-integita

-neautoriz. přís

-důvěrnost

-soukromí

DOS

- fyzická vrstva
- MAC vrstva
- síťová vrstva
- transportní vrstva
- aplikač. vrstva

Škodlivý kód

- phishing
- útoky proti manag.

Stadium	Typická akce
0	Průzkum PC (Serveru)
1	Narušení uživatele
2	Escalation service, útok na službu
3	Vniknutí root
4	Dosažení cíle
5	Průzkum PC (Serveru)
6	Narušení uživatele
7	Escalation service, útok na službu
8	Vniknutí root
9	Dosažení cíle

Typické hackerské akce při kybernetickém útoku

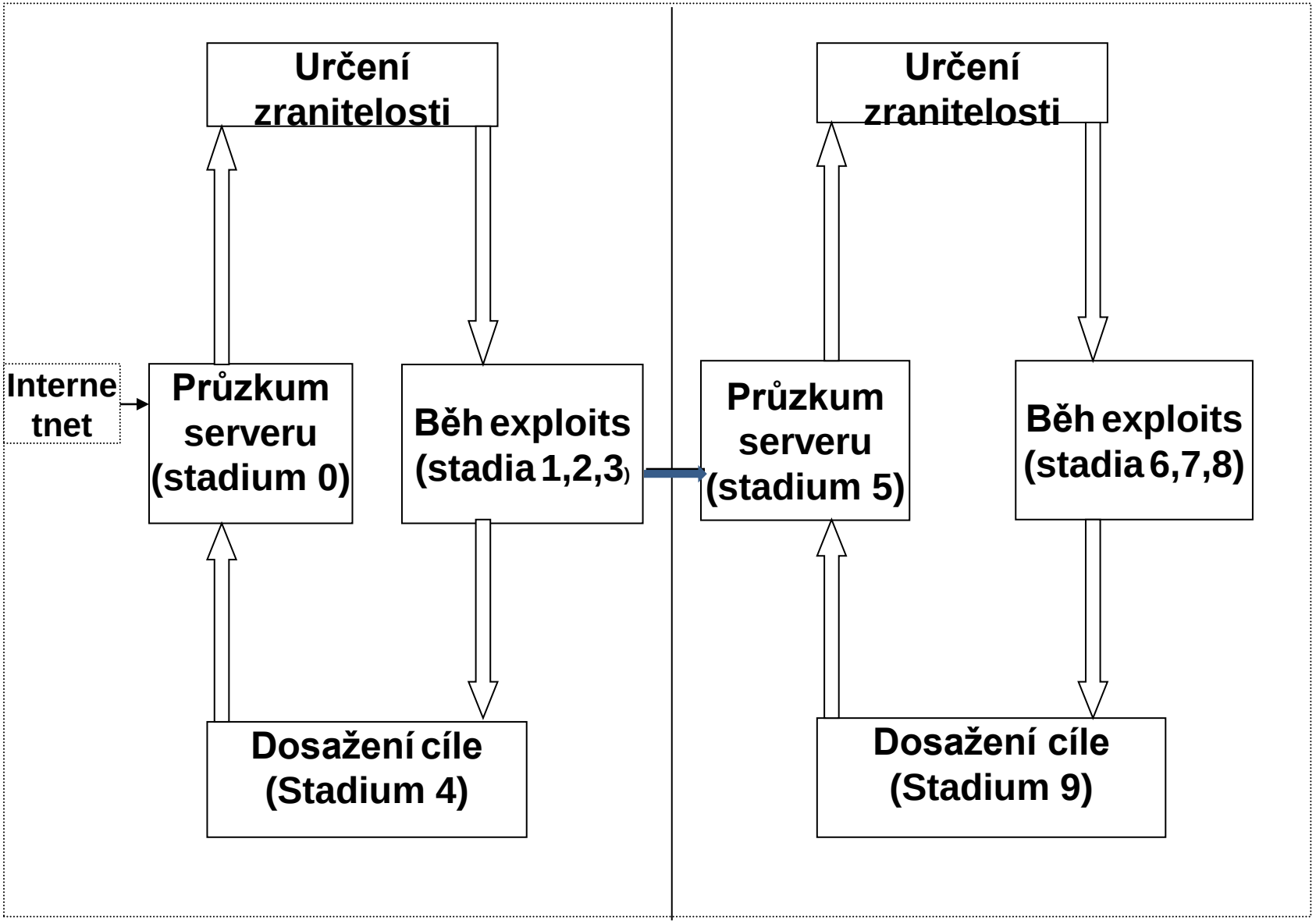
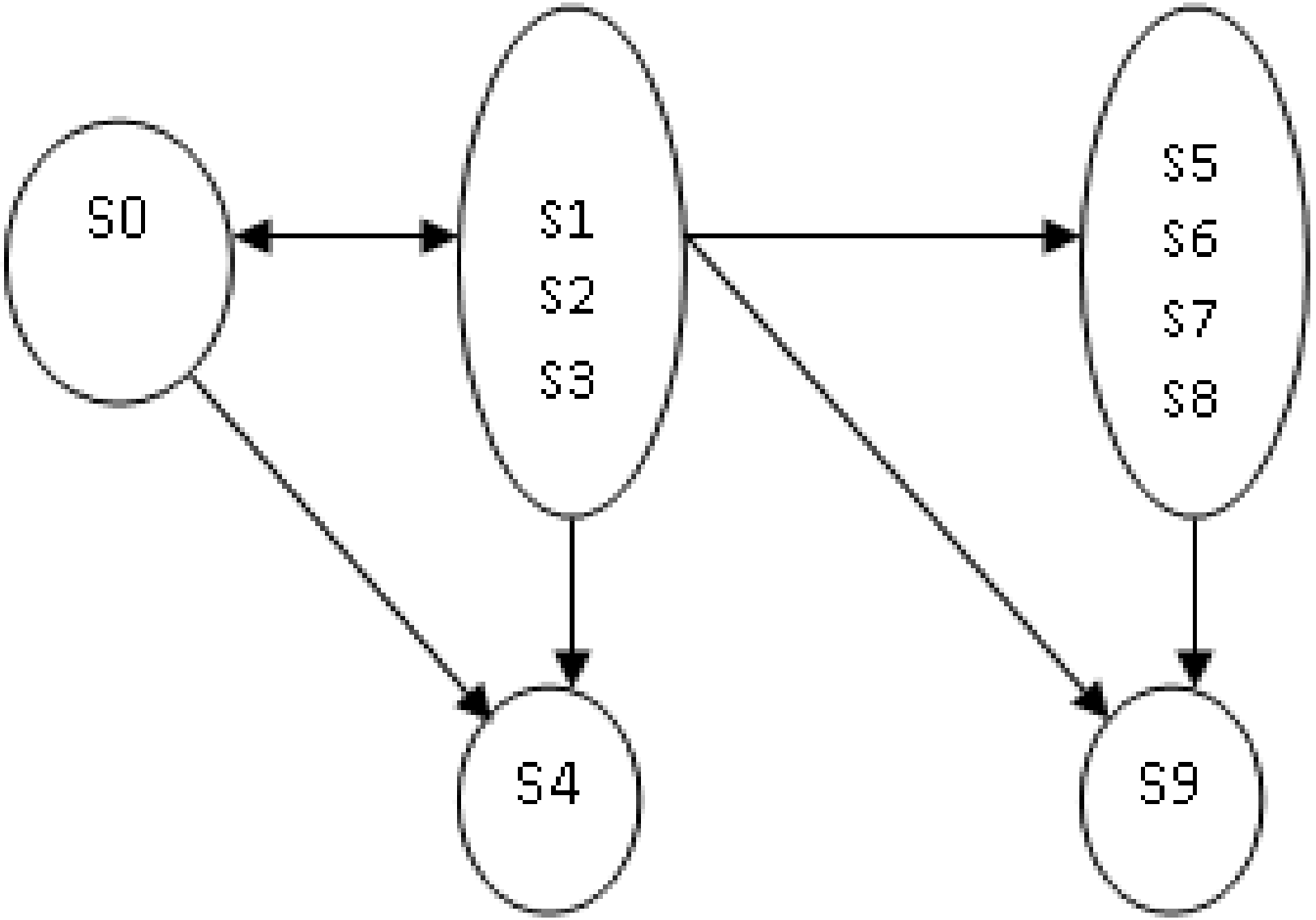
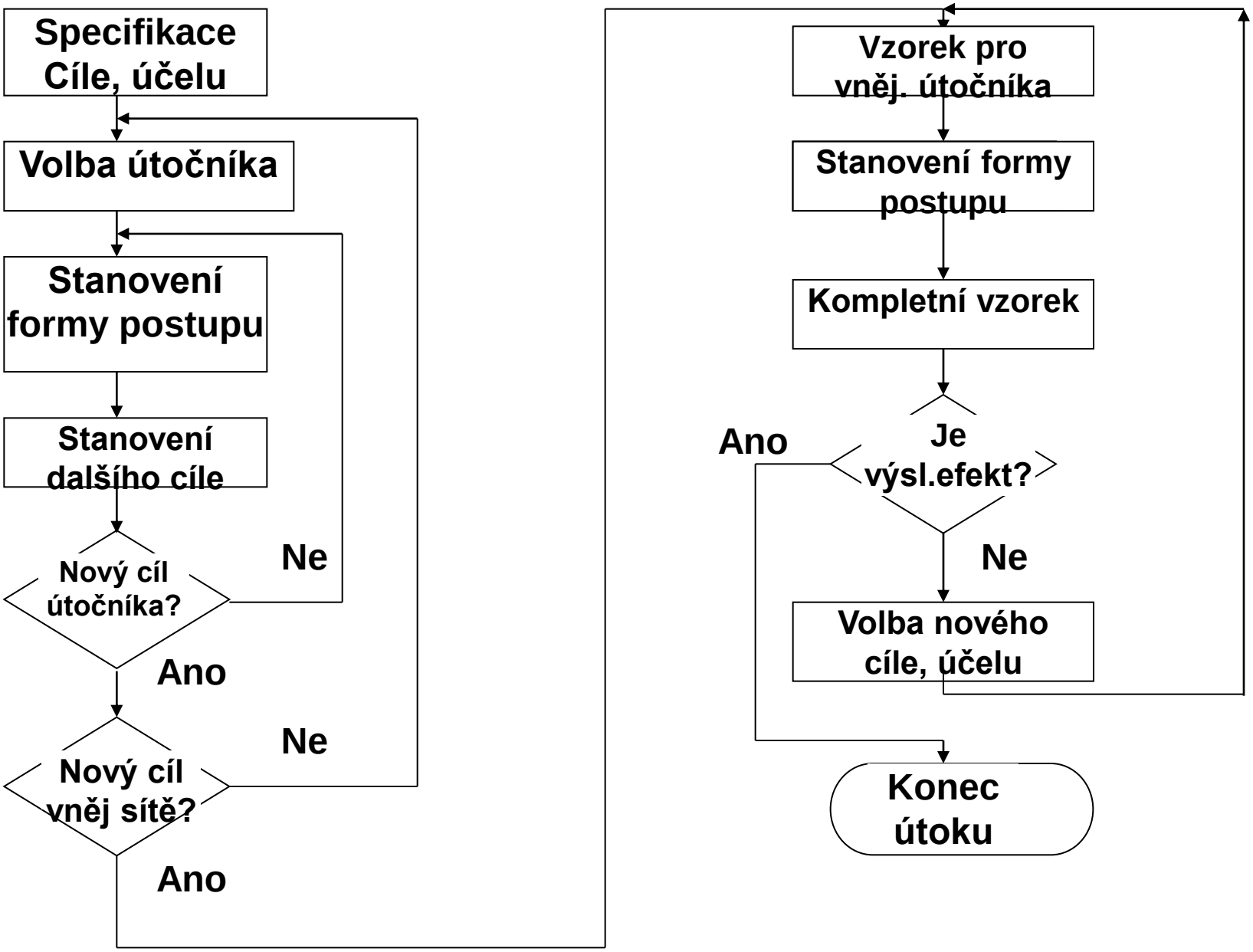


Schéma kybernetického útoku na počítačovou síť z Internetu



Orientovaný graf reprezentující strukturu útoku



Generování automatického útoku

Doporučení

- Zintenzivnit mezinárodní spolupráci policejních sborů.
- Harmonizovat právní normy – jednotná legislativa v zemích EU.
- Potřeba vzdělávání manažerů podniku v oblasti informačních technologií.
- Výchova X útoky zevnitř organizace.

- **Bezpečnostní a spolehlivostní analýza rozsáhlých sítí.**
- **Standardizace programového vybavení pro forenzní analýzu.**
- **Zkoumání sociálně-psychologických faktorů kybernetické bezpečnosti.**

pozar@polac.cz