UFRGS

Monitoring, Attack Detection and Mitigation
MonAM 2006

Honeypots as a Security Mechanism

Presenter: Émerson Virti

Authors: Émerson Virti, Liane Tarouco, João Ceron, Leandro Bertholdo, Lisandro Granville

Index

Honeypot Concept

- **Experiment of Lancer Sptizner**
  - **1999**
  - **RedHat 5.1**

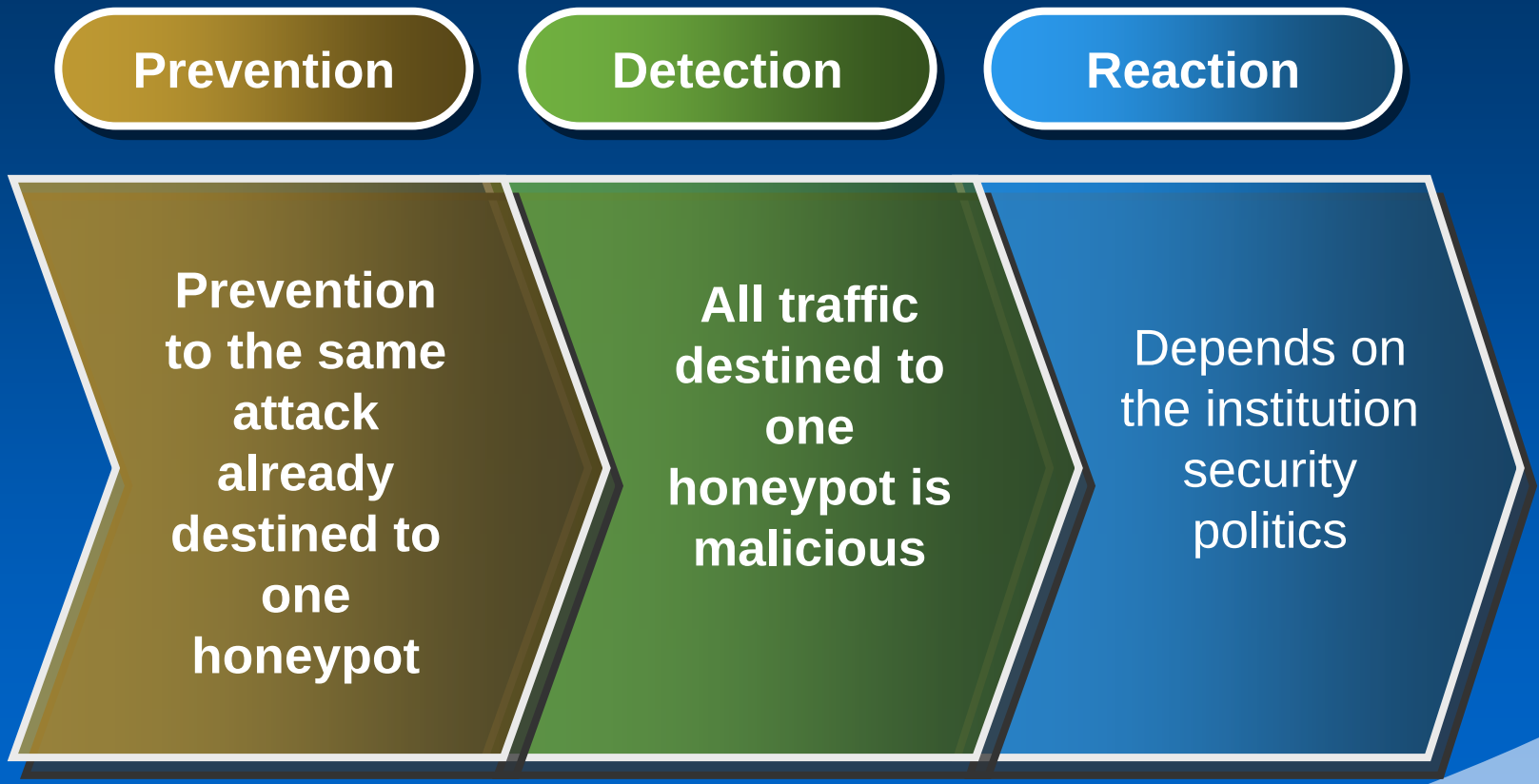
- **Concept:**

A network resource whose function is to be attacked and compromised**.**

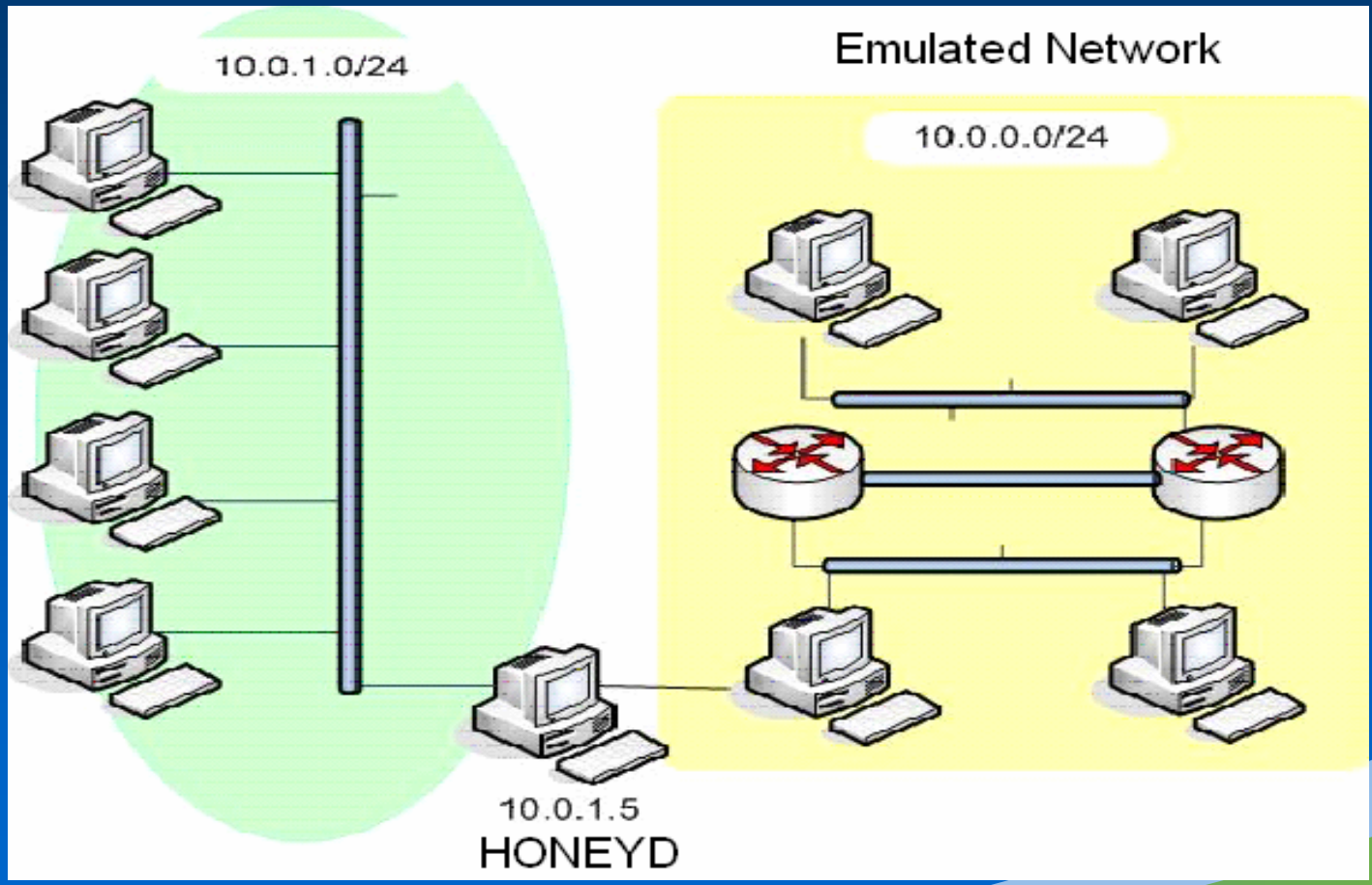
Sptizner

Cooperation for Security

Importance of the Honeypot



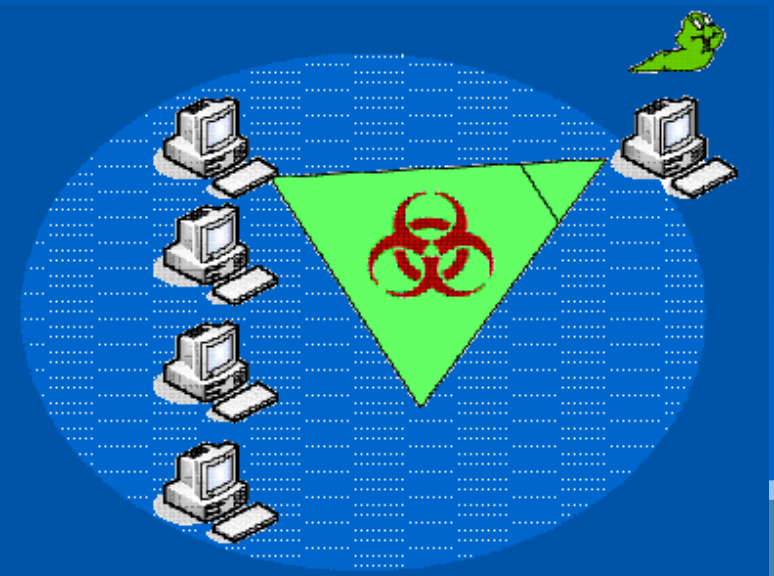
Honeyd Software



Principle of the Proximity

The majority of malwares tries to attack targets next to its addressing space.

"New Fields of Application for Honeypots" – Thorsten Holz



Experiment

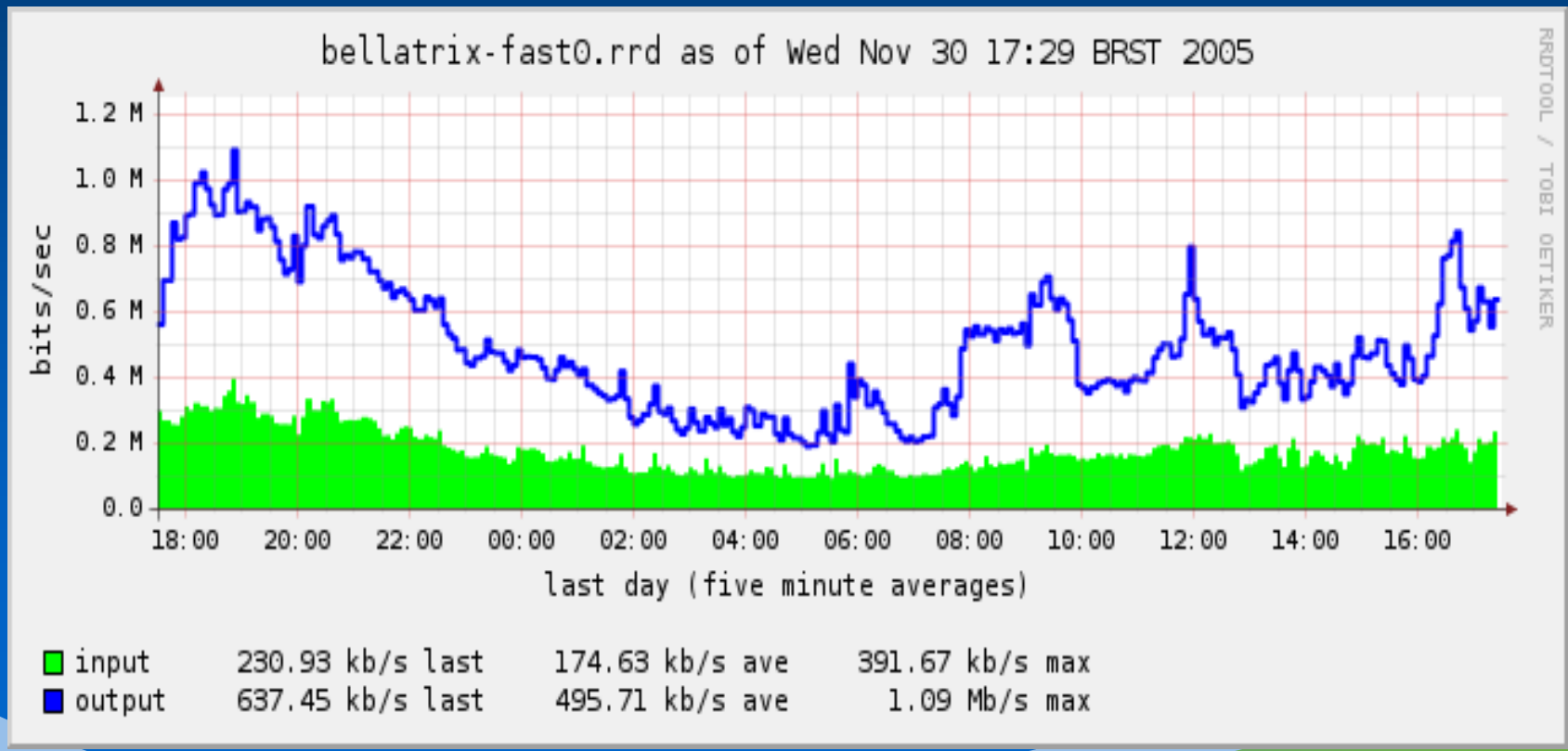
Used blocks IPV4:

Academic	/17
Academic	/18
Comercial	/18
Cable Modem	/20

69.632 emulated computers

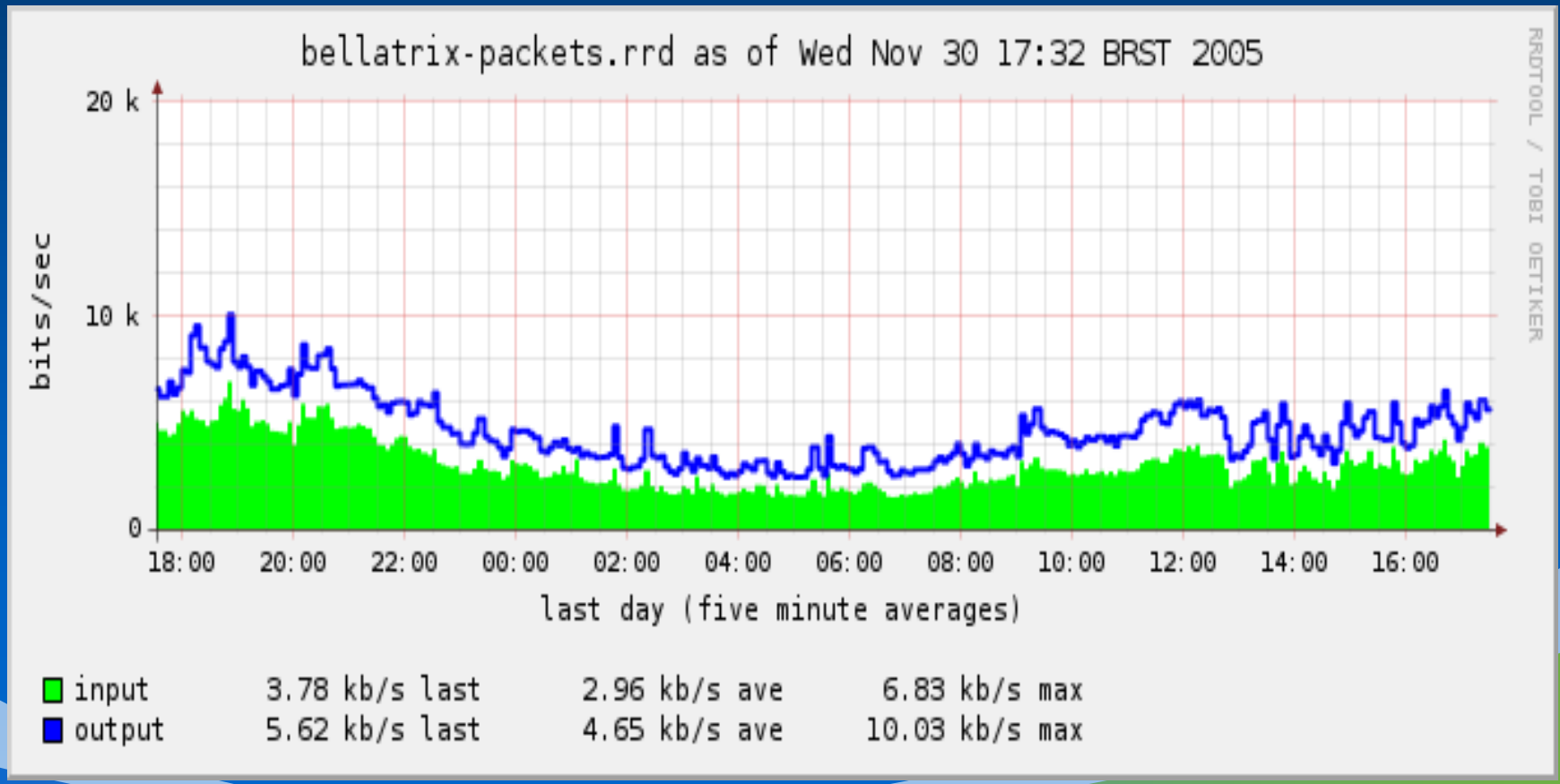
Experiment - Results

Traffic – bit/s



Experiment - Results

Traffic – package/s



Experiment - Results

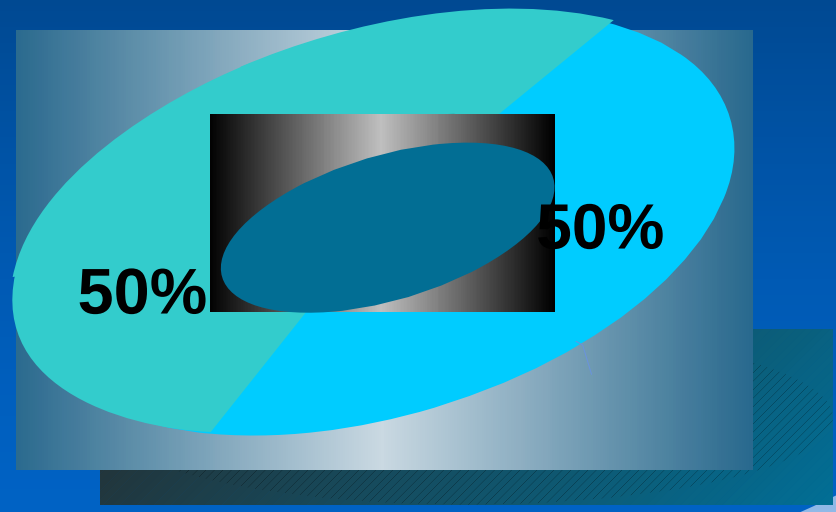
Statistics

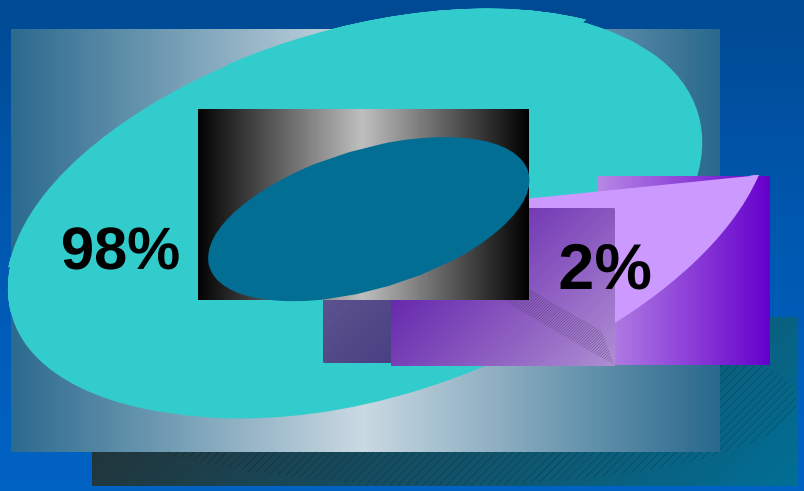
Address Space X Number of Access	Access Per day	Access per IP per day	Acces per IP per min
Academic /18	32.145.835	1977,48	2,75
Comercial /18	3.838.989	236,16	0,38
Academic /17	3.941.556	121,23	0,17
Cable Modem /20	5.172.852	1272,85	1,76

Experiment - Results

Attack Origin – IP source nationality

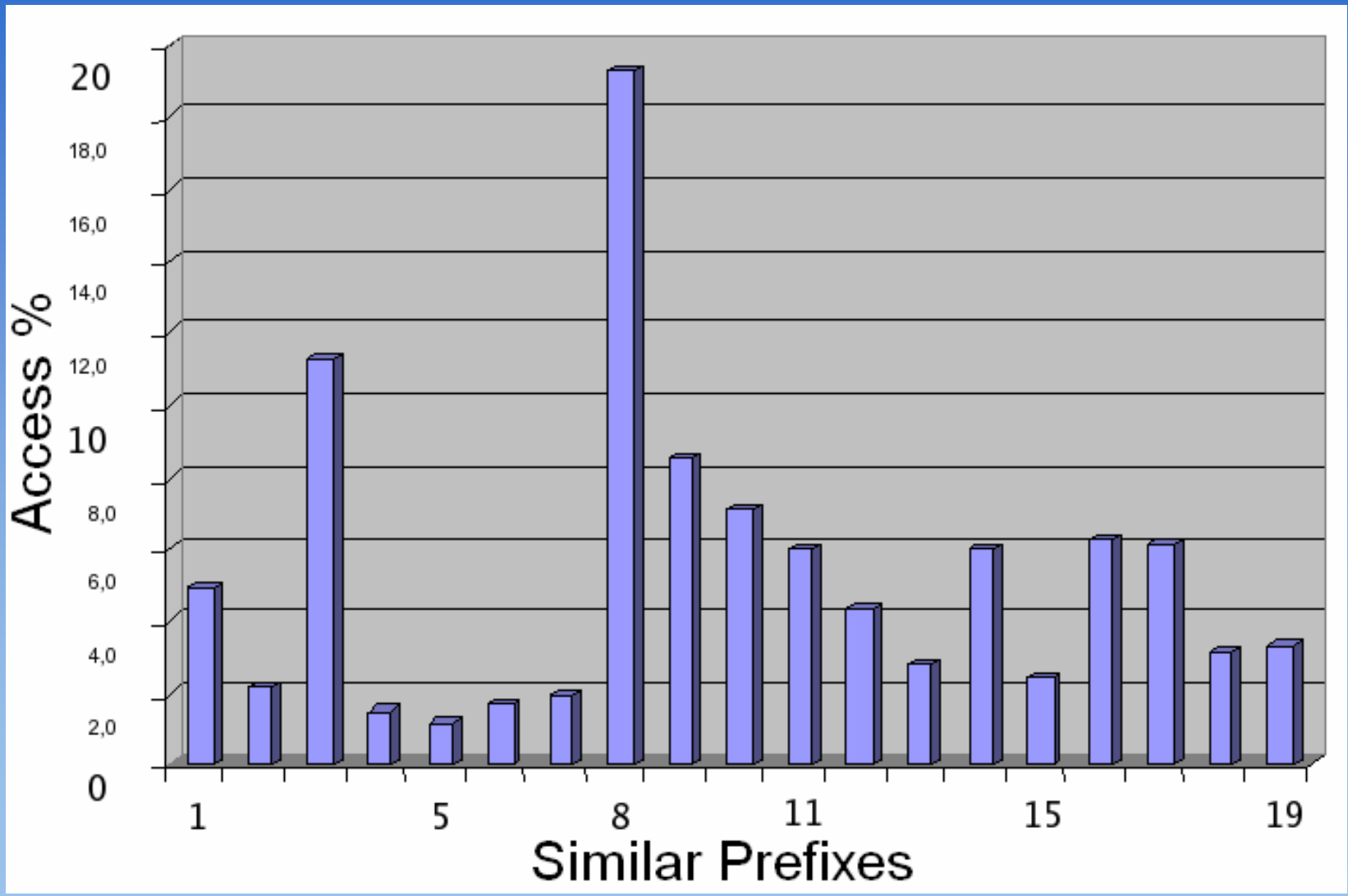
Honeypot Brazilian Block





Honeypot before CIDR Block

Experiment - Results



Conclusion

- Prevention, Detection and Reaction
- Principle of Proximity
- Honeypots as a security mechanism

References

• T. Holz, "New Fields of Application for Honeynets" Diploma Thesis, Department for Computer Science of Aachen University, Germany, 2005

• L. Spitzner, Honeypots: Tracking Hackers. Addison-Wesley, 2003. [Online]. http://www.tracking-hackers.com/book/

• B. Schneier. "Secrets and lies: digital security in a networked world", Willey & Sons , 2000.

Questions?

Émerson Virti
emerson@tche.br

Federal University of Rio Grande do Sul – Brazil - UFRGS