Caractérisation système d'un Botcloud par une analyse en composantes principales

Badis HAMMI

Directeurs de thèse : Guillaume DOYEN, MDC UTT
Rida KHATOUN, ECC UTT

ICD/ERA, Université de Technologie de Troyes (UTT)

24 Octobre 2013

Plan

Plan

Contexte

- Le Cloud Computing
  - Une technologie émergente qui attire fortement l'attention de tous les secteurs
  - Le marché du Cloud de 40.7 milliards de dollars en 2011 va se développer à plus de 240 milliards de dollars en 2020 [R.Stephan ET AL., 2010]
  - Le Cloud Computing représente les services informatiques à la demande

Avantages

- Déploiement rapide
- Réduction des coûts
- Facturation à la demande *pay-for-use*
- Evolutivité à grande échelle

Problématique

Utilisation malicieuse du Cloud Computing

- Attaques très dynamiques et largement distribuées
- L'anonymat de l'attaquant pourrait être garanti
- Les Botnets représentent les plus grands bénéficiaires

[C. Kassidy ET AL., 2011]

- Création d'un large Botcloud
- Réalisation d'attaques DDoS *(flooding et click fraud)*

[P. Hayati ET AL., 2012]

- Création de Botclouds auprès de 5 CSP
- Réalisation d'attaques (DDoS, Shellcode, traffic non conforme et envoi de Malwares)
- Attaques de longues durées (48h pour l'attaque DDoS)

Problématique

Constats

- Réalisation de toutes les attaques avec succès
- Aucune réaction ou contremesure de la part d'aucun des CSP

Objectif

- Proposition d'un système de détection déployé à la source contre les Botclouds
- Originalité
  - Détection à la source des Botclouds
  - Considération des métriques système dans la détection

Plan

Les attaques DDoS

Définition

A denial-of-service attack is characterized by an explicit attempt to prevent the legitimate use of a service. A distributed denial-of-service attack deploys multiple attacking entities to attain this goal
[J. Mirkovic ET AL., 2004].

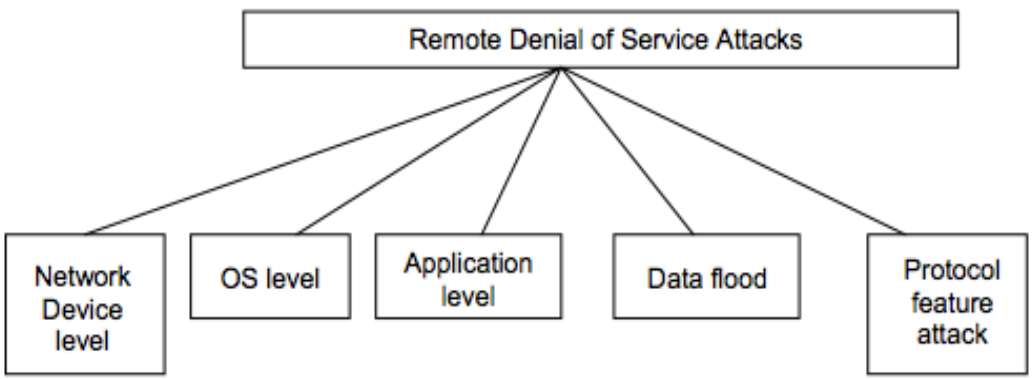


FIGURE: Classification des attaques DDoS [C. Douligeris ET AL., 2004]

Solutions actuelles de détection

- [J. Mazel ET AL., 2011] proposent une approche de détection reposant sur le clustering de flux réseau

  - Approche centralisée
  - Positionnement au point d'entrée du réseau cible

- [S. Loannidis ET AL., 2000] proposent une approche de firewall distribué

  - Repose sur un ensemble connu de règles
  - Echange des règles de filtrage des flux réseau
  - Positionnement au point d'entrée des réseaux cibles

Détection des attaques DDoS

- [J. Mirkovic ET AL., 2005] proposent une approche de détection déployé à la source

- Positionnement au point d'entrée des réseaux sources
- Corrélation des flux réseaux (requêtes/réponses)

Constat

- L'emplacement des IDS est majoritairement du coté de la cible
- Pas de contrôle du système de l'attaquant donc détection par des métriques réseau

Plan

Contexte général et environnement de test

Contexte

- Un CSP publique fournissant un service de type IaaS (ex : Amazon EC2)
- Le CSP contrôle un ensemble de serveurs physiques hébergeant un ensemble de VM appartenant a un ensemble de tenants
- Déploiement d'un Botcloud par un utilisateur malicieux
- Approche de monitoring non intrusive *"Black Box"* au niveau hyperviseur
- Métriques collectées : CPU (%) ; MEM (kBytes) ; TX (kBits/s) ; RX (kBits/s)

Contexte général et environnement de test

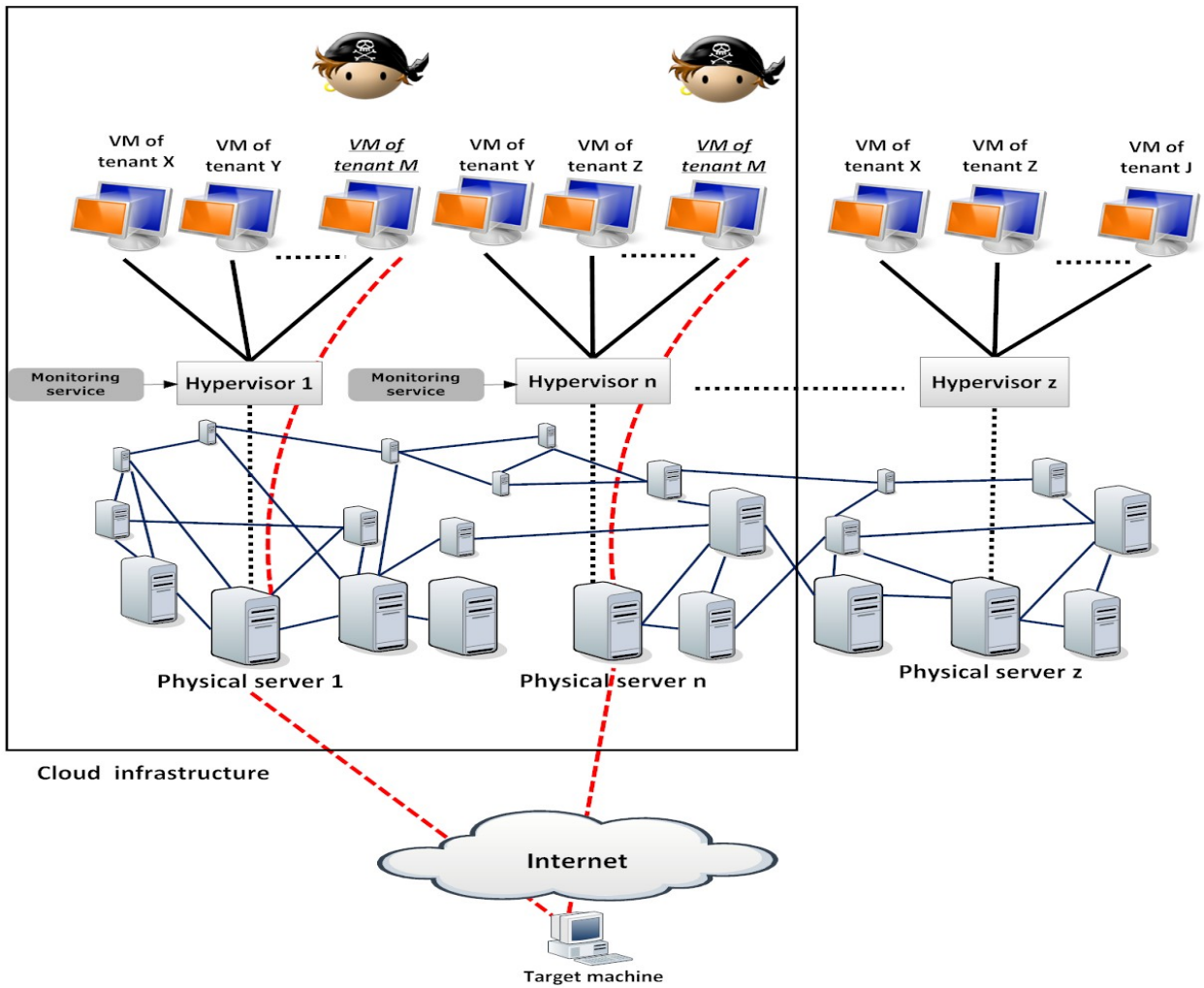


FIGURE: Environnement de test

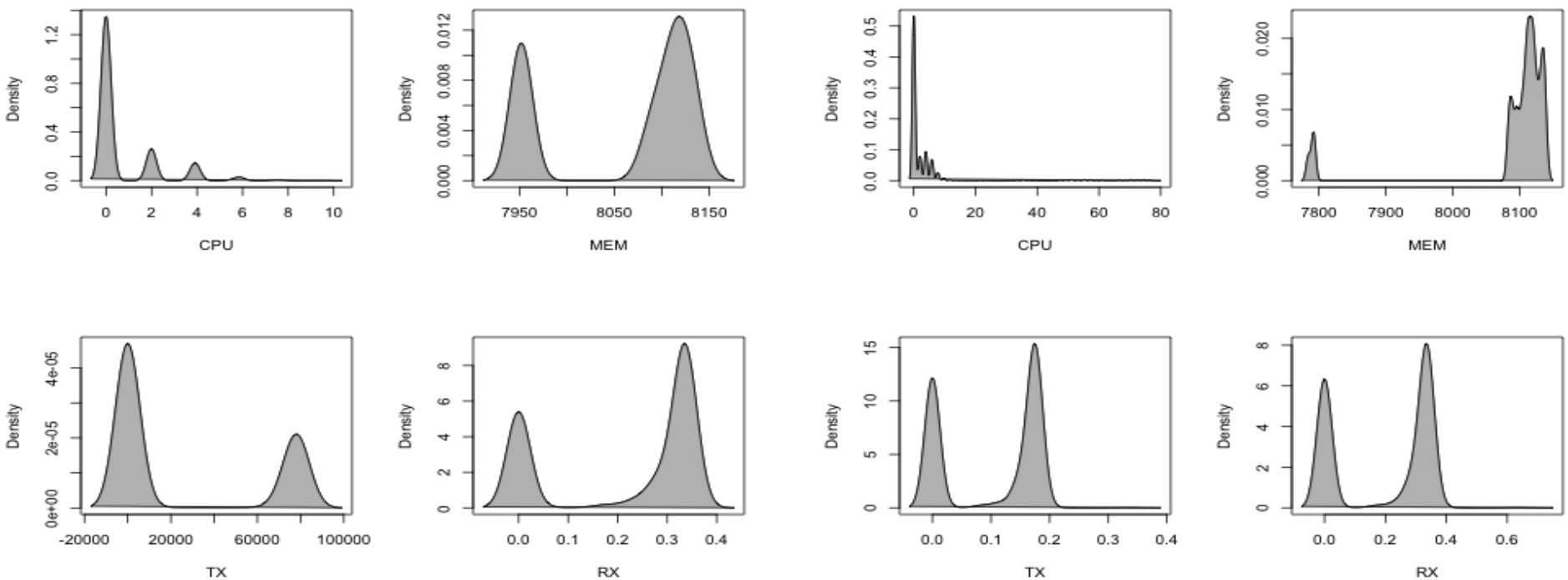
Scénarios

Paramètres	UDP Storm	TCP SYN Flood
Serveurs physiques	40	47
Tenants (attaquant incl.)	103	114
VM (attaquant incl.)	1,198	1,369
Débit d'attaque	10 MB/s	12,500 conn. per second
Durée de l'exp.	1h (état normal)+ 1h (attaque)+ 1h (repos)	
Environnement	Linux-Vserver (Planet-Lab)	
Botcloud (botnet)	Hybrid_V1.0	
Qté. de logs collectés	16,65 GO	

TABLE: Synthèse des paramètres de test

Distributions statistiques des métriques des botclouds

- Cas de l'attaque UDP (gauche) ; cas de l'attaque TCP (droite)
- Métriques : CPU (%) ; MEM (kBytes) ; TX (kBits/s) ; RX (kBits/s)



Analyse en composante principale

- Une méthode de statistique descriptive multidimensionnelle (méthode factorielle)
- Utilise la matrice de variance-covariance ou la matrice de corrélation
- Objectifs
  - Visualisation et interprétation des données à plusieurs dimensions
  - Compréhension des relations entre les différentes variables
- Avantages
  - Aucune hypothèse sur la distribution des données

ACP réalisée sur le tenant réalisant l'attaque UDP

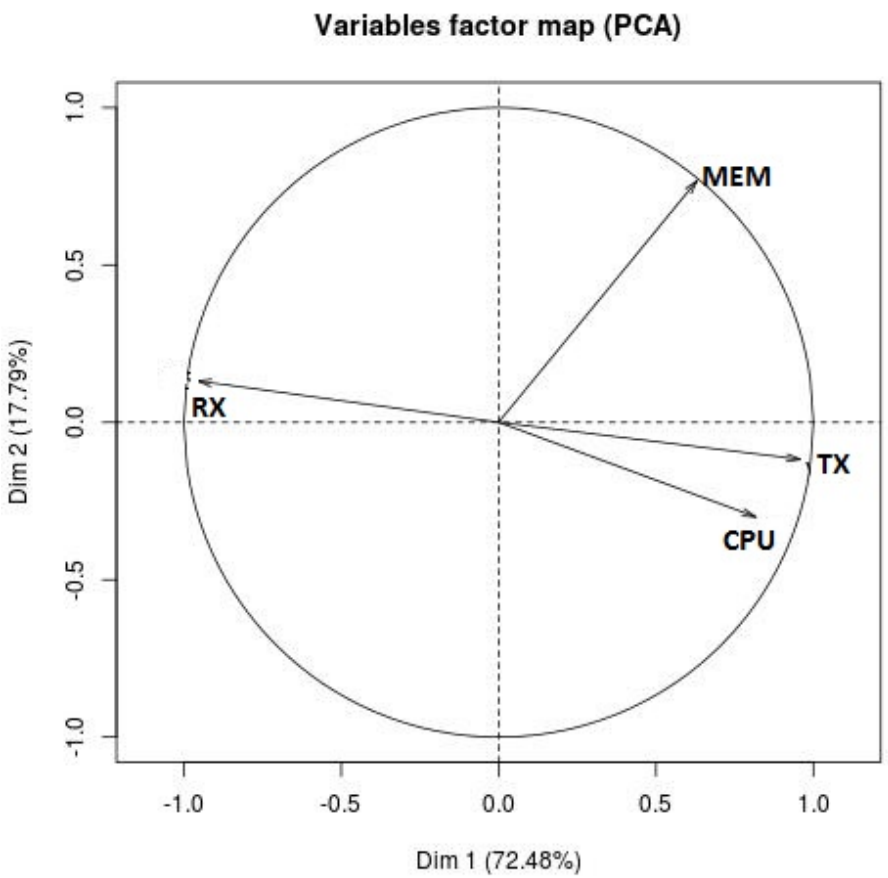


FIGURE: Botcloud

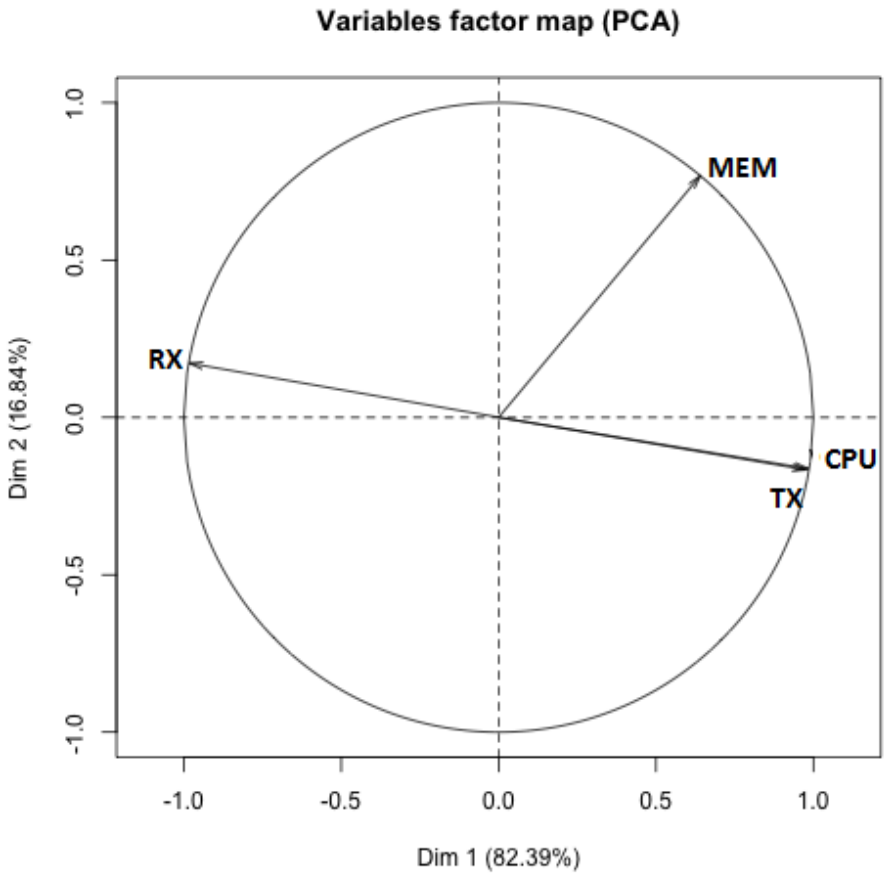
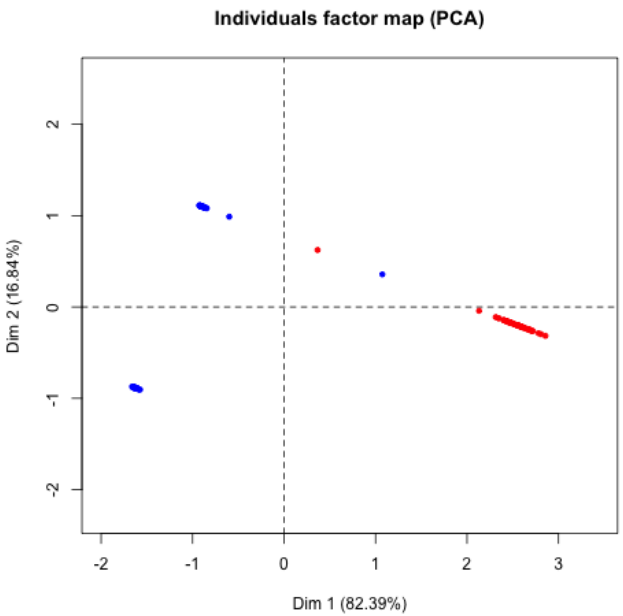
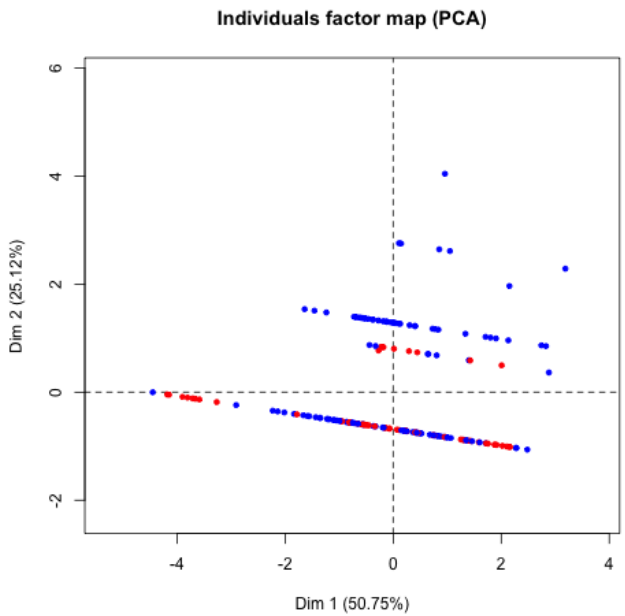
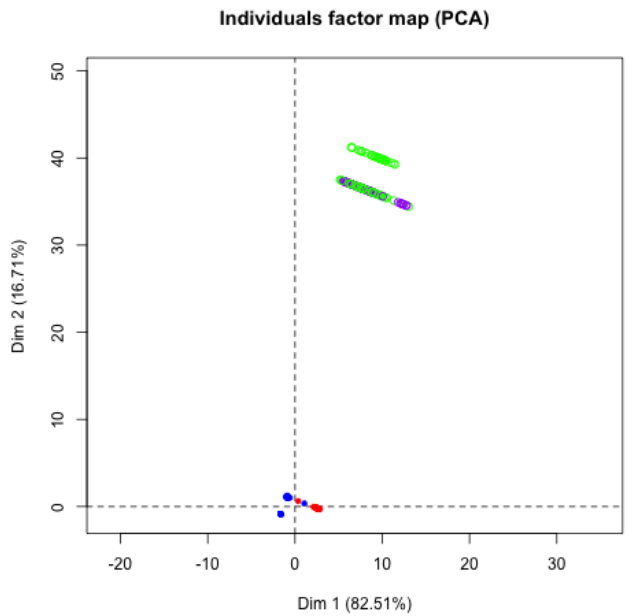


FIGURE: Moyenne du botcloud

ACP réalisée sur le tenant réalisant l'attaque UDP







ACP réalisée sur le tenant réalisant l'attaque TCP

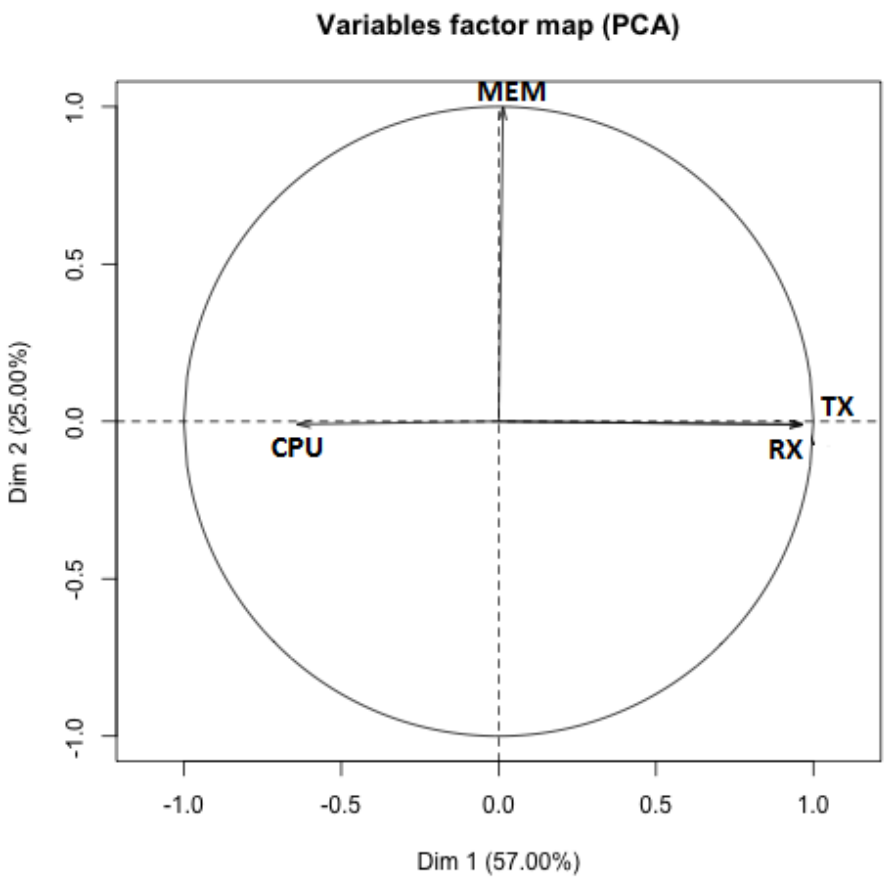


FIGURE: Botcloud

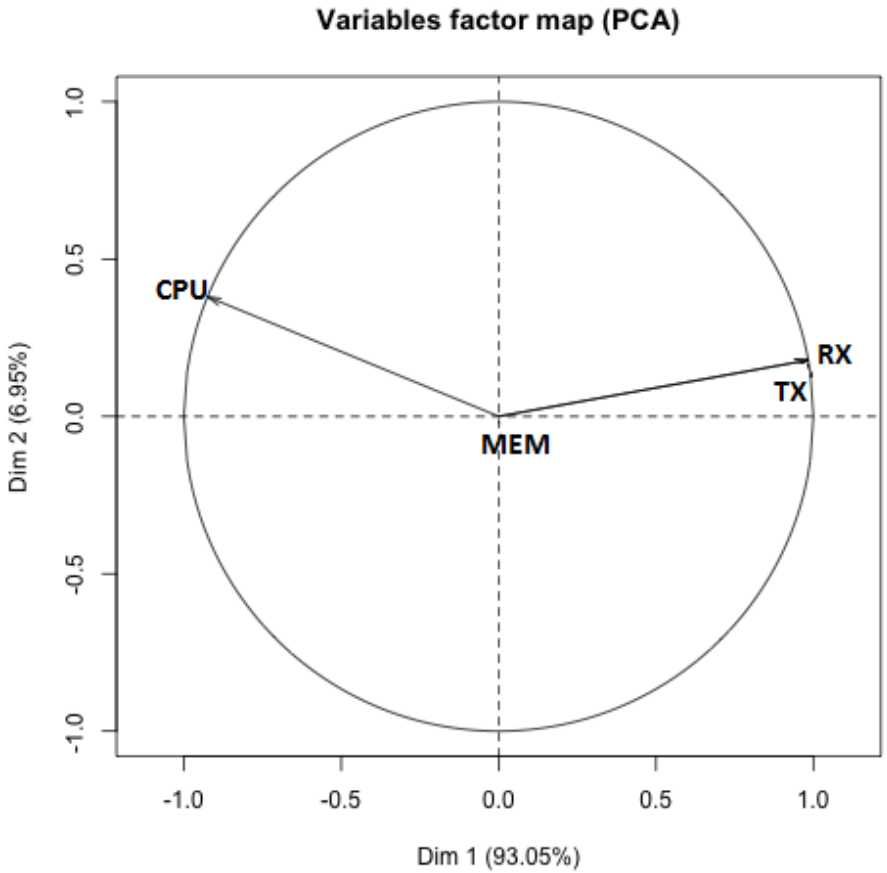
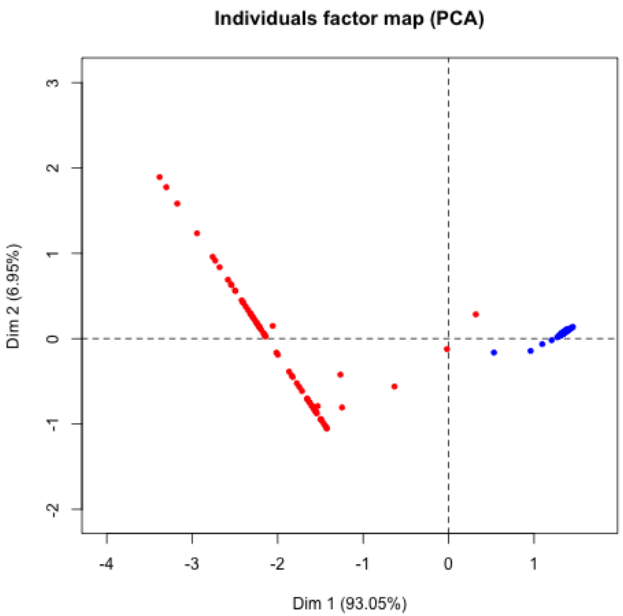
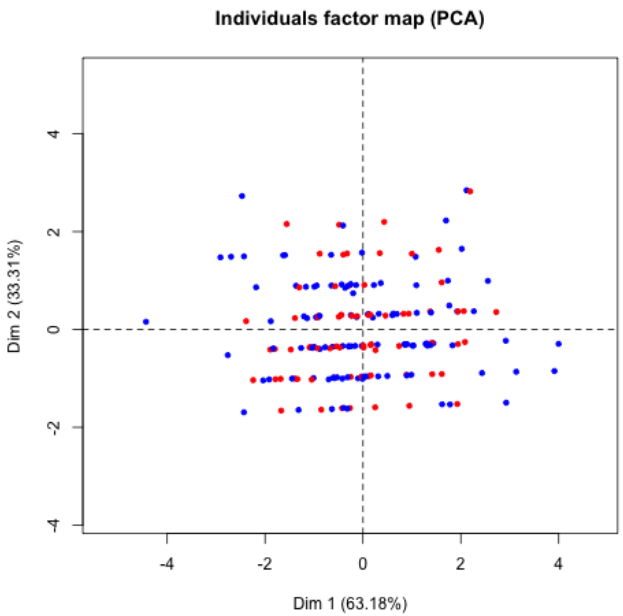
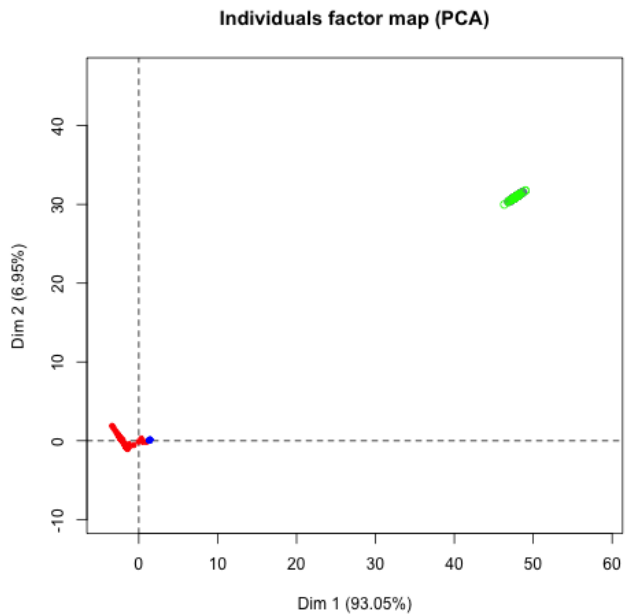


FIGURE: Moyenne du botcloud

ACP réalisée sur le tenant réalisant l'attaque TCP







Plan

Conclusion

Une expérimentation *in situ*

- Caractérisation des attaques DDoS à la source via une ACP
- Considération des métriques système
- Comportement fortement corrélé des VM attaquantes
- Possibilité de séparer l'activité d'un bocloud de celle des tenants légitimes

Perspectives

- Comparaison exhaustive avec l'ensemble des tenants
- Extension à d'autres paramètres d'attaque
- Considération des paramètres réseau dans l'étude
- Proposition d'un mécanisme de détection
- Développement d'une architecture collaborative d'auto-protection


botcloud an emerging platform for cyber-attacks, October 2012.
http ://baesystemsdetica.blogspot.fr.


Kassidy Clark, Martijn Warnier, and Frances M. T. Brazier.
The evolution of cloud computing markets.
Closer 11, 2011.


Christos Douligeris and Aikaterini Mitrokotsa.
Ddos attacks and defense mechanisms : classification and state-of-the-art.
Computer Networks, 44(5) :643 – 666, 2004.


Md. Tanzim Khorshed, A.B.M. Shawkat Ali, and Saleh A. Wasimi.
A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing.
Future Generation Computer Systems, 28(6) :833 – 851, 2012.


S. Ried, H. Kisker, and P. Matzke.
The evolution of cloud computing markets.
Forrester research paper, 2010.


Nahla Ben Amor, Salem Benferhat, and Zied Elouedi.
Naive bayes vs decision trees in intrusion detection systems.
In *Proceedings of the 2004 ACM symposium on Applied computing*, SAC '04, pages 420–424. ACM, 2004.


Byungrae Cha and Jongwon Kim.

Study of multistage anomaly detection for secured cloud computing resources in future internet.
In *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, pages 1046 –1050, 2011.


Wun-Hwa Chen, Sheng-Hsun Hsu, and Hwang-Pin Shen.
Application of svm and ann for intrusion detection.
Computers and Operations Research, 32(10) :2617 – 2634, 2005.


Xin Xu and Xuening Wang.
An adaptive network intrusion detection method based on pca and support vector machines.
In *Advanced Data Mining and Applications*, volume 3584 of *Lecture Notes in Computer Science*, pages 696–703. Springer Berlin Heidelberg, 2005.


Srinivas Mukkamala, Guadalupe Janoski, and Andrew Sung.
Intrusion detection using neural networks and support vector machines.
In *Neural Networks, 2002. IJCNN'02. Proceedings of the 2002 International Joint Conference on*, volume 2, pages 1702–1707. IEEE, 2002.


Gary Stein, Bing Chen, Annie S. Wu, and Kien A. Hua.
Decision tree classifier for network intrusion detection with ga-based feature selection.
In *Proceedings of the 43rd annual Southeast regional conference - Volume 2*, ACM-SE 43, pages 136–141. ACM, 2005.


J. Mirkovic and P. Reiher.
D-ward : a source-end defense against flooding denial-of-service attacks.
Dependable and Secure Computing, IEEE Transactions on, 2(3) :216– 232, july-sept. 2005.


Jelena Mirkovic and Peter Reiher.
A taxonomy of ddos attack and ddos defense mechanisms.
SIGCOMM Comput. Commun. Rev., 34(2) :39–53, 2004.


Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin, and Jonathan M. Smith.
Implementing a distributed firewall.
In *Proceedings of the 7th ACM conference on Computer and communications security*, CCS '00, pages 190–199. ACM, 2000.


Johan Mazel, Pedro Casas, Yann Labit, and Philippe Owezarski.
Sub-space clustering, inter-clustering results association & anomaly correlation for unsupervised network anomaly detection.
In *Proceedings of the 7th International Conference on Network and Services Management*, CNSM '11, pages 73–80. International Federation for Information Processing, 2011.

Merci