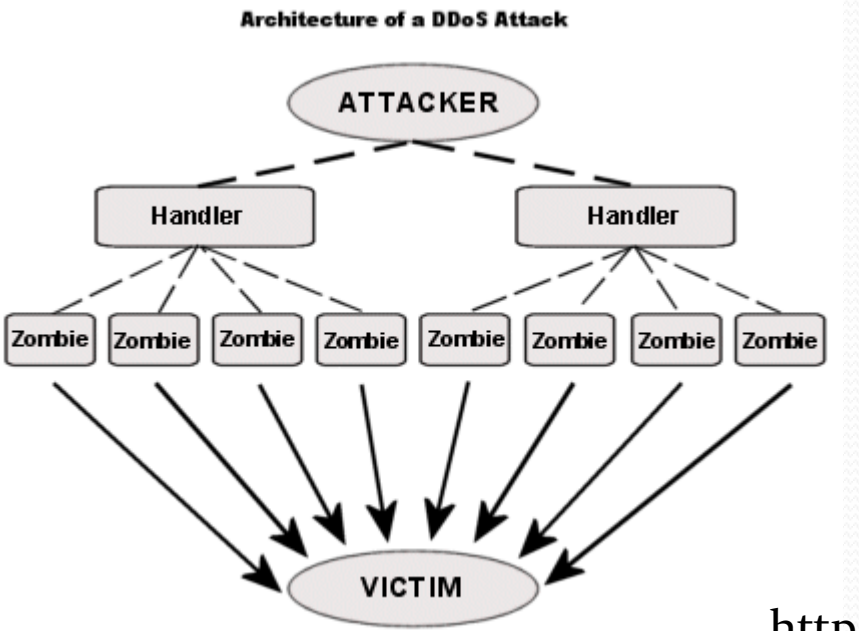
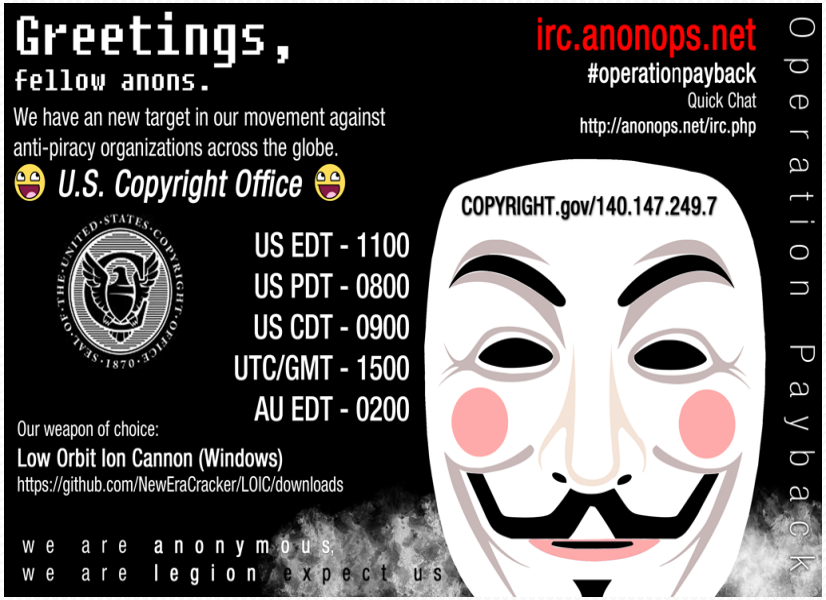
Distributed Denial of Service (DDoS) attacks and Mitigation in Cloud Environments

Mark Shtern

DDoS Attacks

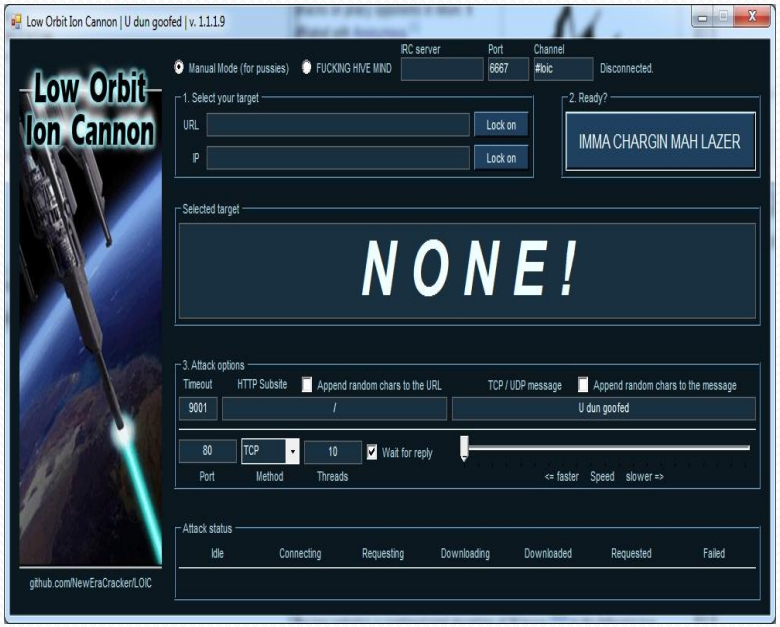




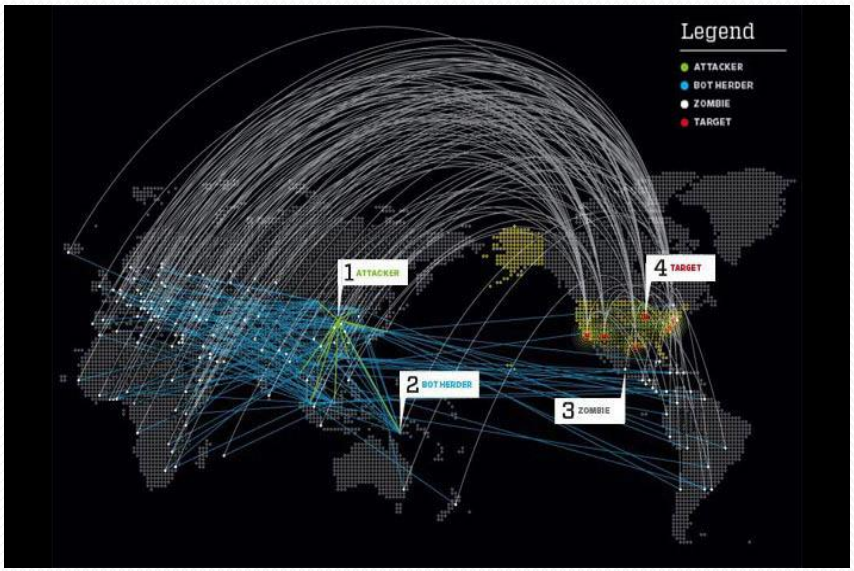
http://en.wikipedia.org/wiki/Operation_Payback

http://www.betterhostreview.com/wp-content/uploads/2013/08/ddos-attack.gif

DDoS Attacks



http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon



http://blog.rivalhost.com/wp-content/uploads/2012/11/DDoS-network-map.jpg

Lower and Slow DDoS Attacks

- Attack aimed at bringing a target down but doing so quietly
- Examples
  - Sending partial http requests
  - Sending small data packets or keep alives in order to keep the session from going to idle timeout

http://www.funnyjunk.com/funny_pictures/3290705/Operation+9fag/

Layer-7 DDoS Attacks

- "An application layer DDoS attack is a form of DDoS attack) where attackers target the application layer"

  (copied from "http://en.wikipedia.org/wiki/Application_layer_DDoS_attack")
- Layer-7 DDoS attacks represent 20% of all DDoS attacks in 2013

  (from http://www.ababj.com/component/k2/item/4354-what-you-should-know-about-worsening-ddos-attacks)
- 37 percent of the respondents seeing application-layer attacks targeting this service compared to 24 percent last year

  (from http://www.securityweek.com/multi-vector-ddos-attacks-grow)
- Application layer attacks may become widespread

  (from http://www.ababj.com/component/k2/item/4354-what-you-should-know-about-worsening-ddos-attacks)

DDoS Attacks

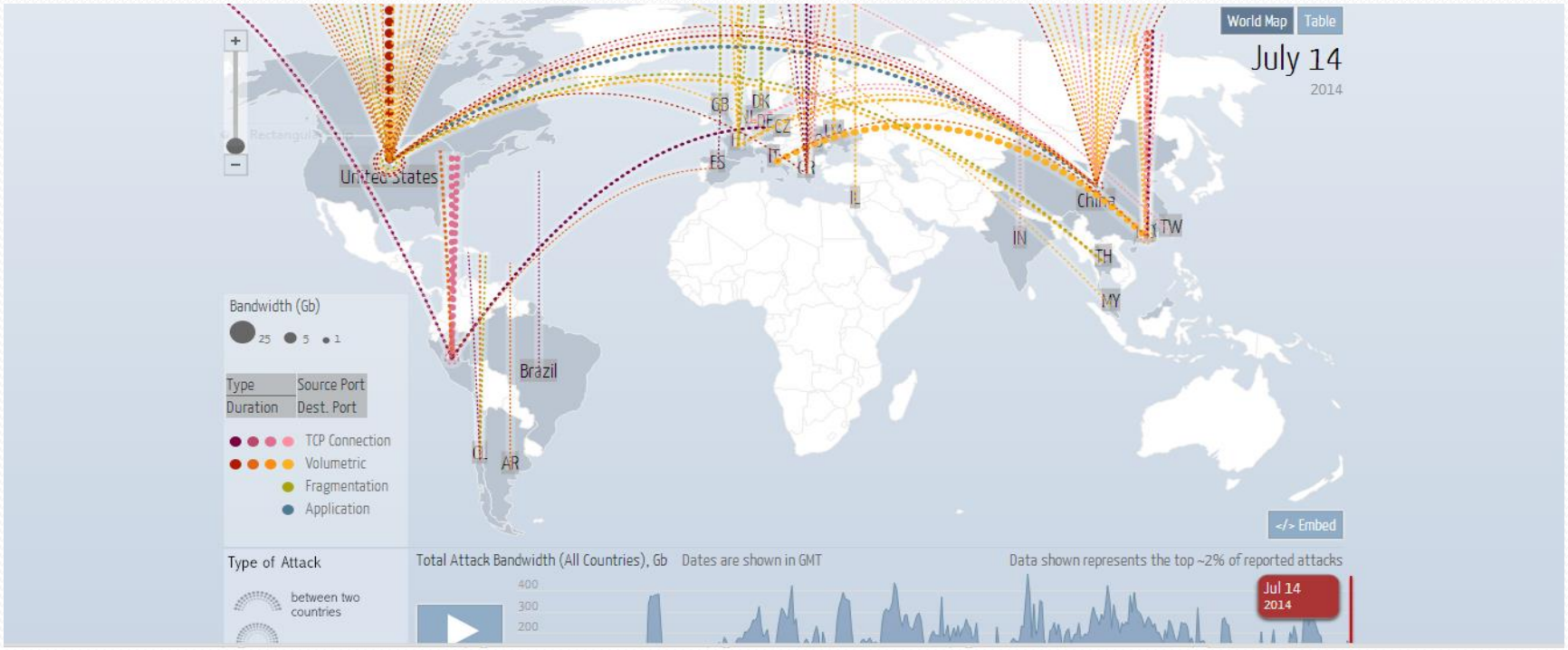
"There is a very clear trend we see in the increased use of complex multi-vector and application layer attacks,"
(from http://www.securityweek.com/multi-vector-ddos-attacks-grow)

"the **reduction in dedicated security** resources among respondent organizations"
(from http://www.securityweek.com/multi-vector-ddos-attacks-grow)

http://www.cnbc.com/id/101461573

Meetup.com is fighting a sustained battle against cyber attackers who are demanding only $300 to call off

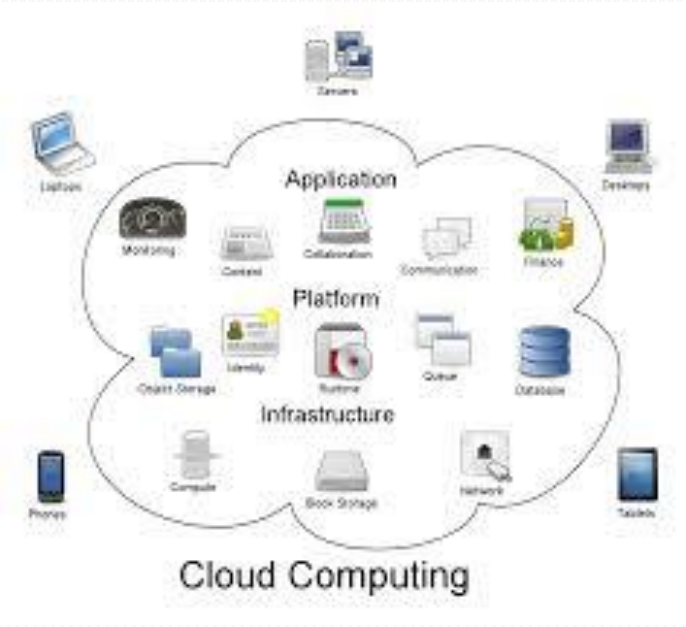
Top daily DDoS attacks worldwide



http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16265&view=map

Software Defined Infrastructure

- Example
  - Infrastructure-as-a-service (IaaS)
- Key property
  - Agility
- Pricing model
  - Pay as you go



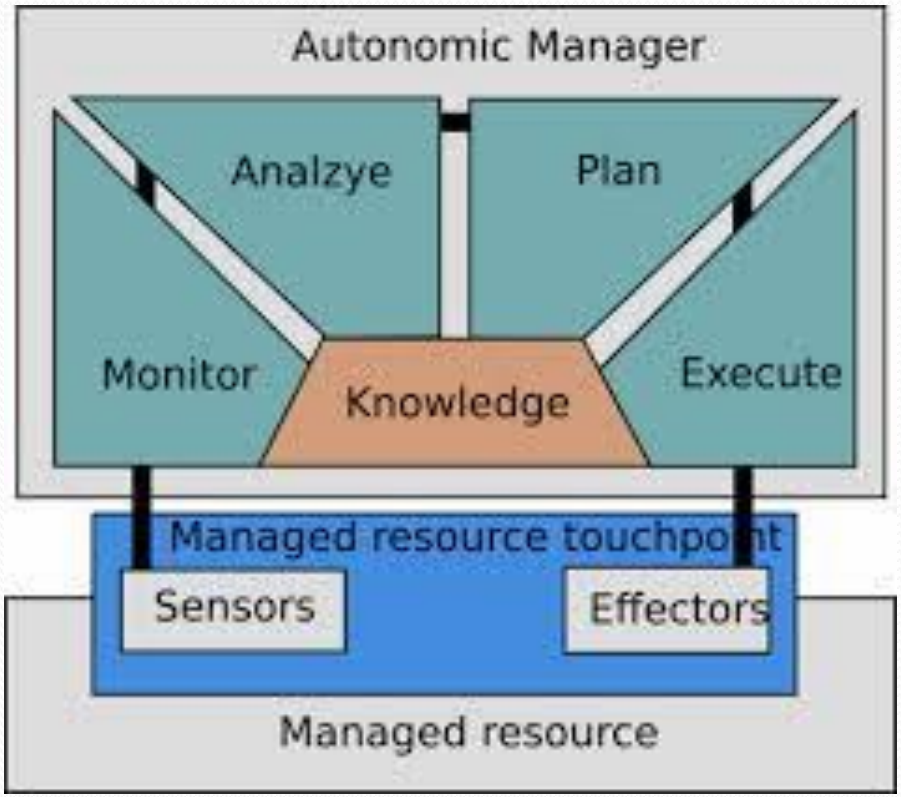
http://en.wikipedia.org/wiki/Cloud_computing

The Changing Management Landscape

- Traditional IT duties
  - Resource capacity planning
  - Security of both infrastructure and production applications
  - Long release cycle
- SDI Ecosystem
  - Security responsibilities
    - Cloud provider - infrastructure
    - Application owner – application
  - Capacity planning: elasticity
  - Short release cycle

Elastic Applications

- Autonomic/Adaptive system



https://wwwvs.cs.hs-rm.de/vs-wiki/index.php/(WS12-01)_Cloud/Dokumentation

Challenges

- Optimization resource managements
- Measurement of running application cost is complex task because of the cost of IaaS resources is not typically available from the provider
- Misuse infrastructure resources and reduction profit due to malicious activities
  - DDoS

Cost-of-Service Attack

- Is to increase the cost of a cloud deployment without necessarily denying service

http://www.rawstory.com/rs/2011/08/02/new-lead-in-1970s-us-skyjacking-case/

http://www.projektwerk.com/en/blog/freelance/category/trends

Resource-consumption Attacks

- Attack increases resource utilization without a corresponding increase in revenue
  - **Autoimmune resource attack** → the user through carelessness or error incurs unnecessary charges on their own resources
  - **Denial of service**
  - **Cost-of-service attacks** → the goal is to increase the cost a cloud deployment without necessarily denying service
  - **Low-and-slow DoS**

Detection

Cloud efficiency metric

- Cost-benefit analysis that compares the current benefit derived from an application to the current cost of running that application on software-defined infrastructure
- Is the ratio of a benefit function:cost function, where both functions update as frequently as possible

Title: A runtime cloud efficiency software quality metric.
Authors: Shtern, Mark and Smit, Michael and Simmons, Bradley and Litoiu, Marin

Cost/benefit estimation

- Cost of total number of resources needed
  - Performance model
- Benefit is income generated by protected application

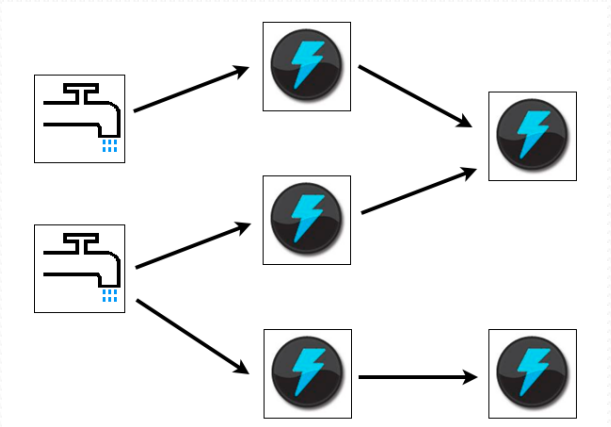
Prices

- Instances
  - On demand
  - Reserved
  - Spot
- Data Transfer
  - Data Transfer IN To Amazon EC2
  - Data Transfer OUT From Amazon EC2
- Storage
- Elastic Load Balancing
- Glacier

http://openclipart.org/detail/169130/mapa-de-redes-by-ainara14-169130

Cost Monitoring

- Twitter storm
  - distributed realtime computation system
- Cloud monitoring
  - CloudWatch, Ceilometer etc

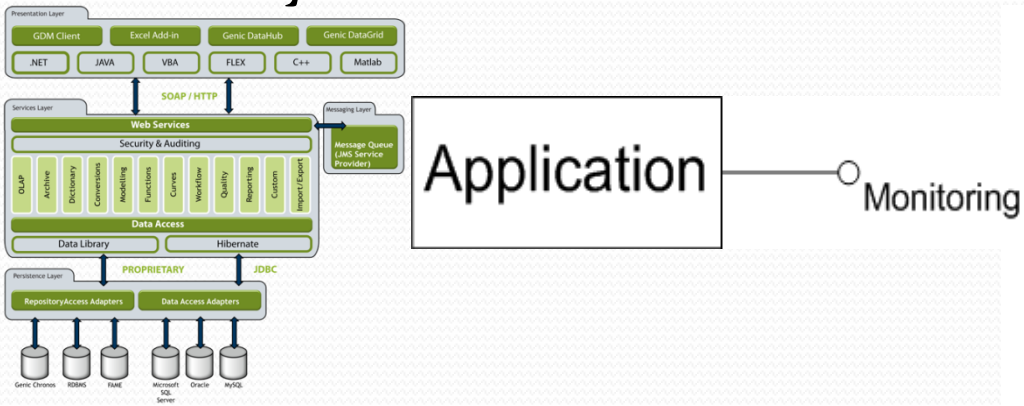


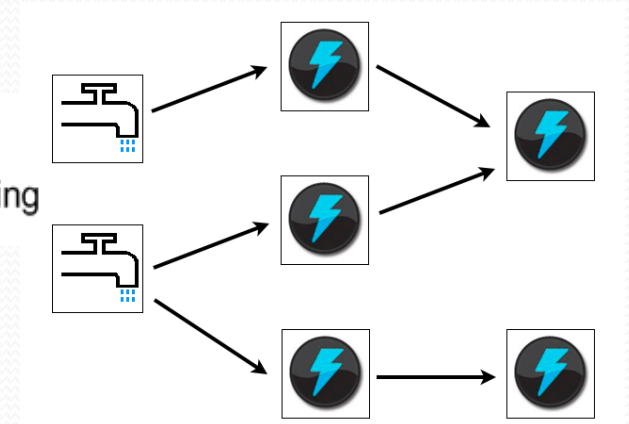
http://www.clipartbest.com/clipart-di85pb8XT

Title: Distributed, application-level monitoring for heterogeneous clouds using stream processing
Authors: Smit, Michael and Simmons, Bradley and Litoiu, Marin

Benefit Monitoring

- Twitter storm
- Information sources
  - Application, Google Adsense API, PayPal, Google Analytics





http://www.datagenicgroup.com/our-products/enterprise-data-management/technical.html

http://www.clipartbest.com/clipart-di85pb8XT

Benefit Monitoring

- Revenue
- Advertising
- Brand awareness
- Customer satisfaction
- Number of repeat customers

Cloud efficiency metric

$$CE = \frac{benefit}{cost}$$

- CE > threshold
  - Profitable
- CE < threshold
  - Overspending

Performance model

- Models hardware/software resources
  - Hardware: CPU, Network
  - Software: Number of threads, Critical sections
- Estimate performance metrics
  - Throughput, response time, CPU utilization

Behavior Analysis

- Baseline
- Behavior Anomaly Detection
  - Statistical mode
  - Machine learning

Cloud Resource Management

- Cloud variability
  - Resources a cloud provider deems identical may have performance variations, by as much as 40%
- Non cost effective action
  - When allocated resources do not meet expectations, an adaptive system's response is to acquire more resources
  - Higher cost without expected benefits

Shark Tank

Shark Tank

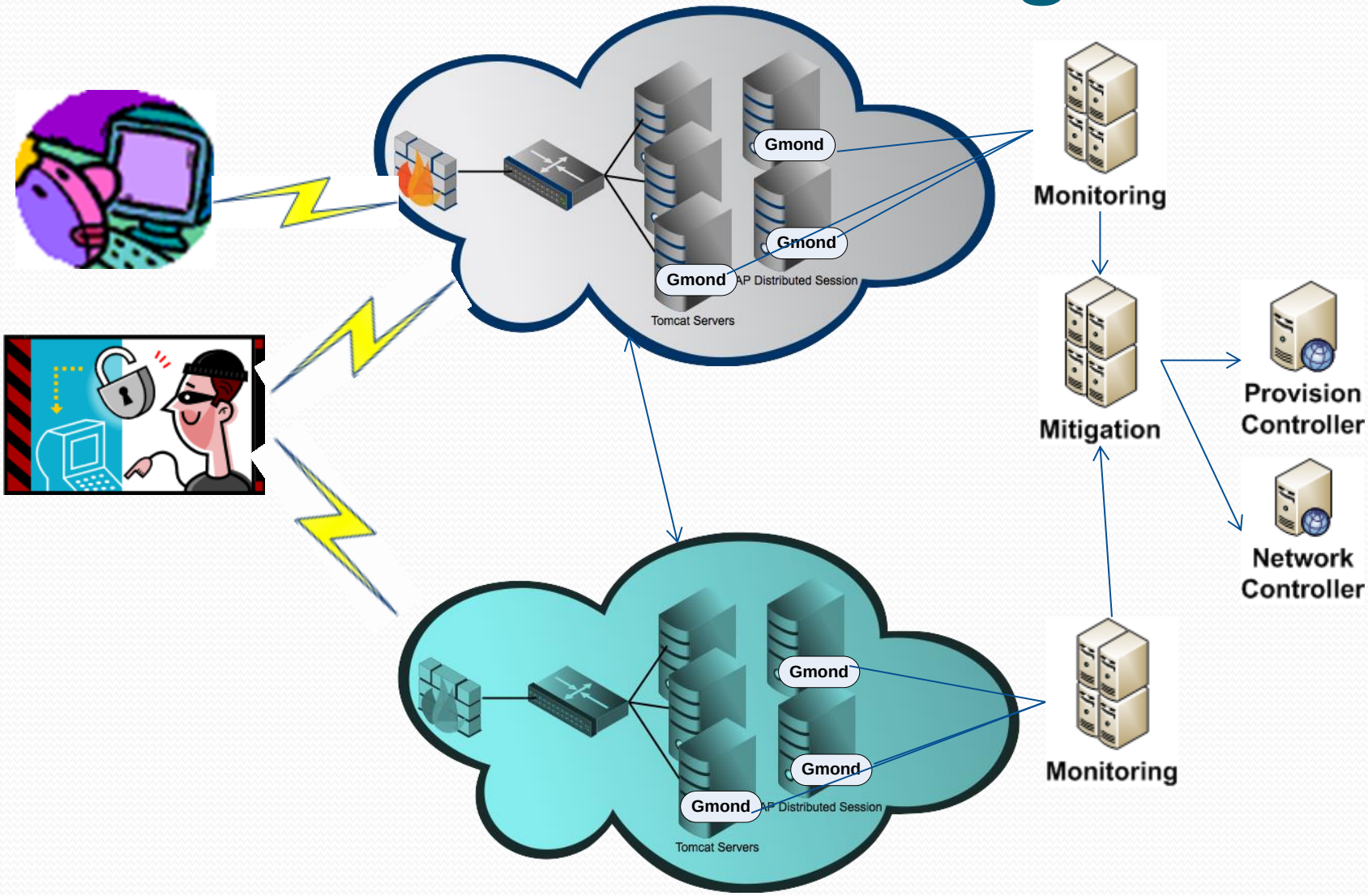
- Is a separate cluster with full application capabilities designed to monitor suspicious users

Title: Towards Mitigation of Low and Slow Application DDoS Attack**s**
Authors: Mark Shtern Roni Sandel Marin Litoiu Chris Bachalo Vasileios Theodorou

Software Defined Infrastructure

- Technology umbrella for infrastructure management
  - Chip-level virtualization accelerators
  - Virtual storage accelerators
  - Network package accelerators
  - Orchestration

Low & Slow DDoS Mitigation



Software Defined Network

- ”is an approach to computer networking that allows network administrators to manage network services through abstraction of lower level functionality”

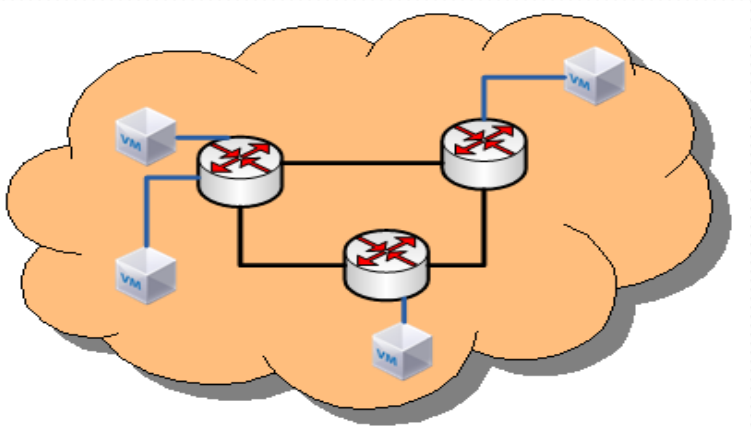
  (from Wikipedia: http://en.wikipedia.org/wiki/Software-defined_networking)
- Openflow
- Service-chaining (Ericsson Cloud System, Contrail (Juniper Network) Opencontrail)

Software Defined Network

- Overlay network
  - VPN/tunnel
- IPTables
- Application-Informed Request Routing

Application-Informed Request Routing

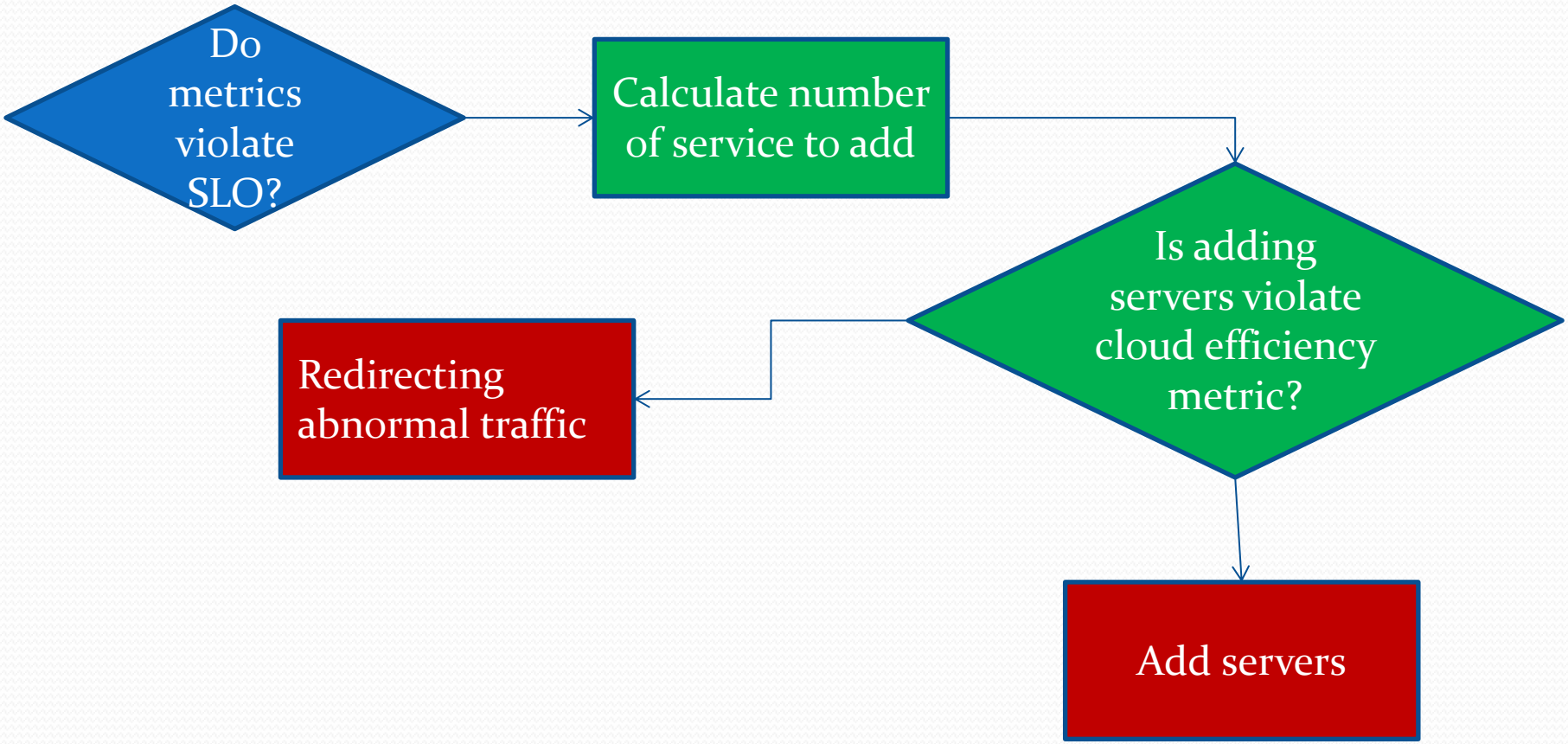
- Application-informed routing allows the application to inform routing decisions
  - Geography, lowest latency, common backbone providers, cost-aware routing



Title: Navigating the clouds with a MAP
Authors: Shtern, Mark and Simmons, Bradley and Smit, Michael and Litoiu, Marin

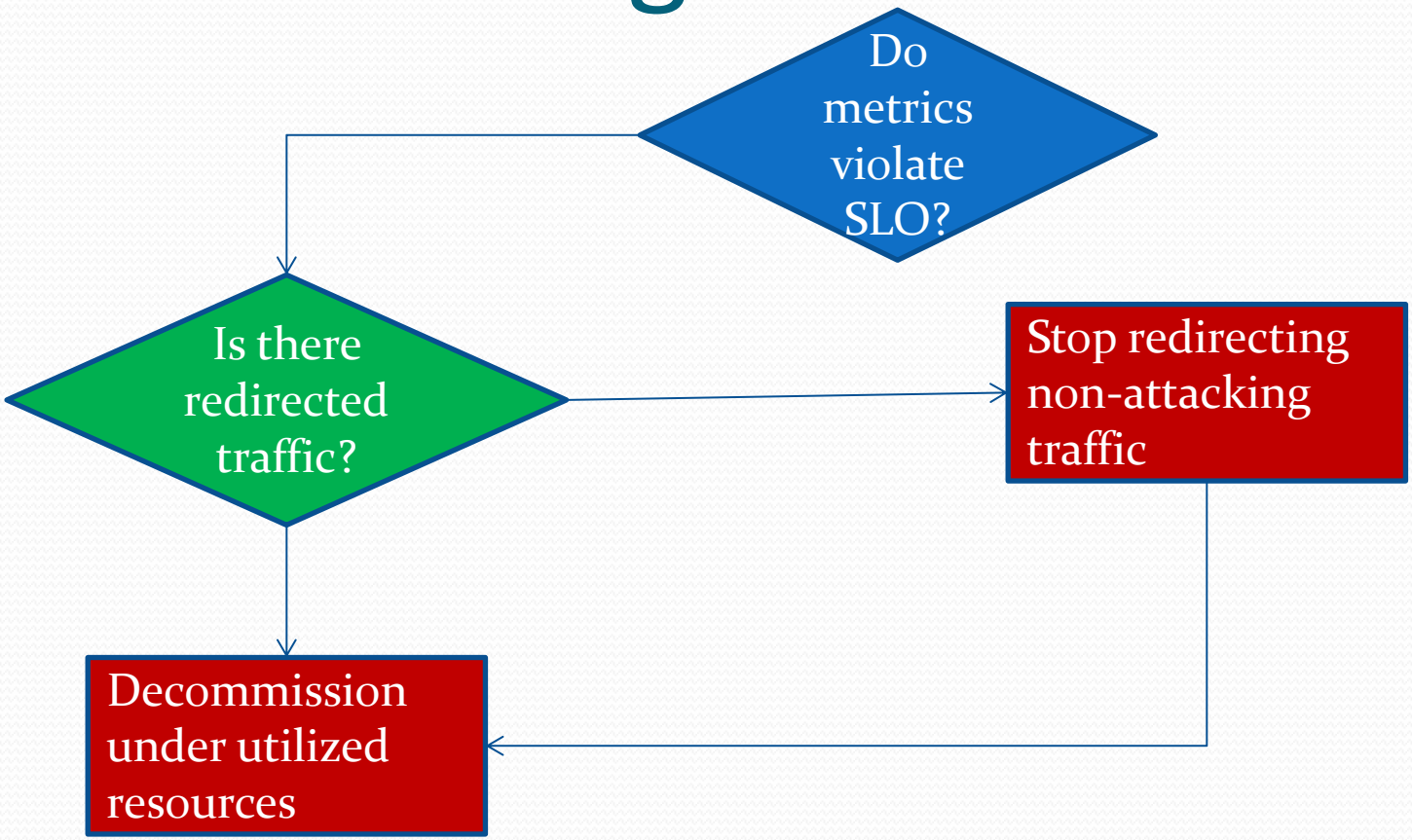
Auto-scaling

Decision engine



Title: Model-driven Elasticity and DoS Attack Mitigation in Cloud Environments
Authors: Computing, Autonomic and Barna, Cornel and Shtern, Mark and Smit, Michael and Ghanbari, Hamoun and Litoiu, Marin

Decision engine



Conclusion

- Discussed algorithm to scale a web application, mitigate a DoS attack, or both, based on an assessment of the business value of workload

Thank you

Q&A