POWER ATTACK: AN INCREASING THREAT TO DATA CENTERS

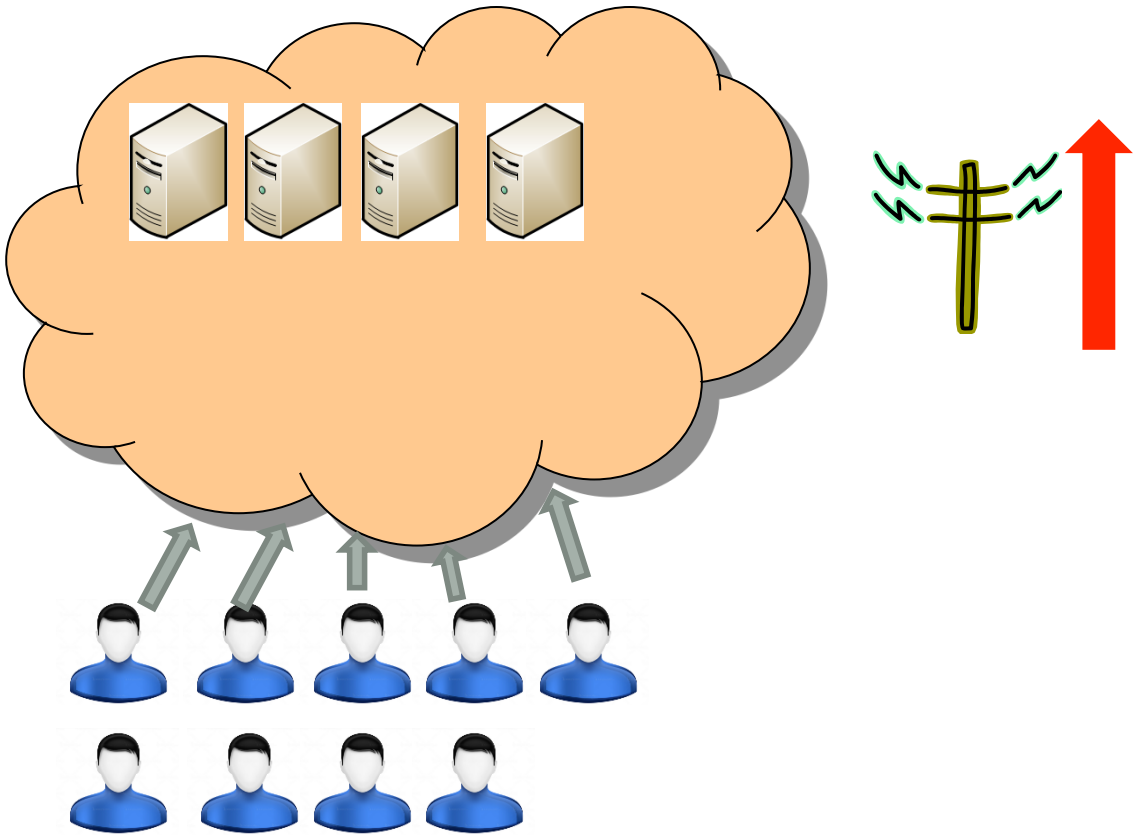
Zhang Xu*, Haining Wang*, Zichen Xu +, Xiaorui Wang+

*College of William and Mary

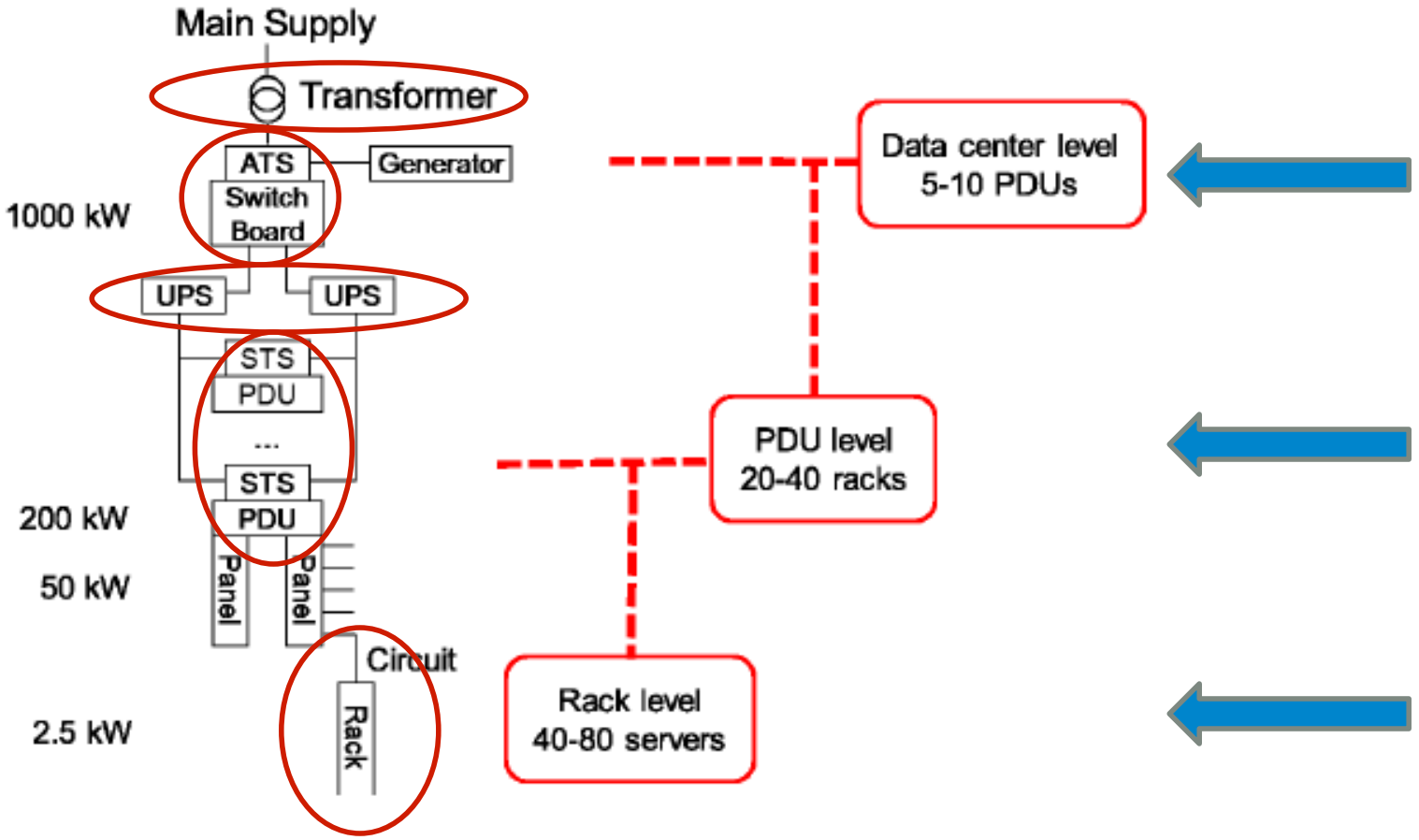
+Ohio State University

Era of Cloud Computing

- Increasing scale of data centers
  - For private and public cloud services



Power Provisioning in Data Centers



Power oversubscription

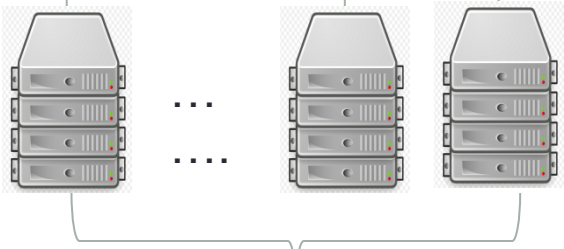
- Increasing power demand v.s. outdated supplying system
  - Upgrading power infrastructures is *costly*: tens of millions dollars!
  - Upgrading power infrastructures is *complicated*: interruption of services
  - Upgrading power infrastructure can be restricted

How to host more servers with limited power?

- The power consumption of different servers/racks rarely peak simultaneously

Assumption Always Holds?

200KW



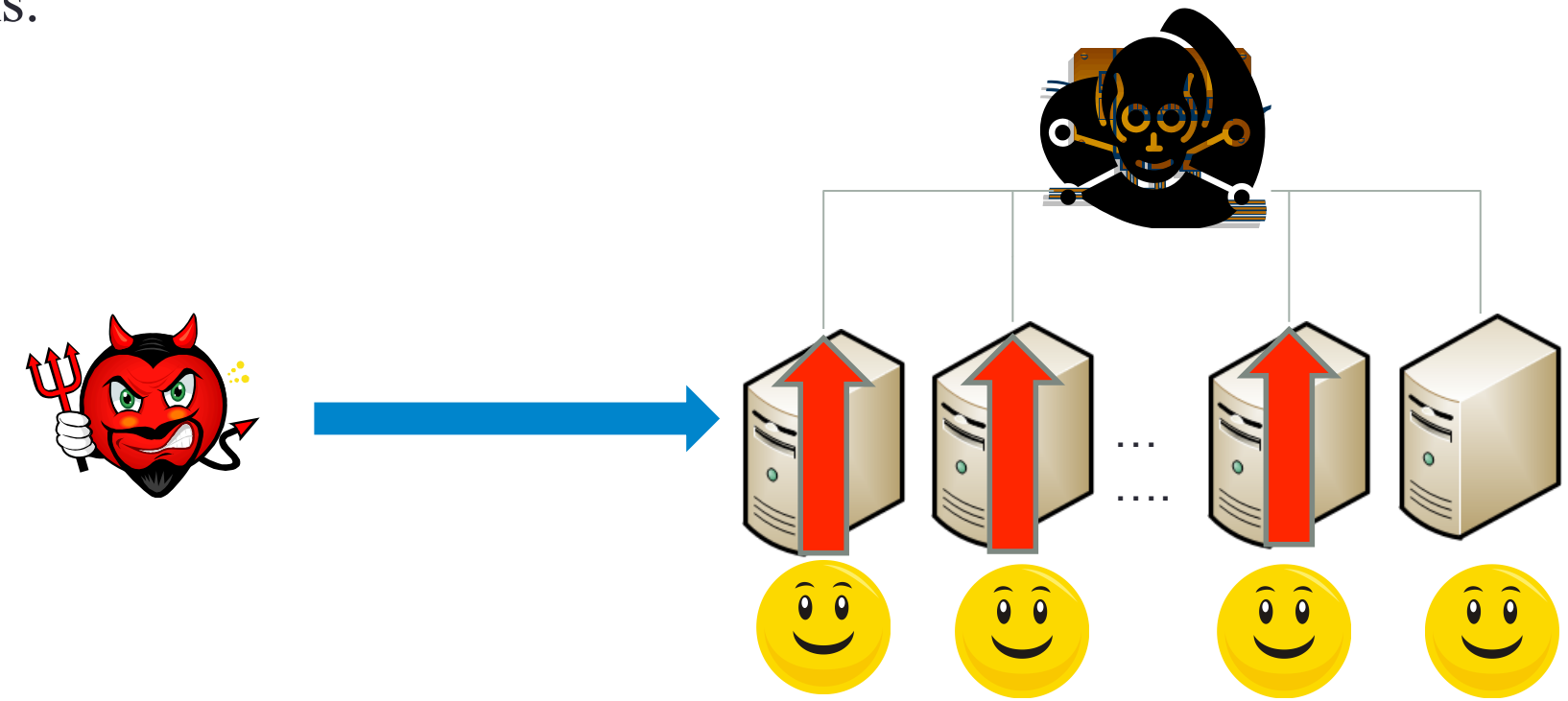
10KW … ….

20

Power oversubscription

Power Attack

- In a data center hosting public cloud services, an attacker can exploit power oversubscription to trip circuit breakers by simultaneously triggering power peaks on multiple servers/ racks.



Threat Model: Target

- Target: tripper CBs in a data center
  - Hosting public cloud service
  - Power oversubscription
  - Power management deployed beyond rack level

- Attacker: individual hacker or cyber-crime organization
  - Behave as normal user
  - Have sufficient resources
  - Locating targets through various probing techniques

Power attack

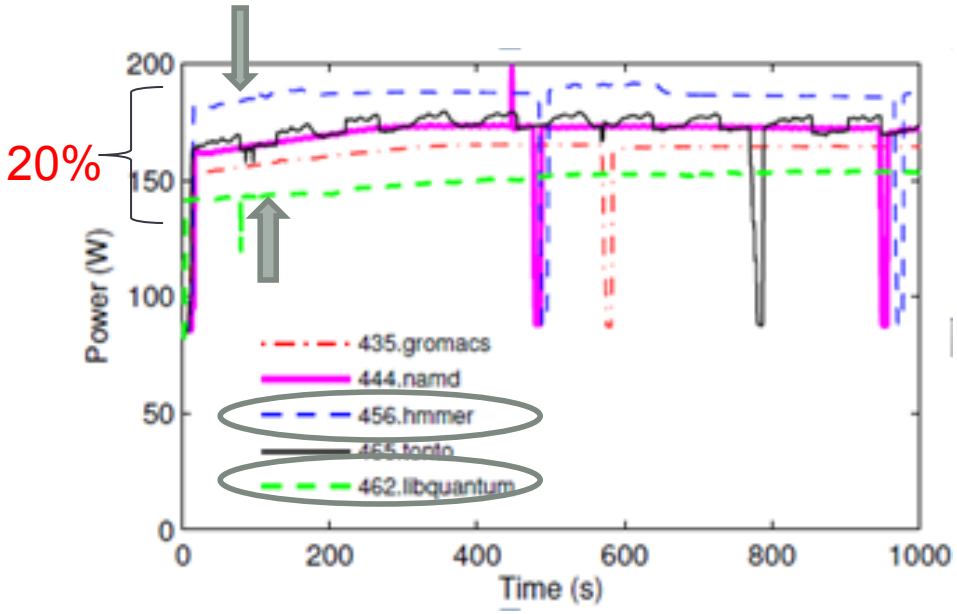
- Rack level attack
  - Physical experiments on testbeds
  - PaaS
  - IaaS
  - SaaS
- PDU/Data Center level attack
  - Simulation based on real world data center trace

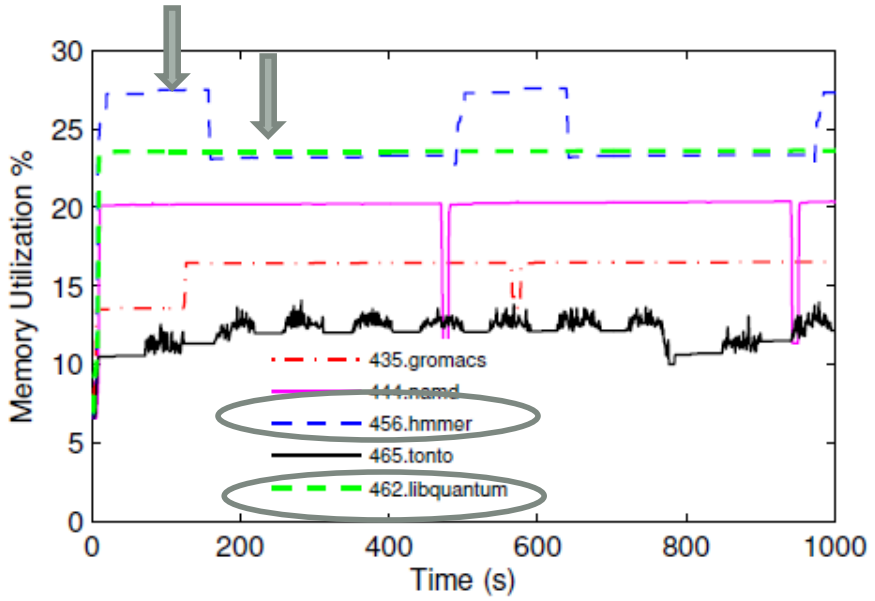
Attacking PaaS

- Attacker needs to manipulate workloads running upon PaaS to cause sudden rise of power consumption
- Utilization-based load balancing may be deployed to prevent workload skew
- Increasing power consumption with fixed system utilization?

Attacking PaaS

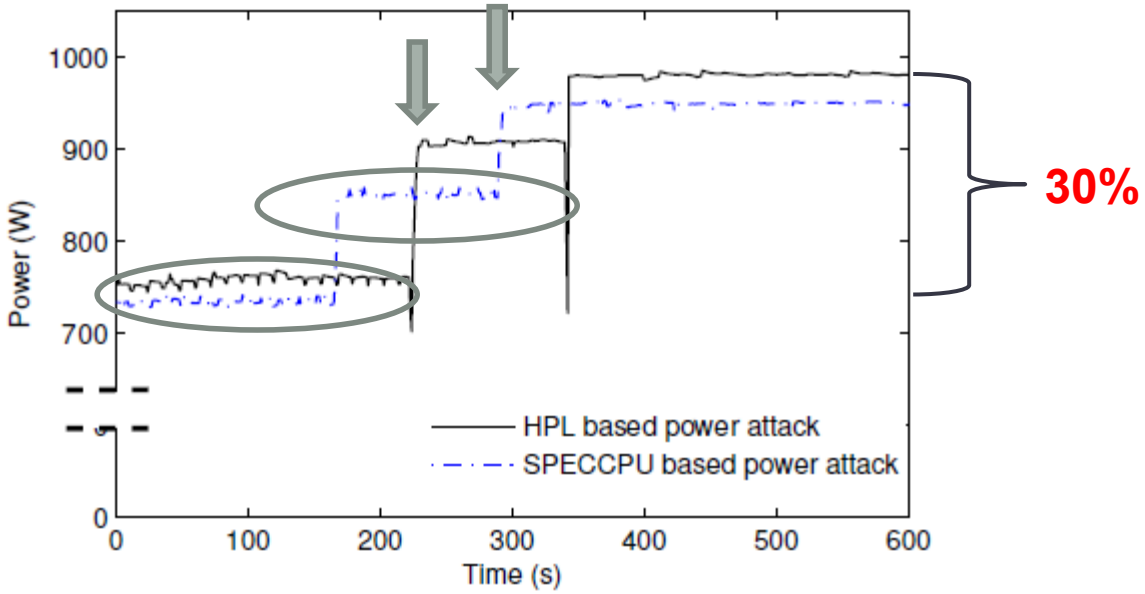
- High performance computing as typical workload in PaaS
  - SPECCPU and High Performance Linpack(HPL) as HPC benchmarks





Attacking PaaS

- Attack Vector in PaaS: Increasing workload and adjusting workload pattern



Power consumption of victim rack under power attack

Attacking IaaS

- Attacker can launch many VMs and run arbitrary workload on them

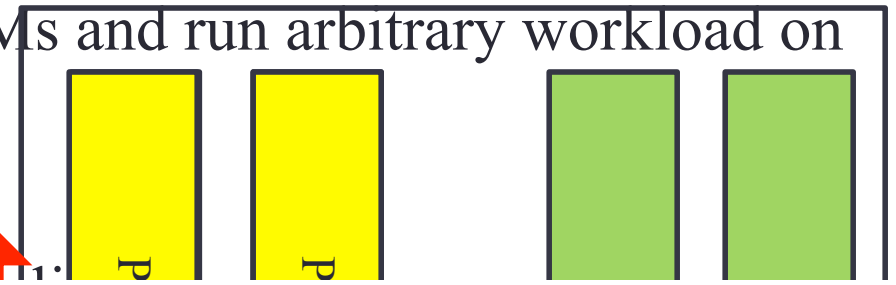
Parasite attacks

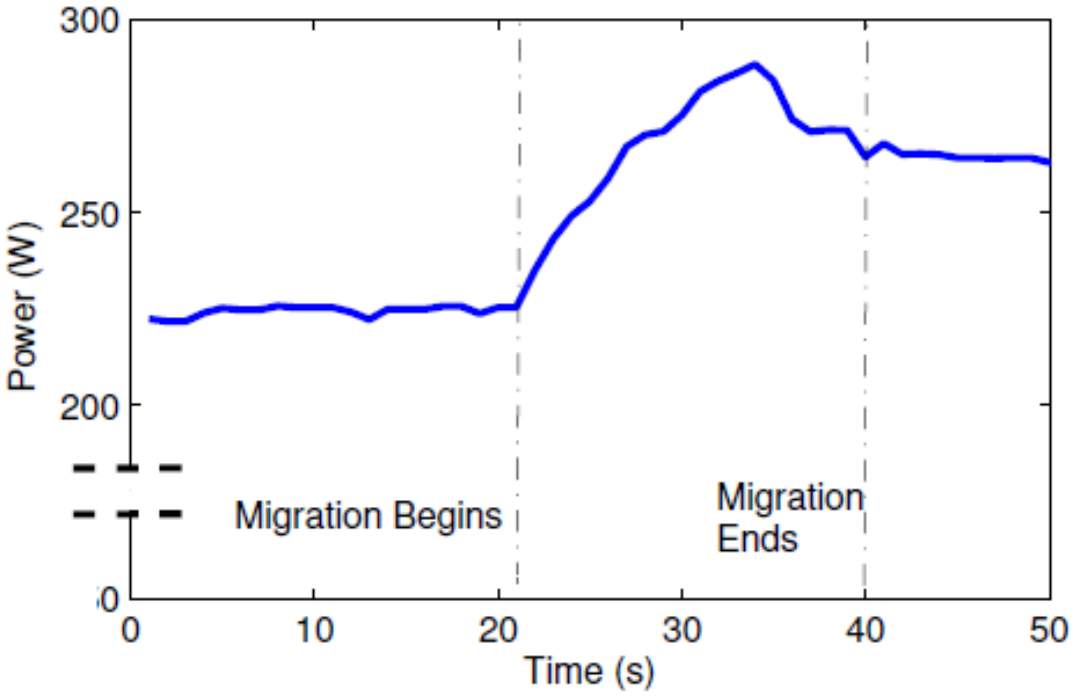
Parasites attack host from inside

- Overhead introduced by

VM Migration

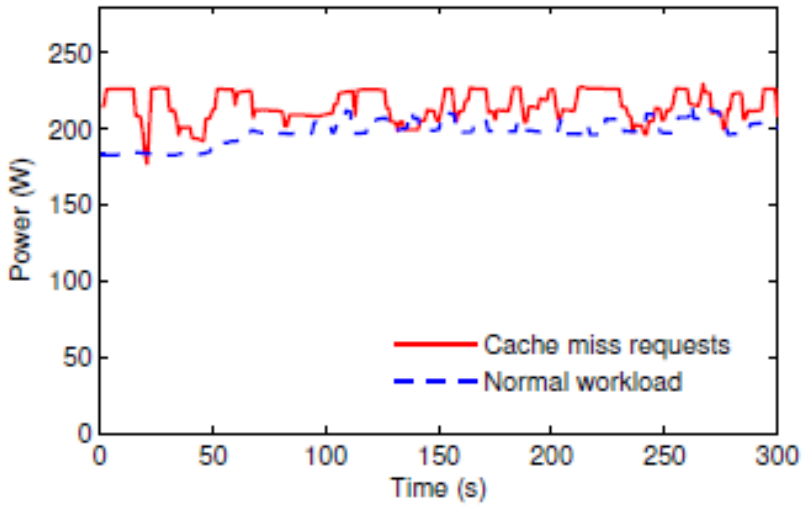
Make rack more vulnerable



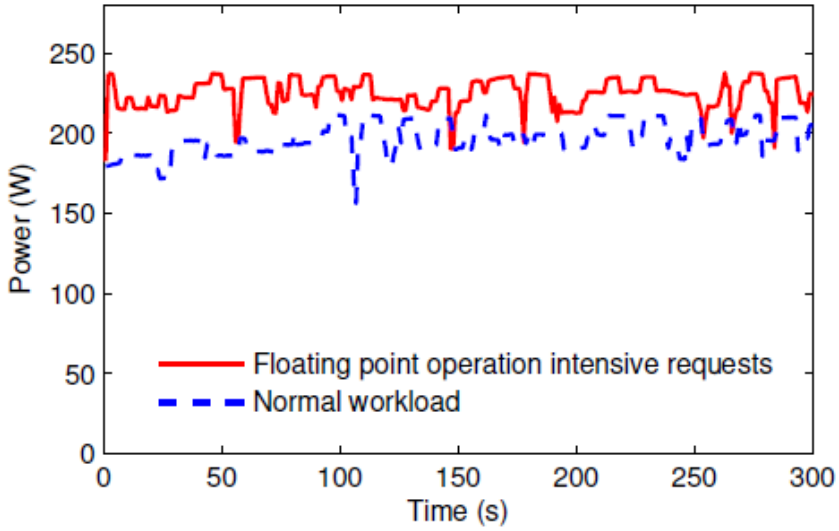


Attacking SaaS

- Web service is the typical workload in SaaS
- Web requests impact a lot on power consumption of web servers
  - Cache miss
  - Floating point operations



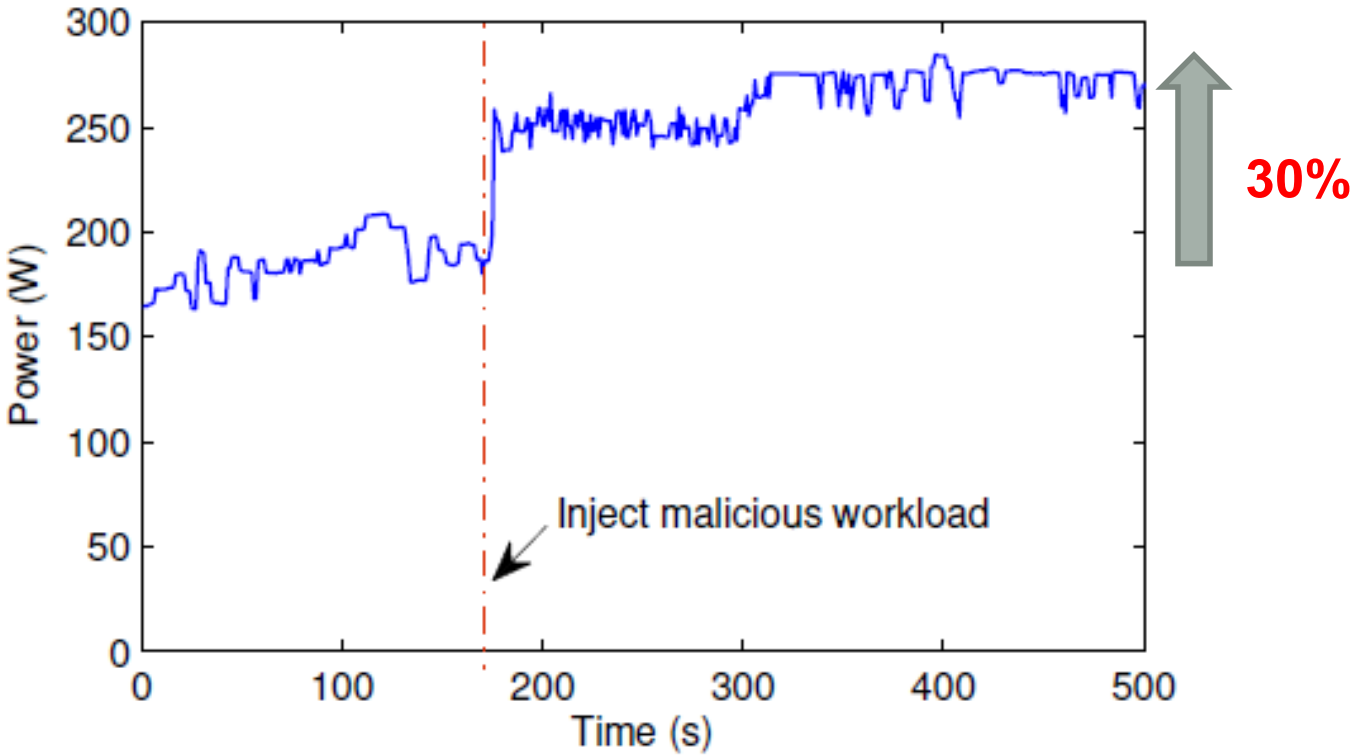
Power consumption under cache-miss requests



Power consumption under fp operation-intensive requests

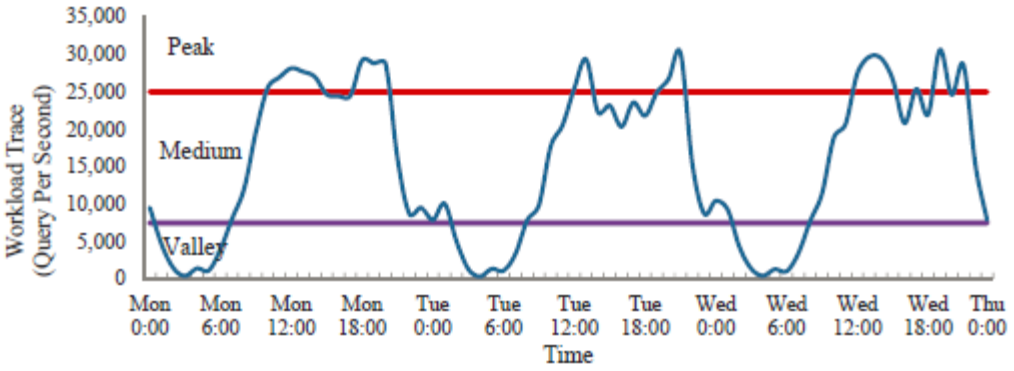
Attacking SaaS

- Power attack towards a web server



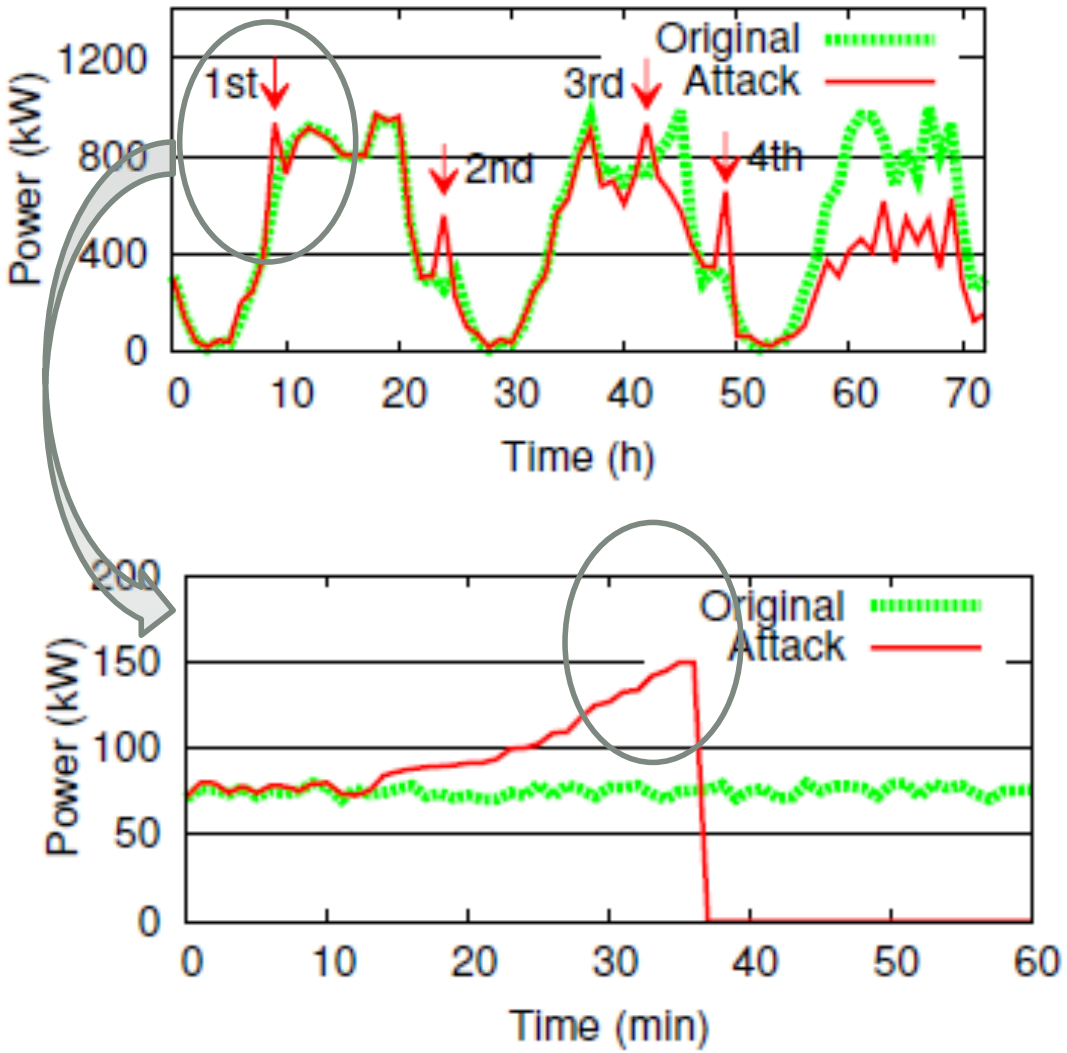
Attack at PDU/DC Level

- Power traces from Google Data center in North Carolina

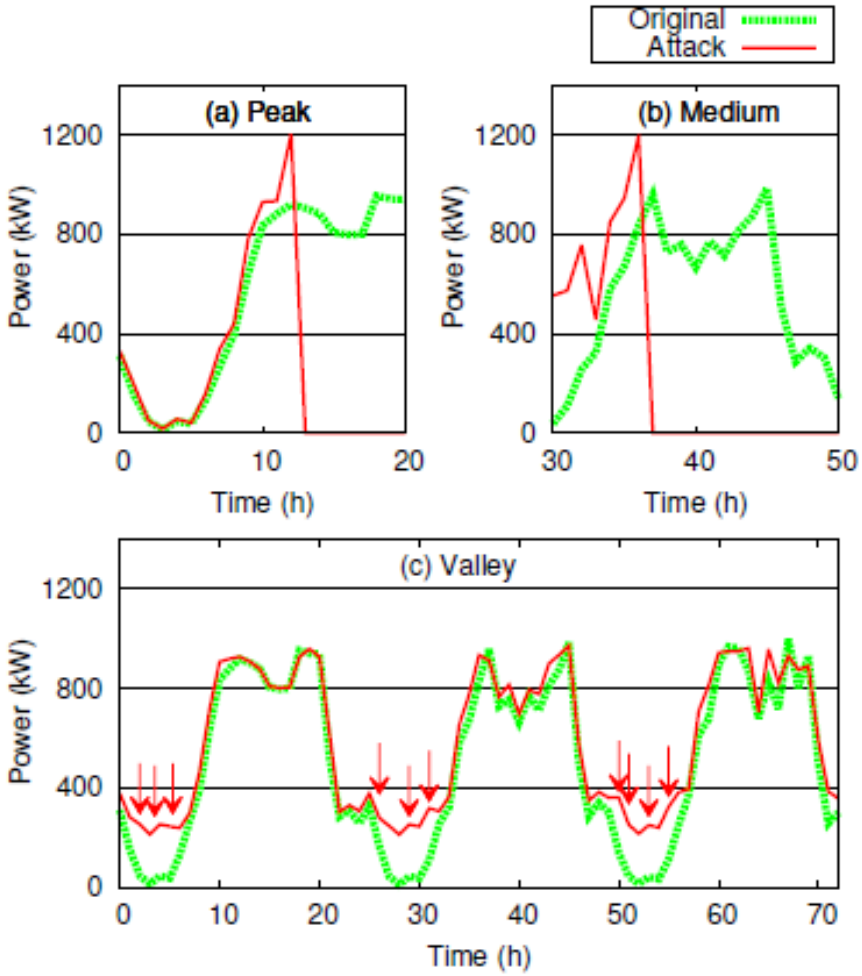


Parameter	Value
# of Servers	139,200
# of racks	approximate 700
# of PDU	approximate 20
# of CBs	approximate 30 (per PDU + per DC)
Capacity of PDU-level CB	150kW
Capacity of DC-level CB	1MW
CPU Per Server	dual-core 2.0GHz Xeon
DRAM Per Server	16GB
Disk Per Server	2TB
Est. Peak Power per Server	240Watt

Attacking PDU



Attacking Data Center



Impact of Power Management Solutions

- Power capping, mortal enemy of power attack?
  - Reactive manner
  - Selection of control period
  - Long settling time
- Server consolidation
- Energy proportionality

Mitigation Suggestions

- Better server level power model
- Power balancing instead of load balancing
- Integration of per-server UPS

Conclusion

- Power oversubscription is a trend of modern data centers
- Power attack is a real threat to data centers that host public cloud services
- New power management solutions may mitigate or aggravate such threat

Thank You

Questions?