Ohm’s Law in Data Centers: A Voltage Side Channel for Timing Power Attacks

Mohammad A. Islam and Shaolei Ren

UC Riverside

Acknowledgement: This work was supported in part by the U.S. NSF under grants CNS-1551661 and ECCS-1610471.
Cloud data centers

![Aerial view of a data center with logos of Google, Amazon, and Microsoft]
This talk is not about cloud data centers

User/Tenant = Virtual machines
Multi-tenant data centers (a.k.a. “colo”)

Managed by Operator

Non-IT infrastructure

Utility (Primary)

Generator

Computer Servers

UPS

ATS

PDU

PDU

PDU
Multi-tenant data centers (a.k.a. “colo”)

A shared data center facility that houses multiple tenants, each managing its own servers...
Multi-tenant data centers are everywhere...

Apple houses 25% of its servers in multi-tenant data centers...

2,000+ in U.S.
Multi-tenant data centers are everywhere…

Percentage of electricity usage by data center type (source: NRDC 2015)

- Multi-tenant: 37%
- Enterprise: 53%
- Google, Amazon, MS, Fb...: 7.8%

Apple houses 25% of its servers in multi-tenant data centers…
Data center security

• Mission-critical infrastructure
• Backbone of digital economy
• 50% growth by 2020
• IoT and edge computing
• ……

Securing the cyberspace is well studied
DDoS attack, network intrusion, privacy protection, etc.
[Mirkovic Sigcomm’04][Zhang CCS’12][Moon CCS’15][Dong CCS’17]…
Data center security

- Mission-critical infrastructure
- Backbone of digital economy
- 50% growth by 2020

Are the **physical** infrastructures secure?

Securing the cyberspace is well studied
- DDoS attack, network intrusion, privacy protection, etc.
  
  [Mirkovic Sigcomm’04][Zhang CCS’12][Moon CCS’15][Dong CCS’17]…
How to attack physical infrastructures?

Multimillion-dollar investment
How to attack physical infrastructures?

Human intrusion

Hacking control systems

Multimillion-dollar investment

Overload using server power

Hacking control systems
How to attack physical infrastructures?

Human intrusion

Hacking control systems

Multimillion-dollar investment

Our focus

Overload using server power

Utility

ATS

Generator

UPS

PDU

Servers

UPS

PDU

Servers

Power

Multimillion-dollar investment

Our focus

Overload using server power

Hacking control systems
Threat model
Threat model
Threat model

Power attack:
Well-timed power injection to overload the shared data center capacity, subject to all applicable constraints set by the operator.
Threat model

Power attacks make outages more likely
(\sim 280x \text{ more likely for a Tier-IV data center } )
Cost analysis of power attacks

Estimated impact of overloads (5% of the time, size: 1MW-10,000 sqft)

Million $/MW/year

Tier-II: 15.6
Tier-III: 8.7
Tier-IV: 3.5

Increased redundancy

Million dollar impact!
How to precisely **time** power attacks?

- Random attacks are unlikely to be successful, while constant full power is prohibited
How to precisely time power attacks?

• Random attacks are unlikely to be successful, while constant full power is prohibited
• Coarse timing (e.g., based on “peak” hours) is ineffective
How to precisely **time** power attacks?

- Random attacks are unlikely to be successful, while constant full power is prohibited
- Coarse timing (e.g., based on "peak" hours) is ineffective

**How to estimate the power load** **without** power meters?
“Wireless” side channels

**Thermal:** Higher power produces more heat
- Requires heat recirculation model
- Slow responses
- Only applicable to raised-floor designs

References
“Wireless” side channels

**Thermal:** Higher power produces more heat
- Requires heat recirculation model
- Slow responses
- Only applicable to raised-floor designs

**Acoustic:** More heat requires more cold air
- Inaccurate timing due to near-far effects
- Limited distance
- Easy to degrade by injecting additional noise

References
A voltage side channel due to Ohm’s Law
Ohm’s Law

\[ V_1 - R - V_2 \]

\[ V = I \cdot R \]
Ohm’s Law

\[ V_1 - V_2 = I \cdot R \]
Ohm’s Law

The voltage at the other end depends on the current

\[ V_2 = V_1 - I \cdot R \]
Ohm’s Law in data centers
Ohm’s Law in data centers

Line resistance

$R$

$R_a$

UPS

PDU

Server

Attacker
Ohm’s Law in data centers

\[ I = \sum I_n \]

\[ I_1 \quad I_2 \quad I_a \]

\[ R \quad R_a \]

UPS

PDU

Server

Attacker
Ohm’s Law in data centers

Ohm’s Law:

\[ V_2 = V_1 - I \cdot R \]

Attacker’s voltage:

\[ V_a = V_{PDU} - I_a R_a \]
Ohm’s Law in data centers

### Ohm’s Law

\[ V_2 = V_1 - I \cdot R \]

- \( V_1 \): Input voltage
- \( V_2 \): Output voltage
- \( I \): Current
- \( R \): Resistance

### Power Load and Attacker’s Voltage

**Power load is included in** \( V_a \)

\[ V_a = V_{PDU} - I_a R_a \]

- \( V_{PDU} \): Voltage at PDU
- \( I_a \): Current through the attacker
- \( R_a \): Resistance of the attacker's circuit

**Own impact**

\[ V_a = V_{UPS} - \sum I_n R - I_a R_a \]

- \( V_{UPS} \): Voltage at UPS
- \( \sum I_n R \): Sum of all node voltages
- \( I_a R_a \): Own impact of the attacker

---

Ohm’s Law in data centers

**Diagram:**

- UPS
- PDU
- Server
- Attacker

**Equations:**

\[ I = \sum I_n \]

\[ I_1, I_2, I_a \]
A voltage side channel

Attacker’s voltage $V_a = V_{UPS} - \sum I_n R - I_a R_a$
A voltage side channel

$\Delta V$ based attack:
Low voltage $\rightarrow$ High current/load $\rightarrow$ Attack opportunity?

Attacker’s voltage $V_a = V_{UPS} - \sum I_n R - I_a R_a$
A voltage side channel

ΔV based attack:
Low voltage $\rightarrow$ High current/load $\rightarrow$ Attack opportunity?

Attacker’s voltage $V_a = V_{UPS} - \sum I_n R - I_a R_a$

Large random variation from power grid
A voltage side channel

\[ \Delta V \text{ based attack:} \]

Low voltage \( \rightarrow \) High current/load \( \rightarrow \) Attack opportunity?

Attacker’s voltage \( V_a = V_{UPS} - \sum I_n R - I_a R_a \)

Large random variation from power grid

- Grid variation = \( \sim 3V \)
- Voltage drop variation = \( \sim 10mV \)
A voltage side channel

ΔV based attack:
Low voltage $\rightarrow$ High current/load $\rightarrow$ Attack opportunity?

How to extract power load information from voltage signals?

Large random variation from power grid

- Grid variation = $\sim$3V
- Voltage drop variation = $\sim$10mV
A closer look at server’s power supply

- **AC 100/240V**
- **AC/DC**
- **Power Factor Correction (PFC)**
- **380V**
- **DC/DC**
- **12V**
- **Voltage Regulator**
- **Server**
- **Power Supply Unit (PSU)**

Diagram: A flowchart showing the process from AC 100/240V through AC/DC, PFC, DC/DC, Voltage Regulator, and finally to the server.
A closer look at server’s power supply

Without PFC

Current draw is bursty
A closer look at server’s power supply

Without PFC

Current draw is bursty

With PFC

Current follows a sinewave with high-frequency ripples
The ripples come from the PFC control
The ripples come from the PFC control

Input voltage sample

PWM Control

Output voltage sample

Reference Current
The ripples come from the PFC control

Power Factor Correction (PFC)

Rectifier

Input voltage sample

PWM Control

MOSFET

Output voltage sample

Diode

Inductor

Actual Current

Reference Current
The ripples come from the PFC control.
The ripples come from the PFC control
Voltage measurement of a Dell server
Voltage measurement of a Dell server

High-frequency ripples caused by PFC
Voltage measurement of a Dell server

High-frequency ripples caused by PFC

Frequency analysis of the voltage signal
Voltage measurement of a Dell server

Frequency analysis of the voltage signal

High-frequency ripples caused by PFC

Frequency spike (at PFC switching frequency)
Can we estimate the power load based on frequency spikes?
Can we estimate the power load based on frequency spikes?

Our intuition says “yes”!
Given a higher current, the ripples need to rise up more during each cycle.
Experiment

- 13 Dell PowerEdge servers
- 3 different server configurations
- 3 different types of power supply units
Power supplies

1. 350W, PFC Switching ~63kHz
   Model: D35E-S1
   Manufacturer: Delta Electronics Inc.

2. 495W, PFC Switching ~66kHz
   Model: F495E-S0
   Manufacturer: Astec Intl. Ltd.

3. 495W, PFC Switching ~70kHz
   Model: E495E-S1
   Manufacturer: Flextronics Intl. Ltd.
PSD vs. server power
PSD vs. server power

Higher power creates taller frequency spikes
PSD vs. server power

Higher power creates taller frequency spikes

Aggregate PSD monotonically increases with server power
PSD vs. server power

![Graph showing normalized aggregated PSD for 1 server across different power levels: low, medium, and high. The graph indicates a significant increase in PSD with increasing power level.]
PSD vs. server power

![Graph showing comparison of PSD vs. server power across different power levels with two servers vs. one server.](image-url)
PSD vs. server power

![Bar chart showing normalized aggregated PSD for 1 server, 3 servers, and 2 servers at low, medium, and high power levels.](image)
PSD vs. server power

![Bar chart showing PSD vs. server power levels]

- **Norm. Aggr. PSD**
- **Power Level**: Low, Medium, High
- **Server Configurations**: 1 server, 3 servers, 2 servers, 4 servers
PSD vs. server power

Aggregate PSD is additive for multiple servers with similar PFC frequencies.
PSD vs. server power

Aggregate PSD is additive for multiple servers with similar PFC frequencies
PSD vs. server power

Aggregate PSD is additive for multiple servers with similar PFC frequencies

Frequency spikes are separated for different types of power supply units
Accuracy of the voltage side channel

Tenant #1

Tenant #2

Tenant #3
Accuracy of the voltage side channel

Estimating power loads with a high accuracy!
Attack only when the estimated power load is sufficiently high
Power attack
Power attack

Tenants’ total power
Power attack

Estimated power loads
Power attack

![Chart showing power attacks and their impact on power and capacity over time.]

- **Power**
- **Capacity**
- **Attack Opportunity**
- **Unsuccessful Attack**
- **Successful Attack**
- **Spectral Power**

The chart illustrates the fluctuation of power and capacity over time, highlighting periods of attack opportunities and successful attacks as marked by blue and red circles, respectively. The graph demonstrates how power attacks can lead to significant variations in the normalized PSD, indicating potential vulnerabilities in the system.
Timing accuracy

[Graphs showing True Positive and Precision percentages against Attacks (% Time) for the Voltage side channel]
Timing accuracy

>50% true positive rate and precision for ~10% attack
Timing accuracy

>50% true positive rate and precision for ~10% attack
Timing accuracy

>50% true positive rate and precision for ~10% attack
Timing accuracy

>50% true positive rate and precision for ~10% attack

Also works with UPS and three-phase power systems
Physical infrastructure sharing means everything but power security.

References