



# One-Location Rowhammer Angriff

Gilian Henke, Dominik Mairhöfer

2. Februar 2018

Aktuelle Themen IT-Sicherheit und Zuverlässigkeit

# Inhalt

## 1 Einführung

## 2 Hintergrund

- One-Location Rowhammer
- Memory Waylaining
- Prefetch Side-Channel Angriff

## 3 Ergebnisse

## 4 Fazit

# Motivation

- Neuer Rowhammer Angriff
- Neue Technik zum Ausnutzen des Rowhammer Angriffs

# Motivation

- Neuer Rowhammer Angriff
- Neue Technik zum Ausnutzen des Rowhammer Angriffs

Wie gut funktioniert der Angriff?

- Durchführbarkeit des Angriffs testen
  - schnell, zuverlässig, unauffällig, ...
  - Voraussetzungen
  - Gegenmaßnahmen

# Der Angriff

- Ziel: Verändern einer ausführbaren Datei ohne Schreibrechte
  - z.B. sudo Datei für lokale Rechteauserweiterung
- Basieren auf drei Teilen
  - One-Location Rowhammer
    - ⇒ Bitflips im Speicher erzeugen
  - Memory Waylaining
    - ⇒ Dateien an bestimmten Stellen im Speicher platzieren
  - Prefetch Side-Channel Angriff
    - ⇒ Virtuelle Adressen in physikalische auflösen

# Der Angriff - Ablauf

- 1 One-Location Rowhammer  
⇒ Finde virtuelle Adresse bei der Bitflip möglich ist

# Der Angriff - Ablauf

- ① One-Location Rowhammer  
⇒ Finde virtuelle Adresse bei der Bitflip möglich ist
- ② Prefetch Side-Channel Angriff  
⇒ Finde physikalische Adressen zu dieser

# Der Angriff - Ablauf

- ① One-Location Rowhammer  
⇒ Finde virtuelle Adresse bei der Bitflip möglich ist
- ② Prefetch Side-Channel Angriff  
⇒ Finde physikalische Adressen zu dieser
- ③ Memory Waylaying & Prefetch Side-Channel Angriff  
⇒ Platziere ausführbare Datei an dieser physikalischen Adresse



# Der Angriff - Ablauf

- ① One-Location Rowhammer  
⇒ Finde virtuelle Adresse bei der Bitflip möglich ist
- ② Prefetch Side-Channel Angriff  
⇒ Finde physikalische Adressen zu dieser
- ③ Memory Waylaying & Prefetch Side-Channel Angriff  
⇒ Platziere ausführbare Datei an dieser physikalischen Adresse
- ④ One-Location Rowhammer  
⇒ Erzeuge erneut Bitflip an gleicher physikalischer Adresse



# One-Location Rowhammer



# Memory Waylaing



# Prefetch Side-Channel Angriff



# Ergebnisse - One-Location Rowhammer



# Ergebnisse - Memory Waylaing



# Ergebnisse - Prefetch Side-Channel Angriff



# Fazit