UNIVERSITÄT ZU LÜBECK

One-Location Rowhammer Angriff

Gilian Henke, Dominik Mairhöfer

2. Februar 2018

Aktuelle Themen IT-Sicherheit und Zuverlässigkeit

Inhalt

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 Rechteausweitung
- Basieren auf drei Teilen
  - One-Location Rowhammer
    $\Rightarrow$ Bitflips im Speicher erzeugen
  - Memory Waylaing
    $\Rightarrow$ Dateien an bestimmten stellen im Speicher platzieren
  - Prefetch Side-Channel Angriff
    $\Rightarrow$ 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

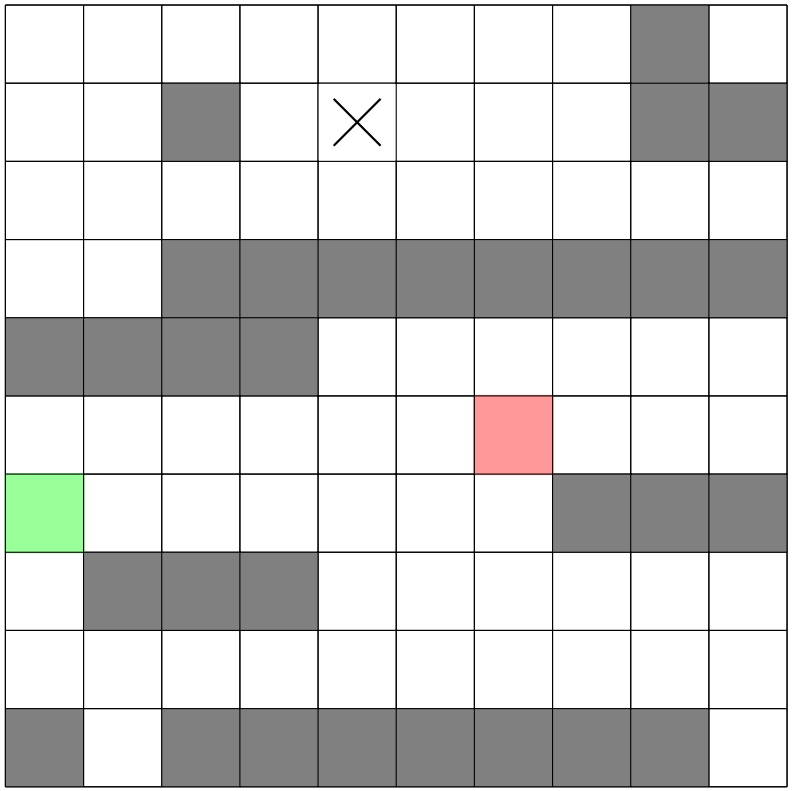
2. Prefetch Side-Channel Angriff
   ⇒ Finde physikalische Adressen zu dieser

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 Waylaying



benutzter Speicher

Ziel

geladene Binary

Prefetch Side-Channel Angriff

Ergebnisse - One-Location Rowhammer

Ergebnisse - Memory Waylaing

Ergebnisse - Prefetch Side-Channel Angriff

Fazit