



ToorCon X – San Diego / CA



Knowing and Enjoying the **Cold Boot Attack**

Bruno Gonçalves de Oliveira (bruno.at.bsdm ail.com)

&&

Jacob Appelbaum (jacob@appelbaum.net)

AGENDA

- Introduction!
- Knowing
- Enjoying
- Yeah, it's simple like that

INTRODUCTION

- WTH is a Cold Boot Attack?
- Why this presentation?
- What do we wanna know and enjoy (and how)?
- Personal motivations
- Why so many questions?

KNOWING

What do we need to know?

- Volatile or Non-Volatile
- DRAM and SRAM
- Decay as a function of charge, time and temperature
- What kind of information do we have there?
- How to escape?
 - no exit

Volatile or Non-Volatile

- Past authors, past theories
 - Peter G.
 - Others
- Volatile (fast decaying) is actually...
(some)time to discharge

DRAMs

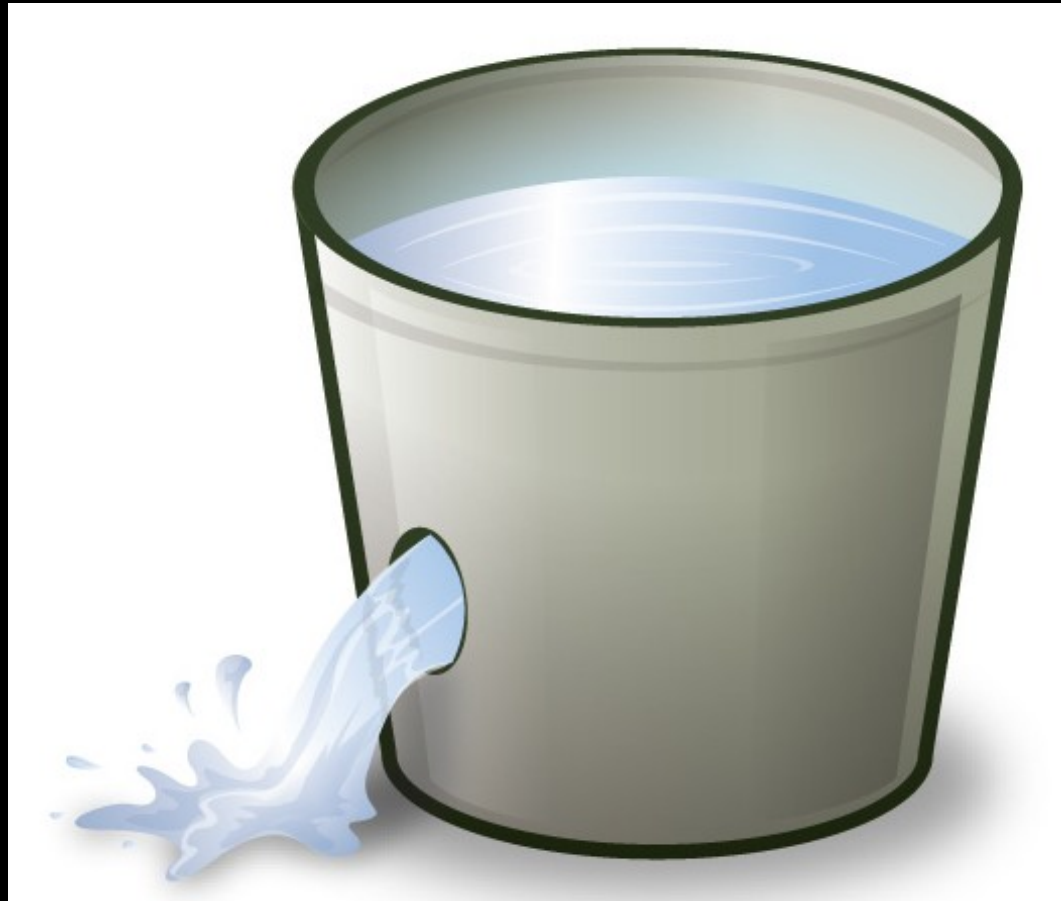
- Transistors and Capacitors
 - Reads capacitors and change its state
 - Stores electrical loads

- How do they work?

- Bitlines (columns) X Wordlines (lines) = Address
 - (<50%) 0 and 1 (>50%)

- Refresh operation

Refresh Operation



\\ by Kriz Barz - icomp.com.br

Decay and Temperature

- Decaying in environment temperature
- Cold temperature
 - Why freeze? Cryogenic!
 - Electrical loads
- Patterns exist
 - See the Mona Lisa image test

Freezin'



\\ by Kriz Barz - icomp.com.br

DATA on DRAMs

- A lot of interesting stuffs
- Users and passwds
- *encryption keys*

Escaping?

- BIOS is our enemy (or allied?)
 - coreboot
- ECC Memory
 - Mandatory scrubbing
- HW Protection
- Not a 100% functional (like everything)

ENJOYING

We need fun to enjoy

So, what do we need?

Physical Access

Remote (dhcpd + tftpd = <3)

A place to store the data

Tools and Imagination

Physical Access

- Booting w/ tools

- iPod

- Any disk

- Special BIOS (coreboot to the rescue)

- Police, thieves, and other forensic specialists

Remote

- PXE netBoot
 - Depending of the BIOS
 - Slide a NIC into the picture

EFI netboot

Currently x86 only

The Data

- A place to keep it
 - Be quick or be dead!

Mainly USB Drives / Firewire

TOOLS

- First of all, what do you want ?
- How can we do it ?
 - Dump the memory
 - Hex reader (very slow)
 - *nix system (we recommend! ;D)
 - Find those keys! (automate it)

Keys are the key

Not just encrypted disks

A lot of keys from different places

Everything is on memory!

KEYS is the key p2

- Extract them
 - How?
 - Brute Force
 - Assuming byte alignment
- Errors make it difficult to recover data
 - Hamming Distance
 - Good theory...
- Tools for that (rsa,aes}keyfinder)

TOOLS p2

- Published:

- <http://citp.princeton.edu/memory/cc>

Download the code.

It's slowly making its way into the
Debian Forensics project

The Method

Dumping

Extracting the important data or
Whatever (DRM? RE?)

Useful for finding “bugs”

Go go Apple!

The sky is the limit

Easy? Maybe...

DEMO

24/09/08

The point

Physical realities

cooling the memory sounds funny
but it only requires canned air

The FBI and the DHS (interns) are using
these techniques in real cases.

You decide if it's an impractical
attack

Thank you!
(Please write anti-forensics
software)