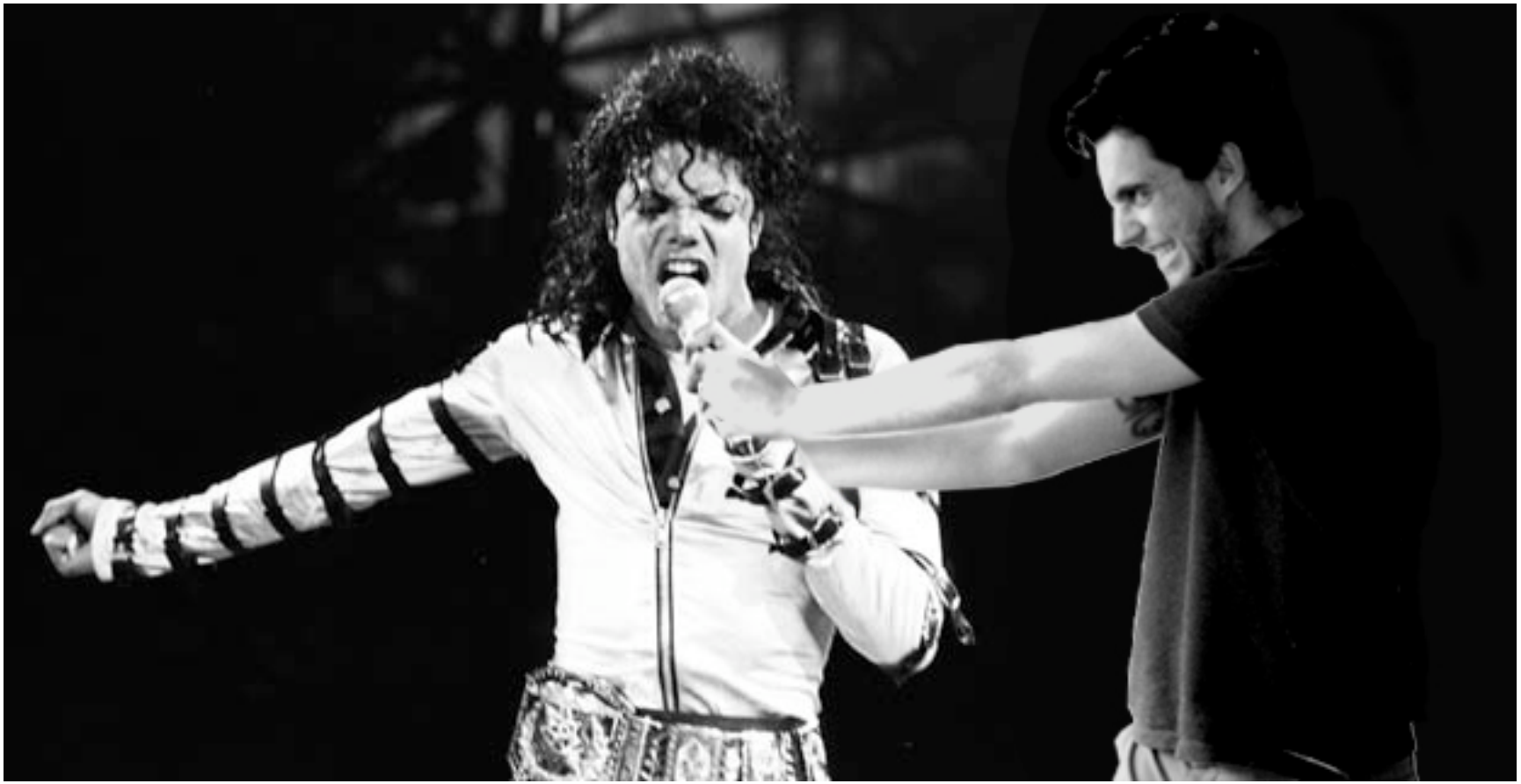
Sharing my Mic with a (pop)Star and a little bit more of Cold Boot Attacks

Bruno Gonçalves de Oliveira

bruno.at.bsdmail.com



AGENDA

- Once upon a time...
  - what happened, where, who shared with me, me...
- Cold Boot Attacks
  - lets see some things
    - physicall stuffs
    - is it so easy?

Once upon a time..

ToorCon X

Jacob Appelbaum

WHO IS HE?

- JORNALIST
- PHOTOGRAPHER
- ACTIVIST
- PHILANTHROPIC
- ENVIRONMENTALIST

Ah! I forgot...

HE'S ALSO A HACKER

AND ABOUT ME?

WHO AM I ?

- COMPUTER ENGINEER
- SECURITY ANALYST
- RESEARCHER IN FREE-TIME
- JOBS JUST RELATED TO COMPUTERS

Ah! I'm not a pretty good person like him...

BEFORE THE PRESENTATION

THE PRESENTATION...

HIM

ME

IN THE FINAL

WHAT DID I WANT TO SHOW?

Cold Boot Attack

Physical Stuffs

- What is the memory?
  - Transistors and Capacitors

- How do they work?

  - Bitlines (columns) X Wordlines (lines) = Address

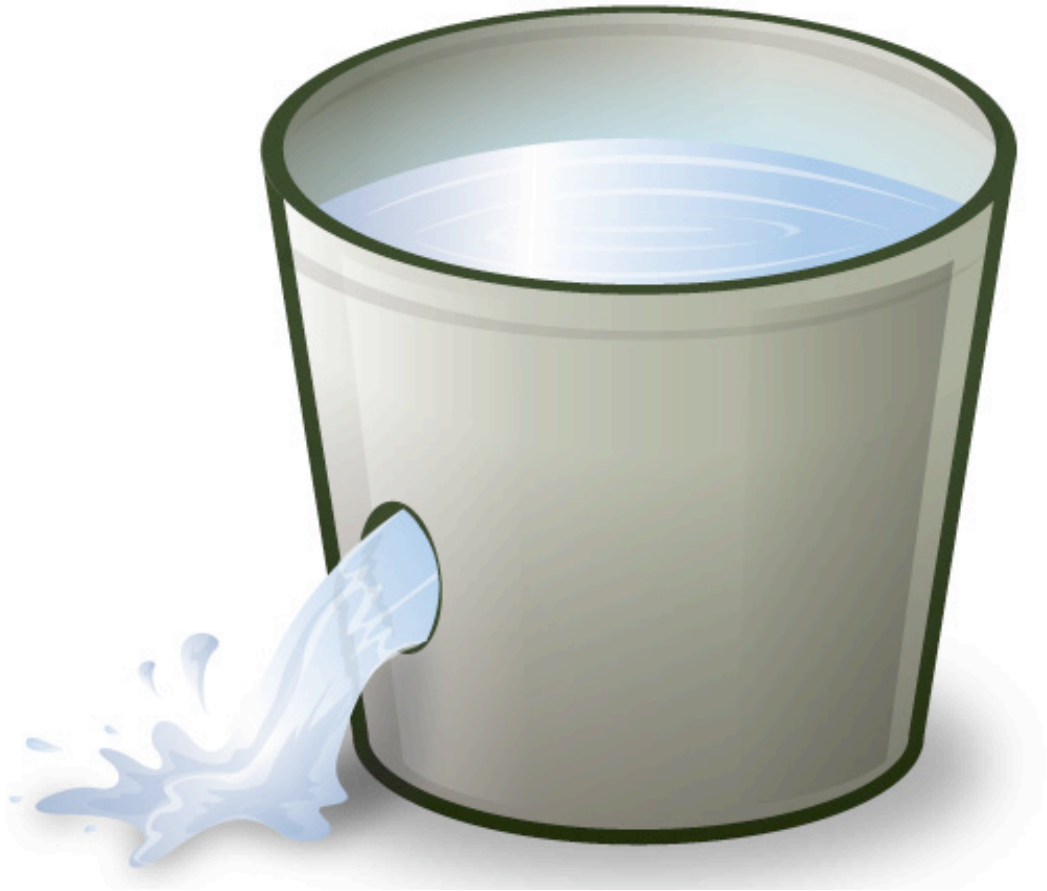
- Refresh Operation!

AND FINALLY...

I'M EXCITED

MY ANALOGY

REFRESH OPERATION

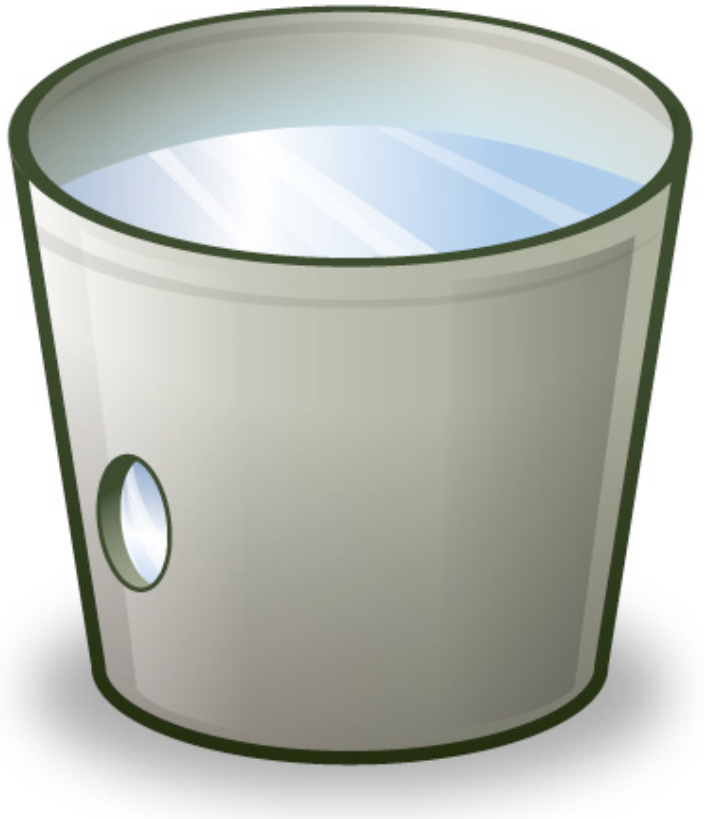


The attack

- Decaying in environment temperature

- Why freeze?

FREEZE MY BUCKET



Easy?

THE TRUTHS

- 1 - Dump the memory and extract the key, just rebooting
- 2 - Dump the memory and extract the key, cooling it.
- 3 – Dump the memory and extract the key, cooling it and changing the memory's machine

The truths 2

- 1 – memory size, usb and firewire speed limitations
- 2 – memory slots
- 3 – memory slots

FILEVAULT STUFFS

ABOUT THEIR TOOLS

HUMMMMM

I'M A TROUBLEMAKER

NEVER BEEN A FAKER

DOIN' THINGS MY OWN WAY

AND NEVER GIVIN' UP

I'M A TROUBLEMAKER

NOT A DOUBLETAKER

I DON'T HAVE THE PATIENCE TO KEEP IT ON THE UP

I'M KIDDING

AH!

DID SOMEONE SEE COLD BOOT ATTACK ON TV SHOW?

SUPER COOL!

BUT THEY DIDN'T USE THE PUBLISHED CODES

I'M KIDDING

AGAIN

NOW SERIOUSLY

They released 5 tools!

- usb/pxe boot image
- efi network boot
- Aes key finder
- Rsa key finder
- Some other code to correct aes

Others tools

- DaisyDuckes – nourl =/
- Usb/cd boot image for dumping – McGrew Security: RAM Dumper http://mcgrewsecurity.com/tools/msramdmp/

THE ATTACK IS VERY INTERESTING

BUT WE HAVE TO BE MORE CRITICAL

SEE THINGS THAT PEOPLE FORGET

I THINK THAT'S ALL FOLKS!

Questions?

Thanks!