Pneumonia, Shardan, Antibiotics and Nasty MOV: a Dead Hand's Tale

Arrigo Triulzi
arrigo@sevenseas.org
@cynicalsecurity

Troopers '15, March 18th 2015

The Glomar slide

In this set of slides a careful observer might notice the absence of an elephant.
This is because of an RSNDA which was willfully signed a long time ago and allowed me to meet and have extremely interesting discussions with some wonderfully intelligent and gifted people.
Due to the above any question about the elephant will unfortunately be "Glomarised" (©1975 Langley, VA).

This is also a reminder, to myself above all, that RSNDAs come with consequences.

The cunning plan

Ancient History

- Computer History
- Nuclear History
- On Strangelovian affairs

Curiosity

- The Quest
- Ahoy capt'n, firmware ahead!
- The rise of the acronyms
- The Emperor's modified brain

MOVing

- You want to MOV what?
- I have a cunning plan

But Shardan?

- It started as a joke. . .

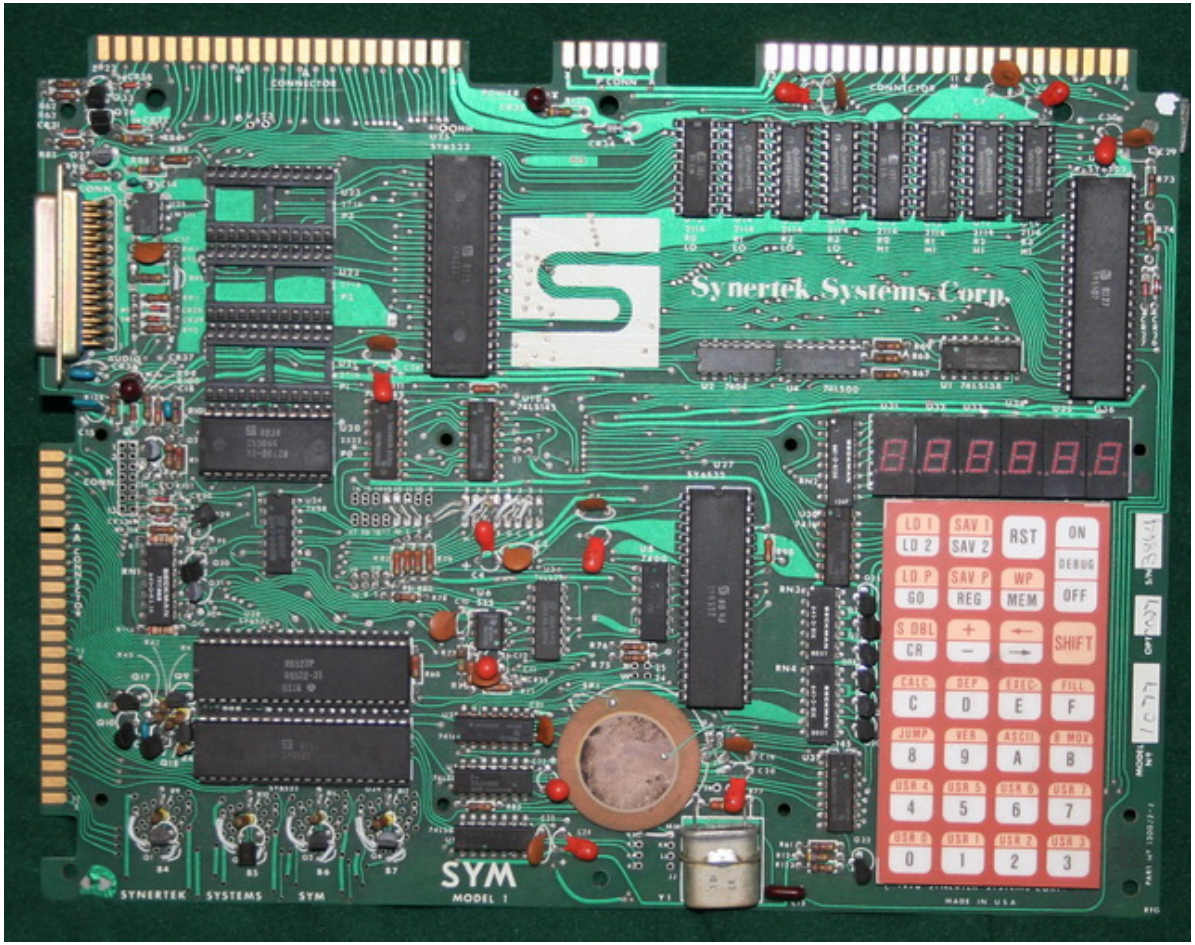
Dead Hand rises

A long long time ago...

Growing up during the Cold War meant being exposed to fun things such as:

- "legal" and "illegal" acoustic couplers and modems,
- TTYs of the physical kind as opposed to `/dev/tty`,
- all sorts of MOS 6502 computers,
- an Onyx C8002 Zilog Z8000 running Unix Version 7,
- terminals like the ADDS Viewpoint 60,
- a BBS in Sofia with "interesting" assembler code...

Synertek SYM-1



Onyx C8002

ADDS Viewpoint 60

still a long long time ago. . .

At the same time the Cold War also meant nuclear weapons were pretty much reaching their peak at the same time as the toys in the previous slides.
Different people react in different ways.
One decided to go off and explain to his class as the end-of-elementary school project the (unclassified) details of thermonuclear weapons and cruise missiles.
This was the beginning of a lifelong scholarly interest in the field.
To put it in perspective my relatives thought that the Italian translation of *"Nuclear explosions and earthquakes: The parted veil"* by Bruce A. Bolt was a brilliant birthday present.

Some nukes in the morning . . .

A crucial aspect in nuclear warfare is the concept of a "decapitation attack" where the enemy takes out the C&C before it has a chance to order a retaliation strike or indeed take any action.
In a Cold War scenario based upon deterrence it quickly becomes apparent that defence against a decapitation attack is of utmost importance for deterrence to be credible.
Both sides developed sophisticated means to guarantee that the C&C structure would not be compromised: from missiles being launched to broadcast the retaliation launch codes to intricate chains of command specifying who could fly with whom where and when.
But only one side had the ultimate plan.

Enter Система «Периметр» stage left...

Система «Периметр», Systema "Perimetr", was designed starting in the mid-60s when the Russians became concerned by the increasing accuracy of the US ICBMs.
The initial version was a relatively mild 30-missile salvo which would carry launch orders to the most remote units across the vast Russian territories.
The final version, allegedly still operational depending on the accounts, is a fully automated monitoring system which, on detecting certain specific parameters (radiation, blast, flash, lack of communications), automatically initiates the launch sequence for all surviving ICBM missiles.
This is known as a "Dead Hand" system or, ever since Kubrik's *Dr. Strangelove*, a "Doomsday machine".
To be fair there is also a quaint Western counterpart.

Enter the *letters of last resort* stage right...

The British "letters of last resort" are identical handwritten letters which are prepared for each of the four missile submarines of the Royal Navy by the Prime Minister when he takes office.
In the letter are the instructions to the captain of the submarine about what to do should the United Kingdom cease to exist which are believed to be one of: retaliate, do not retaliate, place yourself under allied command, or use your own judgement.
The evaluation by the captain on the fate of the United Kingdom relies, amongst other things, on checking if BBC Radio 4 is still on-air.
The letters are destroyed, unread, when a new Prime Minister takes office.

Towards the ultimate rootkit

Ever since meeting the fine assembler on the Sofia BBS a quest to improve on those designs has always been in the background while many other events took place.
Initially the target was software but it rapidly became obvious that the answer was in hardware, influenced, in no small part, by the experiences of the 1990s while my father worked for “Il Moro di Venezia” as the “Electronic warfare wizard”, i.e. “figure out how the other boats get their speed by decoding the data we can sniff from the helicopters”.
The first results were presented at a closed meeting in 2008, then PacSec in 2009 and finally at CanSecWest in 2010 as “Project Maux” culminating with the “Jedi Packet Trick”.

Firmware in many colours, justified and in bold

Going back to the 1980's let me introduce the Integral Data Systems Prism P80 *colour* printer:

This beauty was micro-processor controlled and fully programmable. . . which, unsurprisingly, lead to the first forays into firmware modification.

Firmware on a sailing boat

Say you have a budget described as “infinite” and you are tasked to figure out how and why your opponent’s AC-1 yacht performs in a particular wind condition.
What do you do?

- fly a helicopter over their training area,
- record, from a particular angle, the sail, keel and flap shapes,
- pump them in big computer & simulate.

But that is a bit boring and, frankly, obvious even in 1990.
Remember your budget says ∞ . . .

Firmware in a sail?

A rather more interesting option is:

- take your sail and place sensors in it,
- connect them in real-time to a minicomputer in the hull,
- place the elder version of the author on board,
- have him approximate the sail shape to the model, reprogramming and tuning “in real-time”.

Net result: reach the finals of the America’s Cup.
A minor snag is the elder is a physicist so the differential geometry is done by the younger who is a mathematician.
As they say: “it runs in the family”.

Of network cards, option ROMs and EFIs

Network cards were an accidental interest, piqued by bad checksums in tcpdump on OS X 10.3 on a PowerBook, fuelled by a DECstation in the nuclear bunker and the eternal smouldering of the quest for the ultimate backdoor.
The other rising star though was (U)EFI and with it the beautiful observation that "option ROMs" were still around. A 2006 iMac, the very first Intel iMac, was the beginning of "Project BooShoo". The idea was to introduce persistence via EFI modules and "doing stuff" using the Option ROM calling.
The project was rather brutally interrupted at the end of 2010.

Descent into the brain

Part of my "training" was being shown AMD 2900 bit-slicing design and the parallels between it and the "new" CISC instruction breakdown into μOPS were inevitable.
At the same time it was impossible to forget the *"enable microcode updatation (sic)"* which had made its appearance in the AMI BIOS of my dual Pentium Pro.
A "quick" analysis of the microcode update files gave nothing, at least at the time but help was on the way:
"Opteron Exposed: Reverse Engineering AMD K8 Microcode Updates"
On the SecuriTeam website on 26th July 2004...

Descent into the brain - continued

Out went the Pentiums, in came the Opterons. . .
The path was now clear:

- understand the microcode update file,
- modify the microcode update file,
- inject and see what happens.

The *good* news: to fix a bad microcode update all you need to do is power-cycle.
The *bad* news: to fix a malicious microcode update all you need to do is power-cycle.

Descent into the brain - continued

We now have to understand the microcode update.
Let us assume we have a microcode expert in the family who so happens to be an ancient AMD 2900 wizard. Hand over microcode in 2004, spend several years with him, decide what to modify, prepare it, produce it.
The product is “Nasty MOV”: only *ten* years in development but now happily working on several AMD cores derived from the AMD K8 core mentioned in the original SecuriTeam post.

“I find this JMP, disturbing”

- load modified microcode (as root)
- microcode modifies certain “interesting” privileged instructions, e.g. AMD-V, AMD-VI, AVIC
- you think your hypervisor is being a hypervisor but in practice it is being subverted

“Oh wow, so cool!” – not really. . . remember the power-cycle problem?

Sticky, Nasty MOV

We need Nasty MOV to stick, aka "persistence" and it is pretty clear that power cycling will always get rid of us.
Having said this we have a weapon in our arsenal.
Remember how AMD-VI & associated IOMMU technologies are meant to protect us from PCI-to-PCI transfers and prevent the "Jedi Packet Trick"?

But if we subvert AMD-VI then our NIC firmware is back in the game!

I want to persist!

The cunning plan:

1. takeover the NIC with nicssh (*from the outside*),
2. inject Option ROM into firmware (via nicssh),
3. wait for reboot (or poke via NIC),
4. EFI boots, executes Option ROM,
5. Option ROM updates microcode,
6. microcode update disables microcode update,
7. microcode update takes over AMD-VI & friends,

Since we own the boot process we have persistence.

Finally weaponised as of February 2015.

ShardanConf 2014

It was meant to be a private joke between two mathematicians over Twitter, it turned out to be an involuntary test of my Dead Hand.

What happened next is that I caught pneumonia. . .

The Awakening

```
dead_hand:noping12h:lastbad:nicshot_bootstrap:
```

Fire!

```
dead_hand:nicshot:gwhack:prime=73:ipmiburn:\
fspread=3:
```

Erase

```
dead_hand:ustart:uspread=bnx,amd,nvdia:\
underworld=torb:wipekeys=0000:wipealg=pgut001:\
syswipe:
```

The End

```
dead_hand:comms=underworld,silent:syslive:cincoff:
```

Credits

- Enno & the ERNW crew
- 1,3,7-Trimethylpurine-2,6-dione
- my cubs for asking questions
- Toby for asking good questions
- the amazing gang at the elephant (you know who you are)
- obviously having a hacker father. . .

References

I promise to fill this one up, see Twitter or my lynx-friendly website at https://www.alchemistowl.org/somelinkoranother.

In the meantime why not enjoy the fine *PoC||GTFO* mirror at https://www.alchemistowl.org/pocorgtfo/ and its wonderful contents?