Security Now! #565 - 06-21-16

Control-Flow Enforcement Technology (CET)

This week on Security Now!

- The reality behind the "Palantir got owned" story
- Confirmation of the danger of SMS as a 2nd factor
- A frightening IoT camera experience
- Some confusion over the GotoMyPC full password reset
- The machine under the machine: Do our systems have a designed-in rootkit?
- Deep dive into Intel's forthcoming anti-hacking Control-Flow Enhancement Technology!

SPONSOR INSERT

Security News

How Hired Hackers Got "Complete Control" Of Palantir
https://www.buzzfeed.com/williamalden/how-hired-hackers-got-complete-control-of-palantir

- This was a bit of a click-bait article. In the first place, the hired hackers, part of a so-called "Red Team", were deliberately let in by simulation of a phishing eMail. So the real question was, once in, what could they accomplish.
- The answer was "quite a lot, actually."
- A VERY useful exercise that somehow got public and unnecessarily embarrassed Palantir.

One Time Passcodes Sent via SMS Intercepted and Used to Hack Accounts
https://www.ptsecurity.com/wwa/news/72669/ (Positive Technologies)

- <quote> (Press Release)
  Positive Technologies' researchers able to compromise many popular social media sites by hacking SS7 network, intercepting an OTP, resetting passwords and taking ownership of accounts

  Positive Technologies, a leading provider of vulnerability assessment, compliance management and threat analysis solutions, today confirmed its researchers have exploited a flaw in the SS7 protocol to intercept one time passcodes (OTP) used by many online services to reset passwords. Facebook, WhatsApp, Telegram, Twitter and many other online services, offer password resets via SMS message but instead of strengthening security, this ability actually introduces a vulnerability hackers can, and will, exploit.

Positive Technologies' researchers recorded themselves demonstrating the hack against Facebook and WhatsApp accounts, with the owner's permission, proving the dangers of this authentication method.

I bought and returned a set of WiFi connected home security camera.
Forgot to delete my account… and I can now watch the new owner.
https://m.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected

- <quote>
  A few months back I purchased a Netgear Arlo home security camera set. I set up an online account, connected the cameras, tried them out for a few days and ultimately changed my mind. They were returned to the store and I never gave it another thought...until today. I got a random email alerting me that the camera had detected motion...but I don't have any cameras. So I logged into my online account and I can see the new owner, their house, and everything they're doing. Netgear obviously doesn't have a system in place to prevent cameras on multiple accounts. If I'm not mistaken, anyone could get the serial number off your cameras and link them to their online account, to watch and record your every move without your permission. A creeper dream. Does anyone else see this as a serious security flaw on Netgear's behalf?

  I'm even happier that I returned them now.

  /// Subsequent edit ///
  I left a message with Netgear this morning (6/20). Received a return call from a Senior Support Engineer saying they are aware of this issue. Since the cameras aren't supposed to be resold, I suppose they didn't think it would be an issue. I was assured they were working on a fix within the next 3 weeks to prevent cameras on multiple accounts and force a hard reset on the cameras if cameras were previously registered in the system.

SMG NOTE: Several others tweeted the same "zero configuration" Netgear webcam experience.

After suffering a "very sophisticated" attack, GotoMyPC forces all users to reset their passwords.

- When they named their service "GotoMyPC" they probably didn't mean it quite so literally.
- http://status.gotomypc.com/incidents/s2k8h1xhzn4k
  - <quote> Dear Valued Customer, Unfortunately, the GoToMYPC service has been targeted by a very sophisticated password attack. To protect you, the security team recommended that we reset all customer passwords immediately. Effective immediately, you will be required to reset your GoToMYPC password before you can login again.

  - <quote> Investigating: "We have experienced an issue which requires you to reset your password if you are having trouble logging into your account. Please reset your password through the "Forgot Password" link if you are having trouble logging into your account."

- But then, John Bennett, product line director at Citrix, said that once the company learned about the attack, it took immediate action. But contrary to previous published reports, there is no indication Citrix or its platforms have been compromised, he said.

    - "Citrix can confirm the recent incident was a password re-use attack, where attackers used usernames and passwords leaked from OTHER websites to access the accounts of GoToMyPC users," Bennett wrote in an emailed statement. "At this time, the response includes a mandatory password reset for all GoToMyPC users..."

Intel x86's hide another CPU that can take over your machine (you can't audit it)
https://boingboing.net/2016/06/15/intel-x86-processors-ship-with.html
Damien Zammit:

- <quote> Recent Intel x86 processors implement a secret, powerful control mechanism that runs on a separate chip that no one is allowed to audit or examine. When these are eventually compromised, they'll expose all affected systems to nearly unkillable, undetectable rootkit attacks. I've made it my mission to open up this system and make free, open replacements, before it's too late.

Acronyms:

- Intel Management Engine: IME or ME
- 32-bit ARC Processor
- Active Management Technology: AMT
- Older system: Intelligent Platform Management Interface: IPMI

An OS-independent means for the enterprise management of systems.
The ME is capable of accessing any memory region without the main x86 CPU knowing about the existence of these accesses.

It's like "Ring -3"

- Ring 3: Userland
    - (Rings 1&2 exist in the hardware (ring is two bits) but never got used)
- Ring 0: The Kernel
- Ring -1: The Hypervisor
- Ring -2: "SMM" System-Management-Mode
- Ring -3: , a special mode that Intel CPUs can be put into that runs a separately defined chunk of code. If attackers can modify the SMM code and trigger the mode, they can get arbitrary execution of code on a CPU.

What most creepy is that it runs a TCP/IP server on the network interface and packets entering and leaving the machine on certain ports ***bypass any firewall running on your system.***

- ME cannot be disabled on systems using the Core2 series processors.
- And... Intel keeps most details about ME absolutely secret.
- There is no way for the main CPU to tell if the ME on a system has been compromised.
- No way to repair a compromised ME.
- No way to know if malicious entities have been able to compromise ME and infect systems.

Intel DID design the code to be essentially impossible to hack:

- The integrity of the firmware's public key is verified with an SHA256 hash and checked against the proper value embedded into a ROM in the chip.
- Then that RSA public key is used to verify the signature of the flashable firmware before it begins to execute.
- Then a custom hardware decompressor inflates the compressed firmware into the IME processor's RAM at runtime.
- Thus... only specially compressed firmware sign with Intel's matching private key will ever be runnable within the IME subsystem.

SpinRite

Corey Grant in Livingston, Texas
Subject: Testimony
Date: 03 Jun 2016 10:50:11
:
Greetings!

I am a network engineer in rural east TX and moonlight on the side for a few local businesses. I got a distress call about a PC that would not boot. This machine had lots of tax data from previous years that she was actively using for research. I have used SpinRite many times to increase performance of lagging desktops, but this was the first time it actually resurrected a dead machine! She is happy and I am a hero! Thanks to you.

Miscellany

MailStore Home 8

- I now have 2.5 GB archived and indexed for instant access
- Now MailStore Home v9.7.1
    - Windows 7, 8 & 10
- http://www.mailstore.com/en/mailstore-home-email-archiving.aspx
- A Central Archive for All Emails
- Internet mailboxes such as Gmail or Yahoo! Mail
- Any POP3 and IMAP mailboxes
- Microsoft Outlook 2003, 2007, 2010, 2013, 2016
- Windows Mail und Windows Live Mail
- Microsoft Exchange Server 2003, 2007, 2010, 2013 and 2016 mailboxes
- Microsoft Office 365 (Exchange Online)
- Mozilla Thunderbird and SeaMonkey
- PST, EML and other files
- (And ... my creaky old Eudora v7.1)

Control-Flow Enforcement Technology (CET)

- http://blogs.intel.com/evangelists/2016/06/09/intel-release-new-technology-specifications-protect-rop-attacks/
- https://software.intel.com/sites/default/files/managed/4d/2a/control-flow-enforcement-technology-preview.pdf
- https://software.intel.com/en-us/isa-extensions/cet-preview

Two new concepts and features:

- A new "ENDBRANCH" instruction
- A new "shadow stack"

Steve Ballmer made a lot of news when, "running" Microsoft, he ranted of buffer overflows:

- "How can it be possible that we are STILL having these problems?!?!?!?!"
    - (So he left and paid way too much for a basketball team.)

A Steve Fintel @jsfintel

- I see your Security Now topic for next week is Intel CET. I was the Atom Processor CPU planner when we got approval to integrate CET into Atom (ahead of Core on Xeon). When I was preparing the material to 'pitch' CET to management, I pointed people to SN-211 to explain what ROP was.

The ROP (Return Oriented Programming) problem

- DEP (data execution prevention) has locked down data memory to prevent its execution.
- So clever hackers realized that they could successively invoke snippets of code at the end of existing subroutines as "proxies" to accomplish the work they needed done. Typically this is a bit of privileged kernel code to lift their own privilege restrictions to allow them full freedom.

ENDBRANCH:

- A "nop" on all existing chips allowing its transparent use on older processors.
- On "CET enhanced" chips, it must be the target of any CALL or JMP instruction (not local branches).
- The beauty of this is its implementation: a simple state machine watches the instruction pipeline. When any qualifying CALL or JMP instruction is seen, the immediately-following instruction *must* be "EndBranch"... In other words, the CALL or JMP instruction must have transferred control to an *expected* location having an "EndBranch"
- What this means is that CALLs and JMPs can then ONLY CALL or JMP to expected and intended locations within the code.

The SHADOW STACK

Background: The concept of a local, software accessible, "stack".

- Arguably one of the greatest innovations in computer science.
- A single place to store BOTH program temporary data and control-flow information.
- (It we had it to do over, we might change that... since that's the source of all the trouble!)
- It will always be paged into memory, so very fast to access.
- A super-convenient place to place subroutine parameters.
- A natural place to store subroutine call return addresses.
- A perfect place to store subroutine LOCAL (temporary scratchpad) variables.

When everything works perfectly there are no problems.

But many applications use the stack to hold external data received.

This is inherently DANGEROUS because that stack ALSO contains control-flow information!!

The normal "Execution Stack" is autonomously manipulated by Call and Return instructions.

The "Shadow Stack" is a hidden, inaccessible stack, which is ALSO autonomously manipulated by Call and Return instructions -- but contains NO DATA. So the control-flow portions of the two stacks should ALWAYS be synchronized! And any time a return address is "popped" of the stacks, the addresses are compared to verify that they are identical.

It's brilliant and simple and, because it's implemented in processor hardware/microcode... zero overhead.