SSTIC 2016 Keynote

Brad Spengler – grsecurity

Rennes, France

June 1 2016

Outline

- Update since PaX Team's 2012 keynote
- Advisory notice
- State of infosec union
- The future

Update (grsecurity)

- KSTACKOVERFLOW
  - Kills stack overflow vuln class on 64-bit archs
- RANDSTRUCT
  - Randomizes layout of critical marked structures
  - Auto-randomizes pure ops structures
- HARDEN_IPC
  - Automatic “umask” of sorts for IPC objects
  - Prevents harm from common cases of overly-permissive IPC
  - Based on research by Tim Brown
  - http://labs.portcullis.co.uk/whitepapers/memory-squatting-attacks-on-system-v-shared-memory/

Update (grsecurity)

- ARM v6/7 KERNEXEC/UDEREF
  - Provides protection equivalent to i386
  - Uses ARM domain support
- USERCOPY improvements
  - Message queue buffers allocated in separate slab cache
- RAND_THREADSTACK
  - Response to exploit by Exodus Intel against Asterisk
- DENYUSB
  - Prevents recognition of all new USB devices after system boot
  - Or temporary allowance via sysctl toggle

Update (grsecurity)

- Various “smaller” features/improvements
  - DEVICE_SIDECHANNEL
  - CHROOT_RENAME
  - Limiting *at() use in chroot to descendants of dir fd
    - Based on report by Jann Horn

Update (PaX)

- Per-slab object sanitization
  - Contributed by Mathias Krause
- CONSTIFY improvements
- SIZE_OVERFLOW improvements
- STRUCTLEAK
- LATENT_ENTROPY improvements
  - Feeds boot-time RAM contents into entropy pool
  - After-boot entropy extraction (interrupt/fork codeflow etc)
- REFCOUNT improvements
  - Non-public plugin to automate discovery of FPs
  - PPC port by Rodrigo Branco
- UDEREF/x64 improvement
  - PCID enhancement

Update (PaX)

- RAP
  - Just launched limited form in public 4.5 patch last month
  - Verification of type hash on indirect control flow transfers
  - < 1/5th total RAP size in LOC
  - Death of ROP/JOP/etc

Advisory notice

- Very difficult for any single person to have an all-encompassing view of security
- I've worked in the industry in several capacities
  - Specifically not in internal security department or exploit development
- Following are observations over the years from perspective of:
  - Free software developer
  - Defense/technology-focused
  - Maintaining intellectual independence
- I've also invited the suggestions/feedback of several unnamed individuals in various segments of the industry whose opinions I greatly respect
- Everyone has an agenda

State of infosec union

- Central claim: lack of critical thinking and gullibility for hype in infosec leads to poor security decisions, perverse priorities, and questionable ethics
- To deal with problems and change the current state, those problems must first be exposed

State of infosec union

- Still obsessed with bugs in 2016 AD
- More bugs than ever
  - NSA in grandma's threat model
  - Nearly every unprivileged app now CVE-able
- Despite bug obsession, security is improving
- Memory corruption attacks trending away from generic to application-specific
- Less being done with bugs in public
  - How many exploits against current state of art vs state of art in 2000?
  - Nearly no "real" Metasploit mem corruption exploits since hacking advanced past 0x0c0c heap spray
- Every good exploit shop today has data-driven attack frameworks targeting weird machines and explicit interpreters for browsers/etc
  - For all the Project Zero talk of their individual bug finding, these guys just fuzz another bug to plug into their framework and laugh their way to the bank

State of infosec union

- More data, less insight
  - Verizon DBIR report
  - Posting hundreds of presentations/papers online that are neither fact-checked nor understood doesn't make one a security expert
- Too many conferences, not enough quality to fill them all
  - Junk hacking
  - Plain false/misleading presentations with hyped up abstracts
- Conferences poor method of knowledge transfer
  - Good method of making audience *feel* "knowledge" transfer
  - Accept that it's basically show-and-tell, that understanding of a topic requires more than an hour, sometimes with weeks/months/years of background knowledge

State of infosec union

- Charlatans/Captain Hindsight “thought-leaders”
- Many trying to get famous/rich quick
- Promoting bad advice to increase infosec handouts
- General infosec populace depends on “authority” to call these out
  - Not done by most until there’s already a safe bandwagon to jump on
  - Calling out hype/lies harms profiting off them
  - Isolates from rest of infosec if not playing along
  - Tone argument – nice-sounding liars are preferred
- Too much effort to expose falsehoods vs effort to create them

State of infosec union

- Entitlements abound
  - Extortion games played by “researchers” entitled to payment for unrequested work/non-existent bug bounties
  - Leeches entitled to free everything, never contributing to anything
- Lots of “experts” talking/complaining but few people creating/publishing things of importance
- State of art is far beyond what remain largest individual threats
  - APT is fashionable, widespread threats are not
  - Political / interface issues
  - Office macros / hidden file extensions / gullible users
  - Giving apps enough rope via poor defaults, overly-expressive languages

State of infosec union

- 2003, Bugtraq:

It's clear that "len" is a signed integer and if "len" is negative this problem will
lead into an overflow since:
  if ((tmp = (xdrs->x_handy - len)) < 0) { --> This check will be evaded!!

and we'll end up in:
                memcpy(addr, xdrs->x_private, len);

BUT I must tell you; your argument about remote code execution does NOT seem to be correct
in Solaris/SPARC (especially in rpcbind) Unless you can prove me otherwise.

memcpy() will die with a negative len (even with 0x80000000) and Sun's memcpy() implementation
ain't ghetto like Free/Open/NetBSD so no cool tricks like GOBBLES' nose-job/scalp will work on it!

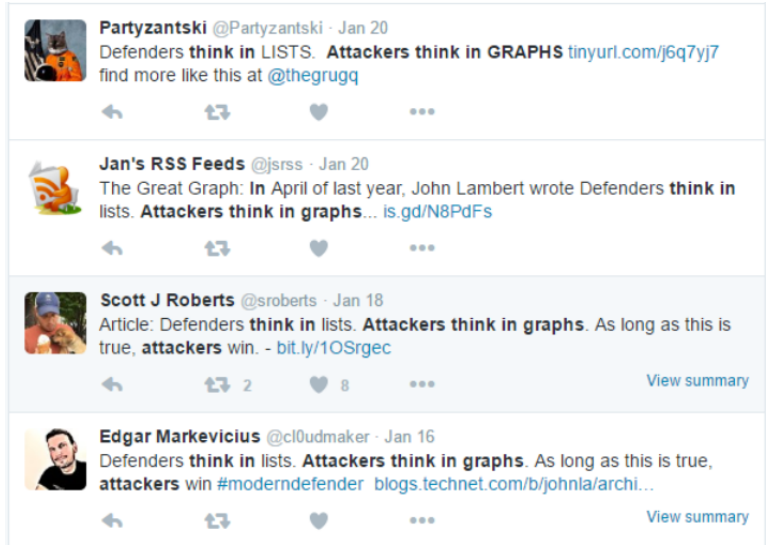
please enlighten us how come this is exploitable (Remote Code Execution in your words) ????

Regards,
Sinan

- Lots of good technical talk happening in the open, a sense of trying to achieve a common goal

State of infosec union

- 2016, Twitter

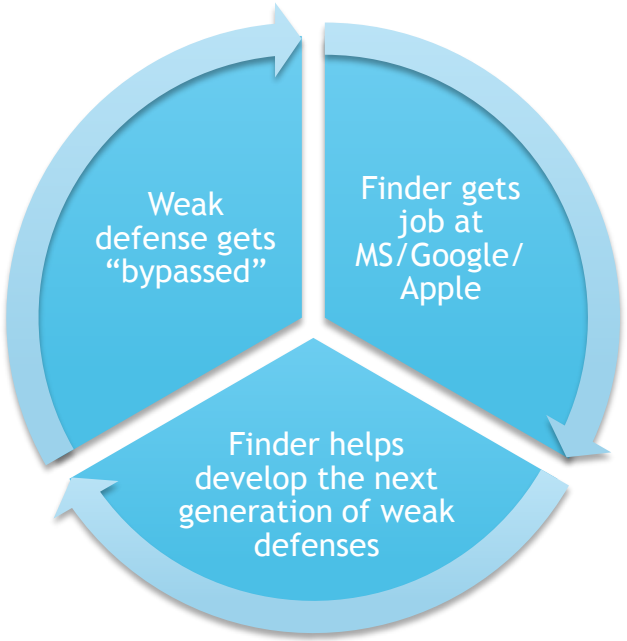


- Memes, oversimplifications, “proof” by analogy
- Strategically designed/provocatively worded to get the most attention
- Corrections/dampening expectations never as visible (e.g. BadBIOS)

State of infosec union

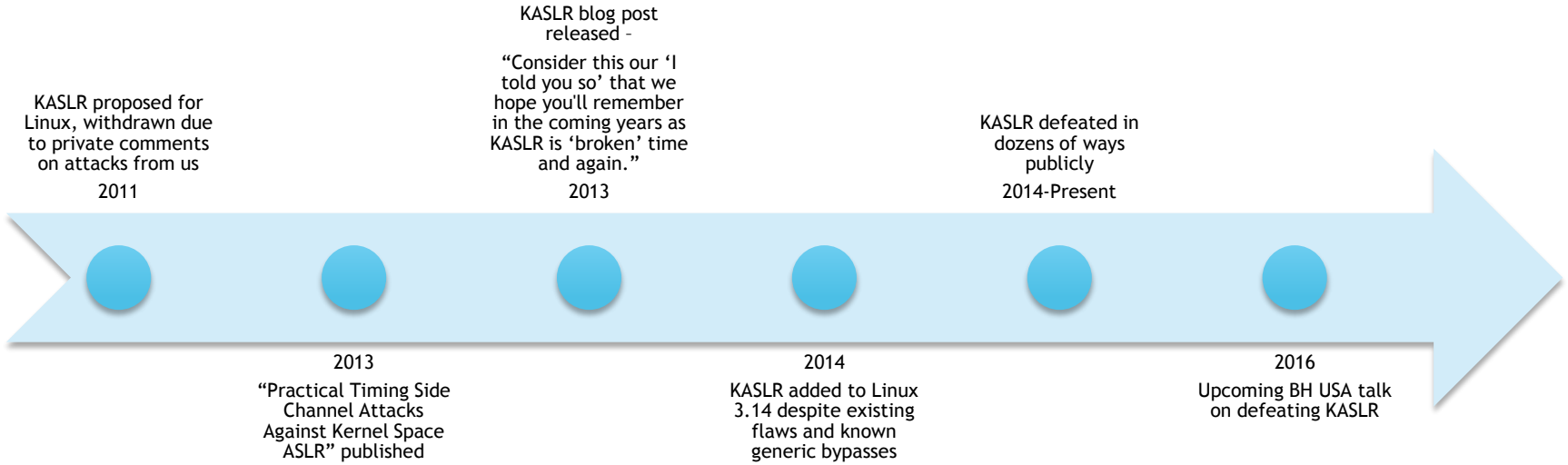
How bad assumptions lead to an industry protecting itself from its own “professionals”

State of infosec union



Cycle of "it's better than nothing" mitigations

State of infosec union



Ignoring security principles feeds the circus

The future

- Have to imagine a world where current state of art in grsecurity becomes widespread
- No more arbitrary code execution, no more executing existing code out of order
- Memory corruption driven to application-specific data-only attacks on weird machines
  - http://www.cs.dartmouth.edu/~sergey/wm/
- Each technique more valuable than the sum of bugs killed by members of Project Zero whose names are not James Forshaw
- Necessary shift from privilege escalation to privilege abuse
- Exposing and closing these techniques will produce real security improvements

The future

- Maybe we'll realize that there are a million different ways to add some hardening that will help against some cookie-cutter exploits
  - Doesn't mean they should be implemented – everything comes with some associated cost or tradeoff
  - One tradeoff is a false sense of security if the defense can't possibly accomplish what it's marketed for
  - Stop designing memory corruption defenses around a script kid model
- Realize if a security feature will take years to iron out all its existing bypasses or vulnerabilities introduced from new attack surface, it's not worth it
- Realize attackers take the path of least resistance
- Realize that security will never be achieved through bug reduction

The future

- Won’t fix most of the aforementioned complaints
  - Opposing motivations/rewards too great
- Can only suggest how to be a useful member of “community”
  - Critical thinking
  - Learn it’s OK to say “I don’t know”
  - Use valid criticism as an opportunity for improvement
  - Reject the race for fame, submit a beefy paper to a content-rich ‘zine like Phrack
  - Don’t seek shortcuts, put in the necessary work and learn fundamentals
  - Anyone can complain, fix something

Questions?

- Thanks to my ~dozen reviewers/complaint contributors
- Thanks to the SSTIC committee for the invitation
- Thank you for your time!