==Phrack Inc.==

Volume 0x10, Issue 0x46, Phile #0x02 of 0x0f

|=--------------------=[PHRACK PROPHILE ON XERUB]=--------------------=|
|=---=|
|=-------------------------=[Phrack Staff]=--------------------------=|

|----=[Specs

```
          Handle: xerub
             AKA: concat(*given_name, surname)
                  <insert other silly names made up during my teen years>
   Handle origin: Completely made up. Any semblance with literary or real
                  life is purely coincidental. The X is to be read like a
                  Latin X, or even the the Greek letter X, if you prefer,
                  but never like 'sh'. Also, Quake3's Xaero is my cousin.
Age of your body: Old enough to remember the horrors of the Eastern Bloc.
                  Also XOR AX, AX is faster than MOV AX, 0. Change my mind!
 Height & weight: 170+ & slender
     Produced in: Romania
            Urlz: https://github.com/xerub, https://twitter.com/xerub
       Computers: AMD K5, K6, Pentium Pro, Celeron, Core2 Duo, Core-iX
      Creator of: The concept of kppless jailbreaks [sic]
       Member of: XXX
        Admin of: XXX
        Projects: 0x41con
           Codez: img4lib, ROP compiler, many other incomplete tools used
                  in jailbreaking
    Active since: Around the turn of the millennium
  Inactive since: 2020
```

|----=[Favs

```
   Actors: J.P. Belmondo, Gheorghe Dinica.
    Films: Brazil, Blade Runner, Fight Club.
  Authors: Raymond Chandler, Oscar Wilde, Aldous Huxley, George Orwell.
 Meetings: 0x41con, Warcon early editions.
      Sex: Promiscuous & dirty.
    Books: Dead classics, mostly. No technical book ever.
    Novel: The Picture of Dorian Gray.
  Meeting: Richard Feynman, +ORC
    Music: Deep Purple, Led Zeppelin, Queen before '92.
  Alcohol: Single malt scotch, straight. Red dry wine.
     Cars: BMW
    Women: Young, tall and slender with a sexy ass.
      Men: Nop.
     Food: Italian, SE Asian seafood.
   I like: Freedom, sunny weather, unhealthy habits, scantily-clad babes.
I dislike: Hypocrisy, political correctness, authority, the philosophical
           Left. Zealots of any kind. Fat people occupying two seats in a
           bus.
```

|----=[Life in 3 sentences

After being raised in a rural area, I went to high school in a medium-sized city. High school changed my life, because it meant the opportunity to use a real computer. During university, a nasty car accident paused my studies, but around the same time I landed a couple of jobs, ultimately settling for a security company and staying with them ever since.

|----=[Passions, what makes you tick

Understanding the intricate details of a machinery. Any machinery, starting with mechanical ones down to the most complex Rube Goldberg-esque software exploits. But the true joy begins when I build such machineries myself. Even when not doing vulnerability research, I spent my hacking days close to the hardware, squeezing the last bit out of it; be it 3D graphics cards

drivers or x86 protected mode system software.

|=---=[Memorable experiences

Going backwards in time that would be: the two 0x41con meetings; greetz to all the people involved, here's to hoping for the next one. My first trip to East Asia; amazing history, amazing people, amazing food. My very first iOS vulnerability - a dyld codesign bypass; I was stupid enough to pass it down to someone who then used it without my permission. Taking apart my 1.1.2 OTB iPhone and performing a baseband hardware unlock by pulling the A17 trace high, following geohot blogposts. Understanding the genius behind ZMist. Trying, and failing to crack SoftIce; I guess I wanted to have my name on it but I had to settle with Marquis de Soiree instead. The first contact with a computer; it changed my life.

|=---=[Quotes

"The smart way to keep people passive and obedient is to strictly limit the spectrum of acceptable opinion, but allow very lively debate within that spectrum" -N. Chomsky

"The robber baron's cruelty may sometimes sleep, his cupidity may at some point be satiated; but those who torment us for our own good will torment us without end for they do so with the approval of their own conscience." -C.S. Lewis

|=---=[What's your opinion about Phrack?

I am often asked by young people how and where to find materials related to hacking and my invariable response would be Phrack. They can find here pretty much everything, from the venerable stack overflows -- Aleph One's Smashing the Stack for Fun and Profit -- to the most complex hacking of relatively modern software. Phrack is THE place to learn about hacking.

|=---=[What you would like to see published in Phrack?

I believe the most valuable articles are those describing techniques and not specific bugs. Two of these seminal papers were extremely important to me: nemo's Modern Objective-C Exploitation Techniques and saelo's Attacking JavaScript engines. These are only a couple of papers which allowed hackers to pull their magic for years to come. We definitely need more of these!

|=---=[Who or what inspired you to start hacking?

Razor 1911. As a boy, I imagined I would like to crack games and play them for the rest of my life.

|=---=[We know that no one will ever admit he's part of the underground,
        but, when and how did you enter it? :>

I did NOT enter the underground when I created my first keylogger, I think. I just found out about TSR (terminate and stay resident) feature of DOS and set out to steal some user passwords from the school lab. INT 09 ftw!

|=---=[What do you consider your most notable technical achievement?

I guess the most anticipated response to this question would be: owning the bootchain. It's not, let me explain why: the bootchain is a mixed blessing. While it is regarded by many as a Holy Grail, it is truly a white elephant. First, it was never really needed for continuing research; second, speaking of such rare bugs is a one-way trip to killing them; and third, most of the time they end up used by entities I personally would not like to have them.

My bootchain research started somewhere in 2015 and ended around 2017, and while it did produce a couple of bugs, I do not consider them to be notable technical achievements, because they pretty much lack complexity, with the exception of the most useless one: the HFS+ iBoot stack overflow.

While this may sound bizarre, I do not rate my hacking on the value of the

end goal itself, but on the complexity of the attack. Most of my exploits were, in turn, my most notable technical achievement up to that respective point. If I had to pick one, it was getting shell into a locked iPhone, about five years ago. And then again this year, with CVE-2021-30737.

|=---=[Related to the previous question: Can you give us some background information? How and why did you come up with this? Can you give us an anecdote story related to it?

Back at the time it was considered an extremely hard job, except for owning the bootchain. It happened in the wake of the FBI vs Apple lawsuit over backdooring iOS. I set out to do it with the help of some friends, but we were using some freshly patched bugs. As a result, it didn't end up being very useful, but the full chain was probably one of the most complex I have ever written. Also, the experience I accrued during the process helped me greatly to repeat it five years later using an 0day with minimal effort.

|=---=[You have published a lot of work (code, keys, etc) on Apple-specific technology. What do you find attractive about Apple as a research target?

All the cool kids were doing it. Besides, in the beginning, it was fun to break into an iPhone, if only to stick it to Apple who thought their OS was impregnable. But on the other hand, I truly liked their phones, both from a hardware and software standpoint.

|=---=[When have you started looking into Apple technology?

I think it was in December 2007, when I got my first iPhone. My boss gave it to me at the company party as a reward for something I can't remember. There is a strong probability the whole deal involved bribes and women of dubious moral standards.

|=---=[What's your opinion about Apple's stance on software and hardware security?

Apple has a lot of code to deal with. The sheer amount of their own code makes security bugs become almost a certainty, but they are alleviating this by compartmentalisation and other security mitigations, with varying degree of success. Their bug-fixing sucks, most of the time it is either an incomplete patch or downright a bad one. They also use a lot of third party code, but do not seem to do a good job of tracking security fixes in those libraries. This leads to some of the most embarrassing security problems.

On the hardware front they are doing a pretty good job, however. Isolating the sensitive crypto material in the Secure Enclave outside the Application Processor is probably one of the best ideas they had so far. Unfortunately, they overlooked a couple of things in the early models (mainly 32bit SEP), allowing them to be hacked with relative ease.

|=---=[What's the future of Apple-related security research (not only jailbreaking, more generally speaking) in the light of ARMv8.3 features (PAC, etc) and Apple's hardware security measures according to your opinion?

PAC is a good mitigation because it significantly raises the bar of gaining an initial foothold, at least in certain scenarios. However, when PAC first landed it was not as pervasive as it should have been, protecting only code pointers while leaving out crucial data pointers: CoreFoundation runtime, internal kernel structures, etc. Apple will also add MTE to their chips in the near future, which may raise the difficulty of future exploits even more. But then again, it all depends on how it will be implemented.

Unfortunately, Apple-related security research boils down to either use a Security Research Device or use an exploit chain to break into the iPhone for further exploration. The former is a strong No for many people because of Apple's Terms and Conditions, while the latter implies an n-day or even a 0-day. In the near future we can still go that route, but as the current devices become obsolete and newer ones come packed with hw mitigations, it

will become increasingly difficult.

On the bright side, the Macs are slightly more open for the time being and fortunately for us, the same research often applies to their mobile devices because they share an enormous amount of code with the Macs. This somehow postpones the aforementioned problems for a while.

Another solution would be to resort to iOS/device emulation, but that holds an uncertain future and is not available to the public at large. I have no experience whatsoever in this area.

|=---=[Is the Apple "underground" still as strong as it was, say, 5 years ago? Relating to the previous question, what do you thing about its future?

It certainly is not. Many talented researchers have left, become inactive, got a job (at Apple or elsewhere) or entered the exploit market.

|=---=[What open problems and emerging technologies do you think are good research topics? Current and future.

The best research topics are those areas that are not very well understood, especially in closed, proprietary systems: basebands, wifi firmwares, etc.

|=---=[Do you prefer offensive or defensive research? Which of the two do you think helps learning and understanding more?

I certainly like both. Defensive is much, much harder though. My personal experience tells me it's easier to go the offensive route, and move to the other side once you have gained enough insight and experience. This allows you to have a clear image about a mitigation in your system: what are you supposed to defend, where is the security boundary, how is this mitigation helpful, etc.

|=---=[What's your take on the IT security industry vs. "the underground"?

For a long time, the underground was the crucible from where the new talent emerged. In the past, it was the only place where one could find knowledge and acquire true skill. And the Dark Side is more appealing to youngsters, especially during their teen years. But as they grow older, they need to get real jobs and oftentimes they join the Industry. On top of that, things have changed, because nowadays one could learn about security in school, or from the myriad of published exploits. This means the Industry can bypass the underground, which is beginning to fade.

|=---=[Some claim that the hacking scene is growing old and that there are not enough talented young people interested in hacking to replace it. What are your thoughts on this?

I believe there is enough talented young people interested. The "problem" is that they are snatched as young as possible by the Industry, lured by fat paychecks. As such, their voyage through the hacking scene is rather short, if at all. This may lead to a starvation of the scene, at least to some degree.

|=---=[What is your advice to the new hackers reading this?

Start early, when you have enough energy, time and ideas. Do not dismiss old techniques and bugs, there is always something to be learned in those lessons. Most often than not, there is an overlooked bug next to the one that just got patched. Also, no amount of books, slides and papers can beat hands-on experience, ever. Roll up your sleeves and prepare to dive in.

|=---=[What was your most "enlightening" insight so far? Either technical or not (or both).

Time is our most precious resource during our lifetime. It is probably the only thing one can never recoup or buy. Use it wisely and enjoy life. Hack away as long as hacking brings joy and satisfaction, and then move on.

|=---=[What is your stance on full-disclosure vs non-disclosure? Are there
        situations where both are needed, or is it one or the other?

I am leaning towards full-disclosure. While there may be circumstances in which non-disclosure is preferable, I still think full-disclosure raises the awareness of certain bugs and forces both the software vendor and the customers to realize the gravity and patch as soon as possible.

|=---=[What is the future of hacking? The future of "the underground"?

Very few hackers are left to hack for the sake of hacking. Most of them get early jobs in security, but oftentimes they end up doing boring stuff. On top of that, the bar for hacking the most interesting targets nowadays is much higher than, say ten or twenty years ago. My personal feeling is that hackers gonna hack, but the golden age is behind us now.

|=---=[What do you think is the role of Phrack in the current "scene" that
        is dominated by "cons"?

Cons are a great way of meeting friends, new people in the field, have fun and generally speaking, do networking. However, a deck of slides will never be as detailed as a white-paper, or an elaborate article. And this is where Phrack shines. Another aspect is that Phrack goes back in history. There is plenty of material starting from the simplest to the more complex hacking techniques and it is the go-to place for a newbie.

|=---=[What do you think the biggest infosec challenges for the next 5
        years are/will be? And what should be done about them?

The harder problem in the short to medium future is to protect our privacy. On one hand, governments are pressuring for backdooring crypto and on the other hand, dubious entities are trying to break it. I have no idea how will this pan out, but I'm not very optimistic about it. Governments will eventually have their way, babbling something about the Greater Good or something along that vein. The other guys will have their way by trying to own the endpoints, but that is not likely to happen en masse.

Speaking of the endpoint security, I believe the web browsers and their ever-increasing complexity will be the bane of our existence for years to come. The browsers wield way too much expressive power on the client-side which can be used to bypass all sorts of mitigations.

Another issue that plagued us for the past several years, vaguely related to the above, is the multitude of breaches that happened left and right, exposing troves of user data from big corps' supposedly secure databases. The easiest way to prevent such disasters is to avoid storing said data, but I'm afraid that will never happen, because it conflicts with their mercantile interests.

|=---=[Open question. Anything more you would like to say to Phrack
        readers?

I would like to thank the Phrack staff for this honour, I am both flattered and humbled for being prophiled. That said, I'm pretty sure there are at least several dozens of hackers who are ten times better than me, or have lived much more interesting lives. Kudos to all of you, you know who you are!

|=[EOF]=---=|