A Praise for Hackers

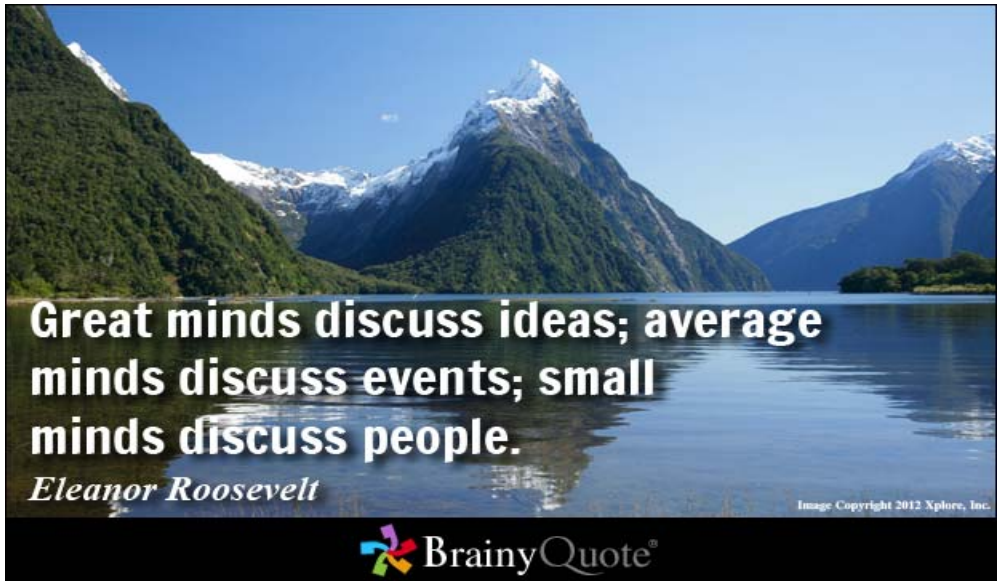
Rodrigo Rubira Branco (BSDaemon)
rodrigo *noSPAM* kernelhacking.com
https://twitter.com/bsdaemon

“As the area of our knowledge grows, so too does the perimeter of our ignorance”

Neil deGrasse Tyson

Why this is dangerous

- This will be one of the things we will discuss:
  - Does the position of someone really matters??
  - Should we trust everyone?
  - Judge the idea, not the person. Refute what someone says, not who he is.



Corporate Disclaimer

- I don't speak for my employer. All the opinions and information here are my responsibility

- Interrupt me if you have questions or important comments at any point.
    - **IMPORTANT: No, I'm not part of the Intel Security Group (McAfee)**

Personal Disclaimer

- I do not represent the hacking community. I do not represent anyone, but myself
- In my opinion, no one can actually represent the hacking community, not even a subset of it (like for example, hackers from a given location)
- What I can do, is to give MY opinions on it, based on my observations. That means, a very limited, narrowed view of what hacking is and represents
- Given the size of the audience and variety of profiles, it is hard for me to define the right message (too technical, no technical at all, career, older people than me, younger people than me…) -> Forgive me in advance if you feel underestimated or not valued

So true…

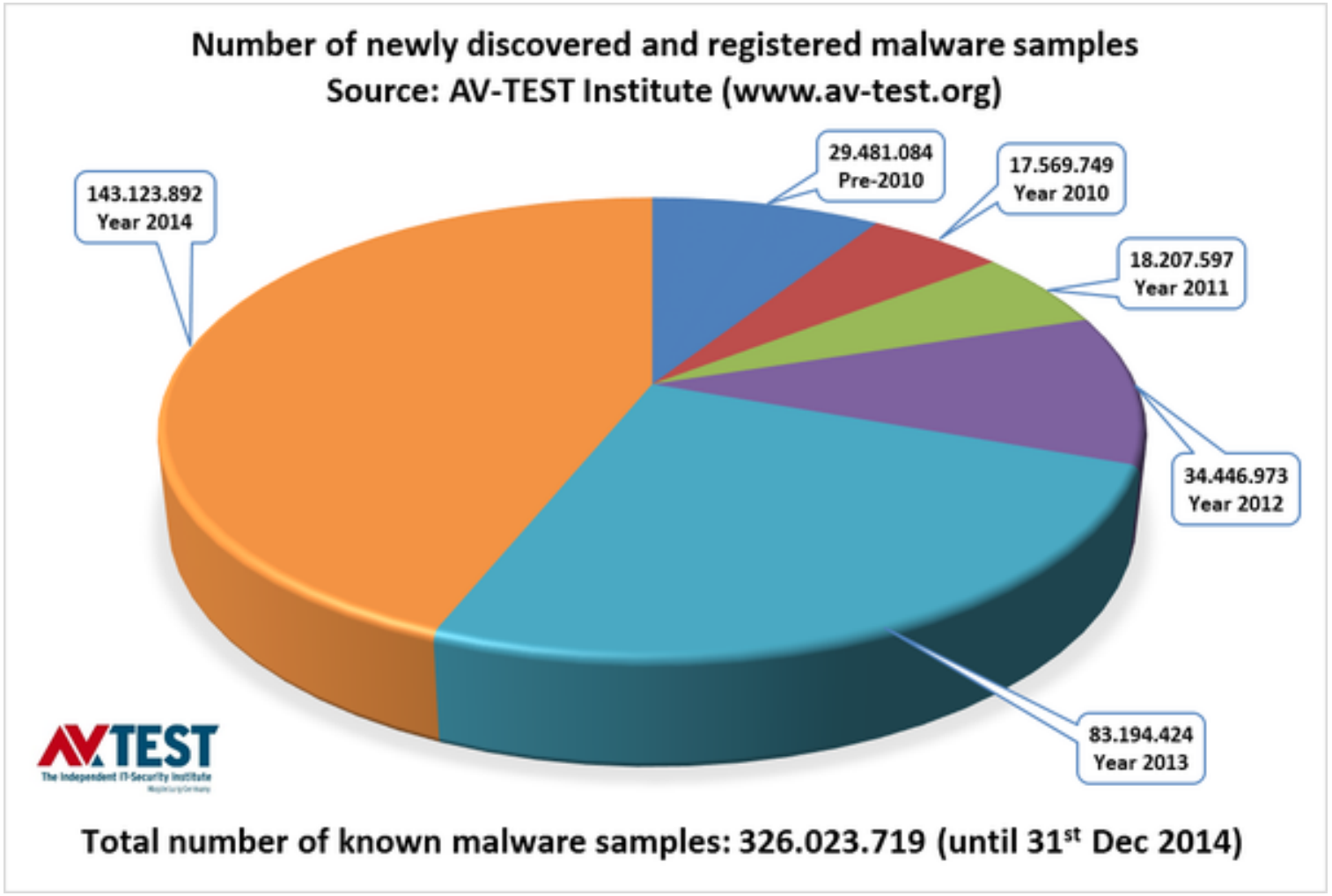
- “*No Chess Grandmaster is normal; they only differ in the extent of their madness*”
  - *Viktor Korchnoi*

- **“No hacker is normal; they only differ in the extent of their madness”**
  - BSDaemon

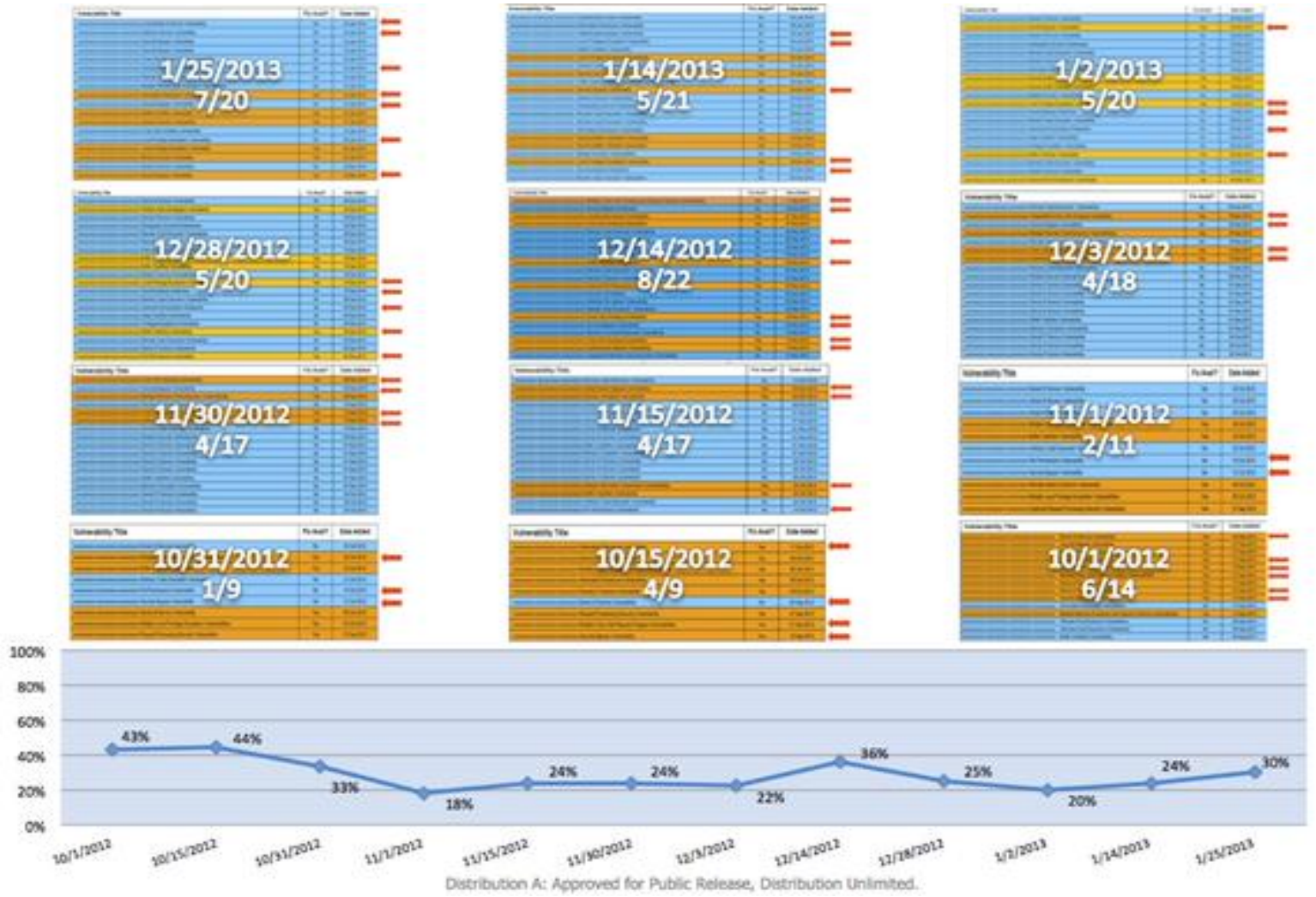
Objectives

- The world changed, we must change as well
- Try and disseminate what/how people can do to contribute to the hacking community that I know
- Praise the work of hackers changing the world, their importance and propose other areas to research

Why are we here?



1/3 of Government Systems Vulns is in the Security Software



Source: Tweet by @dotMudge

To start the conversation

- When you receive an idea, tip, recommendation remember to evaluate it in your own context to see if it applies to you -> Your decisions, your impacts (positive and negative ones)

- Be honest at least to yourself (try to be more critical to yourself than you are to others, even if you don't share your findings)
  - This will help you, and only you

Why a keynote is always difficult

- Shows that we getting old ☺ And as so, we have lots of histories to share

- We need to balance the content, we can't be technical, but we are in a technical event after all :/

- Reemphasizing that if you don't agree with what I say, just don't follow. If you do, follow, change ☺ the consequences are on you either way.

Three Points to Take Out

- Care more about what YOU do than what others do (unless they really damaging people)
  - Researchers should have fun and enjoy what they do
  - Even if they are capable of more, why assume they want to do more?

- Treat information you receive as data, process and get to your own conclusions on it
  - Deepness of analysis depends on importance

- Disseminating information is different than disseminating garbage (are we at the information age or at the garbage pass age?) -> Are you *REALLY* helping?

Information or just data?

- When you receive an information, treat is as just data (unprocessed), do your own analysis and criticism before considering it an information
  - Deepness of the analysis depends on the importance/impact of that information

How to study? How do you learn?

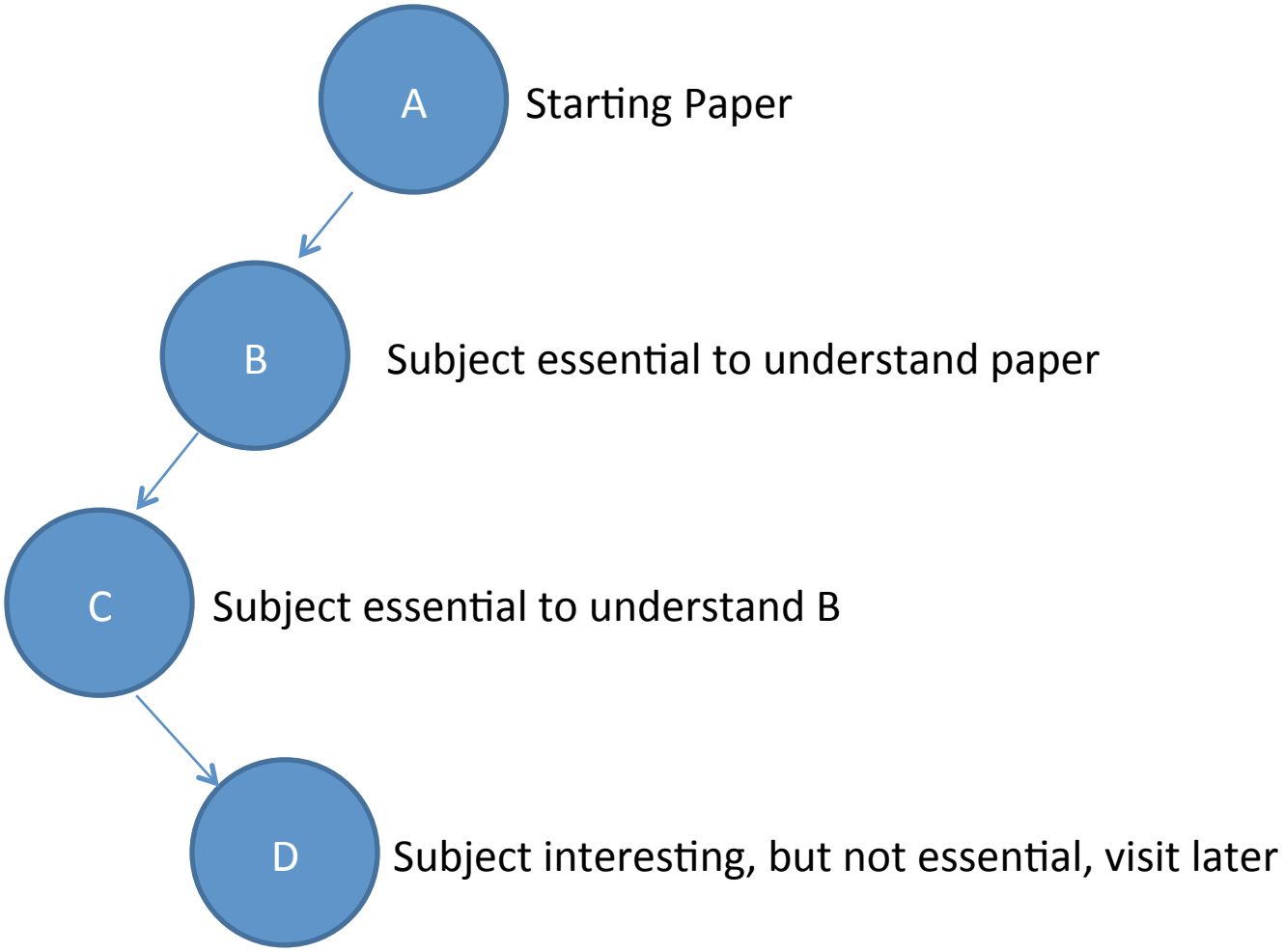
- When you want to study a paper, understand what are your expectation of learn (for example, you want to learn a new exploiting technique)

- Start reading, and for each item you know nothing about, create an item in a tree -> leftmost if it affects the learning of the subject matter; right if it does not

- Go deep, on topics first.

Source: Adapted from the book “Think like a grandmaster” – Alexander Kotov

Study Tree
I'm bad with graphics, but it is not binary



Great, but what to prioritize?

- Mikhail Botvinnik was a three-times world champion of chess and had as pupils Anatoly Karpov, Garry Kasparov and Vladimir Kramnik

- Even after that, it was said that he listened to basic chess lessons in the radio. The reason: To always remind of the **fundamentals**. Keep them sharp
    - NOTE: I've not added a reference because I couldn't find one, maybe I mixed names of the grandmasters. If you have a reference on that, please send it my way ☺

The Fundamentals

- The essence behind computation did not change:
  - The Turing Machine model of computable problems exists even before digital computers (1936)
  - Chomsky work on language hierarchy work is from 1950's
  - TCP/IP is from 1980
  - The essence of PC architecture too ☺

Learning x Memorizing

- *"Memorization of variations could be even worse than playing in a tournament without looking in the books at all."*

  – *Mikhail Botvinnik*

- "*Never memorize something you can look up in a book*"

  – *Albert Einstein*

Learning Plan?

- Once in a chess competition, grandmasters were analyzing a position -> They mostly agreed a given side had advantage (let's say white)

- Capablanca was passing by and was asked to give an opinion: he said black had a clear advantage (!)

- When told to demonstrate it, instead of doing moves, he just changed the entire position to something new -> To the surprise of the grandmasters, there were nothing white could do to avoid the game to get into that position
    - NOTE: I've also not added a reference because I couldn't find one, maybe I mixed names of the grandmaster. If you have a reference on that, please send it my way ☺

Did you really learn to the point that you can extend?

- “*Chess books should be used as we use glasses: to assist the sight, although some players make use of them as if they thought they conferred sight*”
  - *Jose Raul Capablanca*

- “**If you really know, you can hack**”
  - BSDaemon

“Sharing is Caring” or not

- We are in the information age. But most of what we receive is actually trash

- Before sharing something you saw, what about read, understand, think? Somehow people hide behind the ‘sharing is not endorsement mantra’. I can share interesting things that I do not endorse (for example, to start discussions, to demonstrate another viewpoint)

- People that read what you share trust you, are you really helping them sharing whatever you see just because it is new? That is how hoaxes spread. You are also judged by that (after all, do you have the time to read everything you just forwarding or not? Or all your time is spent finding things to share, but you never actually study them?)

“Publish fast”

- People mistake helping the community with publishing whatever crappy comes to their minds

- This can be attributed to the misunderstanding of the open-source community of publish it fast
  - But you don’t discuss things with people first?
  - Before you publish something, think if you are really helping the community or if you’re making people waste their times: Because that damages the community, it does not help anybody!
    - So think about your objectives: Do you just want to show-off or you really believe you contributing to the community? There is a huge difference there!

New generations

- New generations come naturally to replace and be superior to the previous ones (if you believe in evolution)

- Probably in the audience there are already many (or most) people that are much better than me (not that difficult). And that is natural!

- There will be always a collision of ideas, and the previous generations obviously don't want to lose their importance! The difference on that natural collision is the way you challenge:
  - Is that thru technical superiority or;
  - Personal things? Which in practice should be considered irrelevant (I really don't care which car you drive, how much money you have or to whom you did a blo**** to get all that ☺)

The new speed?

- *"Half the variations which are calculated in a tournament game*
  turn out to be completely superfluous.
  Unfortunately, no one
  knows in advance which half"
  – *Jan Tinman*

- We somehow nowadays expect results before the 'a**-working time'

Constructive Criticism

- I think this is bull****
- Generations will conflict and ideas will be challenged:
  - But challenge the idea, not the person (why the person matters? Is he rich, tall, fat, weird…)
  - Transform garbage in chocolate ☺ -> If you actually refute the idea, or demonstrate it wrong, than the field evolves
- There is no such a thing as junk hacking
  - We should hack because it is cool and we have fun
  - Anything else is not hacking (even if it is a great technical accomplishment)
  - I prefer simple, but true than very hard/complex but money-moved
  - And btw, since when the media coverage of something shows its importance??

Trust

- Trust is given, not deserved
- It is the way that humans are, that's why social engineering works!
- This is also what generates the problem, because security is something counter-natural, and people see hackers as paranoids
  - **Trust should not be transitive either**

Is hacking growing? Or is the Scene Dead?

- FX foresaw "The extinction of hackers" in a paper from 2005 (which by the way changed my career and ideas)
- But is hacking dead? How come if we see more and more hacking-related things? Look into the size of this conference ☺
- The matter is hacking used to be an underground culture (or sub-culture) and now it is mainstream
  - People get confused between technical expertise and hacking mentality (from the original sub-culture)
  - Corporate interests and intelligence agencies influence the hacking communities, sharing, publications and others
- In the past EVERY computer user was a programmer. Don't you miss "when men were men and wrote their own device drivers"?
    - Quote: Linus Torvalds, 1991.

The scene is dead…?

- **“***Chess is not like life... it has rules!***”**
  - *Mark Pasternak*

- “**and so does CTFs**”
  - BSDaemon

Learning from Others
Russia x Brasil

- Both countries have continental sizes
- Both countries have strong willed people, which can be demonstrated by the military history of Russia and by the economic growth of Brazil (ok, not that much lately)
- Share common vocabulary words ☺
- Both seems to be relevant in the malware creation arena -> Ok that is not really important for the argument
- **So why we see much more Russian researchers??**
  - **Russians are proud of Russians**
  - **They help each other, they promote each other**
  - **They support other researchers, instead of point fingers, instead of supporting foreign ones**

Evolving the community?

- *"Some part of a mistake is always correct"*
  - *Savielly Tartakover*

- *"an accumulation of small advantages leads to a supreme advantage."*
  - *Wilhelm Steinitz*

Hackers are changing the world

- Lots of hackers currently work for big corporations and/or independently
- They working on pushing defensive technologies in hardware, operating systems and many different software
- They also working on finding and patching security vulnerabilities

Art x Exploiting

- *"Chess is the art which expresses the science of logic."*
  - *Mikhail Botvinnik*

- **"Exploitation is the art which expresses the science of logic"**
  - *BSDaemon*

- **"If exploiting is an art, we have poetic license"**
  - *BSDaemon*

Your career, your choice(s)

- It is possible to do interesting and important research in different scenarios, each with its own challenges:
  - Independently (using personal time, or making that your own company)
  - In a small company (either one that offers prime services or one that gives plenty of free time)
  - In a big corporation (in research or product security teams)

Offensive and Defensive Research are Important

- Offensive research is important to keep the state-of-the-art knowledge and understanding of offensive strategies

- Defensive research is extremely important to be sustainable (just fixing bugs is not enough as a durable strategy that deals with modern development growth and software dependency)

“There will be always bugs”

- Engineering process tries to catch and fix those

- That do not mean we can’t work on mitigations of capabilities once those bugs exist
  - And the performance trade-off of current/existing mitigating techniques demonstrate they are real/ practical

Defensive Research

- There is a clear need for defensive research and projects like grsecurity/PaX need to be praised, helped, admired, learned from
- They advanced the field, created the ideas that came many years later to modern hardware and OSes
- They are **STILL** years ahead!

Open-source x Hacking
Linus x Researchers

- **Disclaimer:** I have nothing against Linus, I actually appreciate his work and find his communication style quite funny (btw, what is the problem with the monkeys? Penguins do it too)

- The problem is not only Linus, but how we see security research in general as well
  - Offensive is cool
  - Defensive is boring, useless

Creative Activity

- *"Chess, like any creative activity, can exist only through the combined efforts of those who have creative talent, and those who have the ability to organize their creative work."*
  - *Mikhail Botvinnik*

A message to Linux Developers

- Instead of trying criticizing the lack of engineering knowledge, why don't you try to see if maybe you don't have a lack of understanding over the complete problem? (the security problems)

- Why not give the option to your users to use the best security possible at least?

- Remember that most big area maintainers are actually employees of big corporations and maybe they are not really doing what is best for the community but what they are told to (see, everyone actually might have a hidden agenda, so careful with hoaxes and what you believe)

Psychologically Brutal

- "*Few things are as psychologically brutal as chess*"
  - *Garry Kasparov* -> He clearly never contributed to the Linux kernel ☺

What can we improve?

- We researchers are culpable too:
  - Every time we demonstrate a bypass of something, we forget to mention the many times that something is actually useful
  - We also forget to mention what is the actual state of the art for the given technology we bypassing, and which mistakes were made in the specific implementation we targeting ☺

Sources:
http://www.washingtonpost.com/sf/business/2015/11/05/net-of-insecurity-the-kernel-of-the-argument/
https://forums.grsecurity.net/viewtopic.php?f=7&t=4309

Ego breakage

- “*I like the moment when I break a man’s ego*”
  - Bobby Fischer

What the future holds?

- Understand what security is really about and what are the real security aspects of a system:
  - Complexity is bad;
  - Assumptions are dangerous;
  - Composition of systems != the security of each element of that system
  - What is formally proven is not necessarily correct if the pre-requirements and simplifications of the computing model are not correct as well (if they lose power)

Conclusions

- Care more about what YOU do than what others do (unless they really damaging people)
  - Researchers should have fun and enjoy what they do
  - Even if they are capable of more, why assume they want to do more?
- Treat information you receive as data, process and get to your own conclusions on it
  - Deepness of analysis depends on importance
- Disseminating information is different than disseminating garbage (are we at the information age or at the garbage pass age?) -> Are you *REALLY* helping?

The end!! Really is !?

Rodrigo Rubira Branco (BSDaemon)
rodrigo *noSPAM* kernelhacking.com
https://twitter.com/bsdaemon

“As the area of our knowledge grows, so too does the perimeter of our ignorance”

Neil deGrasse Tyson

Conclusions

- Care more about what YOU do than what others do (unless they really damaging people)
  - Researchers should have fun and enjoy what they do
  - Even if they are capable of more, why assume they want to do more?
- Treat information you receive as data, process and get to your own conclusions on it
  - Deepness of analysis depends on importance
- Disseminating information is different than disseminating garbage (are we at the information age or at the garbage pass age?) -> Are you *REALLY* helping?