Open Source & Cybersecurity

Harnessing the power of distributed communities worldwide to improve & create state of the art cybersecurity software

ANSSI – 10th of November 2016 – Washington D.C

Introduction

A few words about me….

Charles-H. Schulz, 37, living in Paris, works for the ANSSI. 10 year contributor to the OpenOffice project, co-founder of the Document Foundation and the LibreOffice project since late 2009.
Other projects: Mandrake Linux, Mandriva, OpenMandriva, Mu mail indexer…

Open Source is not « free as in beer ». It’s just something else people don’t quite understand.

What's Open Source, really?

A few ideas....

> A specific set of development practices

> A precise way to license software

> The implementation of «software freedoms »

> Values for the digital age

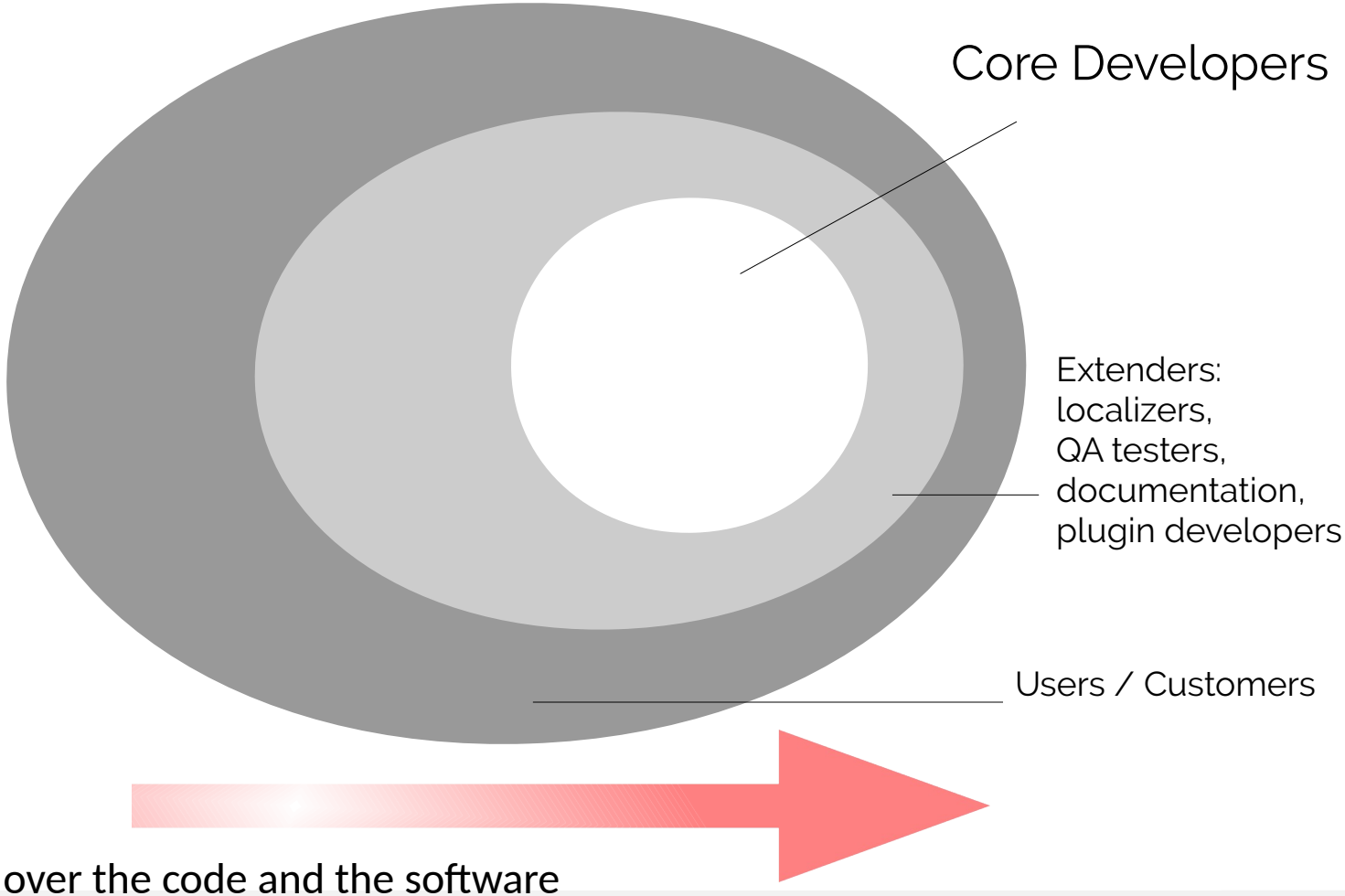
> A philosophy for hackers

> New business models

> All or some of the above

Understanding Open Source Communities

Everyone benefits from the freedoms conveyed by the software licence(s) of the project



Understanding Open Source Communities

A few key principles

> Free and Open Source projects do work through meritocratic principles

> Only limited democracy may exist within a community

> *« He who ruleth over the Code shall rule them all »*
- Developers do what they want or what they need
- So do other contributors, even though contribution is what matters in the end

> Free and Open Source projects DO NOT CREATE products ever. They create the digital commons necessary to create products based on software.

Obscurity, Transparency, Cybersecurity

Software is not designed with security in mind most of the time.

> Not publishing your code does not make you safer. It only creates an incentive for the bad guys to exploit vulnerabilities of your code.

> Publishing code under an open source license allows others to check it and improve its security (many eyes are better than a few)

> HOWEVER: developers do not operate in the void:

- *Some have mortgages*
- *Most of them have to eat*
- *You need resources to ensure people look at the code*

Case in point: Heartbleed

Making Open Source work for Cyber Security

A few ideas

Open Source Software improves trust and confidence in solutions, platforms & tools.

> Access to the code means you or anyone else can patch it

> Security strategy and processes at project level are absolutely necessary

> Shift in culture needed:

- *Cybersecurity software must be developed with at least some attention paid to securing or hardening the code*
- *No code, no infrastructure is safe for ever*
- *Free & Open Source Software allows interested parties to fix security flaws themselves to a large extent without relying on others to do the job*
- *In the end, community is what makes or breaks an open source software*

Thank you!

Charles.schulz@ssi.gouv.fr
Twitter: @ch_s