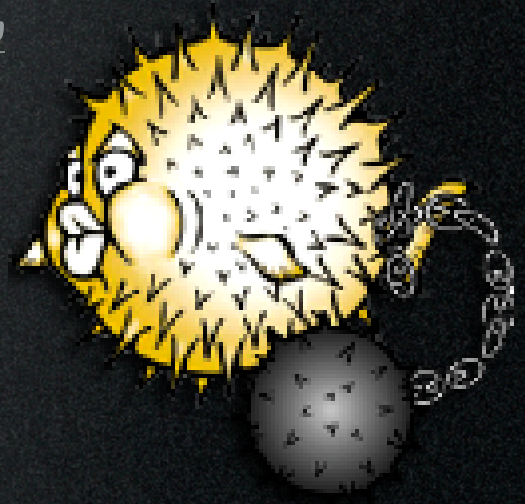
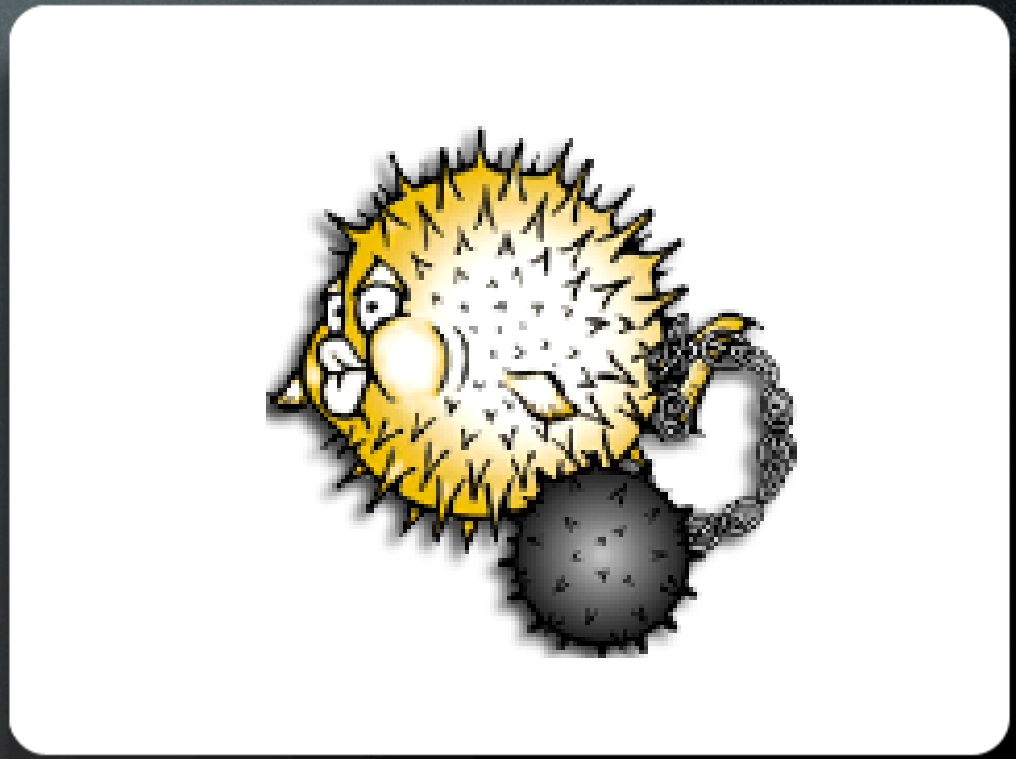
# Information Security in Open Systems

Paula Valença
pvalenca@di.uminho.pt



# What this will not be about...

- ... a study of security and cryptography in OpenBSD...
- ... I know too little to make any serious comment on the subject

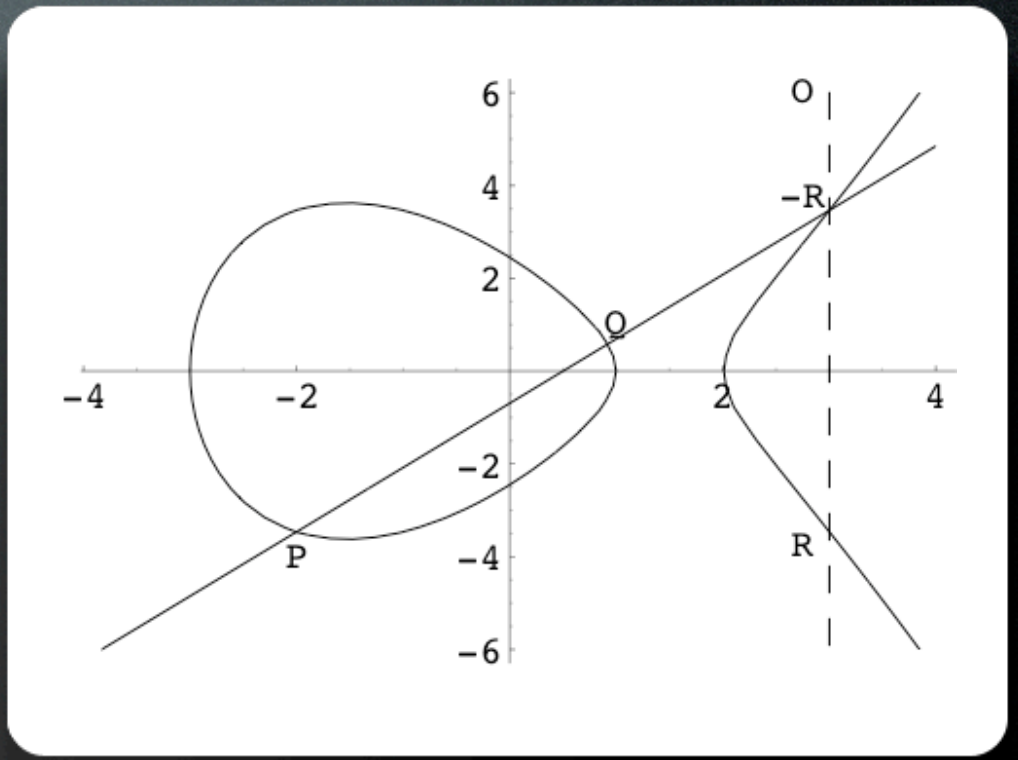


# What this will not be about...

- ... a study of security and cryptography in OpenBSD...
- ... I know too little to make any serious comment on the subject

# What this will not be about

- curves suitable for identity based cryptography
- algebraic attacks on AES
- breaks on SHA-1, SHA-0, MD5



# What this will not be about

- curves suitable for identity based cryptography
- algebraic attacks on AES
- breaks on SHA-1, SHA-0, MD5

# What this will be about

- A light chat regarding the security paradigm and state of situation, from the academia to software developers and users
- WARNING... I am at the most abstract corner you can think of

# Things that get me thinking

- “So say I want a good security software - what should I choose / where should I look at?”
- “How do I know that it is safe to use my credit card with site X?”
- “... does that mean it’s not safe? Have they broken cryptography?”

# The Babel Tower

The researchers

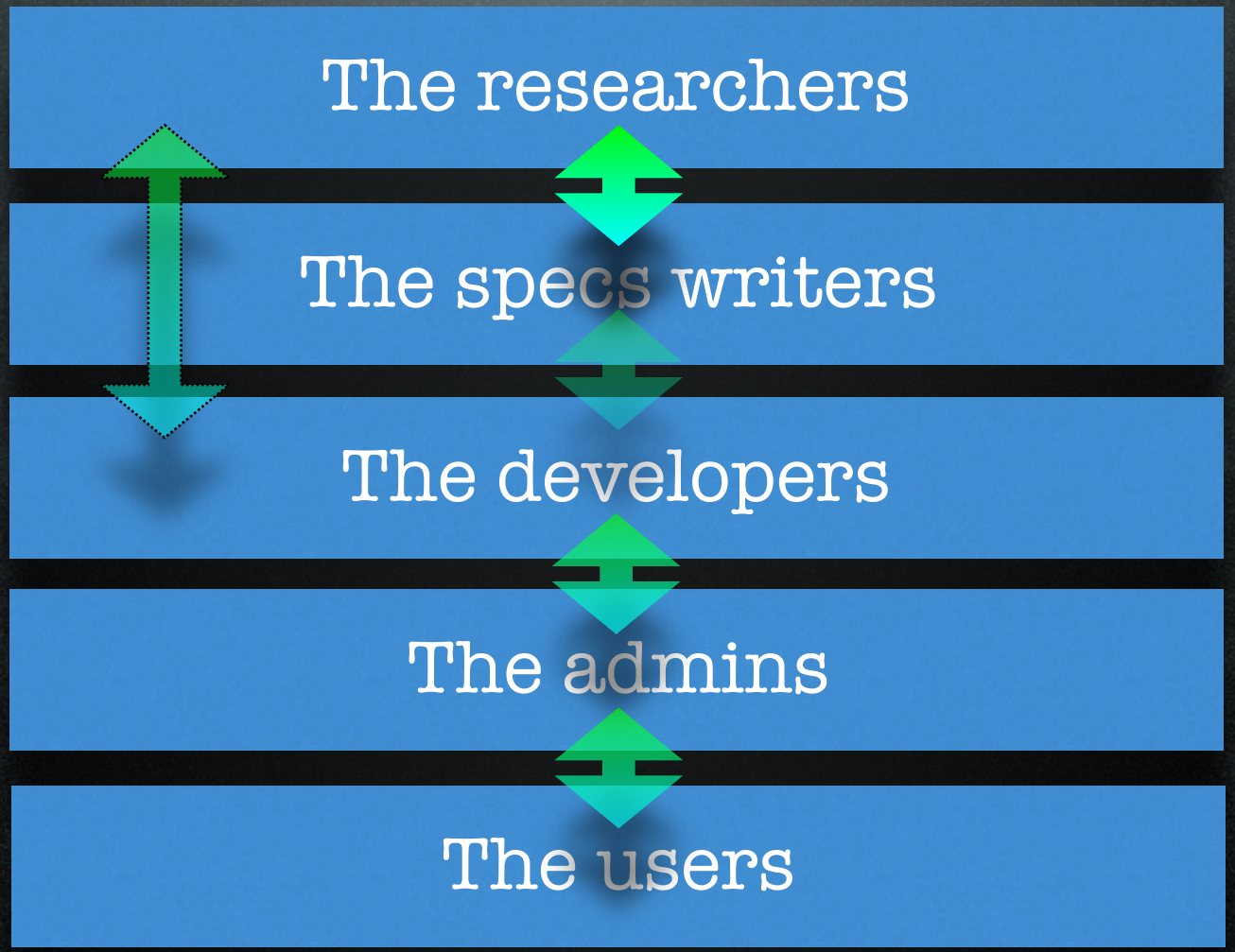
The specs writers

The developers

The admins

The users

# The Babel Tower



# Things slip through the creases

- Phong Nguyen's look at GPG in 2003 revealed compromised ElGamal keys (when sign+encrypt was used)
- Arnold Yau and Kenny Patterson's attacks on IPsec via lack of authentication/integrity protection

# Are attacks realistic?

- For many it's debatable. Cryptographers look at the worst case scenario... take "chosen ciphertext attacks", for example
- And then comes efficiency, flexibility, backward-compatibility
- ... confusing warnings...
- ... still, Murphy's law

# Good things about open systems

- audit, peer-reviews, source code availability...
- does not necessarily mean that it is
- ... and more important still, by the “experts”

# the present and future

- Information security is turning more and more into management that IT: protocols, directives
- ... which are not always clear (take IPsec series of RFCs, for example)
- Schneier's recent article speaks of a shift from apps to services

Questions?
More importantly,
discussion...