Open Source Security

Is Open Source software more or less secure than proprietary equivalents?

Peter SJF Bance CEng MBCS CITP

Technical Director, Rhye Internet Solutions Limited
CESG and BCS Listed Security Adviser

peter.bance@rhyeinternet.com

The Arguments

- Secure coding practices
- Code audit / review
- Developer motivation / integrity
- Vendor liability / commitment
- Distribution mechanisms
- Vulnerability alerting / patching
- Ownership, updates and maintenance
- Security through secrecy (obfuscation)

So who is right?

Clearly, this is a grey area…

The Open/Closed source decision will need to be made based on your situation, taking into account such factors as:

- Corporate policy
- Reliability requirements
- Maintainability
- Security requirements
- In-house knowledge and skills

The question:

Is Open Source software more or less secure than proprietary equivalents?

The answer?

This will depend on your specific situation.

We need a different approach…

Risk Assessment

1. Information Assets (value/impact) – Confidentiality, Integrity & Availability
2. Business Domains (interconnectivity)
3. Attack groups
4. Capability / Motivation ≡ Threat
5. Compromise Paths
6. Opportunity / Deterrence ≡ Likelihood

→ *Is the resultant risk acceptable?*

Only by assessing the risks associated with each individual requirement can we decide whether the “right” solution involves Open or Closed Source products.

Summary

There is no simple answer to the question of whether Open or Closed Source is more secure, and it may be dangerous to generalise.

It is therefore wise to approach this issue on a per-project basis, founded on a realistic and pragmatic assessment of the business, technical and security risks involved.

Further Information

On Google (www.google.com):

- "open source" closed or proprietary
  - research
  - quantify
  - empirical

peter.bance@rhyeinternet.com