Making community decisions

in the absence of consensus

George Dunlap
XenProject Committer
thinking ahead
The Issue
XenProject Security Process

- A well-known place to report vulnerabilities
- A structured way of announcing vulnerabilities to users
- A pre-disclosure list
Pre-disclosure
XSA-7: Intel SYSRET
Discussion goals

• Find the best solution

• Do it in a way which everyone felt their voice was heard
ONE

Make sure you have a fall-back

in case consensus can’t be reached
Process isn’t necessary — until it is
ONE

Make sure you have a fall-back in case consensus can’t be reached
TWO
Have an online discussion but don’t stop there.
Online discussions are great for...

- Identifying important factors
- Clarifying thinking
- Exploring possible solutions
- Understanding implications, pros and cons of different options
Online discussion: Weaknesses

• Favor people who…
  • Like to argue
  • Are articulate, have a high command of English, or type quickly

• Sociological: Favor people who…
  • Feel like they’re in the “in” crowd
  • Think their opinion will be popular

• Hide silent agreement
Social factors and silent argument: Debian systemd discussion
Support for other init systems is recommended, but not mandatory

Packages may require specific init systems if maintainers decide

Packages may not (in general) require a specific init system

Further Discussion

General Resolution is not required

TWO

Have an online discussion

but don’t stop there.
THREE
Summarize the major positions and hold a five-point survey
Four options

• No pre-disclosure

• Pre disclosure to software providers only

• Pre disclosure to software providers and a small number of public cloud providers

• Pre disclosure to software providers most public cloud providers
Five-point survey

• Based on “Identify the Champion”

• For each option, ask people to rate it:
  • This is a great idea, and I would argue for it
  • I am happy with this idea, but I would not argue for it
  • I am not happy with this idea, but I would not argue against it
  • This is a terrible idea, and I would argue against it
  • No opinion
Further details

- “Other options / comments” box
- Anonymous or named?
  - Allow anonymous votes but say votes with a name attached would be given more weight
- Two-week survey window, announced publicly
Outcome

- **33** survey responses
- Only **4** anonymous votes
- Other **29** were a good mix:
  - Developers
  - Distributions
  - Both large and small cloud providers
FOUR

Look for the “center of gravity”
Things to look for

- **Good**: Total approval vs total opposition
- **Bad**: Polarized options, particularly divided by sub-group
- **Good**: Options that are opposed for opposite reasons
Software and all cloud providers

- This is a great idea
- Happy with this idea
- Not happy with this idea
- This is a terrible idea
- No opinion
Write up a concrete proposal
Recap

• Make sure you have a fall-back if consensus fails
• Have on online discussion, but don’t stop there
• Summarize the major options and run a five-point survey
• Analyze the data to find the “center of gravity”
• Make a concrete proposal based on the findings
Questions

Comments / criticism:
George Dunlap <george.dunlap@citrix.com>

References:
XenProject Security Policy (including pre-disclosure list)
https://www.xenproject.org/security-policy.html
Identify the Champion
http://scg.unibe.ch/download/champion/