Dissenting Opinion

Stuart Staniford

Former and maybe future coauthor

Controversy

- I withdrew my name from paper during revision for this workshop
  - Couldn't agree with co-authors
  - Felt the damage estimate was being biased downwards without good reason
- Points of controversy
  - Irretrievable BIOS loss damage rates
  - Retrievable BIOS loss rate
  - Time to repair lost BIOS's

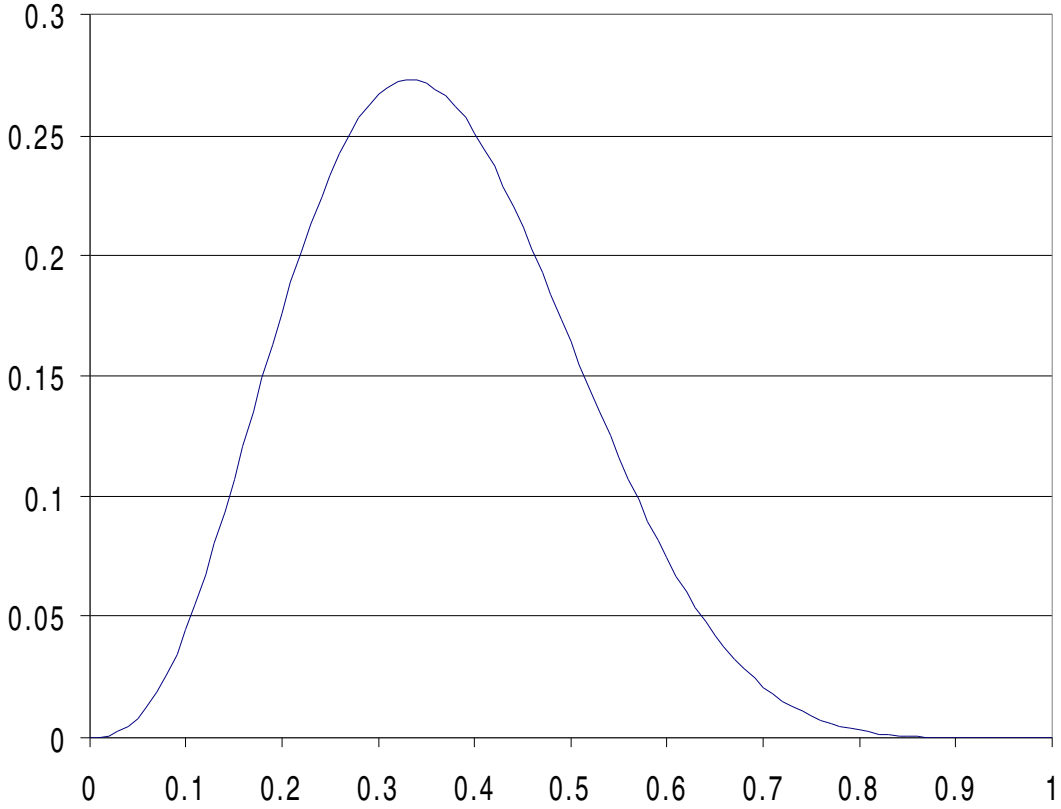
Irretrievably damaged BIOS rate

We measured 3/9

The $50b number assumes 0.1

Here's the likelihood distribution:

Justification: "being conservative"



Retrievably Damaged BIOS rate

Every system surveyed can be reflashed from software

Won't boot without opening the box

6/9 there's an onboard recovery procedure

$50b assumes attacker doesn't bother with 6/9 – inconsistent with premise/title

I assume these systems take 1 += 0.5 weeks to get operational again

- Sysads have to open every box
- 1 sysad per 100 or 1000 systems – usually only touch a small fraction each week
- Procedure unfamiliar

My estimate

Taking all the above into consideration

I get for total damage

- using same underlying linear direct model

$140b (factor of 2 error)

- Error is random error only
- Systematic errors are important here

This analysis is very flawed

- Assume all computers are equally important to economy
  - **Clearly** wrong (must be more Zipf like)
  - Use salary distribution?
  - Computers will move to highest use in crisis (but not instantly)
- Neglect indirect effects
  - Organization A loses additional $$ because B is down
  - Probably a huge effect
- Ignore revenue delay vs loss issues
  - To what extent is lost value-creation made up later in a burst?
- Ignore effects on market/consumer psychology
- “Engineering judgements” in place of surveys
  - This is at least a more-or-less random error, others are systematic
- But we should at least be flawed in an unbiased way!