CSE P 590TU: White Paper Project Proposal
Tony Chan (UW), Kevin Yu (UW), Andrew Cencini (UW)
November, 2005

Software Vulnerabilities: Full-, Responsible- and Non-Disclosure

Abstract

When a software vulnerability is discovered by a third party, the complex question of who, what and when to tell about such a vulnerability arises. Information about software vulnerabilities, when released broadly, can compel software vendors into action to quickly produce a fix for such flaws; however, this same information can amplify risks to software users, and empower those with bad intentions to exploit vulnerabilities before they can be patched. This paper provides an analysis of the current state of affairs in the world of software vulnerabilities, various techniques for disclosing these vulnerabilities, and the costs, benefits and risks associated with each approach.

Paper Structure

The paper will be structured as follows:

Introduction
Software Vulnerabilities: Actual / Possible Losses Due to Exploitation
- Describe the threat of software vulnerabilities, as well as possible losses in the event of an attack. In this case, frame of reference will be the historical record of actual attacks, as well as hypothetical examples built off of existing and possible future attack vectors.
  - The main thrust will be to provide an overview and analysis of major events (Slammer, Code Red, etc.) across multiple categories (not just worms, not just cases of full disclosure, etc.).
- This section will be used for two reasons – one is to introduce the threat field in terms of cost; the other is to provide a scope and set of examples for later sections to work from
  - For example, discussion of the vulnerability, disclosure and exploit that led to the Slammer worm, and the costs (actual and potential) incurred as part of such an incident.

Types of Disclosure: Overview
- Provide a definition of full disclosure, responsible disclosure, non-disclosure, and any other variants that may exist.
- This section will be used to provide a canonical definition (for the purposes of this paper) of each method of disclosure, as well as a mapping between incidents/disclosures in the previous section to the disclosure types discussed here.

Practices, Policies and Proposals
- Provide an overview of the various existing (and proposed) practices and policies for disclosing vulnerabilities.
- This section will be used as glue between the types of disclosure/examples of each type and the next section where we cover the risks, rewards and costs. By the next section, readers should have a good idea of the threat, risks, costs, and examples of incidents and real-world examples of ways in which vulnerabilities may be reported.

Types of Disclosure: Risks, Rewards and Costs
- This will be the meatiest section of the paper. Here we will discuss the various methods of disclosure and historical examples against the backdrop of the previous section on possible

losses. For example, for various scenarios what are the risks, rewards and costs of full-disclosure?

- By the end of this section, it should be clear to readers how various actual and hypothetical examples play out as regards different disclosure techniques. The reader should be able to form an educated opinion about when various disclosure techniques are appropriate and the reader should have a working knowledge of what the various risks, benefits and costs are to the various disclosure techniques for a set of high-level scenarios.

Conclusion

Division of Work

Work will be divided as follows (exact people to carry out the work are TBD at the current moment).

- One person will be chosen to act as the paper coordinator (in addition to contributing on other work being done). This involves:
  - Collecting various sections from section coordinators
  - Assembling sections into final paper
  - Performing initial editing to ensure smoothness/continuity of style and content across sections
  - Solicit feedback on the assembled paper, and make edits as needed.
  - Submit final paper prior to due date.

- Each high-level section (specified above) will have a section coordinator who will:
  - write some (presumably the bulk) of the content
  - collect any content for subsections that are delegated out (For example, in the Actual/Possible losses section, the coordinator may write about several of the examples to be covered there, but other team members may also contribute examples that will be folded in by the coordinator)
  - submit the final draft of the section to the paper coordinator
- Each section will also have a section reviewer (different from the section coordinator) who will:
  - review the compiled section draft from the section coordinator
  - make any edits/changes as needed
- The team should be able to assign section coordinators and reviewers in fairly short order.

- In addition:
  - One team member (not the paper coordinator) will be assigned to write the introduction.
  - One team member (not the paper coordinator) will be assigned to write the conclusion.