

Vulnerabilities and Adversaries in Security

Rick Wash

`rwash@citi.umich.edu`

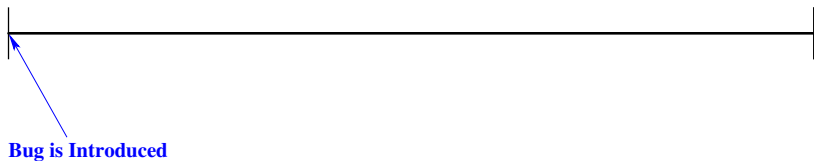
CITI - University of Michigan

October 19, 2004

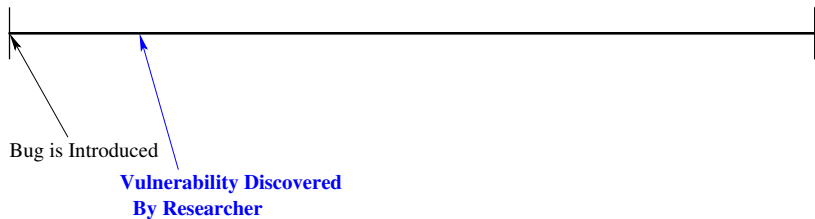
Overview

- ▶ Understanding Vulnerabilities
- ▶ Understanding Adversaries

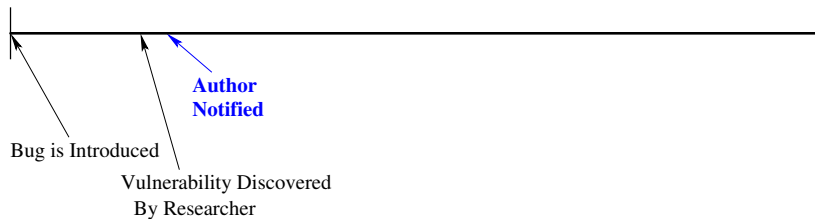
Vulnerability Timeline



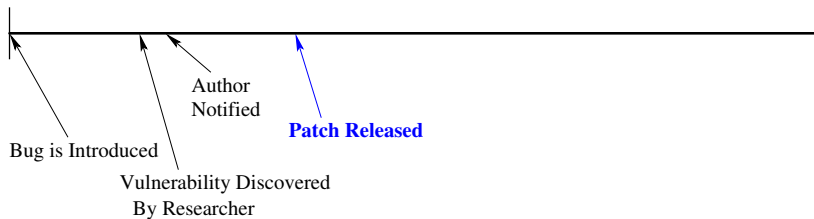
Vulnerability Timeline



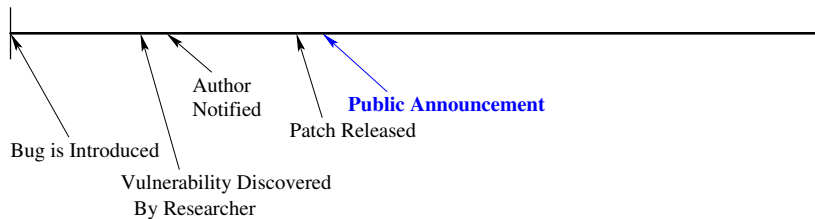
Vulnerability Timeline



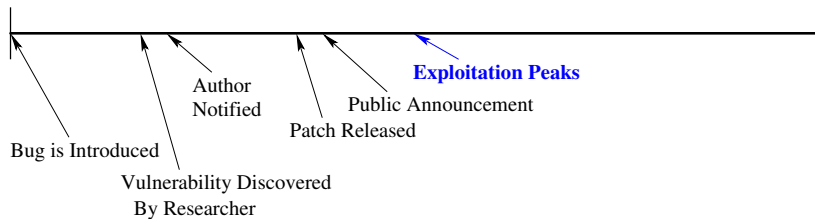
Vulnerability Timeline



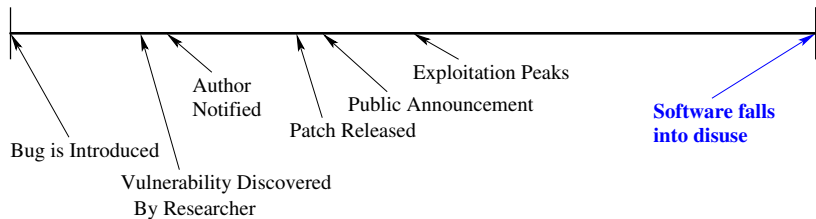
Vulnerability Timeline



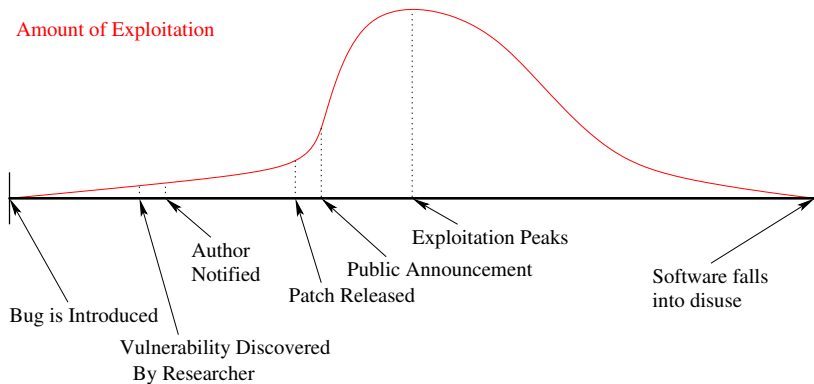
Vulnerability Timeline



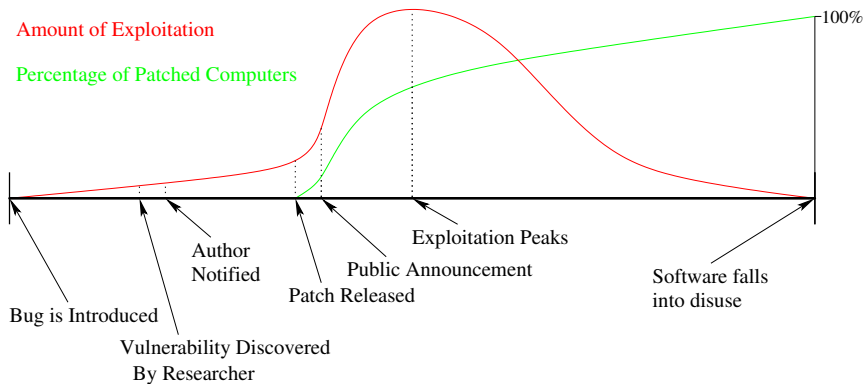
Vulnerability Timeline



Vulnerability Timeline



Vulnerability Timeline



Decisions, Decisions...

Should you disclose vulnerability information? (If so, who should?)

- ▶ Public disclosure helps attackers
- ▶ Public disclosure aids defenders
 - ▶ Understanding the quality and security of software
 - ▶ Research and teaching material
 - ▶ Public Awareness
- ▶ Companies reputation harmed by public disclosure
- ▶ Increase in quality of software
- ▶ Increase in security of software

Decisions, Decisions...

Should you disclose vulnerability information? (If so, who should?)

- ▶ Public disclosure helps attackers
- ▶ Public disclosure aids defenders
 - ▶ Understanding the quality and security of software
 - ▶ Research and teaching material
 - ▶ Public Awareness
- ▶ Companies reputation harmed by public disclosure
- ▶ Increase in quality of software
 - ▶ Rescorla '04 → Not really

Decisions, Decisions...

Should you disclose vulnerability information? (If so, who should?)

- ▶ Public disclosure helps attackers
- ▶ Public disclosure aids defenders
 - ▶ Understanding the quality and security of software
 - ▶ Research and teaching material
 - ▶ Public Awareness
- ▶ Companies reputation harmed by public disclosure
- ▶ Increase in quality of software
 - ▶ Rescorla '04 → Not really

Decisions, Decisions...

Should you disclose vulnerability information? (If so, who should?)

- ▶ Public disclosure helps attackers
- ▶ Public disclosure aids defenders
 - ▶ Understanding the quality and security of software
 - ▶ Research and teaching material
 - ▶ Public Awareness
- ▶ Companies reputation harmed by public disclosure
- ▶ Increase in quality of software
 - ▶ Rescorla '04 → Not really

Research Overview

Can we understand the tradeoffs and incentives in vulnerability disclosure and devise a mechanism that provides better disclosure properties?

- ▶ Identify the important properties of the system
- ▶ Design a model of the existing system
- ▶ Identify mechanisms and analyze their properties

Adversaries and Rational Agents

Adversaries

- ▶ Goals opposite to Defenders
- ▶ Extremely powerful and knowledgeable
- ▶ Focus on making certain actions impossible
- ▶ All or Nothing

Rational Agents

- ▶ Self-interested
- ▶ Bound by resources, *other interests*
- ▶ Focus on causing agents to act in certain ways, even though other actions are possible
- ▶ Mixed strategies, interior solutions

Adversaries and Rational Agents

Adversaries

- ▶ Goals opposite to Defenders
- ▶ Extremely powerful and knowledgeable
- ▶ Focus on making certain actions impossible
- ▶ All or Nothing

Rational Agents

- ▶ Self-interested
- ▶ Bound by resources, *other interests*
- ▶ Focus on causing agents to act in certain ways, even though other actions are possible
- ▶ Mixed strategies, interior solutions

Adversaries and Rational Agents

Adversaries

- ▶ Goals opposite to Defenders
- ▶ Extremely powerful and knowledgeable
- ▶ Focus on making certain actions impossible
- ▶ All or Nothing

Rational Agents

- ▶ Self-interested
- ▶ Bound by resources, *other interests*
- ▶ Focus on causing agents to act in certain ways, even though other actions are possible
- ▶ Mixed strategies, interior solutions

Adversaries and Rational Agents

Adversaries

- ▶ Goals opposite to Defenders
- ▶ Extremely powerful and knowledgeable
- ▶ Focus on making certain actions impossible
- ▶ All or Nothing

Rational Agents

- ▶ Self-interested
- ▶ Bound by resources, *other interests*
- ▶ Focus on causing agents to act in certain ways, even though other actions are possible
- ▶ Mixed strategies, interior solutions

Existing Rationality in Security

- ▶ Resource bounds in cryptography, spam, academic security
 - ▶ Well-defined bounds of capabilities
 - ▶ Assumes adversaries will use all resources at their disposal
 - ▶ Typically tries to find functions that require unrealistic resources
- ▶ Cost/Benefit analysis of security
 - ▶ Buzzword
 - ▶ "Know your enemy" – government or dorm-room hacker?
 - ▶ Don't spend too much to defend against miscreants
 - ▶ Heuristic, not exact

Existing Rationality in Security

- ▶ Resource bounds in cryptography, spam, academic security
 - ▶ Well-defined bounds of capabilities
 - ▶ Assumes adversaries will use all resources at their disposal
 - ▶ Typically tries to find functions that require unrealistic resources
- ▶ Cost/Benefit analysis of security
 - ▶ Buzzword
 - ▶ “Know your enemy” – government or dorm-room hacker?
 - ▶ Don’t spend too much to defend against miscreants
 - ▶ Heuristic, not exact

Research Overview

When and how can a different model of adversaries lead to useful insights in security? Are adversaries rational?

- ▶ Model and understand the incentive structure of security
 - ▶ Why are the attackers attacking?
 - ▶ Why are the defenders defending?
 - ▶ Remember hacking is just a means to an end
- ▶ Understand the adversarial model in light of the incentive structure
- ▶ Classify when and how this model can be used in security decisions