

Detecting past intrusions

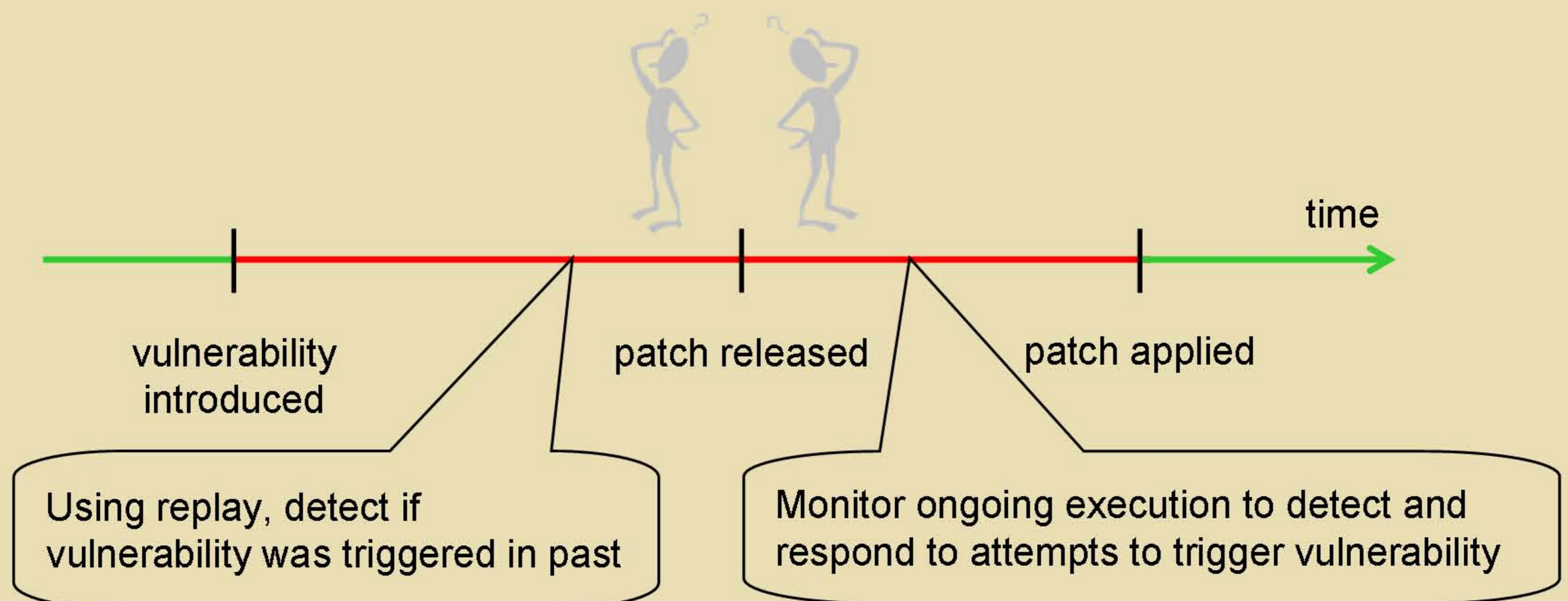
Peter M. Chen, University of Michigan

<http://www.eecs.umich.edu/virtual>

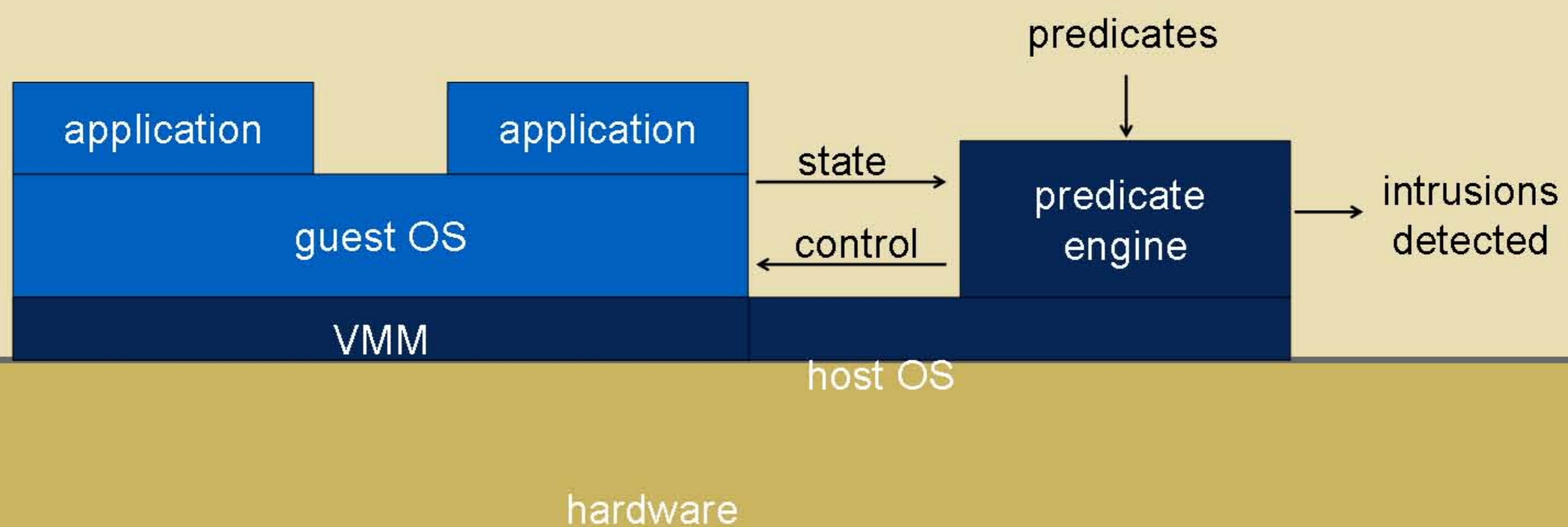


What to do when (not if) you find out you've been running buggy software?

Insight: Patch writer knows exactly what conditions during program execution indicate triggering of vulnerability. Use this knowledge to write exploit-generic, vulnerability-specific predicates that check these conditions.



IntroVirt structure



•Techniques

- Vulnerability-specific predicates
- Virtual-machine replay
- Virtual-machine introspection
- Calling guest functions
- Checkpoint / restore

•Benefits

- No perturbations; safe for production systems
- Accurate detection of intrusions
- Easy writing of predicates
- Low overhead