Deception and Consistency

Matt Bishop
Vicentiu Neagoe

Contact Information

Matt Bishop
Department of Computer Science
University of California at Davis
1 Shields Ave.
Davis, CA 95616-8562

phone: (530) 752-8060
email: bishop@cs.ucdavis.edu
www: http://seclab.cs.ucdavis.edu/~bishop

Goals

- Create confusion in attacker
  - Induce delay in decision making
- Waste their time
- Make them go away on their own
- Distract them towards a different path
  - Stir up curiosity about bizarre behavior
- Blur the line between what is allowed and what is not allowed
- Trigger alerts and heavy analysis

Assumptions

- Previous work assumed consistency is critical to successful defense
  - Attacker gains the advantage is deception is detected
  - Inconsistency will expose presence of deception
- So what?
  - If attacker knows deception is used, they still must distinguish between what is deceptive and what is real

How to Do It

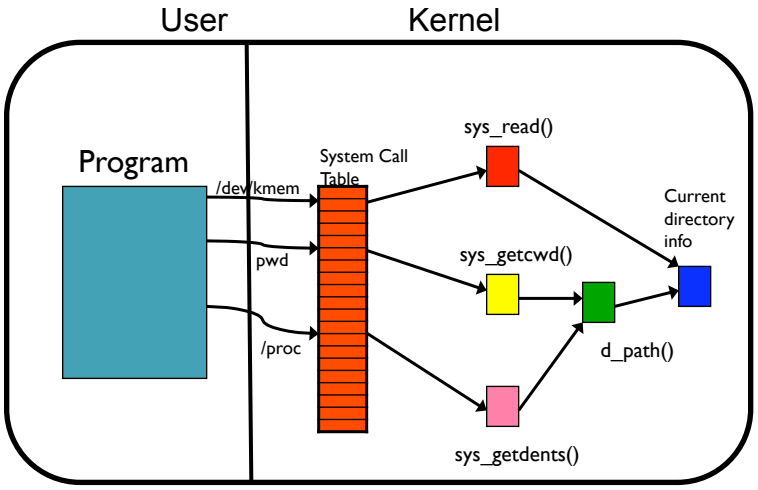
- Inconsistent deception easier to implement than consistent deception
  - Use regular deception techniques but don't worry about consistency
- Make the system behave unpredictably
  - May be malfunctioning
  - Undergoing modification
  - Defense response

Deception: File Deletion

Performed Action	Response	Response truthfulness	Verify response	Verify truthfulness	Consistent
No	Deleted	False	File exists	True	No
No	Deleted	False	File gone	False	Yes
No	Not Deleted	True	File exists	True	Yes
No	Not Deleted	True	File gone	False	No
Yes	Not Deleted	False	File exists	False	Yes
Yes	Not Deleted	False	File gone	True	No
Yes	Deleted	True	File exists	False	No
Yes	Deleted	True	File gone	True	Yes

real system	consistent deception

Consistent Deception



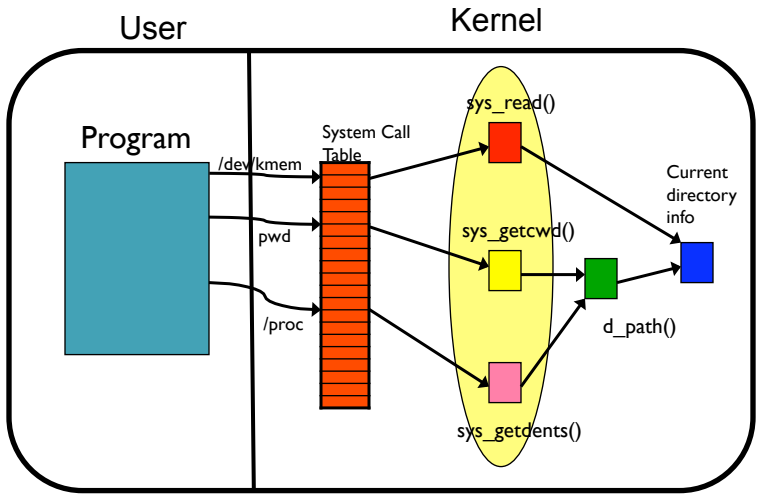
Types of Inconsistency

- Vertical – separate paths return different answers
- Horizontal – same path returns different answer

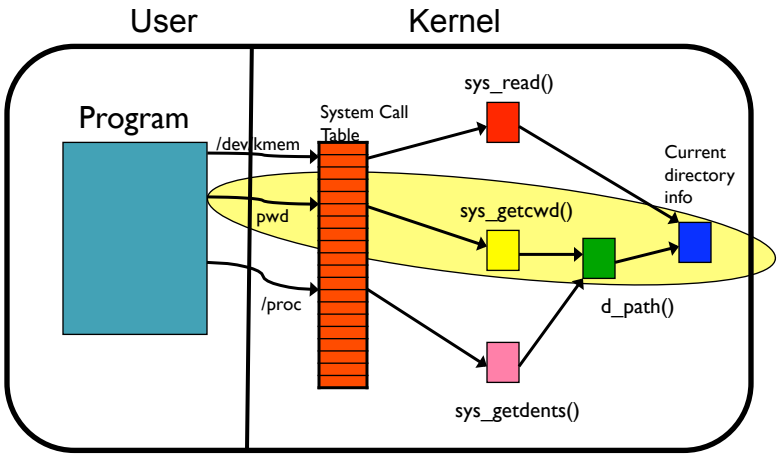
Example

- Process needs to determine its current working directory
  - Relative path names interpreted with respect to that directory
  - Is current working directory the real one or one created as part of a deception?
    - In the latter case, the system wants to lie about the name

Vertical Inconsistency



Horizontal Inconsistency



Additional Notes

- Inconsistency does *not* mean deception
  - System could be flaky or malfunctioning
- If attacker believes deception is being used, may try to evaluate sources
  - The richer semantically a component is, the harder to make it appear consistent
- Many types of inconsistency
  - Data: results vary
  - Semantics: expression of results vary

Project Goals

- Given a file that an attacker wants access to, determine paths through kernel that can be used to obtain information or access
  - Establish methodology to do this
- Add horizontal, vertical deception
- Evaluate how attacker can "break" this
  - How can attacker determine deception is being used?
  - How can attacker distinguish non-deceptive responses from deceptive responses?

References

- V. Neagoe and M. Bishop, "Inconsistency in Deception for Defense," *Proceedings of the New Security Paradigms Workshop* pp. 31–38 (Sep. 2006).
- D. Rogers, *Host-level Deception as a Defense against Insiders*, M.S. Thesis (2004)