What is Wild?

Sarah Gordon
IBM TJ Watson Research Center
Hawthorne, New York

Certification != Protection

- What is “ITW”?
- What is “Product Certification”?
- What are the problems with “ITW” based certifications?
- Future problems
- Some solutions

In the Wild (ITW)

- History of ITW
  - Wild vs. Zoo
- User reports
- Vendor reports
- Joe Wells' and The Wildlist
- Media reports
  - Hare

Anti-virus product Certification

- Purpose of Certification
- Certification Bodies
- Certification and your Organization

Real Life

- WordMacro.Concept
- Reported, analysed July 1995
- Not on WildList until September 1995
- Not included in certification testing compliance until November 1995

Generic problems with WildList based certification schemes

- Lag
- Reporting bias
- Naming
- Hot Zones

NCSA Certification

- 100% of The WildList
- 90% of zoo viruses
- Technical and administrative issues

Secure Computing Certification

- 100% of The Wildlist
- No zoo testing
- Technical issues

ITSEC Certification

- Complex criteria
- 100% WildList
- 90% Zoo
- Threat-type assessment
- Measurement of Threat Tracking

Certification != Protection

- No current certification is perfect
- Administrative, technical, ethical issues
- The WildList is still best measure of viruses spreading in the wild
- Perfect Test Criteria

The future

- New viral epidemiological model
  - Macro viruses
- New protection model
  - Immune System model
- New challenges for certification
  - Resources, technical expertise, administrative concerns

Solutions

- Know what is being certified.
- Know how it is certified.
- Understand the limitations of the certification.

- Don’t rely on certification alone.
- Report virus incidents to vendors.
- Read technical publications