Lecture 19: Firewalls and Intrusion Detection

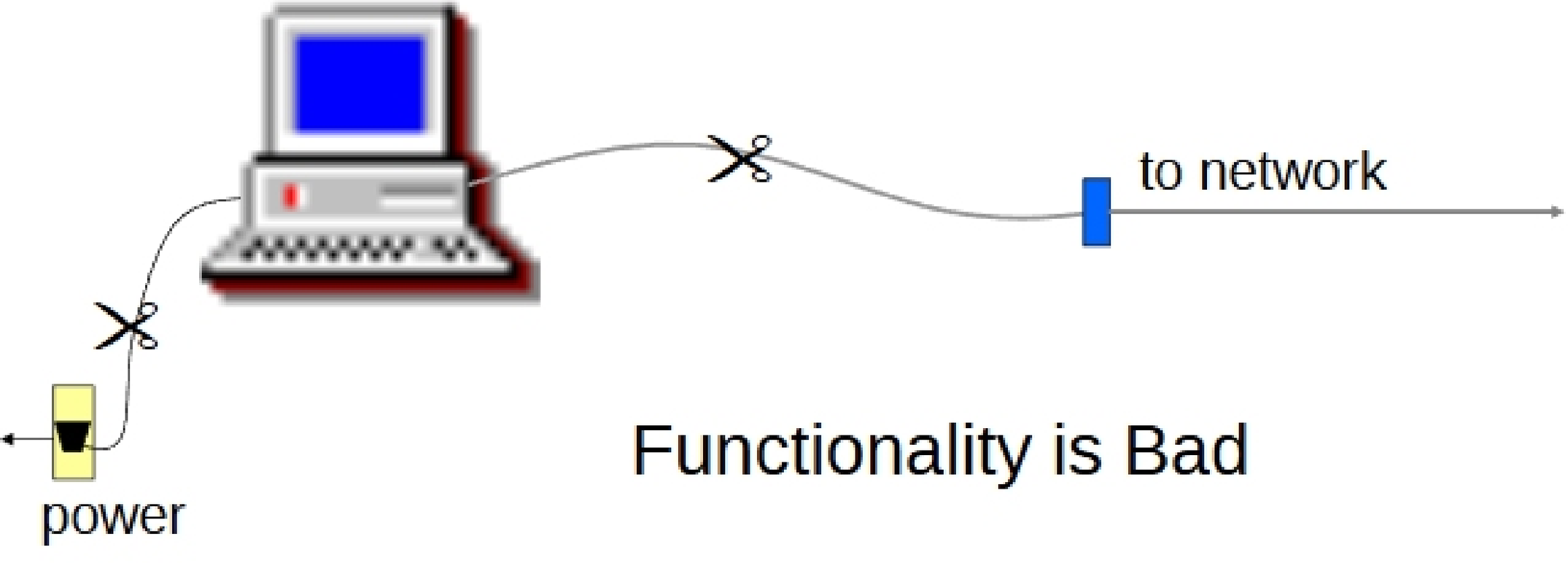
CS588: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/~evans

Malcode Defenses

1. Prevent malcode from running
   - ✓ Virus scanners – recognize known malcode
   - ➢ **Firewalls – drop incoming packets**
   - ✓ Code signing (only run code from trusted sources)
   - ✓ Education – make users smarter
2. Limit damage it can do
   - ✓ Sandbox ("Playpen") – run malcode in protected virtual machine
   - ✓ Reference monitors – enforce policy on execution
   - ➢ **Intrusion Detection**, System maintenance
3. Discourage attackers
   - ▪ Legal – pass laws to penalize attackers

The Best Firewall



Functionality is Bad