

# CONTAINMENT USING VIRTUALIZATION

CS6410

Ken Birman

# Context



- Dramatic growth in Internet worms, viruses, DDoS
- Research community challenged to find ways to somehow respond to this trend
- Today: Two major papers in this area (and two more as extra readings)
  - ▣ **Potemkin: A “farm” to lure viruses and capture them**
  - ▣ **Vigilante: Takes the next step and blocks them**
  - ▣ Asbestos: Taint tracking: Avoiding information leaks
  - ▣ Selective rollback: Back out of contaminated state

# We'll use the authors' slide sets



- Potemkin slides from the SOSP talk by Geoff Voelker, one of the developers of the system
- Vigilante slides from a talk originally by Manuel Costa, lead developer of Vigilante system, then revised by Mahesh Balakrishnan for CS6410

# Discussion questions



- Given that one has captured a virus, what then?
- Vigilante seeks to block viruses. Could an attacker twist this capability and use it to attack legitimate traffic?
- If we can protect data centers better than our personal machines, does this suggest that everything that matters should shift into the cloud?