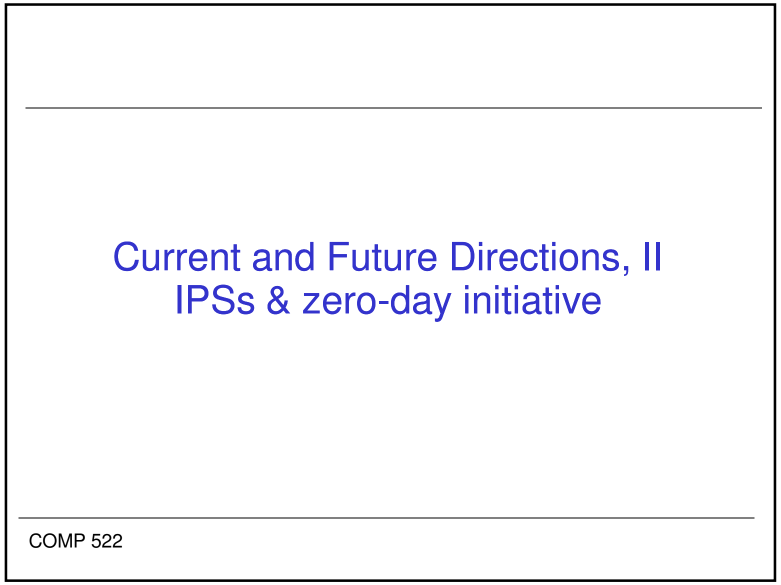
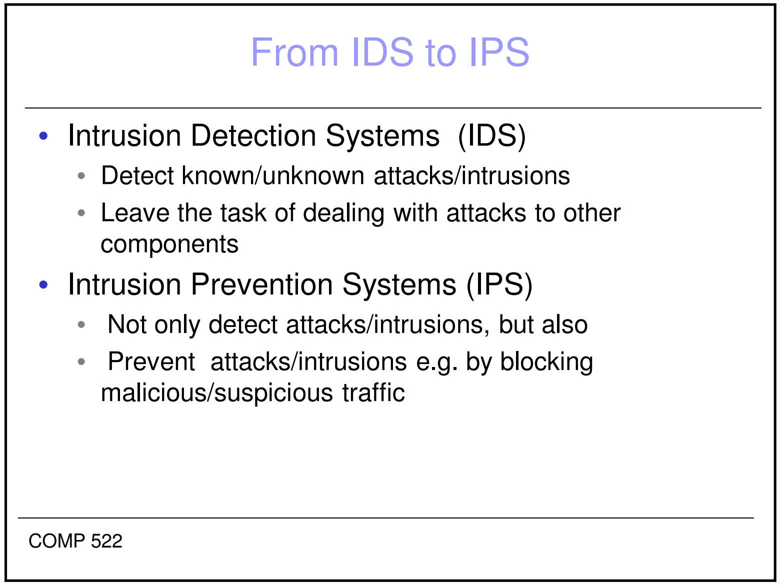
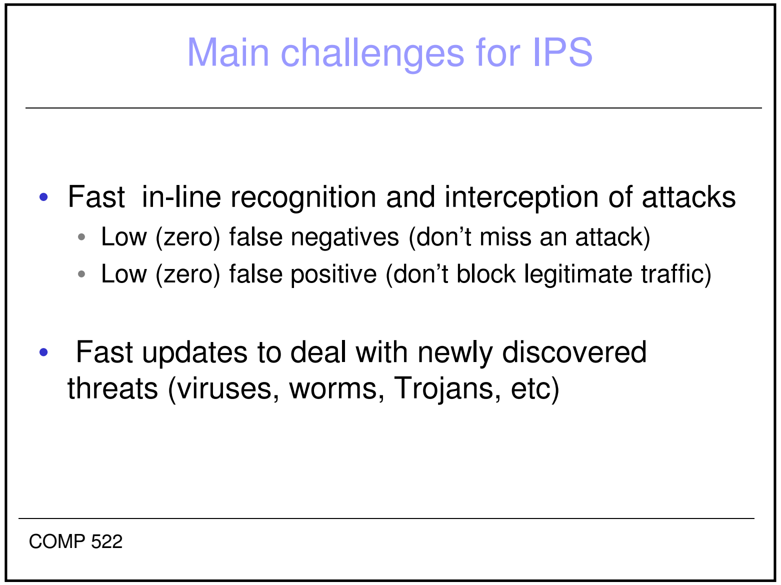


Current and Future Directions, II
IPSs & zero-day initiative



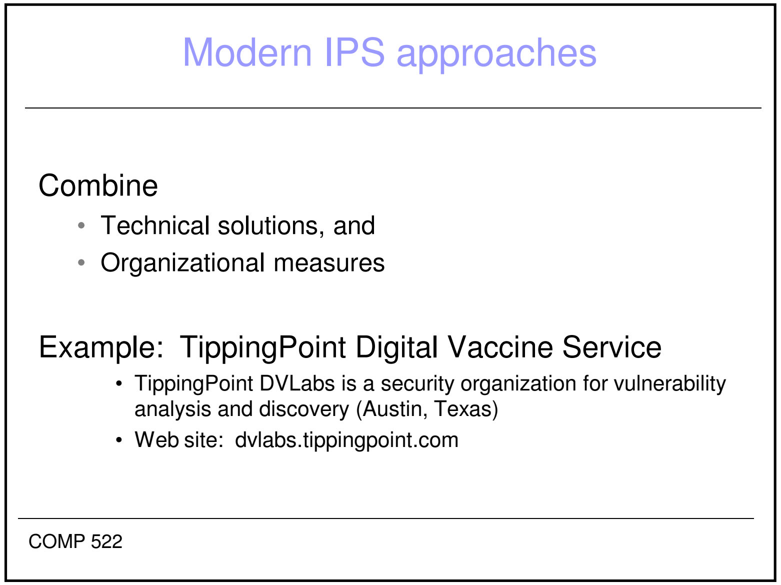
From IDS to IPS

- Intrusion Detection Systems (IDS)
  - Detect known/unknown attacks/intrusions
  - Leave the task of dealing with attacks to other components
- Intrusion Prevention Systems (IPS)
  - Not only detect attacks/intrusions, but also
  - Prevent attacks/intrusions e.g. by blocking malicious/suspicious traffic



Main challenges for IPS

- Fast in-line recognition and interception of attacks
  - Low (zero) false negatives (don't miss an attack)
  - Low (zero) false positive (don't block legitimate traffic)
- Fast updates to deal with newly discovered threats (viruses, worms, Trojans, etc)



Modern IPS approaches

Combine

- Technical solutions, and
- Organizational measures

Example: TippingPoint Digital Vaccine Service

- TippingPoint DVLabs is a security organization for vulnerability analysis and discovery (Austin, Texas)
- Web site: dvlabs.tippingpoint.com

Main focus

TippingPoint IPS implements

- high precision **vulnerability** filters:
    - filter not only particular known attacks, but also all attacks using a particular vulnerability;
- signature filters;
- protocol anomaly filters;
- traffic anomaly filters

Information gathering

Zero Day Initiative:

- TippingPoint receives vulnerability research from more than 600 researchers worldwide;
- If you discovered a vulnerability of some software you may register with them and submit it and, if confirmed, you may get paid;
- Filter for the new vulnerability is prepared, tested and released often before it is publicly known
- See details at www.zerodayinitiative.com