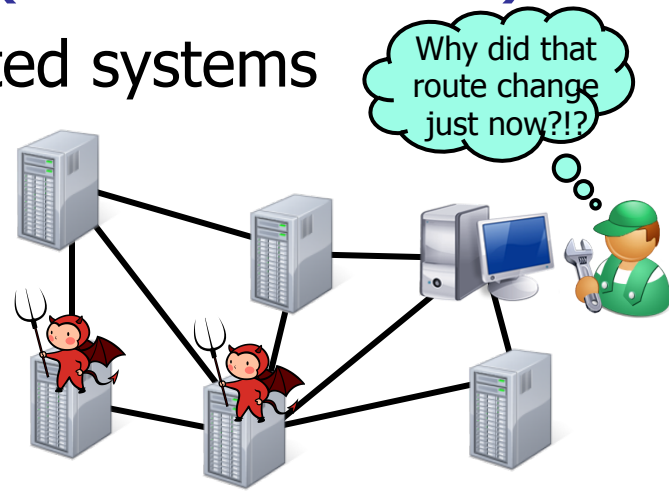
Secure Network Provenance (CNS-1065130)

- Goal: Secure forensics for distributed systems
  - Systems should be able to correctly answer questions about their state, even if they are partially compromised



- Approach: Use provenance
  - Inspired by a concept from databases
- Some key results:
  - SNP algorithm + reference implementation [SOSP'11]
  - Several generalizations of provenance [SIGCOMM'14,HotNets'15]
  - Techniques for secure provenance storage [VLDB'13]
  - Query language for analyzing provenance [TaPP'12]
  - Improved readability for forensic data [SIGCOMM'16]
  - A new way to detect covert timing channels [OSDI'14]
  - Ways to automatically respond to intrusions [NSDI'17]
  - Techniques for privacy-preserving forensics [SIGCOMM'12]