CSci 8271
Security and Privacy in Computing
Day 15: EOS smart contract vulnerabilities

Stephen McCamant
University of Minnesota

Cryptocurrencies and smart contracts

- "Smart contracts" are stand-alone programs whose behavior is moving money or other assets
- Distributed currencies are a natural environment
- Limited support in Bitcoin, mainstay of many successor systems

Smart contract vulnerabilities

- Common setup is a high risk: code is public, but can be hard to update
- Close-to-normal programming languages can be vulnerable if not used carefully
  - Required security check missing
  - Unexpected concurrency

WebAssembly and EOS libraries

- WebAssembly is a code format designed for portability and low overhead
  - Successor to Native Client and asm.js, but not web-specific
- EOS.IO smart contracts are WebAssembly with some specialized libraries
  - E.g. transaction passing, persistent storage
- Authors build a specialized symbolic execution tool

Vulnerability types and prevalence

- Specialized detection patterns over path condition
  - Allow optimizations like skipping irrelevant code
- Fake EOS: 282 unique vul'n
- Fake receipt: 2192 unique vul'n
- Rollback: 84 unique vul'n
- Missing permission check: 662 unique vul'n

Assessing practical vulnerability

- Checked for evidence of real attacks over historic transaction record
  - Heuristic and semi-automated, smaller scale
- 50 attackers, 34 victims, $1.7M in losses
- 27 attacks confirmed, with top 5 accounting for most losses