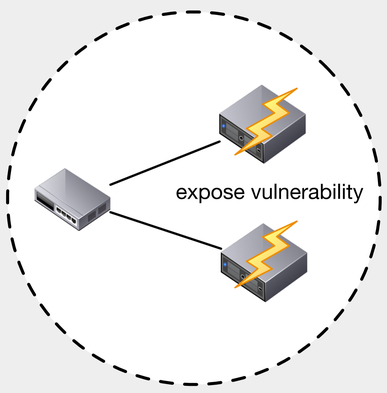
Making the Live Network the Honeypot

Michael Coughlin, Oliver Michel, Eric Keller, Adam J. Aviv

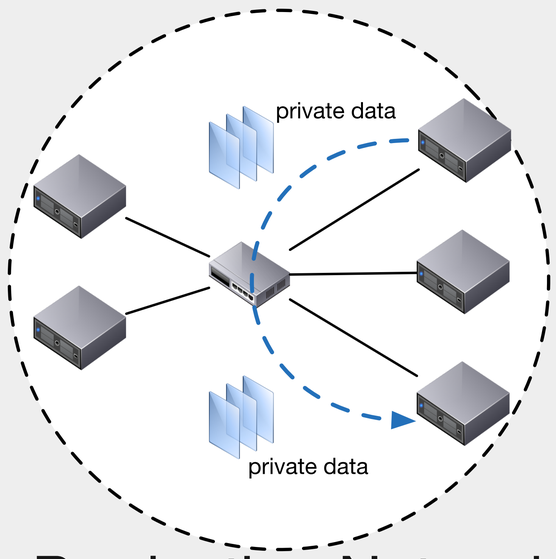
University of Colorado Boulder

Honeypots are not identical to production networks



Dedicated Honeypot

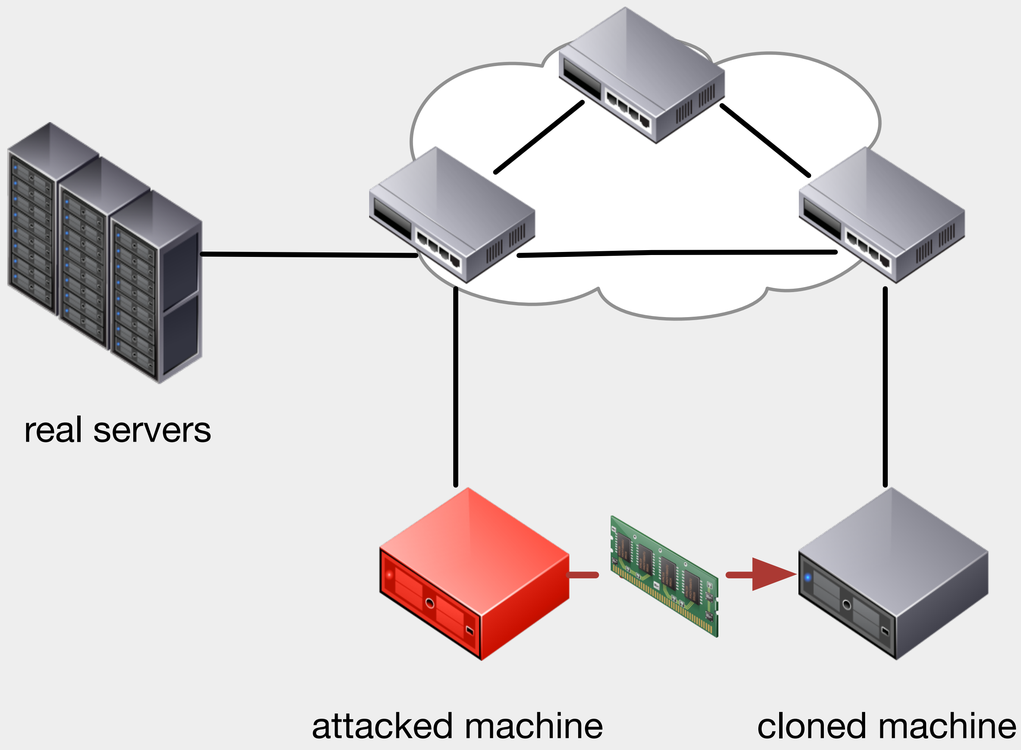
Same network?
Same applications?
Same data?



Production Network

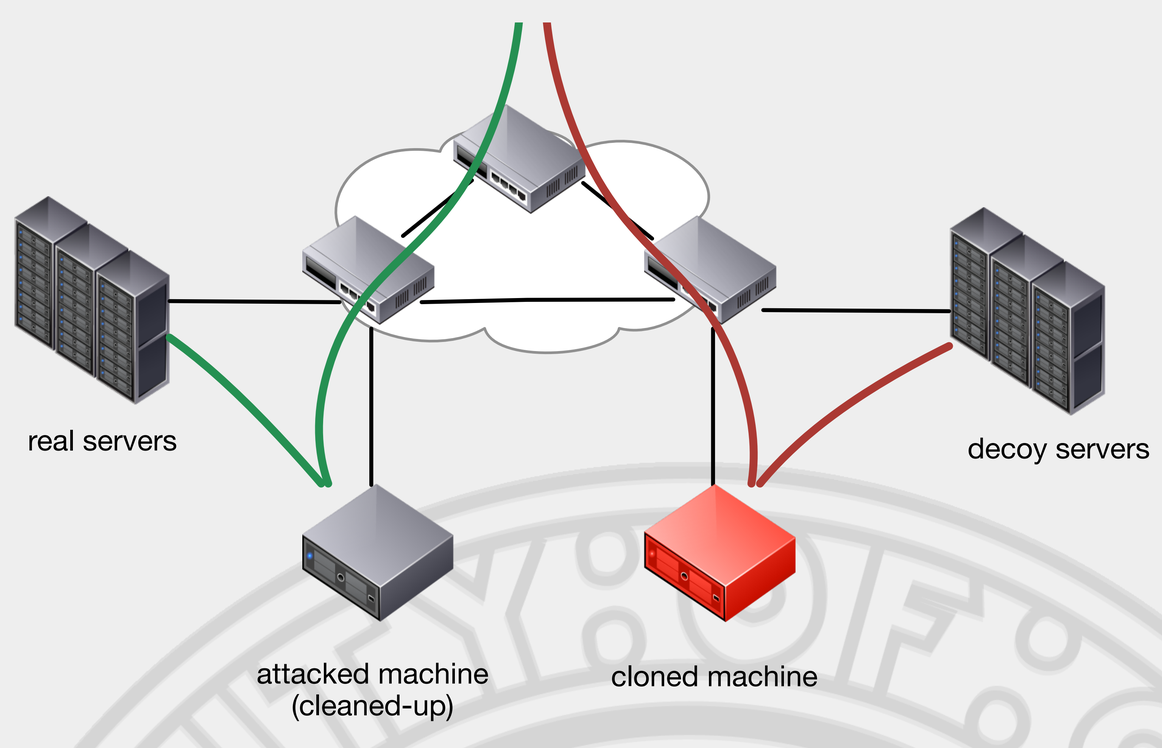
Can the production system be the honeypot?

Challenge 1: Isolate attacker



- Isolate attacker by cloning machine
- Clean-up original machine

Challenge 2: Allow clone to operate



- Create SDN 'active quarantine' of clone
- Utilize NAT to make both hosts appear as one

Challenge 3: Keep data confidential

- Feed misinformation to the attacker

Prototype

- SDN traffic dissection on top of Floodlight
- KVM offline migration

Future work

- Support live cloning
- SDN controller and hypervisor communication
- Covert operation of the system