**Making the Live Network the Honeypot**

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

**Honeypots are not identical to production networks**

Dedicated Honeypot

Production Network

---

**Challenge 1: Isolate attacker**

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

- attacker machine
- cloned machine

- real servers

---

**Challenge 2: Allow clone to operate**

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

- attacked machine (cleaned-up)
- cloned machine

- real servers
- decoy servers

---

**Challenge 3: Keep data confidential**

- Feed misinformation to the attacker

- ~/.ssh/id_rsa
- ~/.ssh/false_id_rsa

---

**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