

Choreographer: Moving Systems to Thwart Automated Attackers

Craig A. Shue, Ph.D.

Cyber Security Research Scientist

Oak Ridge National Laboratory

cshue@ornl.gov



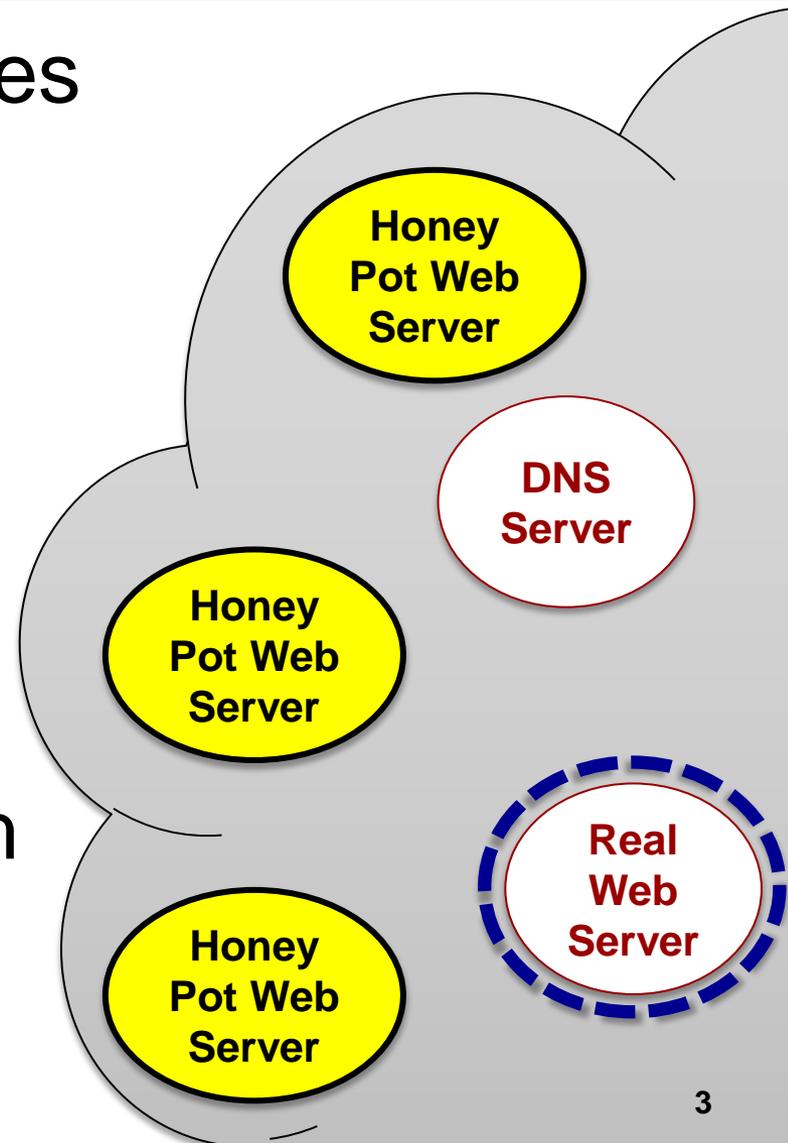
Customer Need

- Attacks on-going and damaging
 - Two stages: Reconnaissance followed by exploitation
- Servers exposed to the public
 - Needed for organization productivity
 - Organizations have many public servers
 - It is hard to protect them all
- Costs are high
 - Loss of sensitive information (\$5.5m per attack in 2011)
 - Reputation damage
 - Mission objective at risk



Our “Gold Nugget”

- Create network landmines for attackers
 - Called “Honey Pots”
- Provide safe path to clients that follow the rules
- Allows centralized control of who can reach organization servers



Approach

- Frequently change servers addresses
 - Hard for attacker to find them by guessing
 - Use mappings between public/private address
- DNS server gives correct address to legitimate users
 - A map to the right server on-demand
- DNS/Choreographer is a gate-keeper
 - Use ISP servers to determine history
- Malicious client/ISP network?
 - Redirect its traffic to a fake (honey pot) server

Benefits

- Attacker scanning effectiveness: 100% → 0.03%
- Detects and stops insider threats from malware
- Variable controls per server
 - “Keyed” DNS requests for sensitive machines
- Protects servers regardless of server application
- Allows examination of the diverted clients
 - Over 95% likely to be malicious users
- Policy decisions based on source network
 - Incentivizes networks to clean malicious clients
- Only minor infrastructure changes needed
- Supports IPv6 and DNSSEC

Competition

- Traditional firewalls can prevent access
 - Based on signatures
 - One hole lets everyone in
 - Allows or denies: no middle ground
- Dynamic and adaptive networks
 - Does not support migrating connections
- Our approach makes explicit decision
 - Before connection starts
 - During connection, if needed
 - Allows granular levels of trust

Risks

- Technical Performance
 - Creates access mapping in < 1 ms
 - DNS server refreshes in < 1 ms for small zones
 - Scaling for larger zones unknown
- Business Risks
 - Approach is straightforward
 - Lower barrier to entry for competitors
 - IT departments often reluctance to change
- Privacy concerns
 - Authorization for monitoring attackers?

Conclusion

- Essentially eliminates effectiveness of reconnaissance
 - From 100% to 0.03%
- Allows granular security controls
- Minimal changes to infrastructure
- Technology Readiness Level 6
- Looking for commercial partners