Rethinking Security in the Era of Cloud Computing

PIs: J. Aikat (UNC-CH); A. Akella (UW Madison); J. Chase (Duke); W. Enck (NC State); A. Juels (Cornell Tech); M. Reiter (UNC-CH); T. Ristenpart (Cornell Tech); V. Sekar (CMU); M. Swift (UW Madison)

http://silver.web.unc.edu

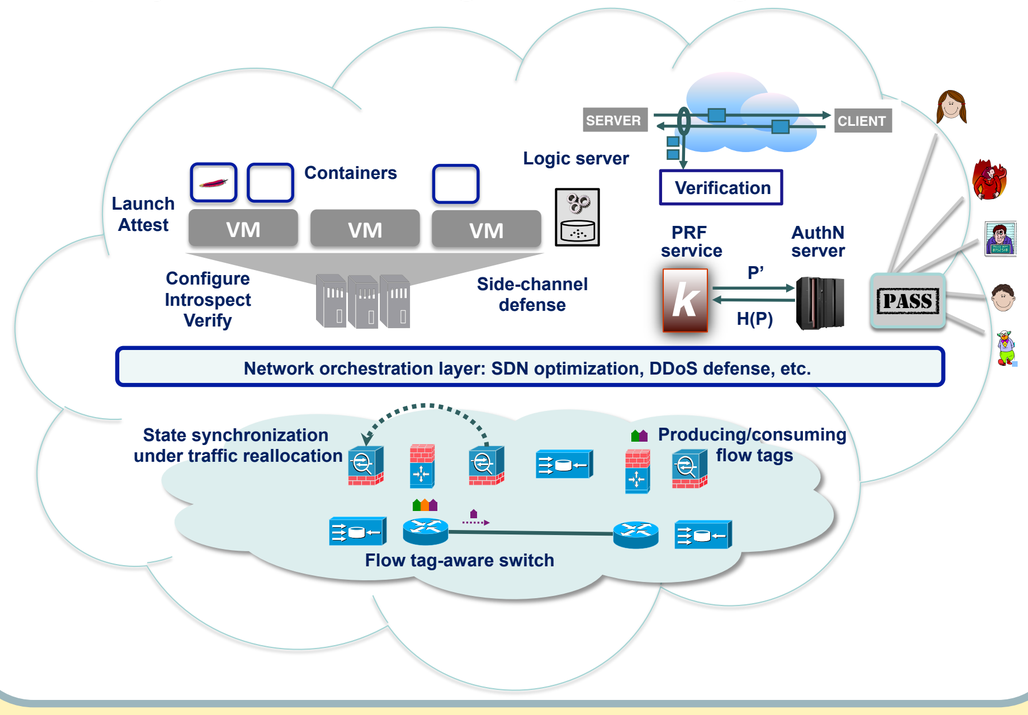
The Cloud as Trusted Partner

Cloud computing is a disruptive trend that offers a rare opportunity to deploy new approaches to computer security.

Key theme: Leveraging trust in cloud operators to address core security challenges for tenants

Cloud providers in a strategic position to support tenant security
- Deeper specialization
- Provider introspection
- A broad view of security-related information, across tenants
- Massive compute resources

Improving tenant security through operator deployed and managed technologies …



Approach

Leveraging clouds as trusted partners to improve security management of …
- *Clients* of tenant servers
- *Infrastructure* services outsourced by tenants
- Dependencies among tenants in the context of tenant *ecosystem*

Engaging with cloud operators, technology providers, tenants, and higher-education instructors
- Annual 3-day Cloud Security Curriculum Development Workshops
- Biennial Cloud Security Horizons Summits

Client thrust
- **Password management**: technologies to harden passwords and to provide password vaults using natural language encoders
- **DoS mitigation**: a cloud-based architecture for flexible and elastic DDoS defense
- **Client behavior verification**: cloud-resident verifiers to detect client misbehavior (and new exploits) through analysis of protocol traffic

Ecosystem thrust
- **Trust management**: a system to provide certificate linking and a scripting engine to produce/consume logical certs
- **Containment**: a service to support a container abstraction at the level of VM clusters
- **Attestation**: a platform to enable attestation up to the container layer

Infrastructure thrust
- **Side-channel defense**: systems to defend against a wide range of cross-tenant side channels
- **Network policy verification**: techniques for automated identification of policy conflicts, verification of safety invariants for clouds, and reasoning of correctness of dynamic service chaining
- **Network resource management**: a framework for writing network optimization applications on top of SDN controllers
- **Middleboxes**: capabilities to allow flexible traffic routing across arbitrary middlebox chains and to synchronize middlebox state with traffic reallocation decisions
- **Network flow monitoring**: a universal approach for flow monitoring that is general yet accurate

Cloud security horizons (CSH) summit
- CSH 2016: ~40 participants; 40% from industry
- Focus on technical exchange and industry input

Cloud security curriculum development
- Education modules to teach cloud security
- ~15 faculty from diverse institutions each year

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Jan. 9 -11th 2017
Crystal City, VA

Project Silver