Review “Policy-Sealed-Data”

Name: Wenhui Zhang

Paper Name：

Santos, N., Rodrigues, R., Gummadi, K. P., & Saroiu, S. (2012, August). Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services. In *USENIX security symposium* (pp. 175-188).

Contribution:

1. Policy-sealed data abstraction. Data is handled only by nodes satisfying customer-chosen policy. (e.g. Handle data only by nodes running CloudVisor; Handle data only by nodes located in the EU)
2. Use attribute-based encryption (CP-ABE) to implement abstraction efficiently: (1) Binds policies and node attributes to node configurations; (2) Ciphertext-Policy Attribute-Based Encryption [Bethencourt07]

Motivation:

TPMs Alone Are Ill-Suited for the Cloud: (1) Stifle VM and data migration across cloud nodes, TPMs root-of-trust not transferable from one node to another; (2) Cloud providers hesitant to reveal low-level cloud details, TPMs abstractions can reveal node’s identity and details of the node’s entire software stack; (3) Commodity TPMs can hinder the cloud’s ability to scale, TPMs’ poor performance may introduce bottlenecks.

Related works:

Newer hypervisors can offer protection from SW admins: e.g., nested virtualization: CloudVisor [SOSP’11], Credo[MSR-TR]. Trusted computing can attest cloud node runs “correct” hypervisor, Trusted Platform Module (TPM).

Methodology:

The client seals the data, encrypt and bind data to policy. The server decrypt data if node meets policy.

Results:

Monitor can attest a large number of nodes, Max throughput: 630 attestation-verifications/sec (E.g., 10K node cluster attests in ~15 seconds)

Monitor can serve many attestation requests from customers

- Max throughput: 4800 attestation-requests/sec
- Increases throughput of standard TPM attestation
- Batches multiple attestation requests into single TPM call
- Speedup orders of magnitude over standard TPM attestation

Take away:

1. Excalibur overcomes TPM’s limitations in the cloud
2. Policy-sealed data: new trusted computing primitive
    a. Flexible sealed storage
    b. Reduce overexposure
3. CP-ABE makes Excalibur scale
    a. Masks low performance of TPMs
4. Evaluation indicates that the system is practicals