TRUSTED PASSAGES

Chengyu Song, Wenke Lee GTISC

Himanshu Raj Microsoft Research

October 5, 2011

Motivation

- Cloud Computing
  - Benefits
    - Elastic
    - Economical
    - Efficient
  - Problem – **TRUST**
    - Large Trusted Computing Base (TCB)
      - Hardware & Firmware
      - Software stack (hypervisor, root VM), Administrators
      - Lacks verifiable measures for security and trustworthiness

Solution

- Storage
  - Cryptography based Proof
- Computation - HyperSafe
  - Reduced external TCB of the VM
    - hypervisor + minimal hardware/firmware (DRTM launch, TPM)
    - Secure VMs with no trust dependence on root VM and administrators
  - Provides measurable hardware rooted trust chain
    - Remote attestation

Communication Challenges

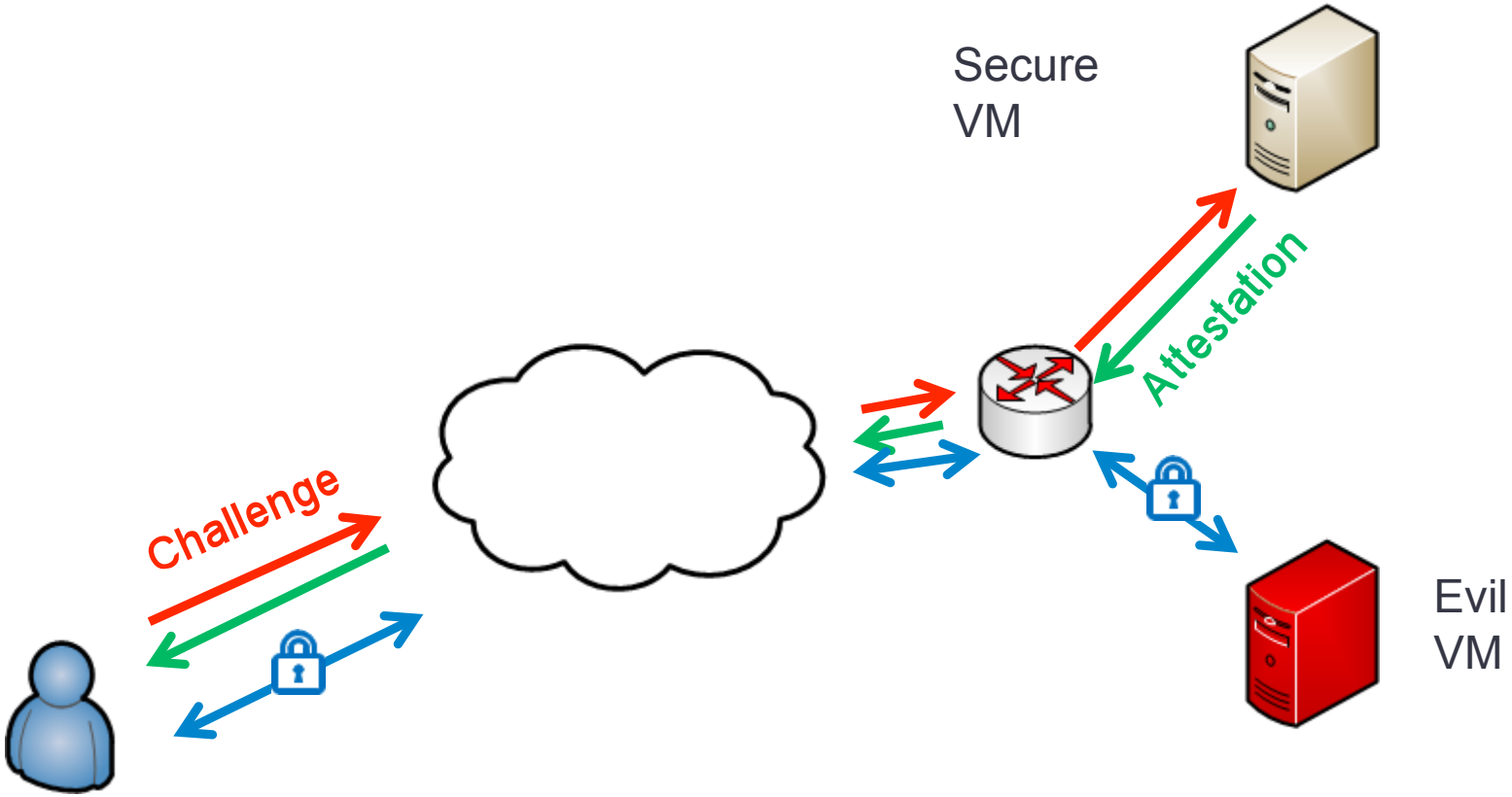
- Problems still exist
  - How to ensure the VM I am connecting to is my VM (VM Identity)?
  - How to build secure communication channel between my VMs (Defeat impersonation)?
  - How to securely provide service to my customers ?
- Existing solutions (SSL/TLS/IPSec) do not help
  - Man-In-The-Middle Attack

Attack Scenario Setup

- **Alice** - cloud service provider
  - Claims deployment of HyperSafe in the infrastructure
- **Bob** - cloud customer
  - Wants to run security sensitive services (e.g. online banking)
  - Has no measures to fully trust Alice
  - But can measurably trust HyperSafe

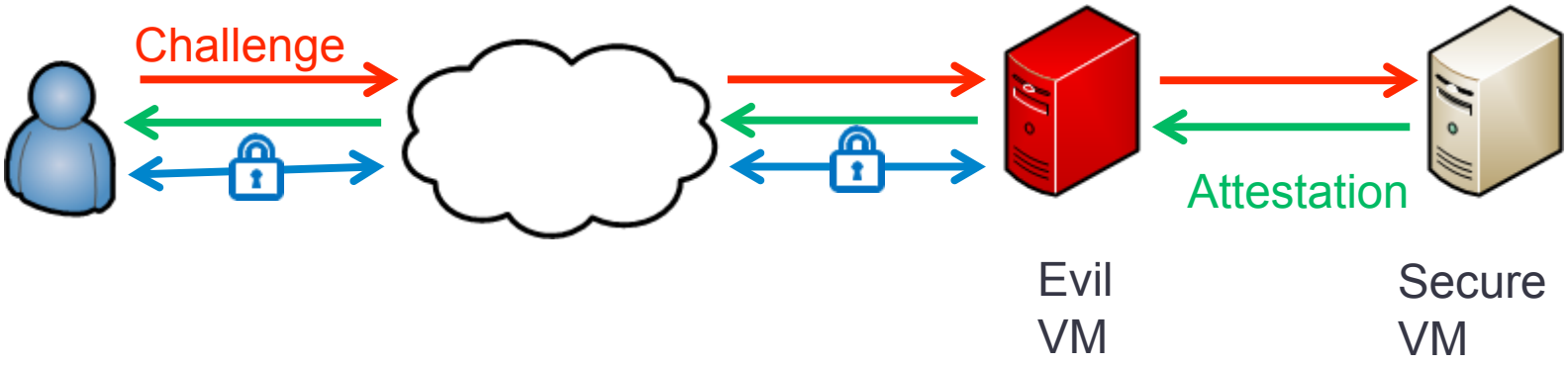
Attack Scenario – TOCTOU

- Bob wants to make sure the rented VM is protected by HyperSafe (secure VM)
- Controlling the whole infrastructure, Alice can redirect further connections to a insecure VM



Attack Scenario – MITM

- How about establishing a secure communication channel before performing the remote attestation ?
- Alice still can launch MITM attack!



TLS Protocol

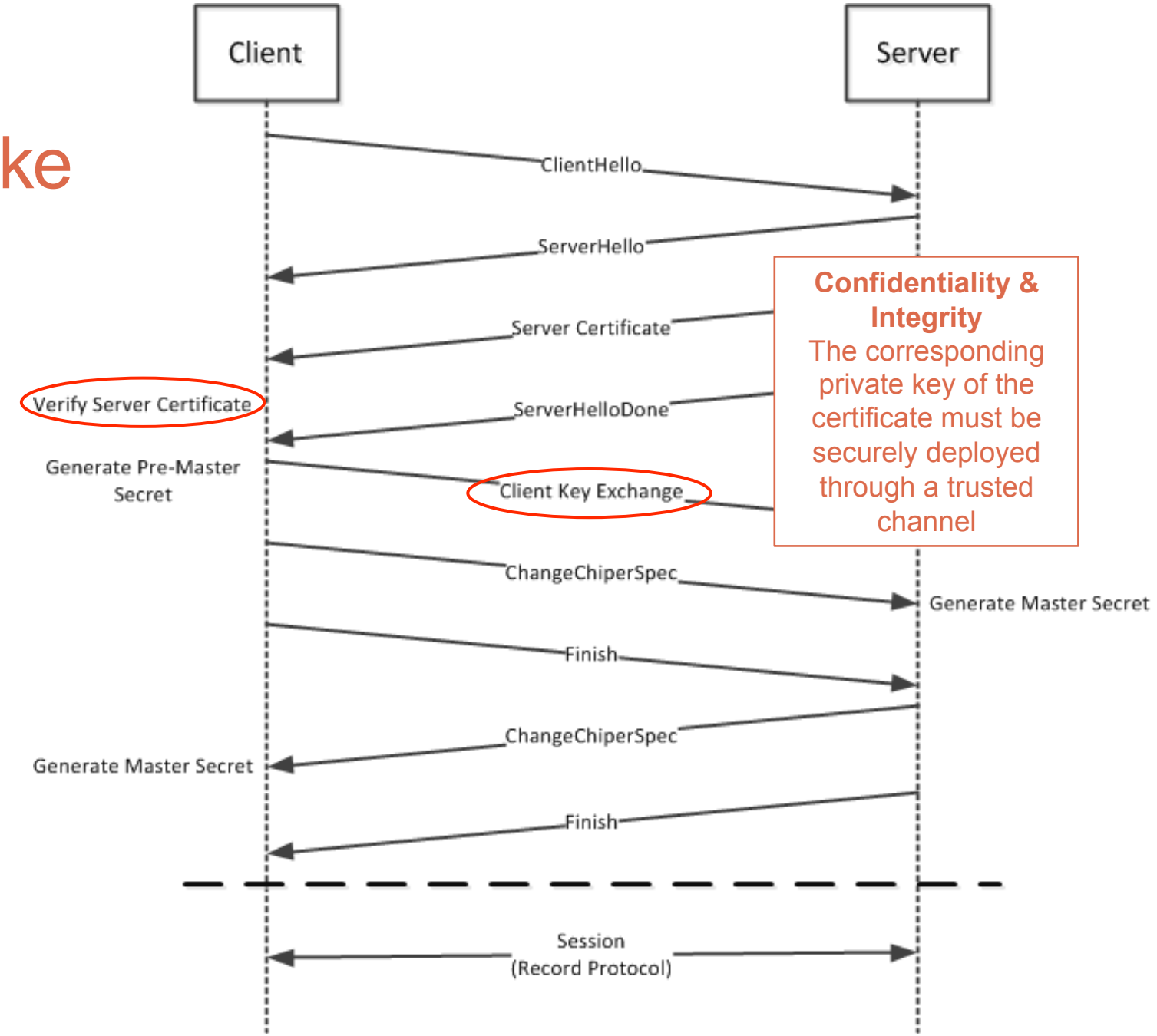
- TLS Record Protocol
  - **Confidentiality**: the content can be encrypted with symmetric cryptography and the keys are generated uniquely for each connection
  - **Integrity**: transported messages can include an integrity check using keyed MAC

- TLS Handshake Protocol
  - **Auth**[illegible] tric crypt[illegible]
  - **Conf**[illegible] ilable to eavesdroppers and man-in-the-middle
  - **Integrity of the negotiation**: the negotiation communication cannot be modified without detection

Why TLS Still Fails ?

TLS Handshake Protocol

Authenticity
The remote server must have a valid certificate signed by a trusted CA



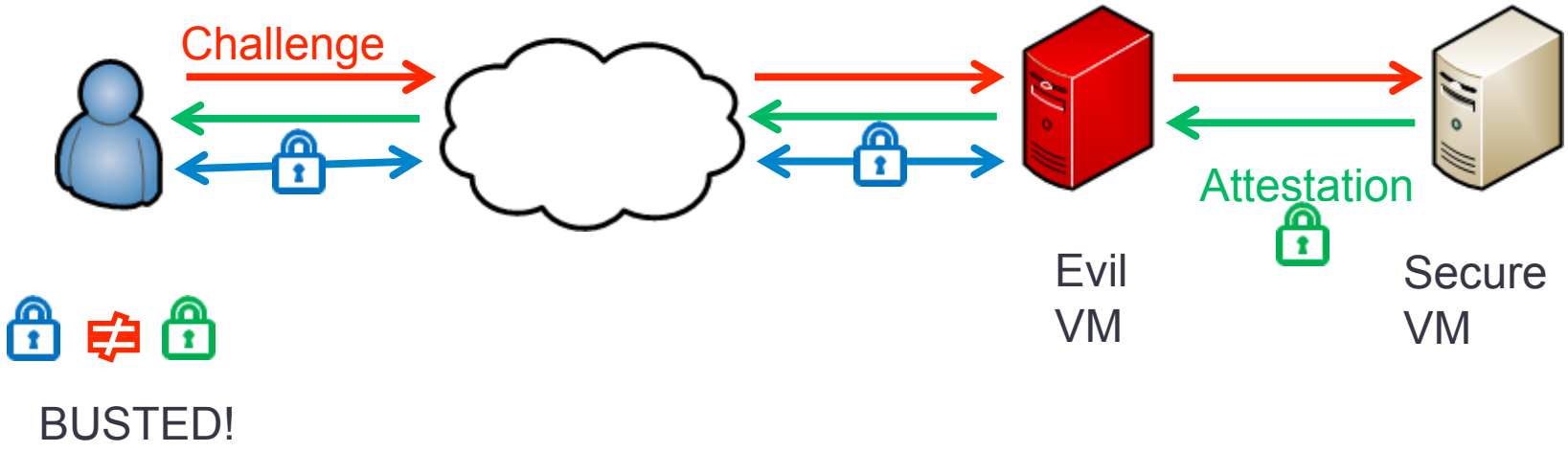
Confidentiality & Integrity
The corresponding private key of the certificate must be securely deployed through a trusted channel

Trusted Passages

- Goal
  - Enable Trusted End-to-End Communication Channel
- Approach - tightly bind a TLS session with remote attestation
  - Remote Attestation & Improved TLS handshake protocol
    - Authenticity & Trustworthiness of the other end
    - Confidentiality & Integrity of the handshake
  - TLS record protocol
    - Confidentiality & Integrity of the following communication

Trusted Passages – Server Identity

- When generating the attestation, HyperSafe will include the public key used to establish the TLS session in the attestation.
- But this is **NOT ENOUGH!** Because the private key is still deployed by Alice.

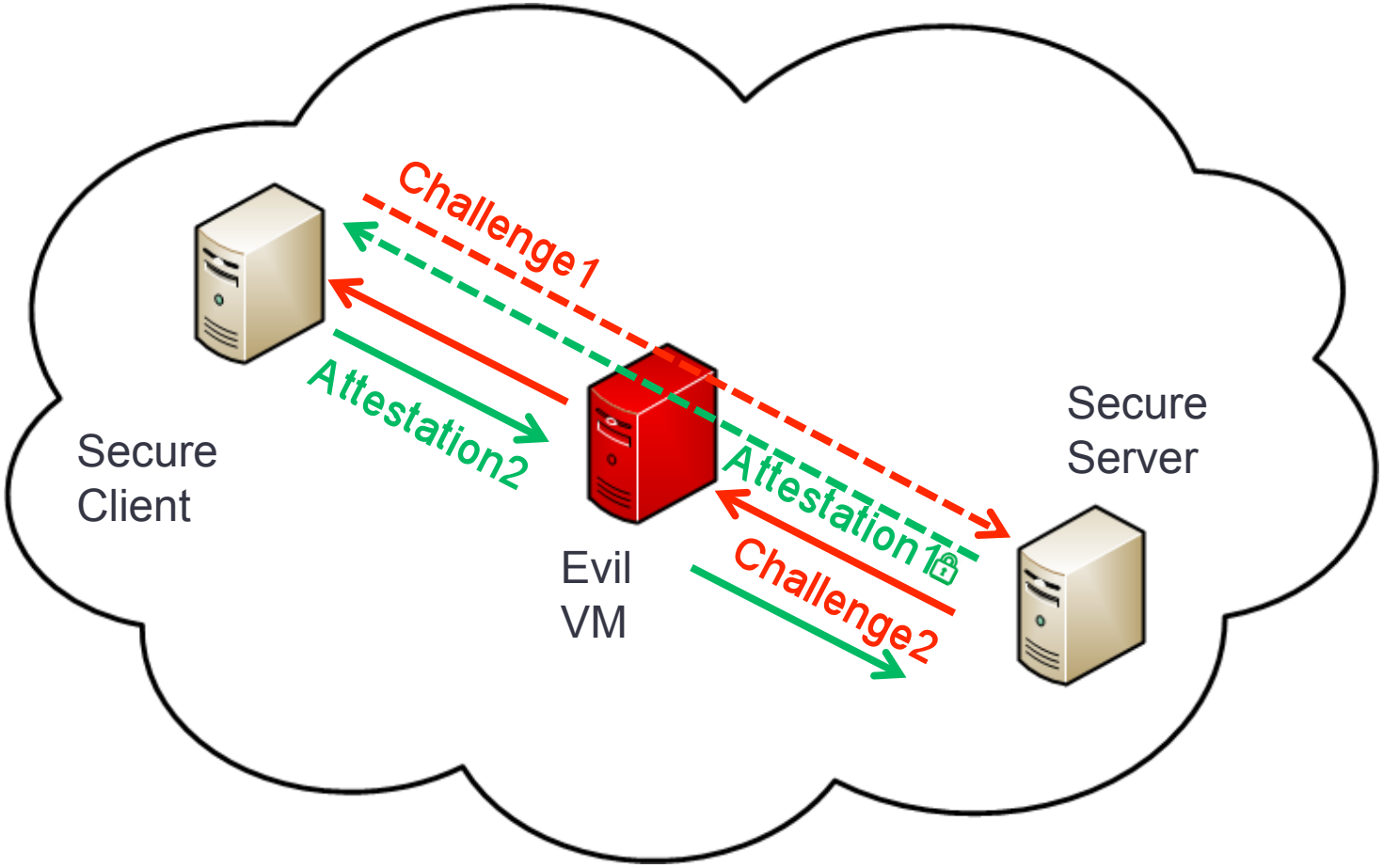


Trusted Passages – Secret Exchange

- How to prevent key abuse?
  - Linking the certificate to a machine (TPM), e.g. create a TLS certificate signed by the TPM [IBM 2006]
  - Still not enough, because eavesdropping is still possible
- How to protect the private key?
  - Let the TCB generate the key pair and keep private key secure
  - Guarantee the key is generated by the TCB via attestation

Attack Scenario – Client Attestation

- When two secure VMs want to establish a trusted communication channel.



Trusted Passages – Secret Exchange

- How to prevent Alice from stealing the secret by impersonating the client?
  - Include pre-master secret in the attestation
  - Still not enough, if the Evil VM has a valid certificate and the Client VM does not check carefully
- How to guarantee the integrity of the Client Key Exchange
  - Include the encrypted pre-master secret

Third Party Scenario

- Bob's costumer will be able to measure the trustworthiness of the service hosted in the cloud
- And Bob will also be able to measure the trustworthiness of his costumer
  - E.g. whether the client runs an antivirus tool with latest signature database

Q&A

Thanks