Cloud security

Haoyuan Li

October 31, 2012

1 A Security Analysis of Amazon's Elastic Compute Cloud Service

1.1 Research Contribution

- Cloud computing is such a great new area, and this is a fun paper, however, what is the paper's research contribution?

  Someone suggestted there is no research contribution in this paper, however, this is a good security manual.

- More general, what is research contribution in security research community?

  New attack, new defense, or both.

1.2 Paper's Potential Improvement

- Have a measurement study to show how important or common the problem described in the paper is. Why are people making these mistakes?
- Propose a solution to solve these issues. For example, design and implement a script to examine all these issues, and fix them automatically.

1.3 Random Number Generation

- Some protocols rely on the random numbers generated by the machine: for example, https. The current random number generation approach works only if it can gather enough entropy from the data sourse.
- The issue about cloud computing: if you take a snapshoot, every time you start it, it starts from a same status. Therefore, it will generate same numbers during the beginning period. There are different solutions for this.
- Why do we believe randomness at the source? If we believe physics' randomness, we can believe it.

1.4 Ethnical Issue

- Is this ethnical to do research on these data without permission from users?
- Public vs private is not a boolean question. Privacy has different defination for different people. It has context. It is also hard to define whether this is ethnical.

1.5 Other Cloud Computing Security Research

- In EC2, users sometimes share a same machine by using different VMs. If there is any sercurity hole in the hypervisor, then one user on a machine could really control the machine, and monitor what others are doing.
- One interesting paper: Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. Traceroute or ping can easily find whether a server is hosting on the same machine or not.
- Side channel. Fill L2 cache completely with Bob's data. Bob can wait for a context switch. And then query the L2 cache and see how much of the L2 cache get a sense of how another VM is doing.
- Defense to co-host VM attack:
  - Amazon provides isolated machines for ec2 types above a m1.xlarge.
  - Scheduling algorithm to avoid.

2 Cryptography Basics

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce[1].

2.1 Symmetric-key cryptography

- Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.
- Symmetric-key encryption can use either stream ciphers or block ciphers. Stream ciphers encrypt the digits (typically bits) of a message one at a time. Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size.
- Figure 1 shows how symmetric-key encryption works.

2.2 Asymmetric-key cryptography

- Asymmetric-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the

[1]Definitions in this section are cited from Wikipedia [1].

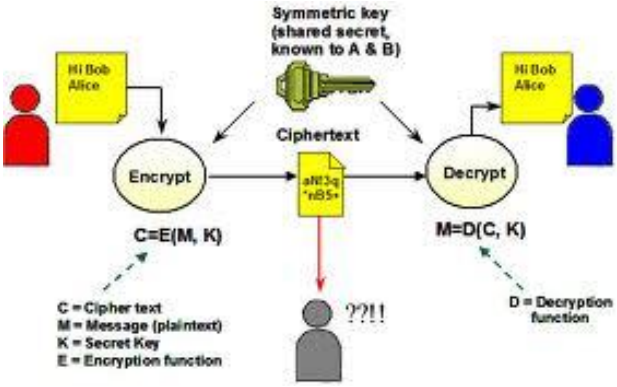

Figure 1: Symetric-key Encryption

key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions (however, the private key can generate the public key). One of these keys is published or public, while the other is kept private.

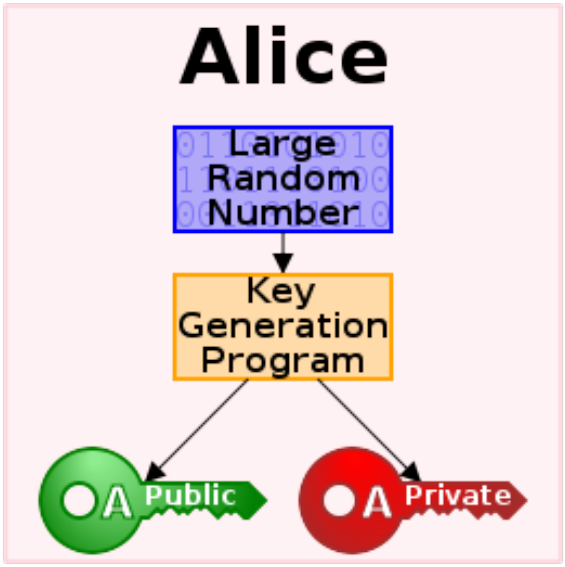

Figure 2: In an asymmetric key encryption scheme, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt. Security depends on the secrecy of the private key.

- Practical considerations
  - Security
  - Computational cost
  - Distribution of a new key
  - Recovery from a leaked key

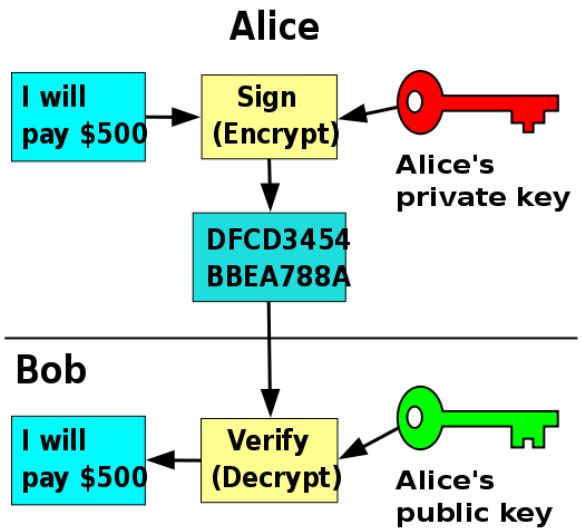

Figure 3: In some related signature schemes, the private key is used to sign a message; anyone can check the signature using the public key. Validity depends on security of the private key.

	Confidentiality	Integrity
Symmetric key (efficient with limitation)	Encryption, Stream ciphers, Block ciphers (AES)	MAC
Asymmetric-key / Public-key	Public-key encryption	Digital signatures (public-key signatures)

Table 1: Comparsion between Symmetric key and Asymmetric key

3 Reference

[1] Wikipedia `http://en.wikipedia.org/`