Kerberos:
An Authentication Service for Computer Networks

B.Clifford Neuman and Theodore Ts'o
IEEE Communication Magazine September 1994

Presented by: Jian-jun Dong

"When using authentication based on cryptography, an attacker listening to the network gains no infor mation that would enable it to falsely claim another's identity. Kerberos is an example of this type of authentication technology…"

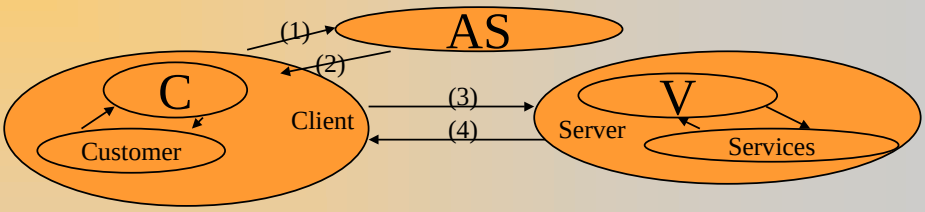
Outline

- **Introduction**
- **Basic Kerberos authentication protocol**
- **How Kerberos works**
- **Vulnerabilities I see in Kerberos**
- **Conclusion**

Introduction

- In computer networks, data my be exposed to unauthorized access. So it is important to protect data from being accessed by an attacker. Encryption techniques are considered to be the most powerful protection to prevent unauthorized access to data. Kerberos is an example of authentication technology, which based on secret encryption keys.

Basic Kerberos authentication protocol

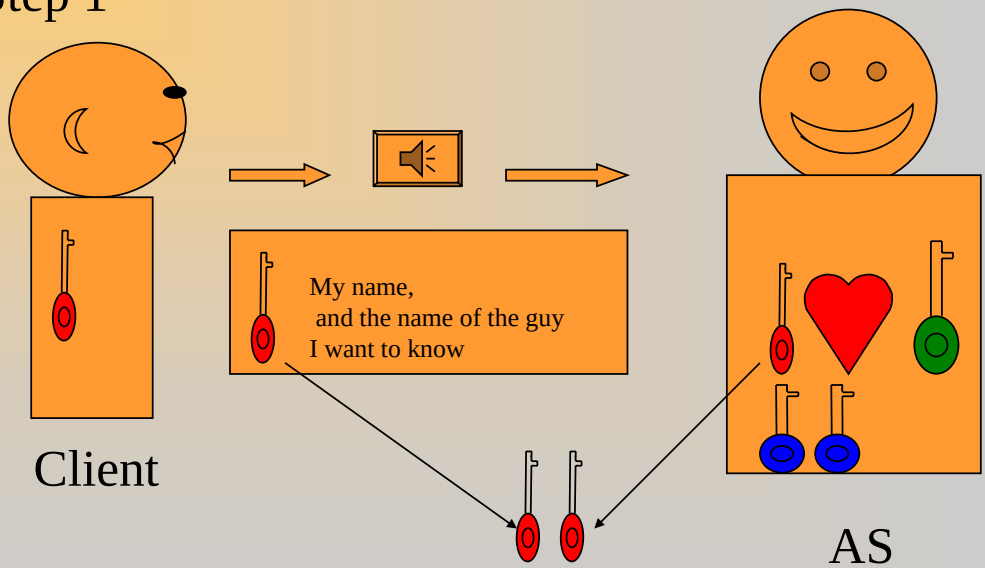


- **AS: Authentication Server, distributes keys and tickets to Client**
- **Client: the entity want certain service from Server**
- **Server: the entity verifies Client's identity and allow Client to access certain service**

- **(1)as_req:c,v,time$_{exp}$, n**
- **(2)as_rep:{Kc,v, v, timeexp,n,…}Kc, {Tc,v}Kv**
- **(3)ap_req:{ts,ck,Ksubsession,…}Kc,v {Tc,v}Kv**
- **(4)ap_rep:{ts}Kc,v (optional)**

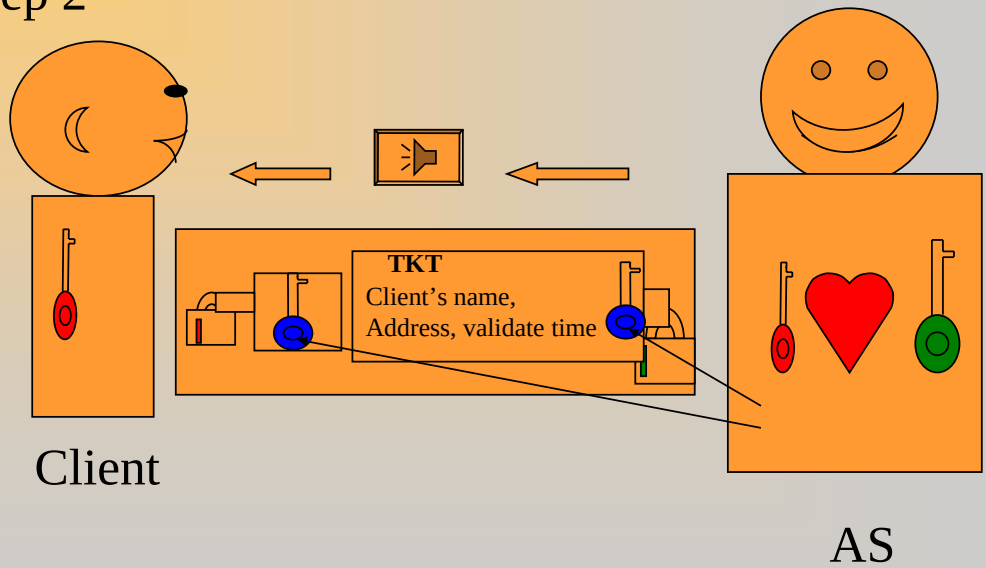
How Kerberos works

Step 1



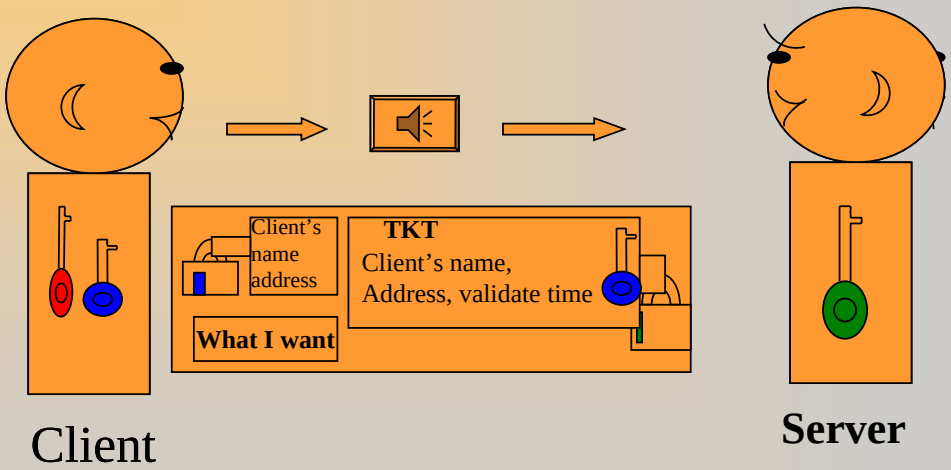
How Kerberos works (continue)

Step 2



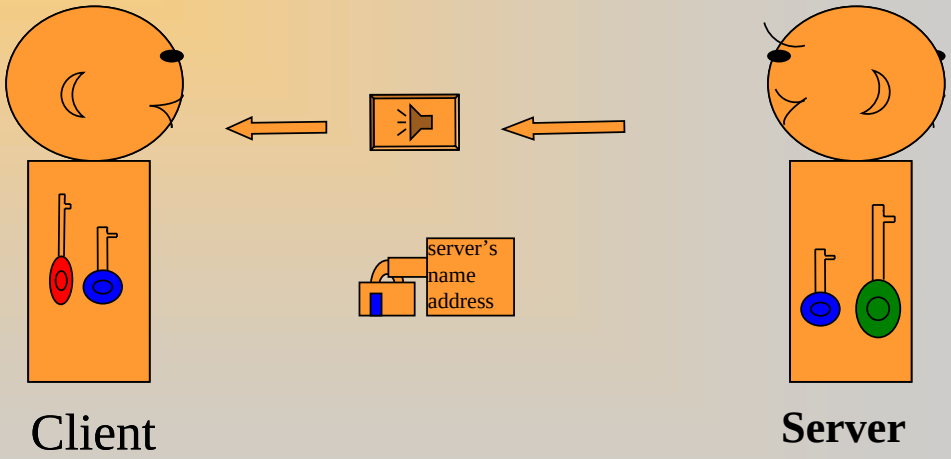
How Kerberos works?(continue)

Step 3



How Kerberos works(continue)

Step 4



Vulnerabilities I See in Kerberos

- AS holds too many keys, if he lost some keys or he is sick will result serious problem.
- When the client first time sends a box to AS, the box is not locked, if someone steal the key inside, this person will be able to impersonate the client.

Question:
Have you got any idea to solve these vulnerabilities?

Conclusion

- This article is a reasonably good tutorial for introducing the basic concept of Kerberos' protocol.
- Kerberos is quite comprehensive, but is not perfect.