Secure the Internet

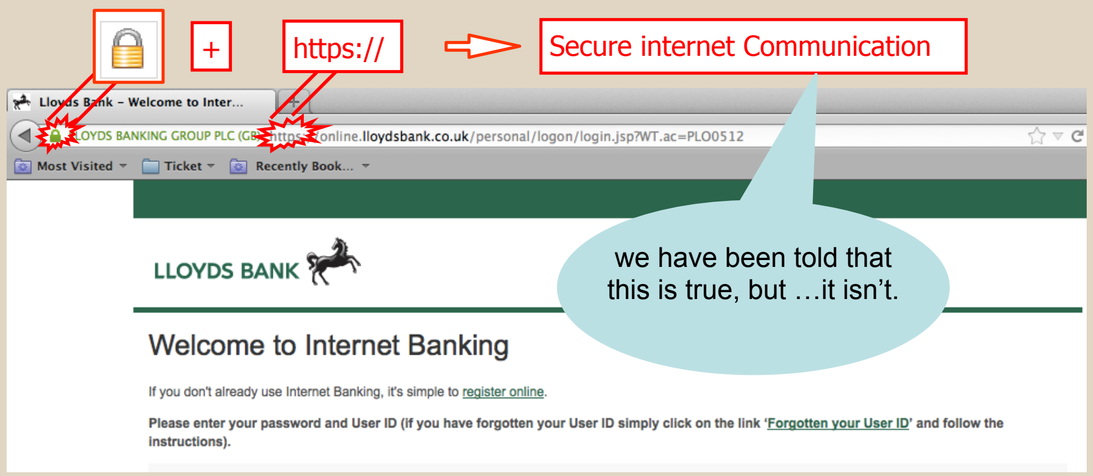
UNIVERSITY OF BIRMINGHAM

Jiangshan Yu, Vincent Cheval and Mark Ryan
Security and Privacy Group, School of Computer Science
jxy223@cs.bham.ac.uk

1. Abstract

We use HTTPS protocol every day to secure our internet communications (e.g. webmail, Facebook, internet bank…), however, today's internet is not as secure as we thought.

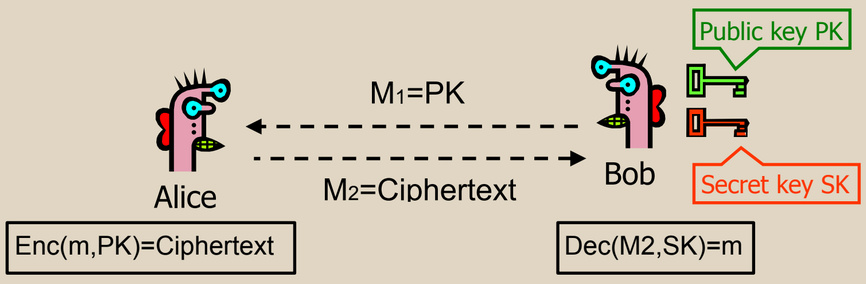
This research aims to enhance the security of internet communications.



2. Background & Problem

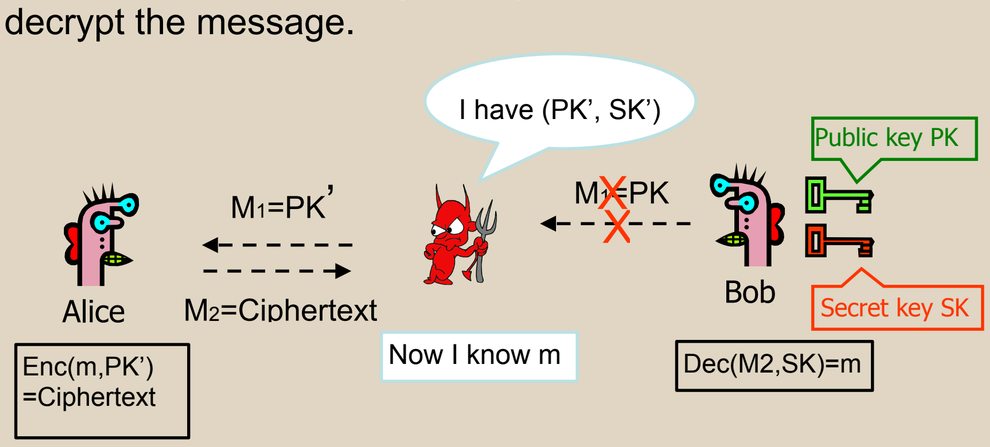
Public key Encryption:

In HTTPS, Alice can encrypt a message m by using Bob's public key PK, and only Bob who has the corresponding SK can decrypt the ciphertext.



Problem:

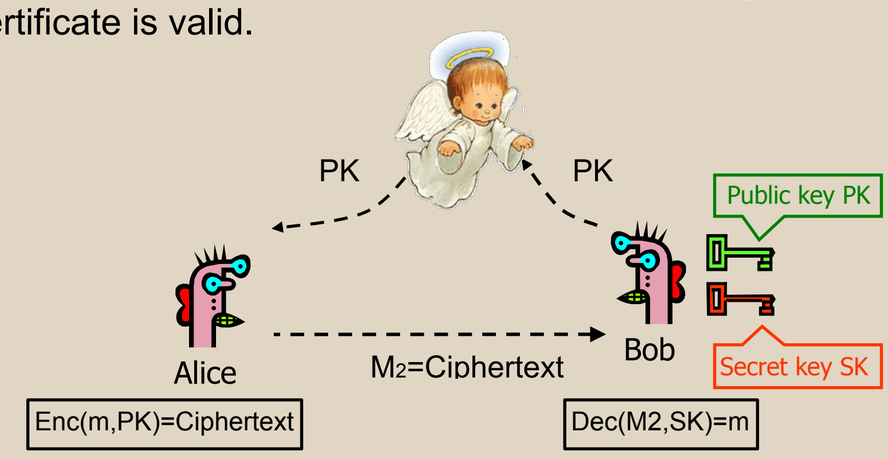
If Alice uses a fake PK given by attacker Eve, then Eve can decrypt the message.



==========

Current Solution:

Trusted parties were introduced to verify the PK carefully, this party will then issue a certificate on the verified PK. The certificate is cryptographically signed, and only the certificates issued by the trusted parties will be accepted. Web-browsers can easily verify whether the signature on a certificate is valid.



Problem:

Trusted parties are assumed to behave honestly, but in fact, sometimes they don't (e.g. because they are hacked by attackers or forced by government agencies). Many attacks on web servers (e.g. Facebook, Gmail, and Hotmail) have been found in recent years.

3. Aims

This research aims to overcome the current flaws by proposing a new public key infrastructure which can get rid of trusted parties but still be able to securely authenticate public keys.

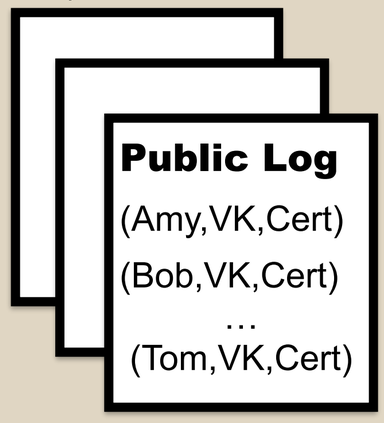
4. Method

We introduced a public, auditable, append-only **log**. The data recorded in the log is (ID,VK,Cert), where ID is user identity, VK is the user's cryptographic signature verification key, Cert is a certificate that states the user's public key for encryption and is signed by Bob's signature signing key.

The log supports some **formal cryptographic proofs**:

- Proof A: the given data is in the log.
  (So one can ensure the data is indeed recorded in the log)
- Proof B: the current log is extend from previous version.
  (So no one can make a valid proof if the data is deleted)
- Proof C: the given data is the currently valid.
  (So the revoked data will not be accepted)

Users should **only** accept the data if and only if it has been recorded in the log, and valid proofs are provided. The correctness of logs can be verified by the cooperation of users' web browsers.



5. Result and Discussion

- By using this new system, the trusted parties are not needed any more.
- All proofs are in size O(log n) (so does the size and time for proof verification). Thus, even if there are a billion certificates recorded in the log, the size of one proof is only around 2 KB, which is considered to be efficient.
- If Bob carefully checked the log at the time he submitted his VK and Cert, and Alice's web browser is not compromised, then the system is secure.
- Bob's signature signing key will only be used to sign a new certificate, so it will be rarely used and will be stored securely offline. This key can also be used for revocation.

6. Further Related Information

- The Sovereign Keys Project, **Electronic Frontier Foundation**
- The Certificate Transparency Project, **Google**
- Accountable Key Infrastructure, **Carnegie Mellon University**

www.bham.ac.uk