
# Encrypted Message Authentication by Firewalls

**Chandana Gamage**

**Jussi Leiwo**

**Yuliang Zheng**

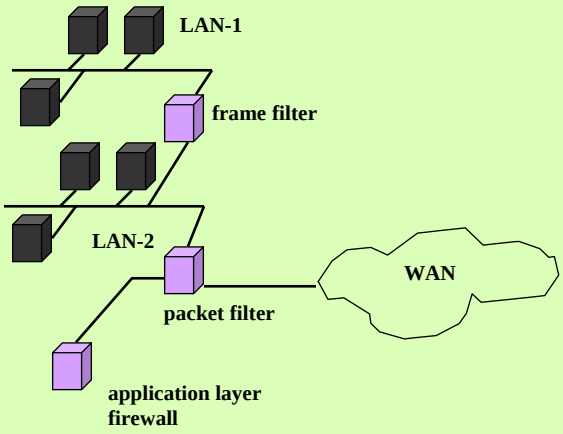
***Monash University***




## Role of Firewalls in Network Security

- **Access control and audit.**
- **Public WAN/Private LAN interface.**
- **To build Private Virtual Networks (PVN).**


## Firewall Location in Networks







## How Firewalls Operate

- Frame filtering at link layer.
- Packet filtering at network/transport layer.
- Message/content filtering at application layer.


## Link Layer

- Filtering is based on frame level (hardware) addresses.
- Can be used inside a LAN.
- Can be used at the “bridge” interconnecting two LANs.




## Network/Transport Layer

- Filtering is based on packet/segment level information.
- Can be used at LAN/WAN interface (router).
- Testing criteria are end-point host addresses, application port type and protocol extension such as IPv6 AH.


## Application Layer

- Filtering can be based on many criteria that are application specific.
- Common/useful general criteria is user authentication.




## Signed and Encrypted Message Handling by Firewalls

- The firewall is an intermediary. It is not the end-node receiver of messages.
- Messages are normally signed (with sender private key) and then encrypted (with receiver public key).
- The firewall cannot verify the signature without first decrypting the message.

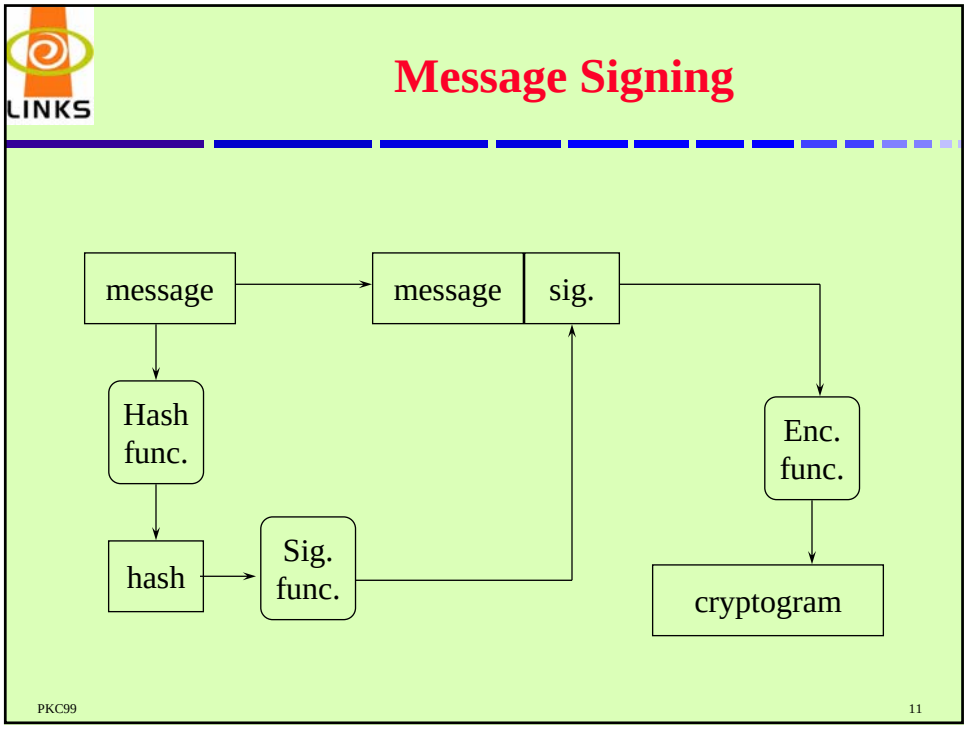

## The Problem

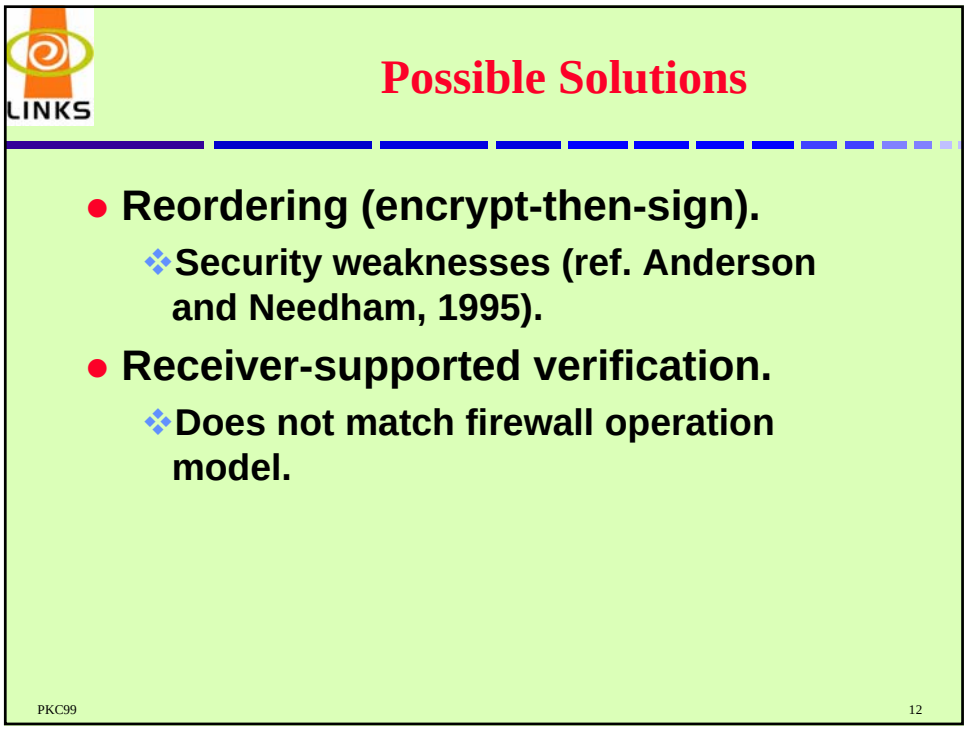
- How can a firewall authenticate sender/receiver binding (using digital signatures) for an encrypted message?




## Properties of a Solution

1. Preserve the standard semantic of sign-then-encrypt.
2. Signature verification without plain text message.
3. No increase in original secure message generation (computational) or transmission (bandwidth) costs.
4. Firewall verification of a message must not cost more than normal end-user verification.


LINKS
Message Signing
message
message
sig.
Hash
func.
Enc.
func.
hash
Sig.
func.
cryptogram
PKC99
11


LINKS
Possible Solutions
Reordering (encrypt-then-sign).
Security weaknesses (ref. Anderson and Needham, 1995).
Receiver-supported verification.
Does not match firewall operation model.
PKC99
12


## Proposed Solution

- **Use a public key cryptographic primitive that combine sign-then-encrypt operations.**
- **The** switching **of two operations (into encrypt-then-sign) will now be** hidden**.**
- **Modify the cryptographic primitive to allow third-party verification.**




## Implementation of the Proposed Solution

- **Uses Signcryption (ref. Zheng, 1997).**
- **Based on Modifications by Bao and Deng (ref. PKC98).**


## Modified Signcryption Scheme

- **Third-party verification of signed messages.**
- **Third-party does not access plain text message.**
- **No change in signed message size.**




## Modified Signcryption

$k = \text{hash}(y_b^x \bmod p)$

$y = g^x \bmod p$

$c = \mathrm{E}_k(m)$

$r = \text{hash}(y, c)$

$s = \frac{x}{r + x_a} \bmod q$

$\Delta \equiv (c, r, s)$

**In original scheme**

$r = \text{hash}(y, m)$


## Modified Unsigncryption

$\Delta \equiv (c, r, s)$

$y = (y_a g^r)^s \bmod p)$

$k = \text{hash}(y^{x_b} \bmod p)$

$m = \text{D}_k(c)$

accept if $\text{hash}(y, c) \equiv r$




## Verification-Only at Firewall

$\Delta \equiv (c, r, s)$

$y = (y_a g^r)^s \bmod p)$

forward if $\text{hash}(y, c) \equiv r$

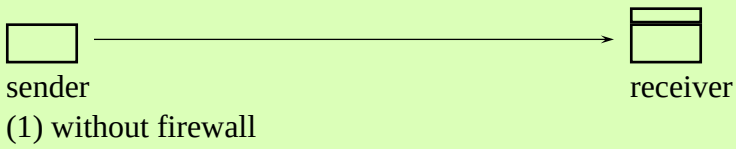
## Computational Performance

- 67% to 92% increase in computational cost for receiver over the original signcryption scheme.
- 17% to 19% decrease in computational cost for receiver over sign-then-encrypt schemes.
- 33% to 46% increase in computational cost for firewall over the original signcryption scheme.

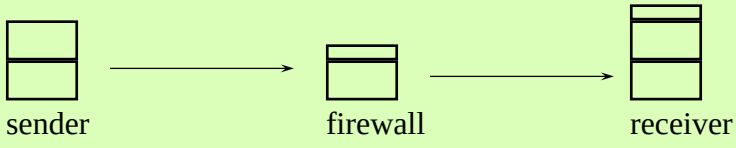


## Computational Cost (1)

Secure message transmission using signcryption

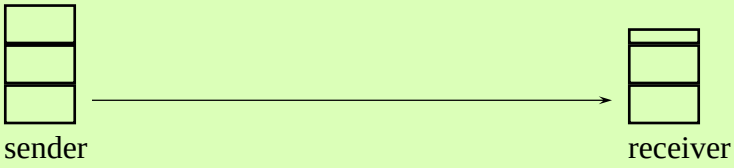



(1) without firewall

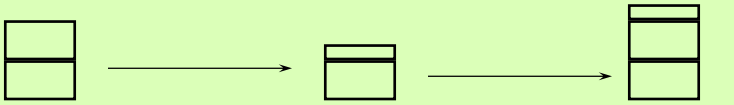



(2) with firewall

## Computational Cost (2)




(1) sign-then-encrypt (DSA/ElGamal) without firewall




(2) Signcryption with firewall



## Conclusion

- **Proposed scheme satisfies the required properties:**
  - **Preserve semantic.**
  - **Verification without plain text.**
  - **Overall computational costs lower than for sign-then-encrypt schemes.**
  - **Low computational cost at firewall.**