Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 03: Application Level Security
Module 03: Email Security – Key Management

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

CASED

Screw-up

Source: xkcd.com

Learning Objectives & Outline

Learning objectives

- Application level security has been designed in a number of protocols; the design of such protocols should be understood using (representative) examples.
- Comprehend supporting functionality such as key exchange and management to enable secure email (using the example of PGP)

Outline

(1) Key management

(2) PGP's Web of Trust

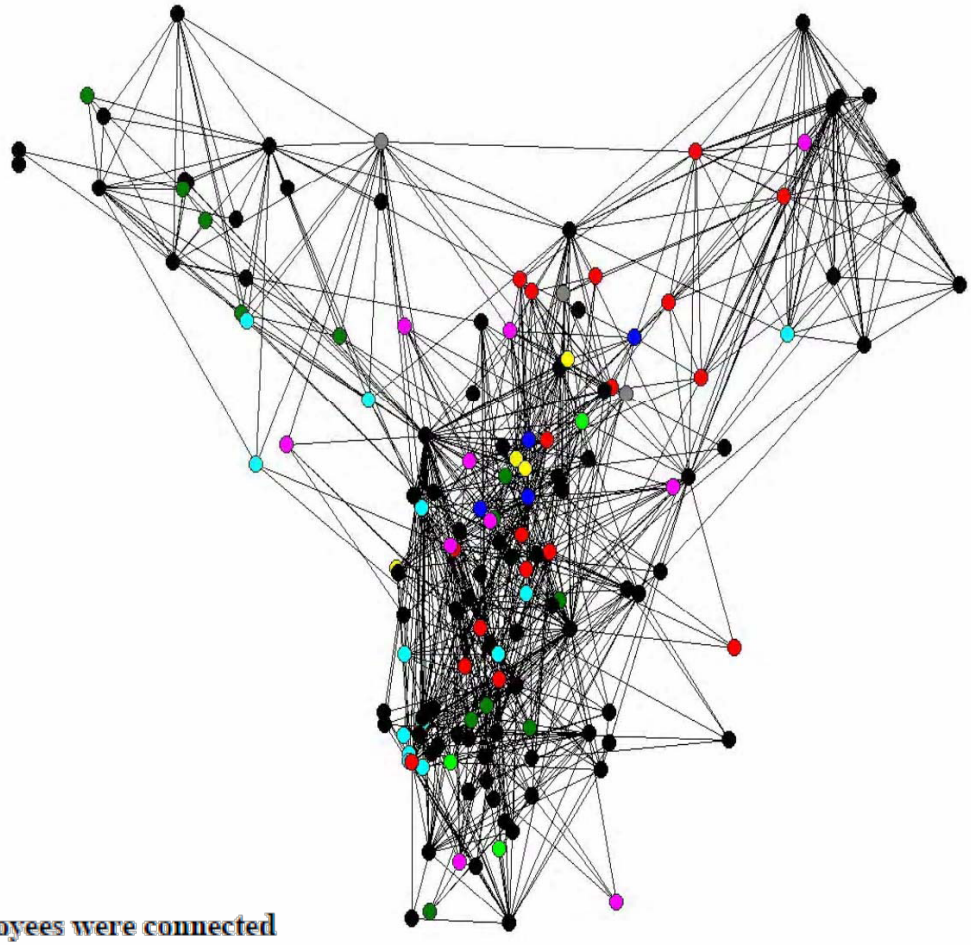
Chapter 03, Module 03

PGP Public & Private Keys

SECURE MOBILE NETWORKING

Motivation

- Can you easily manage key material for all your contacts?
- Here: social email graph of 151 employees involved in the ENRON scandal



The Enron Email Dataset
Database Schema and Brief Statistical Report[1]

Jitesh Shetty
University of Southern California
Los Angeles, CA
jshetty@usc.edu

Jafar Adibi
USC Information Scien
Marina del Rey,
adibi@isi.edu

Figure 7: Network showing how the ex employees were connected
Red: Vice President, Blue: President, Black: Employee (non managerial), Grey: In House Lawyer, Pink: Manager, Dark Green: Trader, Light Green: Managing Director, Light Blue: Director, Yellow: CEO

PGP Public & Private Keys

Since many public/private keys may be in use, need to identify which is actually used to encrypt session key in a message

- could send full public-key with every message
- but this is inefficient

Rather use a key identifier based on key

- least significant 64-bits of the (public) key
- will very likely be unique

Also use key ID in signatures/vcards

- Allows easy retrieval of keys from key-servers (but you probably should not trust this key yet)

How to ensure validity of the key? How to establish trust?

PGP Key Management

"This whole business of protecting public keys from tampering is the single most difficult problem in practical public key applications". --PGP Manual

PGP Key Management does not rely on certificate authorities

- In PGP every user can be considered to be her own CA
- Forms a "web of trust"
  - User signs keys that she trusts (keys of users she knows personally)
  - User can trust keys others have signed (if one trusts these users to the necessary degree)

Users can also revoke their public keys

- The owner issue a key revocation certificate (normal signature certificate with a revoke indicator)
- Corresponding private key is used to sign the certificate
- Revocation is best effort: no guarantees

Source: Stallings

PGP Trust Model

How does Alice obtain Bob's public key?

- Alice physically gets key from Bob
- Or from phone conversation (exchange info on pgp fingerprint = hash of pub key)
- Or gets Bob's key from Claire, who Alice may or may not trust

For one key in your key ring:

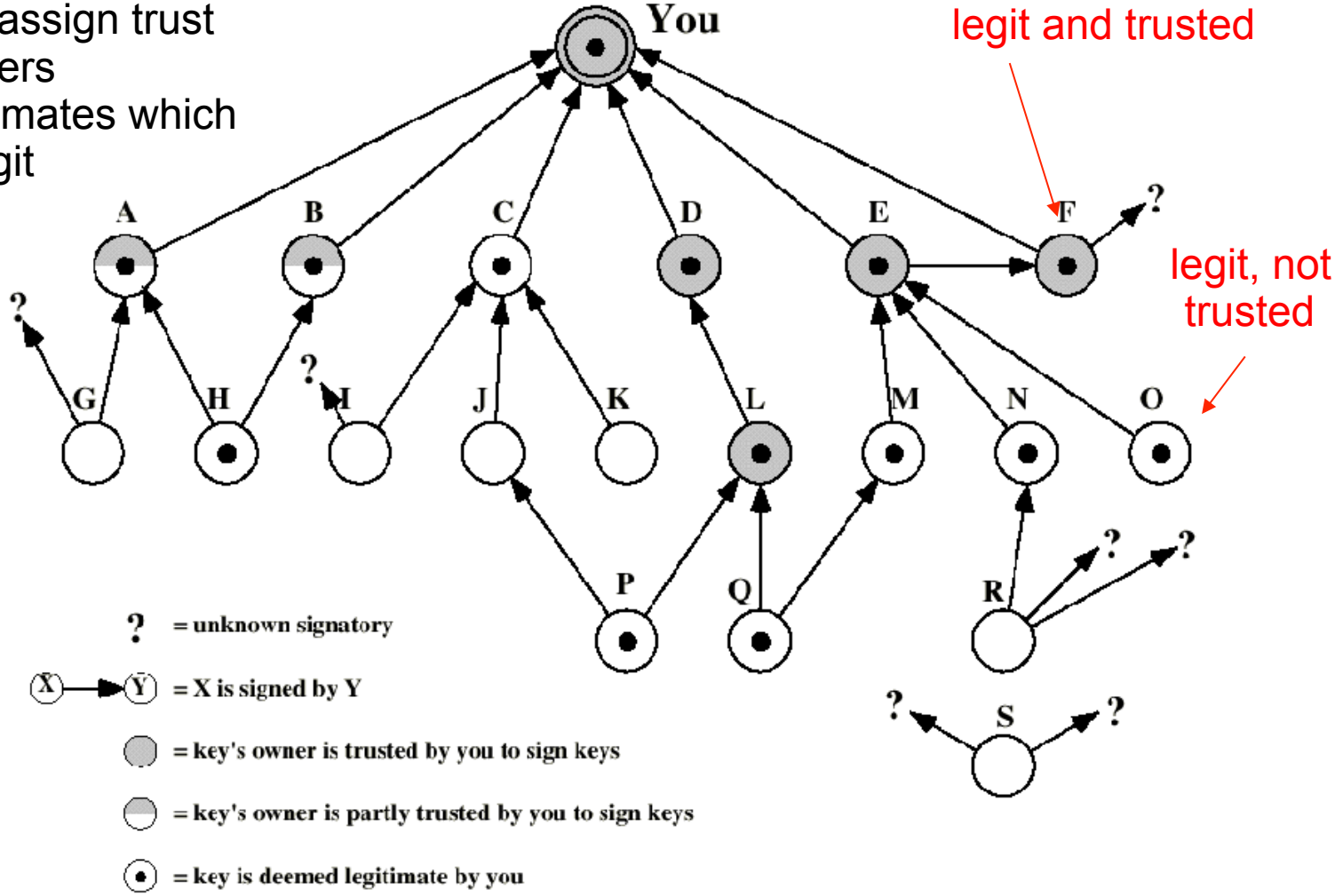
- Can you trust that key really belongs to the person defined by the user-id?
- Can you trust that user-id to vouch for other keys?

For each key on ring:

- Key legitimacy field indicates how much you trust this key to be valid for the associated user.
  - Determined by PGP algorithm
- Signatures for key. Each signature signed with private key of some user
- Also, key ring includes trust values for owners of keys in key ring
  - Determined by you.

PGP's Distributed Web of Trust Model

1) You first assign trust levels to users
2) PGP estimates which keys are legit



Public Key Management: Example

Suppose Alice inserts new public key in key ring. If Alice is owner, trust assigned to Alice is ultimate.

Otherwise, Alice must assign trust value to owner of key:

- unknown
- untrusted
- marginally trusted
- completely trusted
- (different versions of PGP have different trust level strructures)

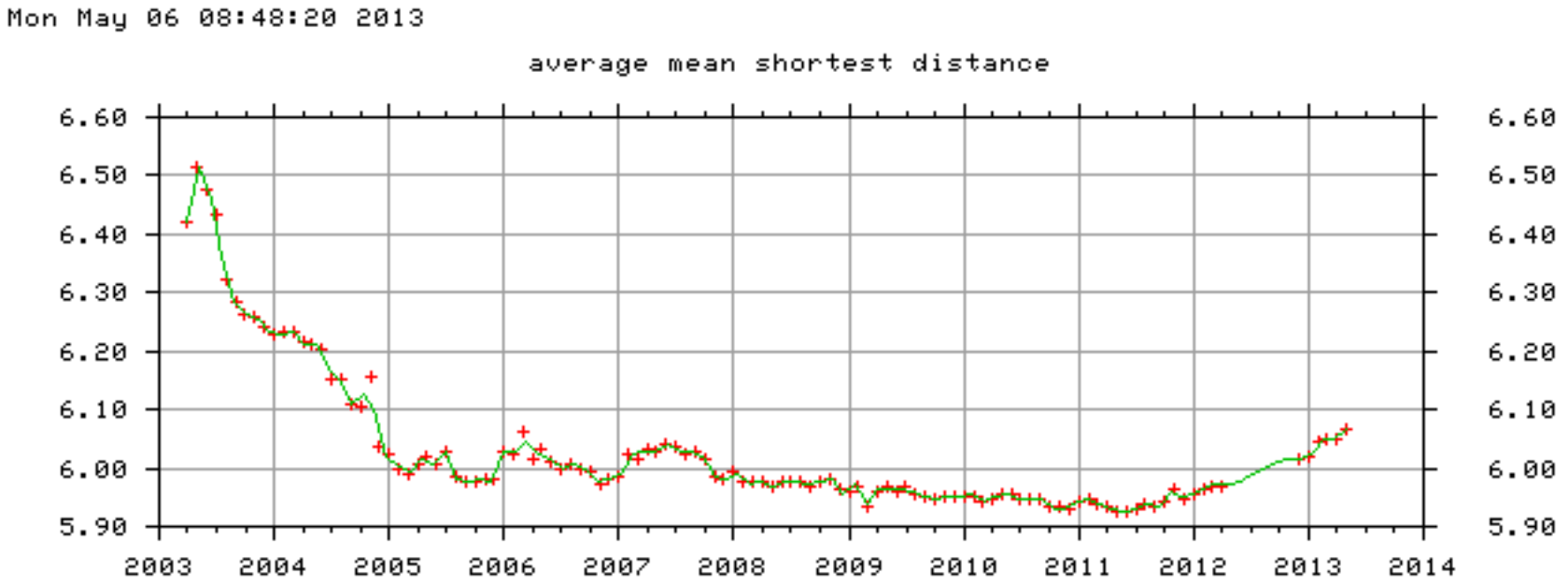
New public key may come with signatures vouching for the key. For each signature, PGP searches ring to see if author of signature is in key ring.

Key legitimacy = legit if one signature completely trusted. Otherwise, determined from formula based on trust of signatures: above threshold, key is considered legit

Some Interesting PGP Key Statistics

Source: http://pgp.cs.uu.nl/ and http://pgp.cs.uu.nl/plot/

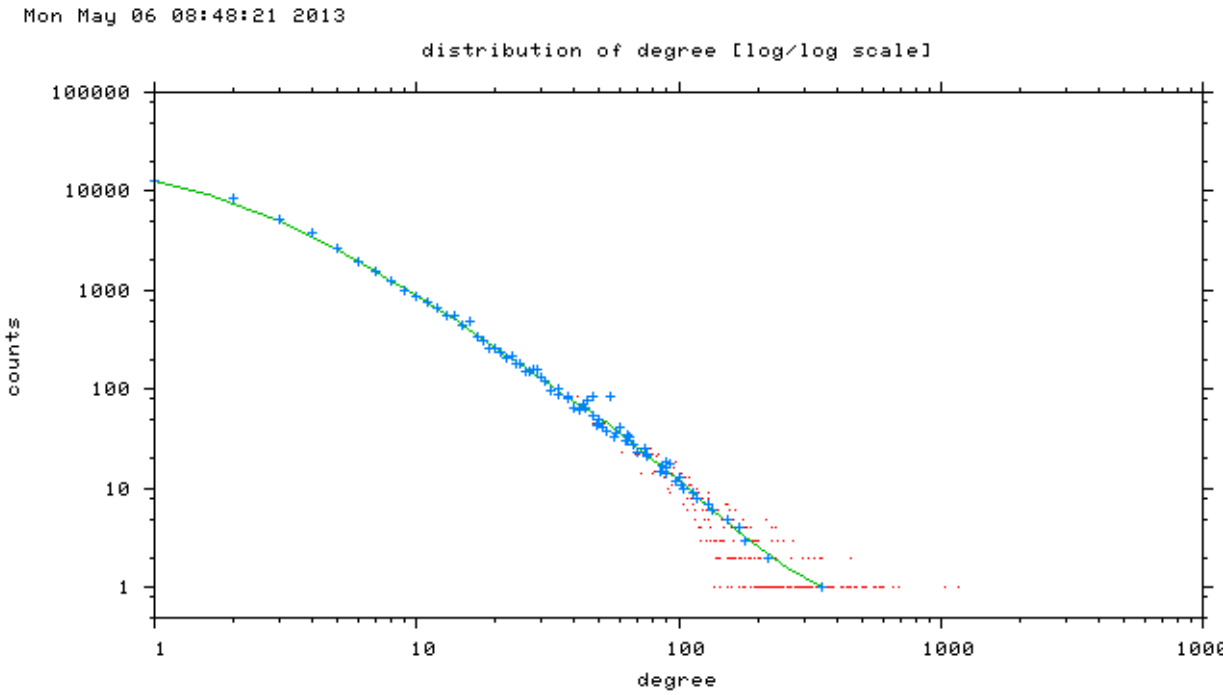
- The PGP web of trust can be viewed as a directed graph where the vertices (node) are the PGP keys, and the edges (directed lines) are the signatures.
- If there is a path from key A to key B, the distance from A to B is the length of the shortest path from A to B.
- The strong set is the largest set of keys such that for any two keys in the set there is a path
- The mean shortest distance (MSD) of a key is the average distance to that key
- The average mean shortest distance (AMSD) is the average of the MSD's of all keys



Some Interesting PGP Key Statistics

Source: http://pgp.cs.uu.nl/ and http://pgp.cs.uu.nl/plot/

- The graph below shows 05/2013 distribution of degree (number of signatures per key) using a log/log scale.
- the red points show the raw degree/count scatter graph
- the blue points show the average degree per count (level)
- the smooth green line follows the blue points
- The graph is very typical for a social network exhibiting the small world phenomenon, a scale-free network.



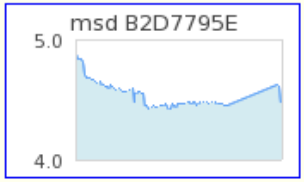
Some Interesting PGP Key Statistics

using: PGP pathfinder & key statistics

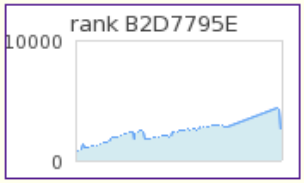
PGP key statistics : Philip R. Zimmermann <prz.at.mit.edu>

PGP KEY pathfinder & statistics

B2D7795E - Philip R. Zimmermann <prz.at.mit.edu>



↑ click for more details ↓



trust paths :

from B2D7795E to [ ] trust paths reset

from [ ] to B2D7795E trust paths reset

see also :

- key statistics in the wotsap analysis by Jörgen Cederlöf
- look up Philip R. Zimmermann on Google

- analysis of the strong set in the PGP web of trust
- FAQs about the PGP pathfinder and key statistics

statistics :

signatures	53
keys signed	1
mean shortest distance (msd)	4.4712
msd ranking	2580

dist	#keys	×
1	53	53
2	914	1828
3	8817	26451
4	19026	76104
5	12704	63520
6	5070	30420
7	1882	13174
8	749	5992
9	303	2727
10	102	1020
11	52	572
12	21	252
13	7	91
14	2	28
total	49702	222232
msd	222232 / 49702	

signatures : 53

- trust paths -> 6F0A2725 stats Allen M. Juinio <aj7845.at.att.com>
- trust paths -> 7E7EC86E stats Andrew Cundiff <andrew.at.cundiff.me.uk>
- trust paths -> F491BD21 stats Ben Wise <bwise.at.alum.mit.edu>
- trust paths -> 24DEF83E stats Bradley Carl Bielenberg <bcbi.at.deakin.edu.au>
- trust paths -> 34A4425C stats Darren Brooker <darren.brooker.at.t-mobile.co.uk>
- trust paths -> D1C4C350 stats Darren John Brooker <darren.at.djbrooker.com>
- trust paths -> 044584B5 stats Douglas Swiggum <Swiggum.at.Waisman.Wisc.Edu>
- trust paths -> 7B2B623A stats Dream Catcher aka BlowFish <3blowfish.at.gmail.com>
- trust paths -> CC1ACD05 stats Eddie Roosenmaallen <eddie.at.roosenmaallen.com>
- trust paths -> BA886915 stats Elliptical <elliptical.at.sympatico.ca>
- trust paths -> 5FFA5B44 stats Elliptical <elliptical.at.sympatico.ca>
- trust paths -> 1511EDF8 stats Enoch Ko <chempilot.at.yahoo.com>
- trust paths -> 3CA3496C stats Fr[illegible]d[illegible]ric POTTER <frederic.at.potter.fr>

PGP Key Rings

Each PGP user has a pair of key rings:

- public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - For the keys of other users, for each key track:
    - user id: e-mail address, name, address, etc.
    - public key
    - timestamp: date when key was generated
    - key ID
    - key legitimacy
    - signatures
- private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase

Security of private keys thus depends on the pass-phrase security

Source: Stallings

PGP Key Rings

Private Key Ring

Used for indexing

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
Ti	PU_i mod 2^{64}	PU_i	E(H(P_i), PR_i)	User i
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

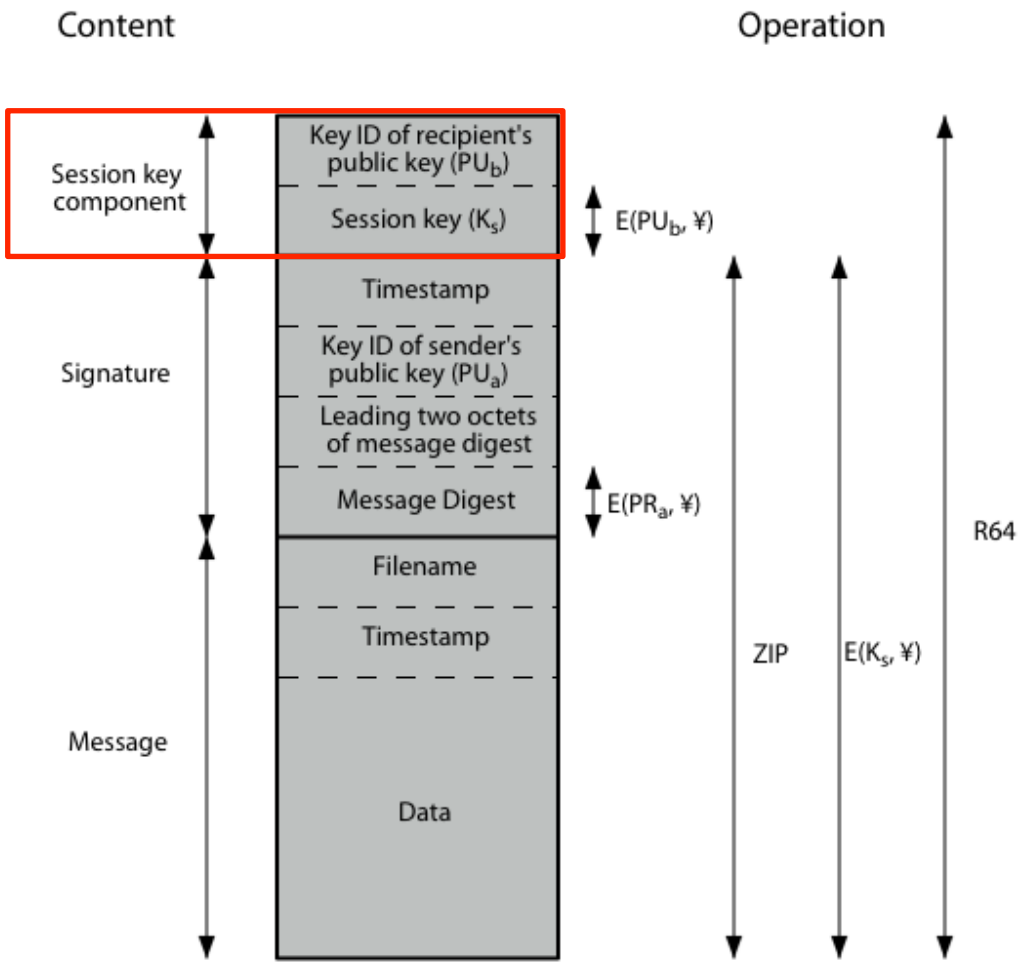
Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
Ti	PU_i mod 2^{64}	PU_i	$trust\_flag_i$	User i	$trust\_flag_i$		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

* = field used to index table

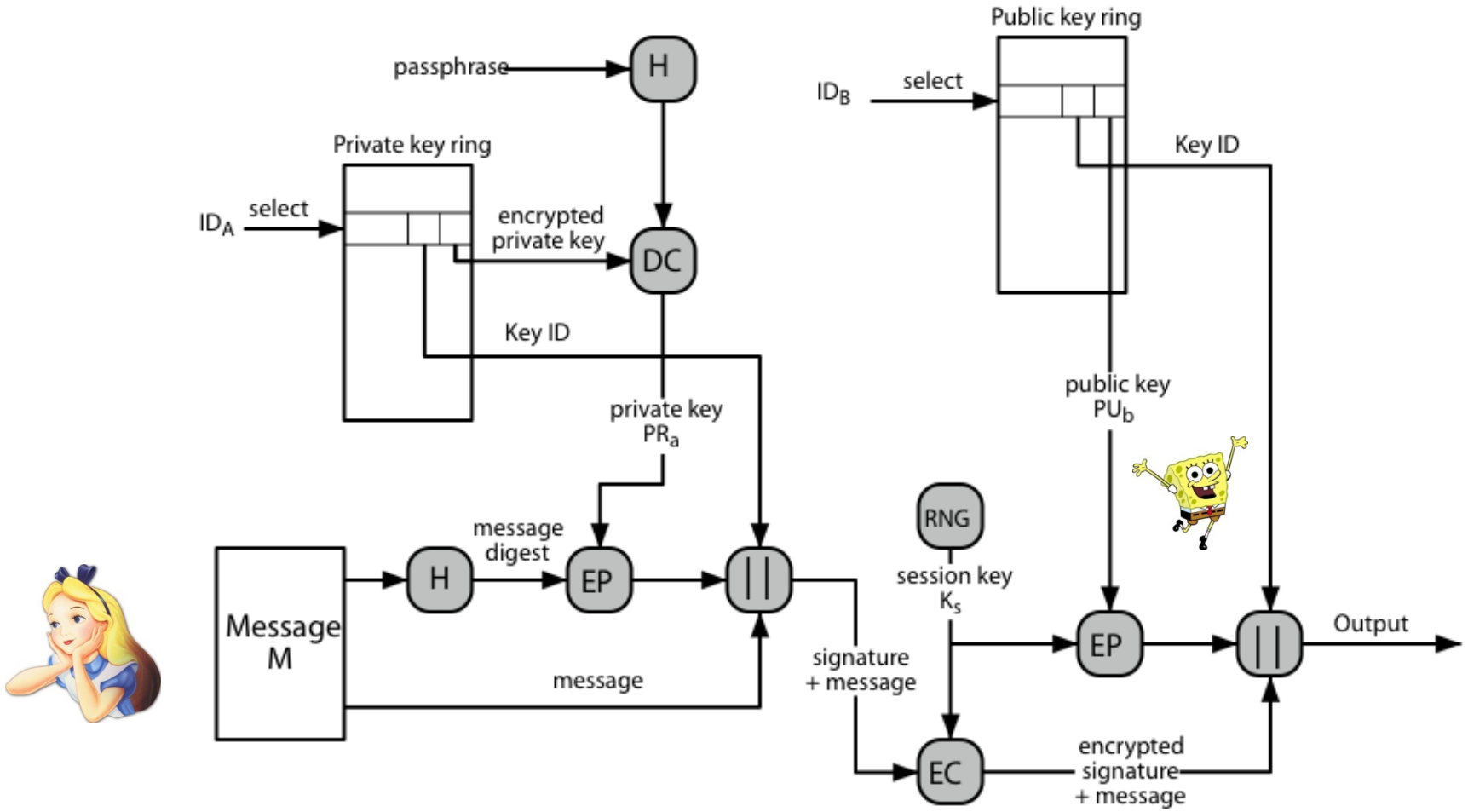
Source: Stallings

PGP Message Format



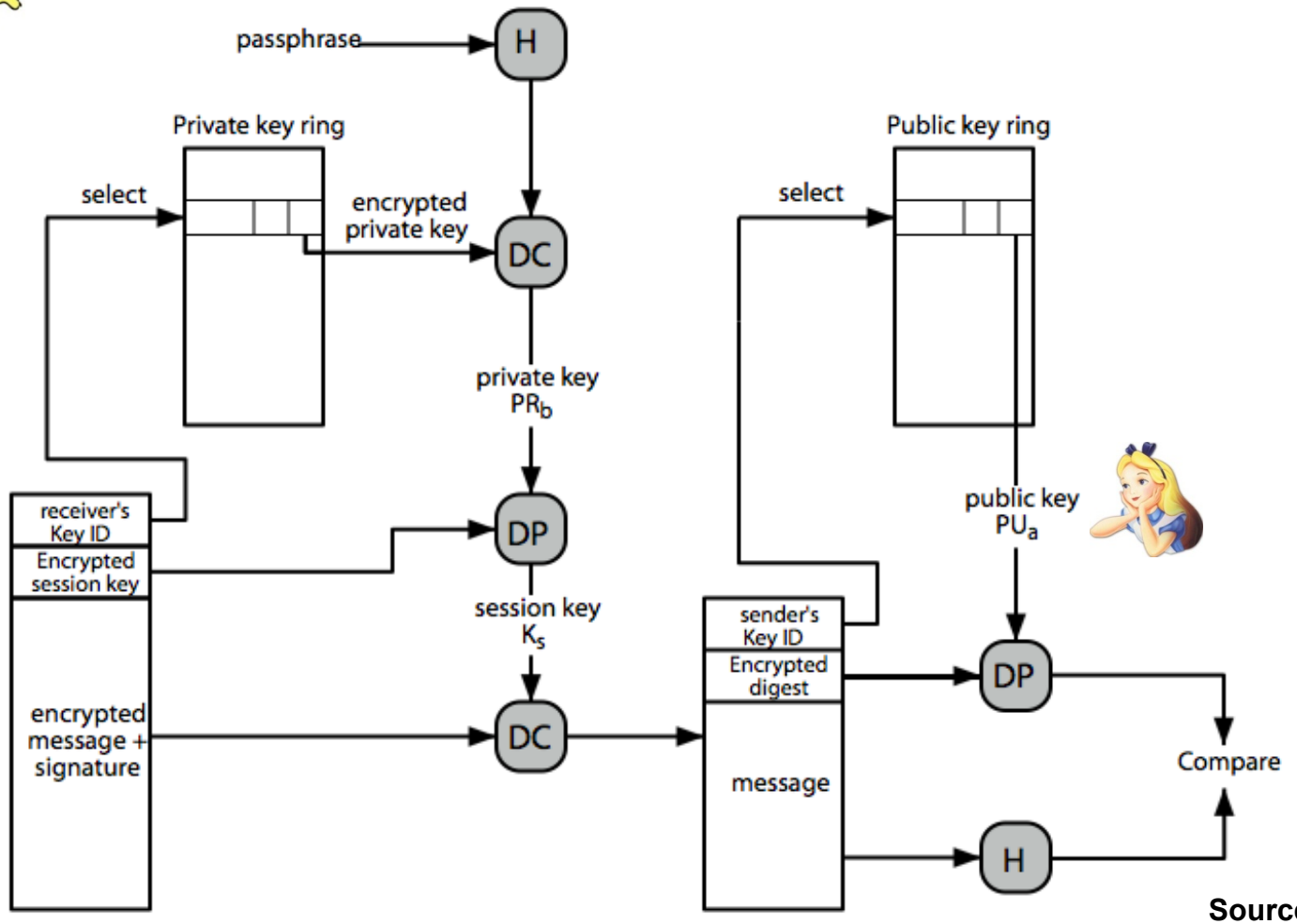
Source: Stallings

Role of Keyring in PGP Message Generation



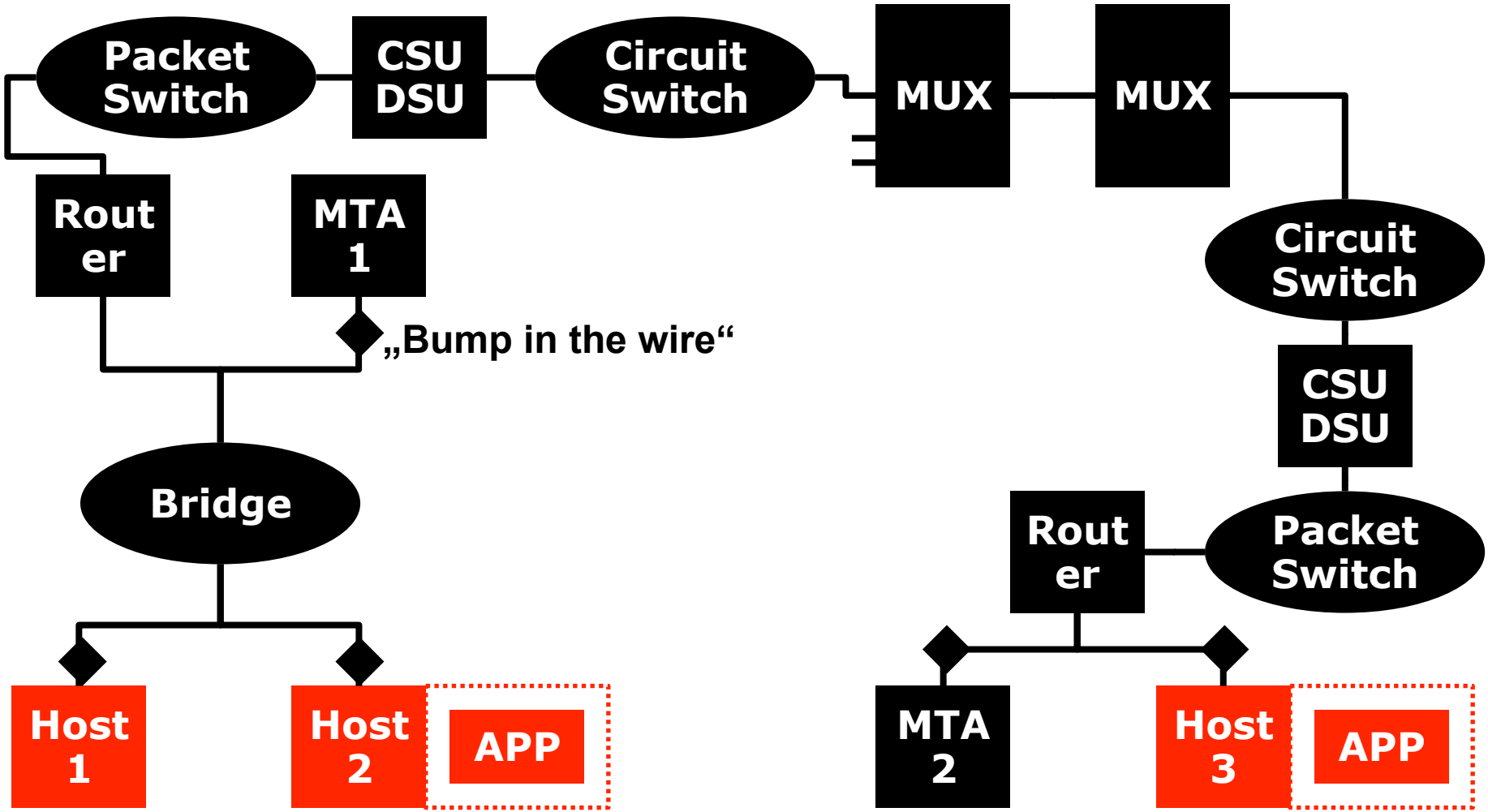
Source: Stallings

Role of Keyring in PGP Message Reception



Source: Stallings

Summary:
L5 Scope of Protection



Summary: Application Layer Security

SECURE MOBILE NETWORKING

Characteristics:

- No network technology dependence
- Significant application dependence (per-application or common API); protocol suite dependence?

Protection

- Black (data protected):
  - circuits & muxes, circuit & packet switches, LANs & bridges, routers, and MTAs!
- Protection granularity: users, applications, PDUs

Security services:

- confidentiality (connection-oriented, connectionless, or selective field)
- data origin authentication, peer entity authentication
- integrity (connection-oriented, connectionless, optional recovery)
- non- repudiation (originator and recipient)

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Some slides courtesy of G. Schäfer (TU Ilmenau) with changes of J. Schmitt (TU Kaiserslautern) and myself incorporated
- Some other slides courtesy of R. Perlman, S. Kent, K. Ross, Y. Chen, W. Stallings (and partners); changes of myself incorporated

Recommended reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-13-046019-6
- [Stallings2014] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2014, ISBN: 978-0-136-10805-4
- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

Copyright Notice

This document has been distributed by the contributing authors as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that they have offered their works here electronically.

It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may not be reposted without the explicit permission of the copyright holder.

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de