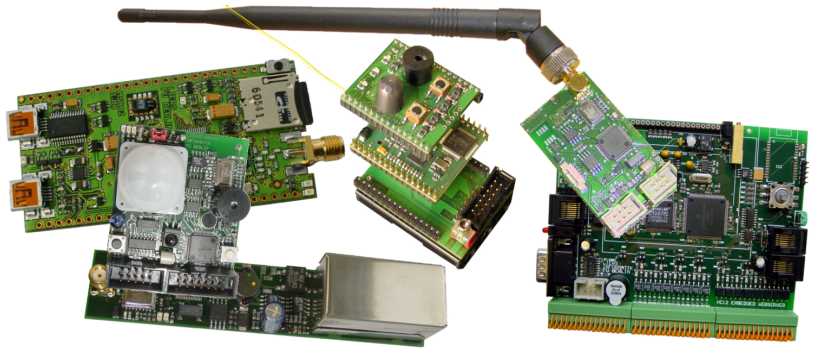


19531 - Telematics

13th Tutorial - Application Layer Protocols

Bastian Blywis

Department of Mathematics and Computer Science
Institute of Computer Science
03. February, 2011

Outline

1. TCP Checksum
2. DNS, SMTP, POP3, IMAP
3. E-Mail
4. DNS Infrastructure
5. Asymmetric Key Cryptography
6. Cryptographically Generated Addresses (CGA)
7. Simple Network Management Protocol (SNMP)
8. Cookies

TCP Checksum

The TCP header contains a checksum field.

1. What algorithm is applied?
2. Which ”parts” of the TCP segment are protected by the checksum?
3. Why does the approach violate the principles of a layered network architecture and why is the violation necessary?

TCP Checksum

1. TCP uses the Internet checksum algorithm like IPv4 and UDP
2. Checksum is calculated over pseudo header, TCP header, and data
3. Mixes network and transport layer data

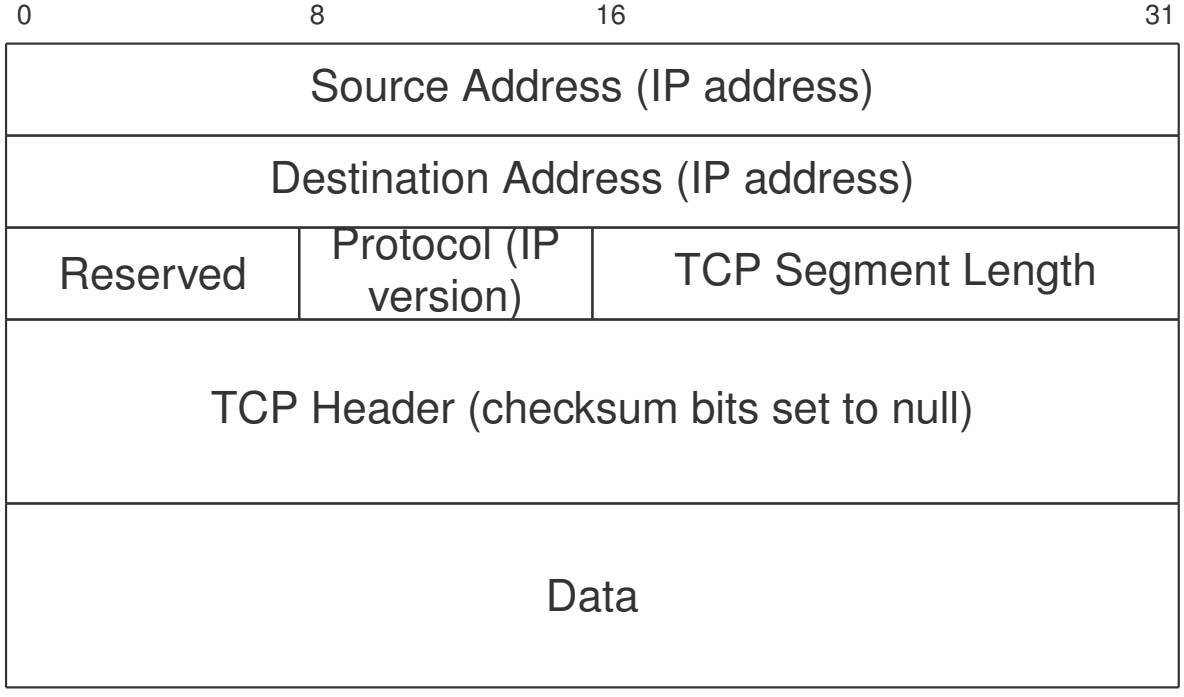


Figure: Relevant parts for the TCP checksum calculation

1. Explain the differences between SMTP, POP3, and IMAP.
2. Let's consider user Bob wants to send an email to user Alice. In order to establish a connection with the SMTP server, the server's name has to be resolved into an IP address by DNS. Explain which messages are exchanged and between which hosts when recursive name resolution is used. Assume that only the name server responsible for the domain `server.org` can answer the request.
3. Now it is Alice's turn to reply to Bob. Explain which messages are exchanged when using iterative name resolution. Assume that only the name server responsible for the domain `server.org` can answer the request.
4. Explain how Bob's SMTP server finds the MTA responsible for accepting email messages on behalf of Alice.

	Bob	Alice
IP address:	192.45.56.127	208.115.92.45
Name server:	192.47.56.2	208.115.92.2
SMTP server:	`mail.server.org`	`mail.server.org`
Email Address:	`bob@realword.org`	`alice@wonderland.org`

Post Office Protocol (POP3) – used to access and extract e-mail from a mailbox, 3 states:

- Authorization
  - User has to provide credentials
  - Commands: USER, PASS
- Transaction
  - Download of messages
  - Commands: STAT, LIST, RETR, DELE, QUIT
  - No selection of individual messages
- Update
  - Update of states, e.g., deletion of emails
  - Termination

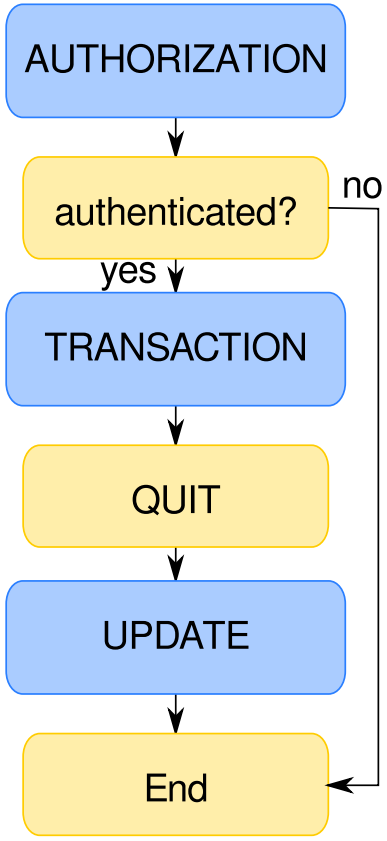


Figure: POP3 State Machine

Internet Message Access Protocol (IMAP) – protocol used to transfer e-mail messages between user's mailbox and an agent, 4 states:

- Not authenticated
  - User has to provide credentials
  - Connection can also be pre-authenticated
  - Commandos: AUTHENTICATE, LOGIN
- Authenticated
  - Management of mailboxes
  - Commandos: SELECT, EXAMINE, CREATE, DELETE, RENAME, SUBSCRIBE, UNSUBSCRIBE, LIST, LSUB, STATUS, and APPEND
- Selected
  - Management of messages
  - Commando: CHECK, CLOSE, EXPUNGE, SEARCH, FETCH, STORE, COPY, and UID
  - Selection of individual messages, can support flagging and filtering
- Logout
  - Server shutdown or connection closed with LOGOUT

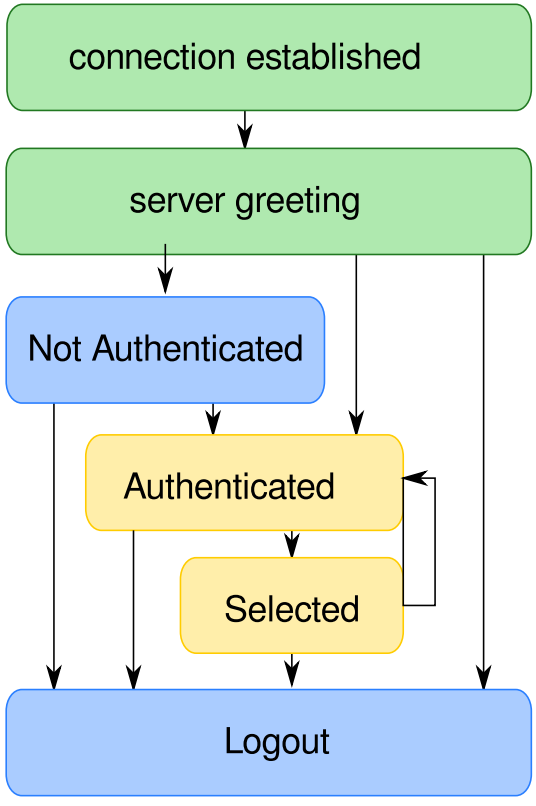


Figure: IMAP State Machine

Simple Mail Transfer Protocol (SMTP)– standard for transferring electronic mail messages from one machine to another ('sending mails')

- Protocol to connect MTAs
- No checksum, no encryption
- Commandos: HELO, MAIL FROM, RCPT TO, DATA, QUIT

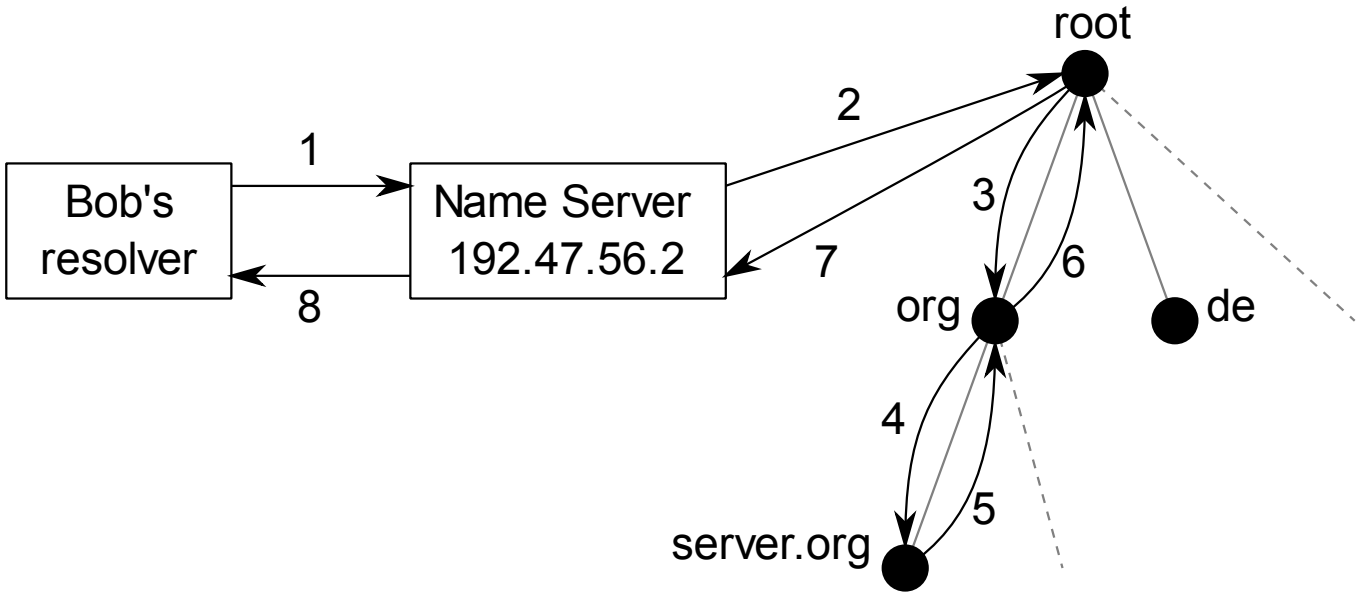
```
$ telnet localhost 25
Trying ::1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 belgrad.imp.fu-berlin.de ESMTP Postfix (Ubuntu)
EHLO belgrad.imp.fu-berlin.de
250-belgrad.imp.fu-berlin.de
250-PIPELINING
250-SIZE 10240000
(...)
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: root@belgrad.imp.fu-berlin.de
250 2.1.0 Ok
RCPT TO: blywis@inf.fu-berlin.de
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hello World
.
250 2.0.0 Ok: queued as B4E5CCCCD7
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Notes

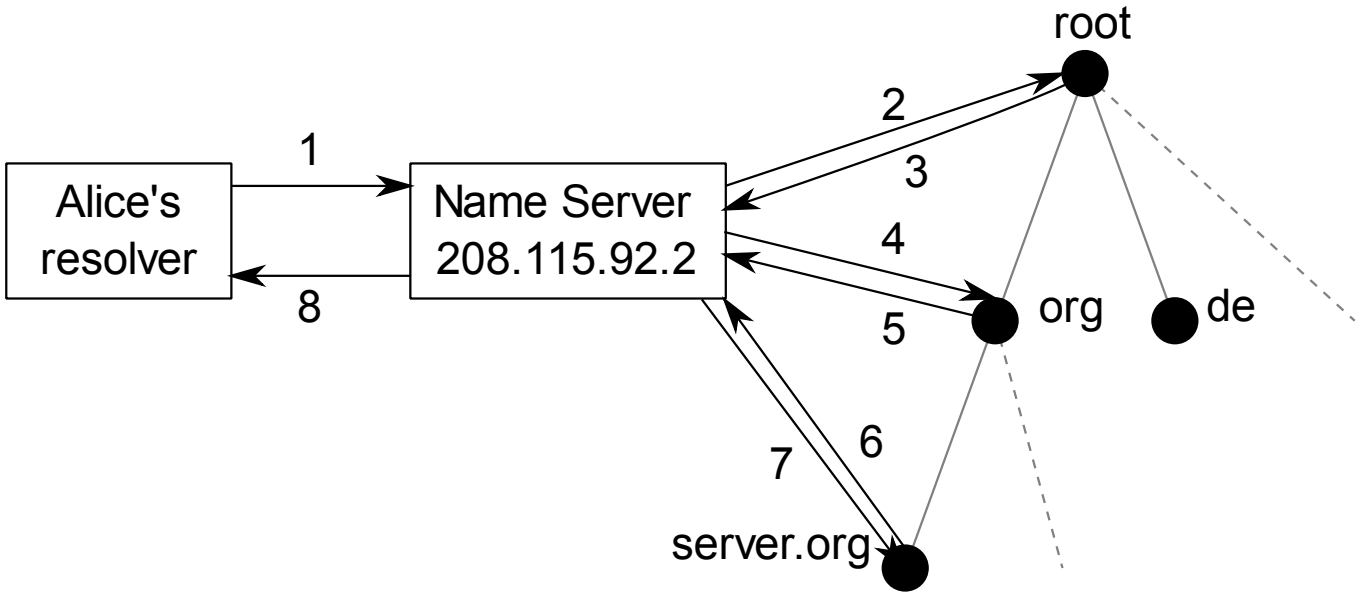
- Many application layer protocols are human-readable ASCII protocols
- You can try to “speak” the protocols yourself with telnet
- Try to capture some packets containing specific strings using `ngrep` or similar tools

```
$ sudo ngrep -d eth0 -i password
interface: eth0 (160.45.112.0/255.255.255.0)
match: password
##########################################################
T 160.45.112.24:35796 -> 216.34.181.45:80 [AP]
  GET /search.pl?query=password HTTP/1.1..Host: slashdot.org..Connection: keep-
  alive..Referer: http://slashdot.org/..Accept:application/xml,
  application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
  q=0.5..User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US) AppleWebKit/
  534.10 (KHTML, like Gecko) Ubuntu/10.10 Chromium/8.0.552.224 Chrome/
  8.0.552.224 Safari/534.10..Accept-Encoding: gzip,deflate,sdch..Acce
  pt-Language: en-US,en;q=0.8,de;q=0.6..Accept-Charset:ISO-8859-1,utf-8;
  q=0.7,*;q=0.3..Cookie: __utmz=9273847.1295944481.1.1.utmcsr=google|
  utmccn=(organic)|utmcmd=organic|utmctr=slashdot; __utma=9273847.124450
  2582.1295944481.1295944481.1295944481.1; __utmc=9273847;
 __utmb=9273847.2.10.1295944481....
##########################
```

Recursive DNS resolution:



Iterative DNS resolution:



Explain how Bob's SMTP server finds the MTA responsible for accepting email messages on behalf of Alice.

Bob's SMTP server resolves the MX record of wonderland.org. The MX record refers to a mail server responsible for accepting email messages on behalf of a recipient's (Alice's) domain.

```
$ nslookup
> set querytpe=mx
> fu-berlin.de

fu-berlin.de    MX preference = 10, mail exchanger = mail.fu-berlin.de

mail.fu-berlin.de       internet address = 130.133.4.67
```

1. Inspect the full email header of a message, which you have received and discuss the contents.
2. Can you approximate when the message was actually sent?
3. How are attachments transfered?

```
Return-path: <des-bounces+blywis=inf.fu-berlin.de@lists.spline.inf.fu-berlin.de>
Delivery-date: Mon, 24 Jan 2011 13:26:22 +0100
Received: from deliver1.zedat.fu-berlin.de ([130.133.4.79])
        by mbox5.zedat.fu-berlin.de (Exim 4.69)
        for blywis@zedat.fu-berlin.de with esmtp
        (envelope-from <des-bounces+blywis=inf.fu-berlin.de@lists.spline.inf.fu-berlin.de>)
        id <1PhLV0-0000C3-GH>; Mon, 24 Jan 2011 13:26:22 +0100
(...)
Received: from belgrad.imp.fu-berlin.de ([160.45.111.22] helo=belgrad.localnet)
        by inpost2.zedat.fu-berlin.de (Exim 4.69)
        for des@lists.spline.inf.fu-berlin.de with esmtpsa
        (envelope-from <blywis@zedat.fu-berlin.de>)
        id <1PhLUA-0003SO-1t>; Mon, 24 Jan 2011 13:25:30 +0100
From: Bastian Blywis <blywis@zedat.fu-berlin.de>
To: des@lists.spline.inf.fu-berlin.de
Date: Mon, 24 Jan 2011 13:25:24 +0100
User-Agent: KMail/1.13.5 (Linux/2.6.35-24-generic; KDE/4.5.1; x86_64; ; )
MIME-Version: 1.0
Message-Id: <201101241325.28103.blywis@zedat.fu-berlin.de>
Subject: [DES] Testbed Problems
X-BeenThere: des@lists.spline.inf.fu-berlin.de
X-Mailman-Version: 2.1.11
Precedence: list
Reply-To: blywis@inf.fu-berlin.de, Distributed Embedded Systems Mailing List
        <des@lists.spline.inf.fu-berlin.de>
```

```
List-Id: Distributed Embedded Systems Mailing List
        <des.lists.spline.inf.fu-berlin.de>
List-Unsubscribe: <https://lists.spline.inf.fu-berlin.de/mailman/options/des>,
        <mailto:des-request@lists.spline.inf.fu-berlin.de?subject=unsubscribe>
List-Archive: <https://lists.spline.inf.fu-berlin.de/mailman/private/des>
List-Post: <mailto:des@lists.spline.inf.fu-berlin.de>
List-Help: <mailto:des-request@lists.spline.inf.fu-berlin.de?subject=help>
List-Subscribe: <https://lists.spline.inf.fu-berlin.de/mailman/listinfo/des>,
        <mailto:des-request@lists.spline.inf.fu-berlin.de?subject=subscribe>
Content-Type: multipart/mixed; boundary="===============0298841459=="
Sender: des-bounces@lists.spline.inf.fu-berlin.de
Errors-To: des-bounces+blywis=inf.fu-berlin.de@lists.spline.inf.fu-berlin.de
X-Originating-IP: 130.133.110.77
X-ZEDAT-Hint: A/A
X-purgate: clean
X-purgate-type: clean
X-purgate-ID: 151147::1295871942-00000C13-B8D6576E/0-0/0-0
X-Bogosity: Ham, tests=bogofilter, spamicity=0.000000, version=1.2.2
X-Spam-Flag: NO
X-Spam-Checker-Version: SpamAssassin 3.0.4 on Algerien.ZEDAT.-Berlin.DE
X-Spam-Status: No, score=0.0 required=8.0 tests=FORGED_RCVD_HELO,
        SPF_HELO_PASS,SPF_PASS
X-Length: 7579
X-UID: 27558
```

Multipurpose Internet Mail Extensions (MIME)

- Email is specified for 7-bit ASCII text, see RFC 2822
- MIME enables
  - Special characters
  - Attachments
- MIME defines
  - Structures in the message body (additional headers)
  - Coding rules for non-ASCII characters
- Content transfer encodings (depends on server support)
  - 7bit
  - quoted-printable
  - base64
  - 8bit
  - binary

Levinson *The MIME Multipart/Related Content-type*
RFC 2387, 1998

```
--Boundary-00=_QTEwGFbtpng199H
Content-Type: application/x-executable;
  name="notebook.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="notebook.pdf"

JVBERi0xLjQNJeLjz9MNCjE0IDAgb2JqDTw8L0xpbmVhcml6ZWQgMS9MIDIyMjQ4L08gMTYvRSAx
Mzc2Mi9OIDIvVCAyMTkyMS9IIFsgNzc2IDIyNV0+Pg1lbmRvYmoNICAgICAgICAgICAgICAgICAg
DQp4cmVmDQoxNCAyNA0KMDAwMDAwMDAxNiAwMDAwMCBuDQowMDAwMDAxMDAxIDAwMDAwIG4NCjAw
MDAwMDEwODEgMDAwMDAgbg0KMDAwMDAwMTIxMSAwMDAwMCBuDQowMDAwMDAxNDU5IDAwMDAwIG4N
CjAwMDAwMDE4NzUgMDAwMDAgbg0KMDAwMDAwMjYzNCAwMDAwMCBuDQowMDAwMDAzMTg4IDAwMDAw
IG4NCjAwMDAwMDMyMzIgMDAwMDAgbg0KMDAwMDAwMzQ3NSAwMDAwMCBuDQowMDAwMDAzNjk3IDAw
MDAwIG4NCjAwMDAwMDM5MjUgMDAwMDAgbg0KMDAwMDAwNDAwMiAwMDAwMCBuDQowMDAwMDA2NTQ5
IDAwMDAwIG4NCjAwMDAwMDY1ODQgMDAwMDAgbg0KMDAwMDAwNjcxOCAwMDAwMCBuDQowMDAwMDA2
ODU1IDAwMDAwIG4NCjAwMDAwMDk1NDggMDAwMDAgbg0KMDAwMDAwOTcwMSAwMDAwMCBuDQowMDAw
```

1. Discuss the vulnerability of DNS.
   - Read the fact sheet issued by the ICANN regarding an attack on the DNS root servers in 2007: Download
   - Additionally, read the (nicely illustrated) article “An Illustrated Guide to the Kaminsky DNS Vulnerability”.
2. What is a DNS amplification attack?
3. Why are we so dependent on DNS?

Discuss!

DNS amplification attack

- Distributed Denial of Service (DDoS) attack
- Abuses recursive DNS servers that accept non-local requests
- Uses spoofed UDP packets
- Small requests can generate large replies (factor ≈ 70)
- DNS servers originally generated only up to 512 byte UDP packets . . . this was changed in RFC 2671

Attack

1. Get botnet or similar infrastructure
2. Generate DNS requests with spoofed source address (victim)
3. Sent request to DNS server(-s) and specify large UDP payload buffer
4. Victim will experience DDoS attack due to many large DNS replies

Vaughn and Evron *DNS Amplification Attacks*
March 17, 2006

DNS Dependence

- DNS is vital for the function of the Internet: Do you know the IP for www.fu-berlin.de???
- Humans do not want to remember four octets (what about IPv6?)
- Domain names are important to enable mobile hosts (decouple locator and identifier)
- DNS is used to distribute Internet traffic geographically
- DNS enables email, can support asymmetric cryptography systems, etc

There are several DNS related attacks! DNSSEC will be one of the most important security topics of the next 5 years.

Discuss public-private key encryption.

1. Explain the difference between symmetric and asymmetric encryption.
2. Discuss the role of the public and private key to implement *encryption* and *authentication*.
3. What is the basic idea of a digital signature?

There are two general approaches for crypto systems:

Symmetric Sender and receiver share the same key.

Public-key Two different but mathematically related keys are used to implement encryption and authentication: a public and a private key.

Encryption: Public key ciphers, private key deciphers
Authentication: Public key deciphers, private key ciphers

A digital signature is used to verify the authenticity of a digital message or document, i.e., that the document was created by a known sender. Typically, the sender hashes the data and ciphers the hash using its private key (signature).

Problem: Can do you trust the public keys and where do you get them from?

- Message Digest 5 (MD5): hashing algorithm
- Rivest, Shamir, Adleman (RSA): public key cryptography (asymmetric)
- International Data Encryption Standard (IDEA): symmetric key cryptography

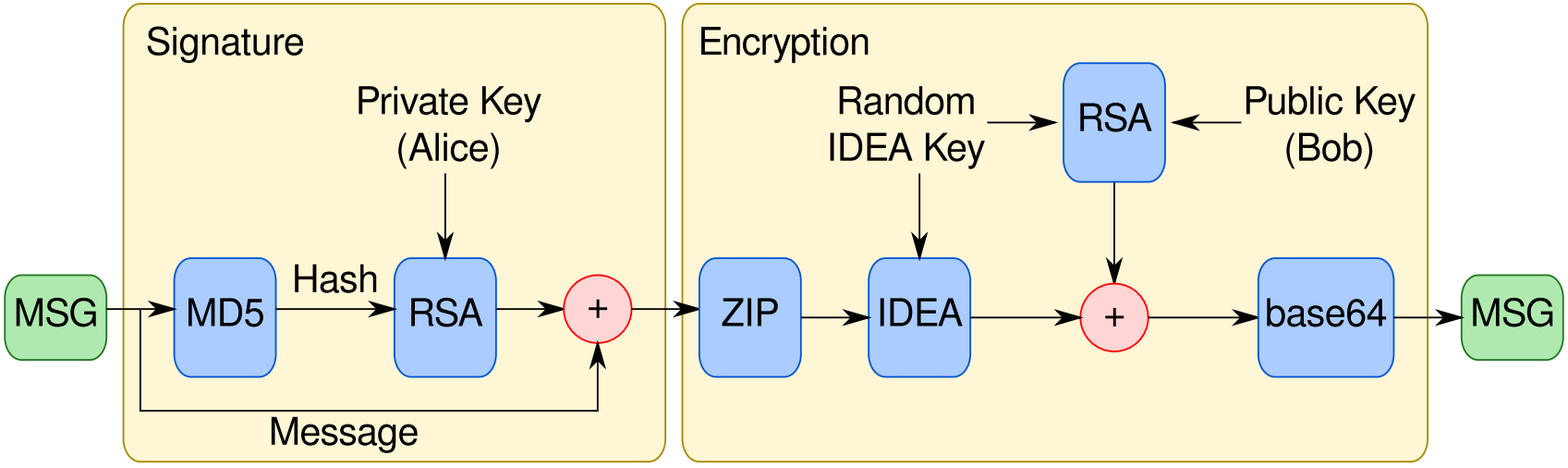


Figure: PGP Example

Read and discuss RFC 3972.

1. Why is a network layer address authentication important?
2. How can you implement an autonomous, self–consistent address authentication?

- Someone can claim to be the owner of your IP address, e.g., ARP or NDP address resolution
- Problem: Mechanism required to ensure that you are the owner of an IP address
- Requirement: Mechanism should work without a certification authority or any security infrastructure

Idea of Cryptographically Generated Addresses (CGA)

- Use a cryptographic identifier as address
- Host generates public/private key pair
- Interface identifier is based on the (hash of) public key
- Public key (+parameters) will be attached to the message
- Binding between the public key and the address can be verified by re-computing the hash value and by comparing the hash with the interface identifier
  $\Rightarrow$ Self-consistent authentication of source address without dedicated infrastructure
- IP address created this way is called cryptographically generated address (CGA)
- Message is signed by the corresponding private key
- CGAs does not work for IPv4 (address length too short)

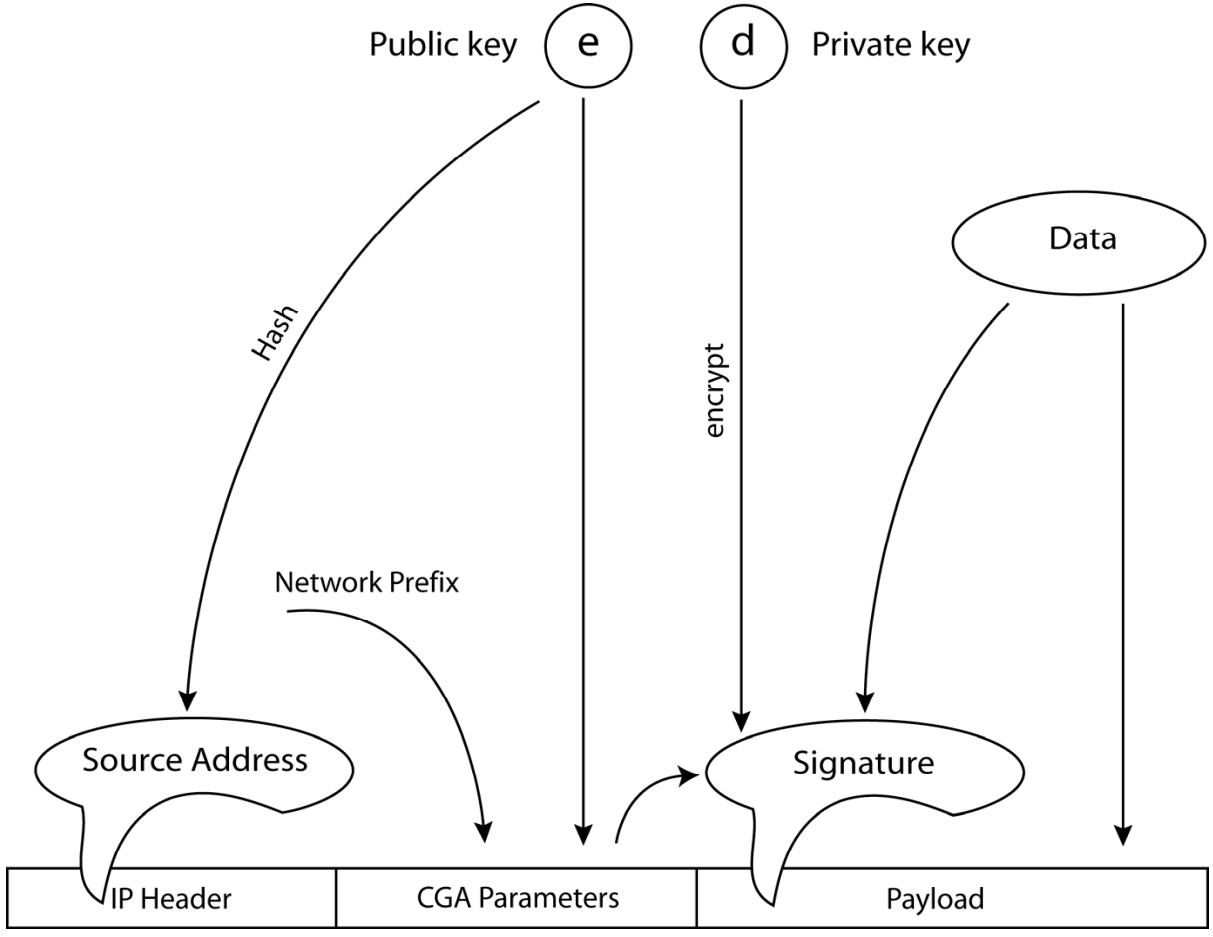


Figure: CGA Encapsulation

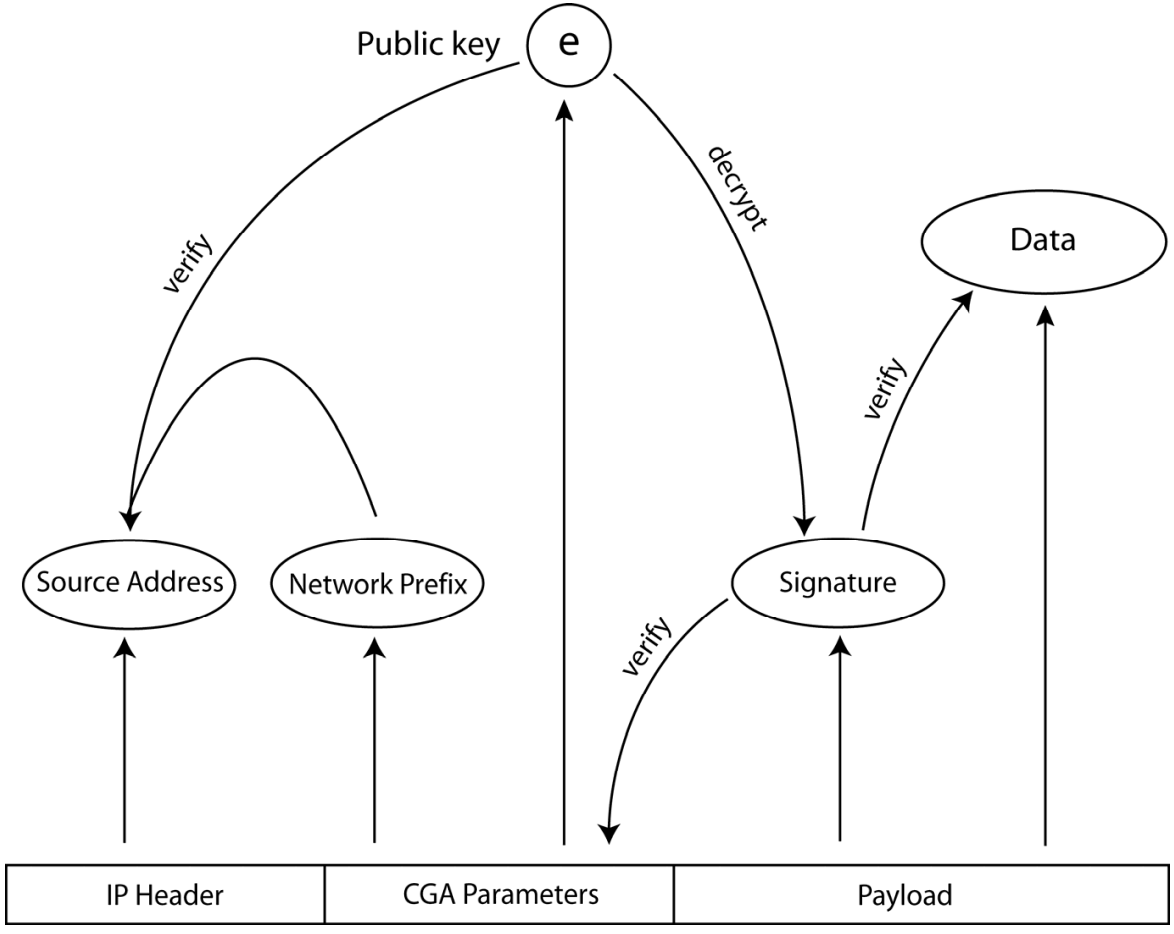


Figure: CGA Decapsulation

1. Which device specific information are mutually available to both the SNMP agent and SNMP management system? How is this information encoded?
2. Explain the difference between *public* and *private* MIB.
3. What is the most important improvement of SNMPv3 in contrast to previous versions?
4. Explain how you can identify the port that a host is connected with on an SNMP capable switch.

Background

- Management Information Base (MIB) specifies a set of variables a managed device must have, operations, and description
- You need an information model: objects to represent specific resources need to be identical on all systems

Solution

- Structure of Management Information (SMI) specifies a set of rules to define and identify MIB variables
  - Generic type: Managed Object
  - Generic data structure: 2-dimensional table
  - SMI standard includes definitions of terms like *IPAddress* (defining it to be a 4-octet string)

Differences between public and private MIB:

Public MIB specifies generic resources, e.g., interface table which may also depend on the device type, e.g., switch

Private MIB specifies vendor and device specific resources

Fundamental improvement of SNMPv3 in contrast to previous versions:

- SNMPv3 = SNMPv2 + Security + Administration
- Provides user-based security model: Authentication & Encryption
- View-based access control enables access rights to MIB
- Backward compatible to SNMPv1 and SNMPv2

Identifying the port that a host is connected with on an SNMP capable switch

- Each switch maintains a forwarding database (“bridge table”)
- There is a public bridge MIB (RFC 4188) for managing MAC bridges based on the IEEE 802.1D-1998 standard
- The forwarding database for transparent bridging is defined in `....mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTable` (1.3.6.1.2.1.17.4.3)

Cookies

Read and discuss Michal Zalewski's article HTTP cookies, or how not to design protocols.

1. Why are cookies required?
2. What is so critical about cookies and why is there no good specification?

Cookies

- Problem: HTTP is a stateless protocol
- Problem: Several applications require a persistent state
- Solution: Store state in file (cookie) on client's system
- Major Problems:
  - Domain scoping: Who may set a cookie for whom?
  - Size of cookies adds up: Web servers could reject large packets
  - Limited cookie jar size: Deletion of critical cookies possible
  - *secure* and *httponly* cookies: Who may actually read/write these cookies?
  - Non-ASCII characters: Unclear specification
  - Session length
- Current situation: Each browser handles cookies individually

The verdict: Multiple unspecific and too late published RFCs as well as incomplete browser support or browser specific behaviors lead to serious problems.

Application	statefull
HTTP	stateless
TCP	statefull
IP	stateless

Thank you for your attention.

Questions?