

Cybersecurity **E-Mail and Cloud Security**

Kasun De Zoysa

Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka

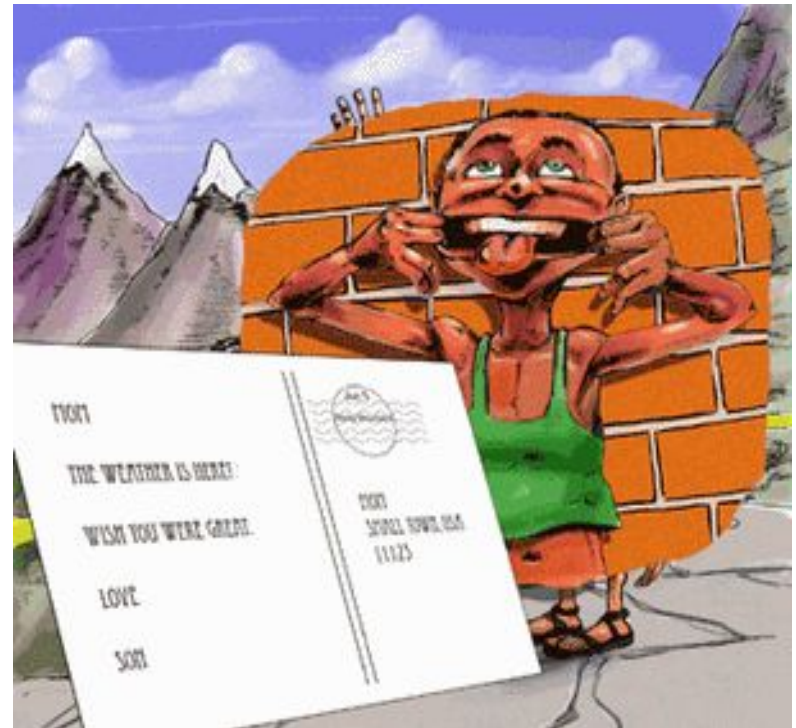
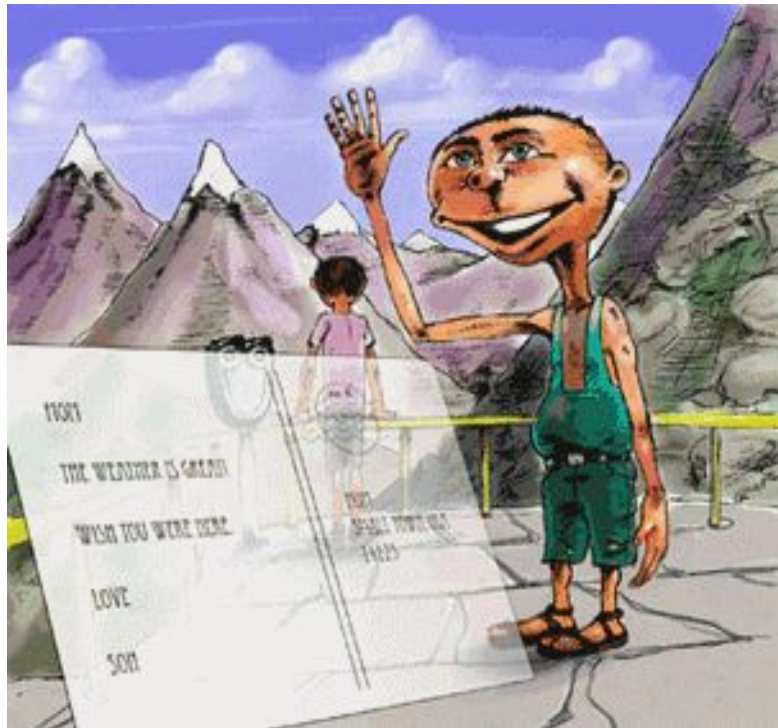
Cybersecurity Wisdom

- **Popular Myth:**
Cybersecurity depends on...
 - firewalls
 - SSL
 - Virus Scanners or IDS
- **Unpopular Reality:**
In a large, Cybersecurity is not achieved by above technologies.



Email is in the Clear

Email – A Postcard Written in Pencil



http://www.cert.org/homeusers/email_postcard.html

E-mail Security

- Pretty Good Privacy (PGP) (www.pgp.com)
 - Philip R. Zimmerman is the creator of PGP.
 - PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
- S/MIME
 - Secure/Multipurpose Internet Mail Extension
 - S/MIME will probably emerge as the industry standard.
 - PGP for personal e-mail security

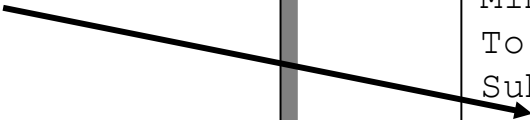


S/MIME
Secure E-Mail for Everyone

MIME content (mixed)

MIME content headers

text/plain
text/richtext
multipart/mixed
multipart/parallel
multipart/alternative
multipart/digest
message/rfc822
message/partial
message/external-body
image/jpeg
image/gif
video/mpeg
audio/basic
application/postscript
application/octet-stream



MIME content headers

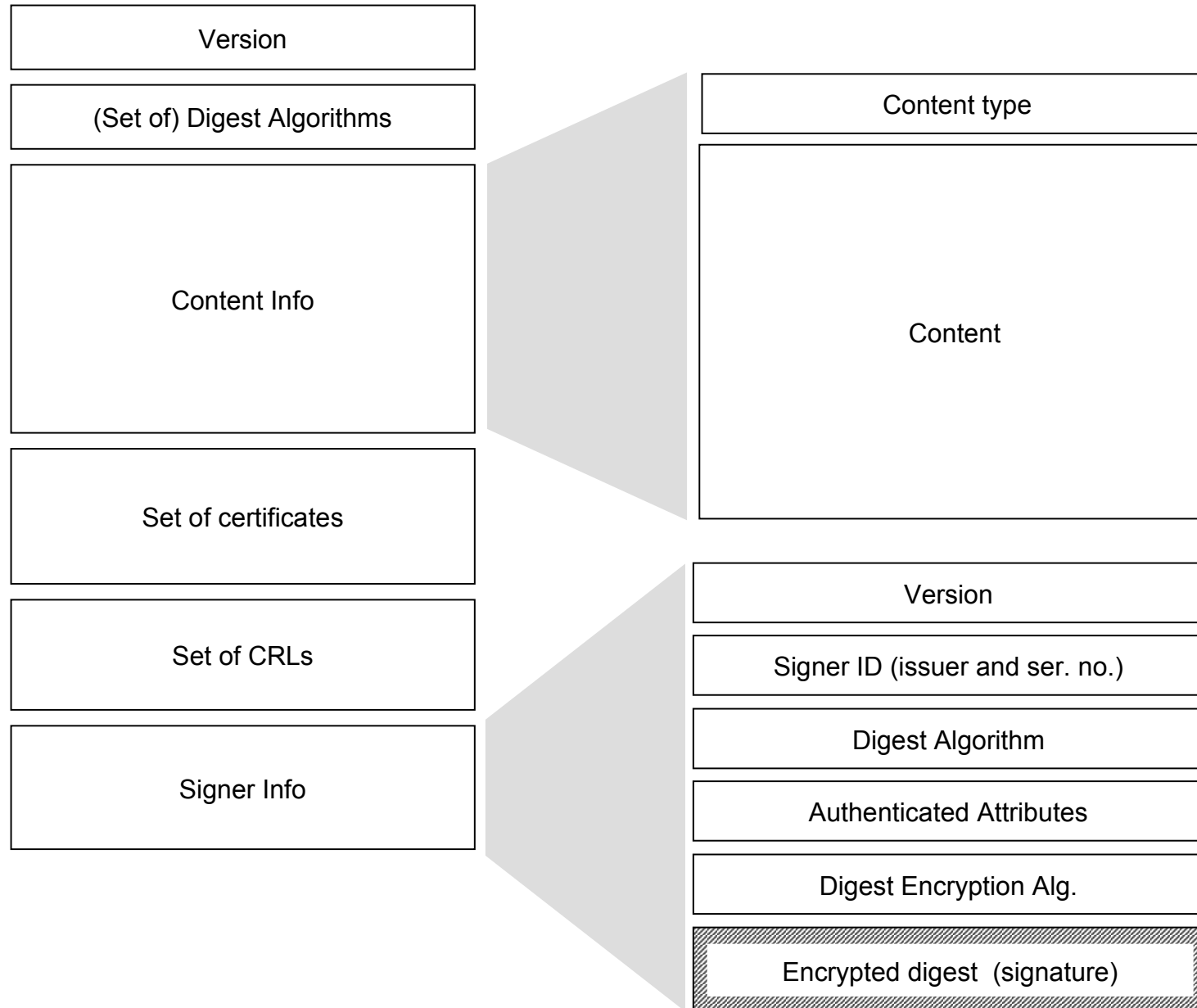
```
From: Dr William Buchanan  
<w.buchanan@napier.ac.uk>  
MIME-Version: 1.0  
To: w.buchanan@napier.ac.uk  
Subject: Any subject  
Content-Type: multipart/mixed;  
boundary="boundary name"  
This part of the message will be ignored.  
-- boundary name  
Content-Type: multipart/mixed;  
boundary="boundary name"  
This is the first mail message part.  
-- boundary name  
And this is the second mail message part.  
-- boundary name --
```

Securing a MIME entity

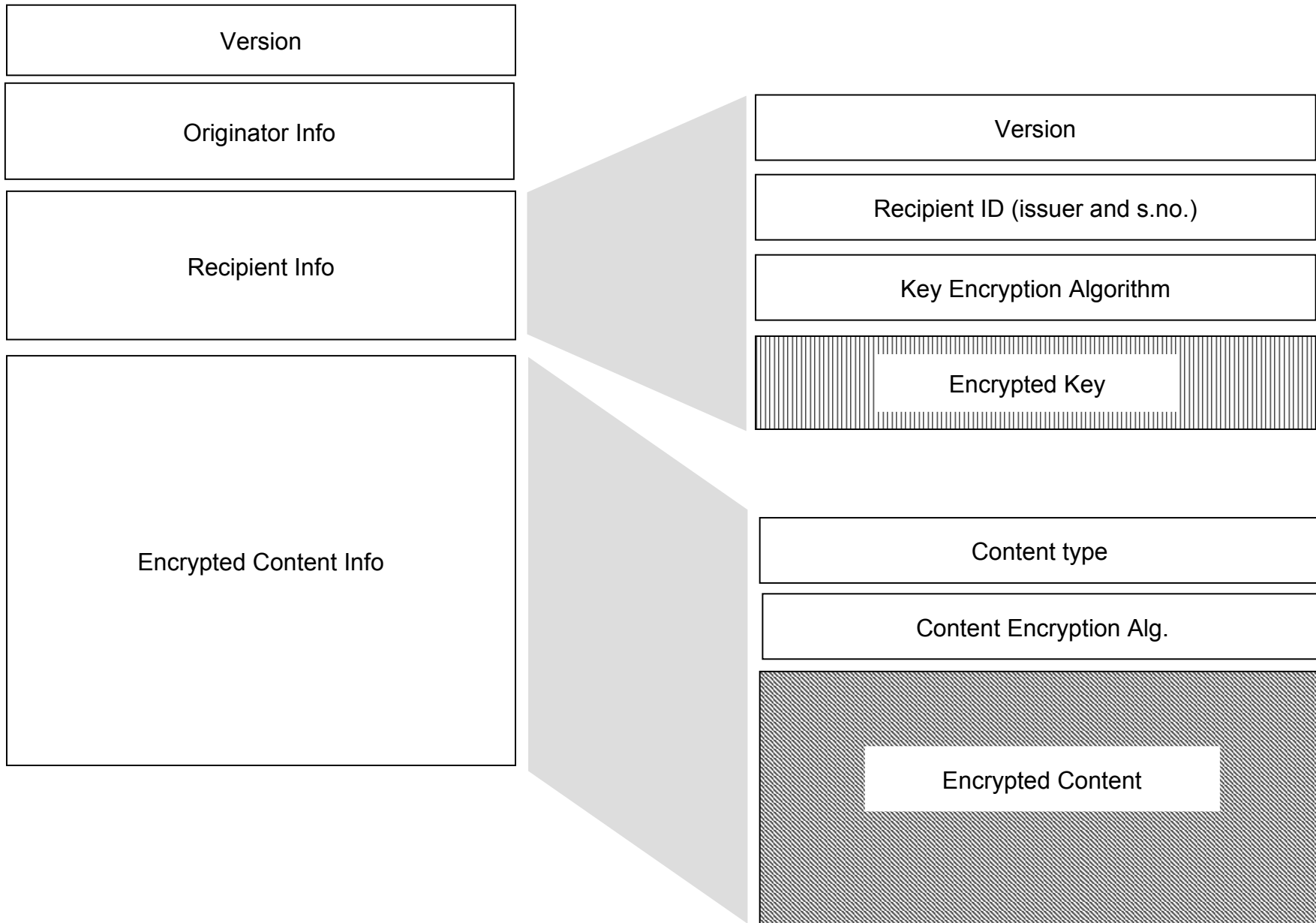
- MIME entity is prepared according to the normal rules for MIME message preparation
- prepared MIME entity is processed by S/MIME to produce a PKCS object
- the PKCS object is treated as message content and wrapped in MIME



PKCS7 “signed data”



PKCS7 “enveloped data”



Enveloped data – Example

Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7m

```
rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6  
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTTrfvbnjT6jH7756tbB9H  
f8HHGTTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4  
0GhIGfHfQbnj756YT64V
```

Clear-signed data – Example

Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha1; boundary=boundary42

--boundary42

Content-Type: text/plain

This is a clear-signed message.

--boundary42

Content-Type: application/pkcs7-signature; name=smime.p7s

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--

S/MIME Functions

- Enveloped Data: Encrypted content and encrypted session keys for recipients.
- Signed Data: Message Digest encrypted with private key of “signer.”
- Clear-Signed Data: Signed but not encrypted.
- Signed and Enveloped Data: Various orderings for encrypting and signing.

User Agent Role

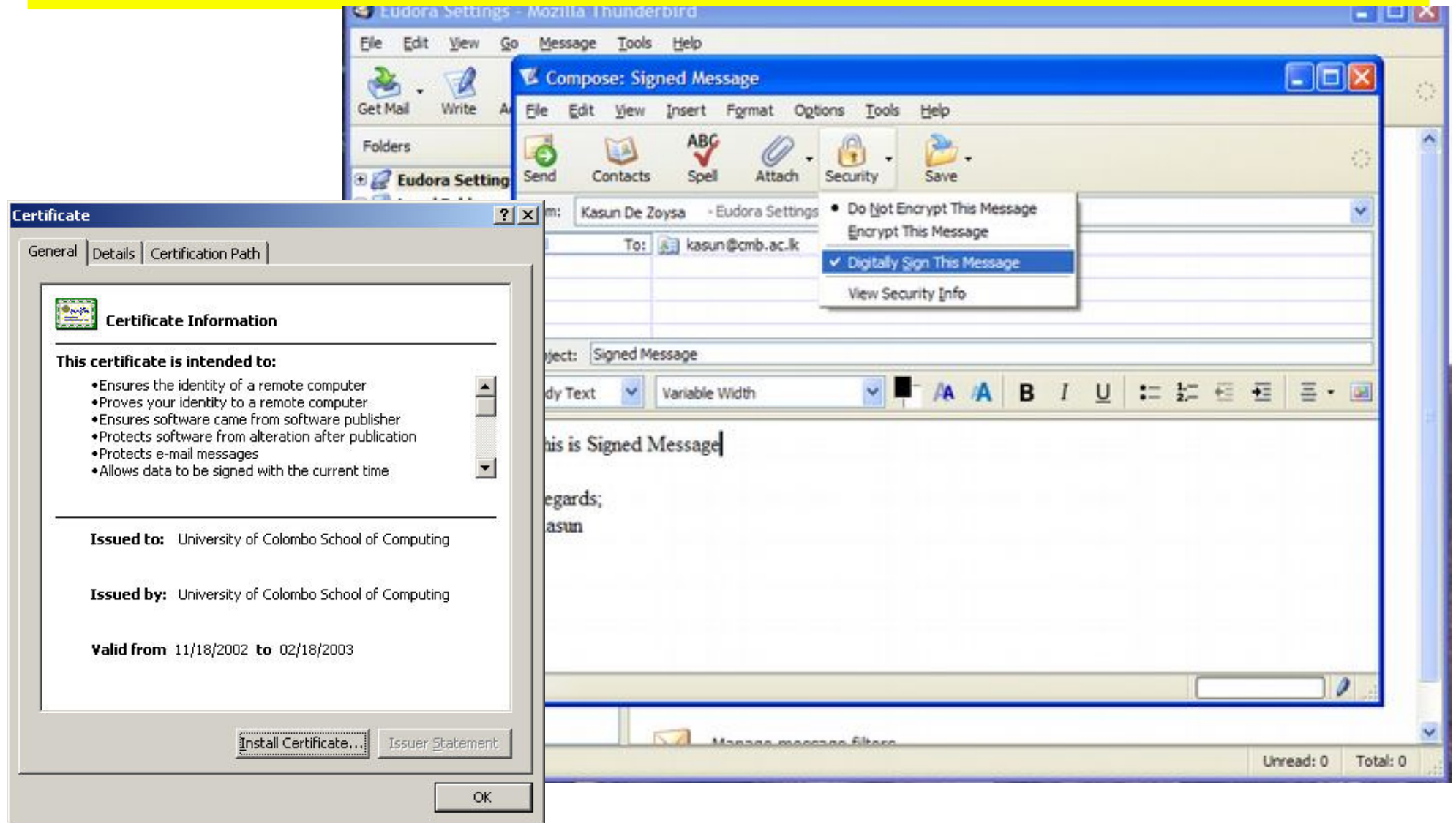
- S/MIME uses Public-Key Certificates - X.509 version 3 signed by Certification Authority
- Functions:
 - Key Generation - Diffie-Hellman, DSS, and RSA key-pairs.
 - Registration - Public keys must be registered with X.509 CA.
 - Certificate Storage - Local (as in browser application) for different services.
 - Signed and Enveloped Data - Various orderings for encrypting and signing.

User Agent Role

- Example 1 : Verisign (www.verisign.com)
 - Class-1: Buyer's email address confirmed by emailing vital info.
 - Class-2: Postal address is confirmed as well, and data checked against directories.
 - Class-3: Buyer must appear in person, or send notarized documents.
- Example 2: UCSC CA (ca.cmb.ac.lk)



Sample Screens



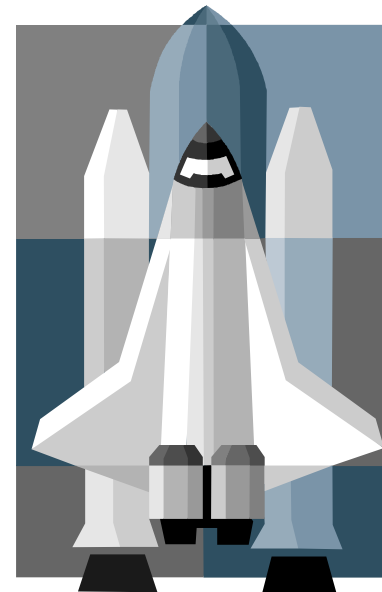
Why Is PGP Popular?

- It is available free on a variety of platforms.
- Based on well known algorithms.
- Wide range of applicability
- Not developed or controlled by governmental or standards organizations

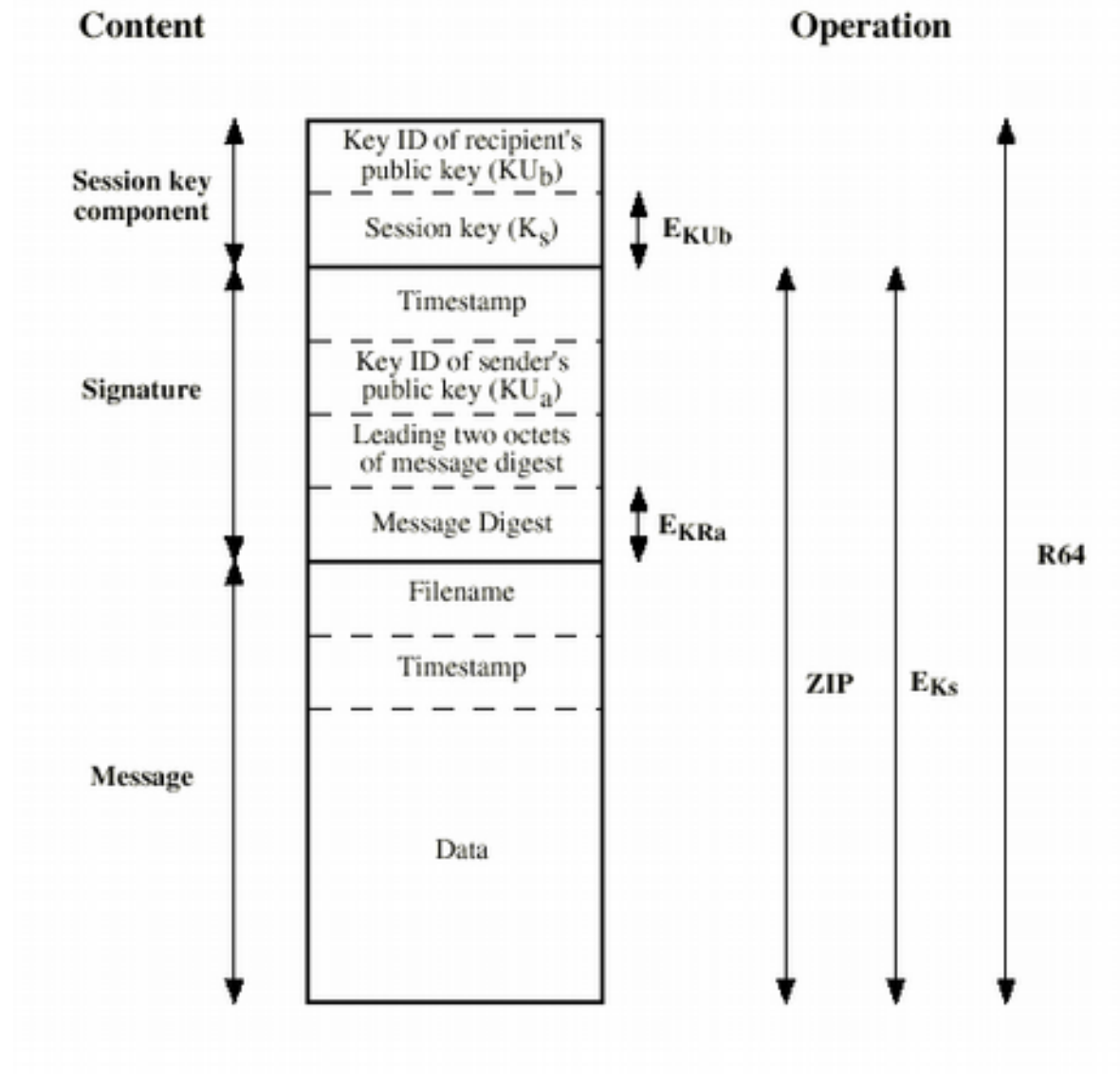


Operational Description

- Consist of five services:
 - Authentication
 - Confidentiality
 - Compression
 - E-mail compatibility
 - Segmentation



Format of PGP



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
 - is least significant 64-bits of the key
 - will very likely be unique
- also use key ID in signatures

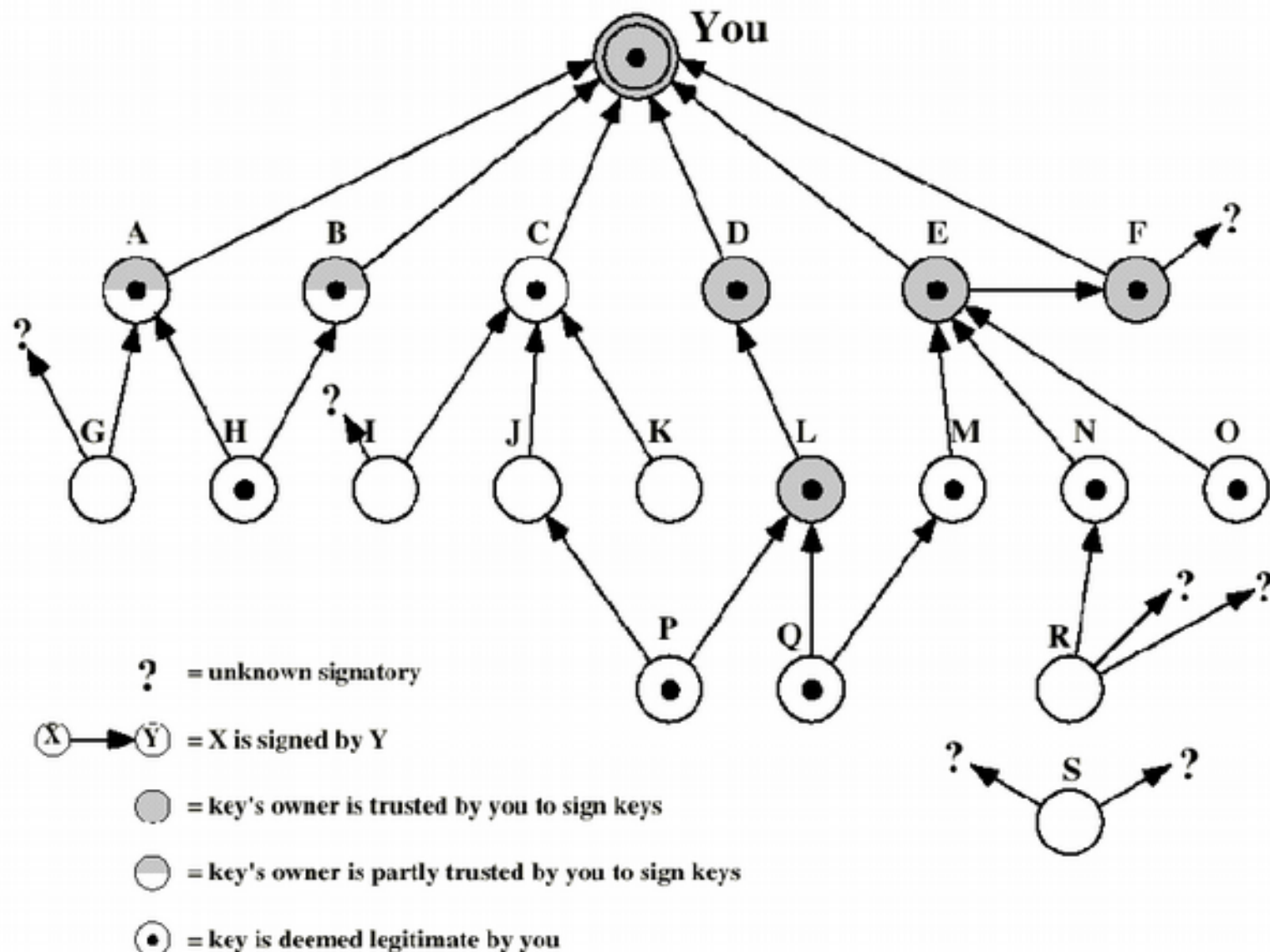
PGP Key Rings

- each PGP user has a pair of keyrings:
 - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
 - private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted key (encrypted with a hashed passphrase)
- security of private keys thus depends on the pass-phrase security

PGP Key Distribution

- PGP adopts a trust model called the *web of trust*.
- No centralized authority
- Individuals sign one another's public keys, these "certificates" are stored along with keys in key rings.
- PGP computes a *trust level* for each public key in key ring.
- Users interpret trust level for themselves.

PGP Public Keys



GPG to Encrypt and Sign Messages

Install GPG

```
sudo apt-get update  
sudo apt-get install gnupg
```

Generate Key Pair

```
gpg --gen-key
```

List Keys

```
> gpg --list-keys  
> gpg --list-secret-keys
```

You'll want to have a public key to distribute

```
gpg --export -a "email" > kasun.pub  
gpg --export-secret-keys
```

GPG to Encrypt and Sign Messages

Import Public Key

```
gpg --import kasun.pub
```

To sign the key

```
gpg --sign-key email
```

You can encrypt messages to Nimal

```
gpg --encrypt --sign -r Namil'sEmail  
name_of_file
```

When you receive a message, simply call GPG on the message file:

```
gpg file_name
```

What is spam?

- Spam is anonymous, unsolicited junk email sent indiscriminately to huge numbers of recipients.
- What for?
 - Advertising goods and services (often of a dubious nature)
 - Quasi-charity appeals
 - Financial scams
 - Chain letters
 - Phishing attempts
 - Spread malware and viruses



How do spammers harvest email addresses?

- **From posts to UseNet with your email address**

When you send email to UseNet, for example your address will be available to simple, automatic programs that are looking at the header which contain email address (From:, Reply-To:, etc). Spammers may easily build huge lists of potential targets.

- **From mailing lists.**

Spammer's regularly harvesting email addresses from poorly configured mailing lists.



How do spammers harvest email address?

- **From web pages**

Spammers have programs, which spider through web pages, check mail to: link, and collect the email address.

- **From various web forms**

Some site requests various details via web forms. E.g.; registration forms and guest books. Some of these sites collect the information and sell it to the spammers.



Existing anti-spamming techniques



Blacklist/Whitelist:

In blacklist technique, list of domains, mail serves, and email address are defined. Then e-mails come from above address will not be allowed. Whitelist technique is the opposite of blacklist technique.

Integrity Check:

Mail can be check and filter if it has the characteristic of spam. However, identifying the characteristics of a spam is very difficult.

Existing anti-spamming techniques



Reverse DNS Lookup:

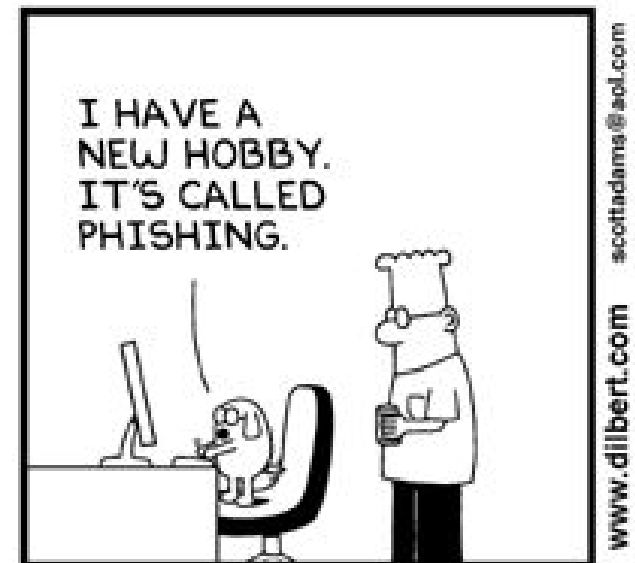
In this technique, when receiving a mail, the IP address of the sending sever is taken and DNS lookup is performed on that address to check whether the e-mail address is a real one or a bogus one.

Rules-based Filtering:

In rule-based filtering, mails are examined according to the specific rules. These rules are defined according to the patterns often used by spammers.

Phishing

- Phishing is an illegal activity that uses social engineering techniques to trick people into giving out personal information.
- Typically you will receive an email that appears to be from a legitimate business or organization asking for verification of personal or financial information.



© Scott Adams, Inc./Dist. by UFS

Phishing Email

- Information asked for in a phishing email may include:
 - Username, userid, email id, email identity
 - Password
 - ID number
 - Birthdate
- Or there may just be a link to click on that takes you to an official looking web site to enter information.

Phishing Technique

- Link manipulation
 - Technical deception designed to make a link in an email and the spoofed website it leads to, appear to belong to the spoofed organization.
- Spoofed website
 - Looks almost exactly like the real thing
- Website forgery
 - A spoofed website that uses JavaScript to alter the address bar to appear legitimate.
- Filter evasion
 - Misspelled words and images instead of text are used to evade anti-phishing filters.

Links in emails?

- Approach links in an email with caution.
- They might look genuine, but they could be forged.
- Copy and paste the link to your web browser.
- Type in the address yourself.
- Or even Google the company and go to their website from the search results.

Phishing Example

Foreign lottery scams are common

MEGAFORTUNE LOTTERY INTERNATIONAL
INTERNATIONAL PROMOTION/PRIZE AWARD DEPT.
REF: MLI/231-ILGI0431/04
BATCH: IPD/17/096/PTNL
RE: WINNING FINAL NOTIFICATION

Sir/Madam, We are pleased to inform you of the result of the Lottery Winners International programs held on the 17th of January 2005. Your e-mail address attached to ticket number 20511465897-6291 with serial number 472-971103 drew lucky numbers 8-66-97-22-71-64 which consequently won in the 3rd category, you have therefore been approved for a sum pay out of US\$ 500,000 000. (five hundred Thousand United States Dollars).
CONGRATULATIONS!!!

Due to mix up of some numbers and names, we ask that you keep your winning information very confidential till your claims has been processed and your prize/money Remitted toyou. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants. All participants were selected through a computer ballot system drawn from over 200,000,000 company and 300,000,000 individual email addresses and names from all over the world. This promotional program takes place annually. We hope with part of your winning you will take part in our next year USD10 million international lottery. To file for your claim, please contact our/your fiducial agent MR.PHILIP GERE of the, MECURY TRUST AGENT TEL: +31-621-488-708 FAX: +31-645-236-856 Email: philipgere900@netscape.net Note that all winning must be claimed not later than 3rd of February 2005. After this date all unclaimed, funds will be included in the next stake.

Please note in order to avoid unnecessary delays and complications please remember to quote your reference number and batch numbers in all correspondence. Furthermore, should there be any change of address do inform our agent as soon as possible. Congratulations once more from our members of staff and thank you for being part of our promotional program.

Note: Anybody under the age of 18 is automatically disqualified.

Sincerely yours,
Mrs Ellen Kloos,
Lottery Coordinator
. REPLY EMAIL TO philipgere900@netscape.net

Phishing Tests

Gophish: Create your own simulated phishing campaigns and track results with this easy-to-use open source platform: <https://getgophish.com/>



Attachments

- Computer viruses and other malicious software are often spread through email attachments.
- If a file attached to an email contains a virus, it is often launched when you open (or double-click) the attachment.
- Don't open email attachments unless you know whom it is from and you were expecting it.



Should you open attachments?

If it is suspicious, do not open it!

- What is suspicious?
 - Not work-related.
 - The email containing the attachment was not addressed to you, specifically, by name.
 - Incorrect or suspicious filename.
 - Unexpected attachments.
 - Attachments with suspicious or unknown file extensions (e.g., .exe, .vbs, .bin, .com, .pif, or .zzx)
 - Unusual topic lines: “Your car?”; “Oh!”; “Nice Pic!”; “Family Update!”; “Very Funny!”

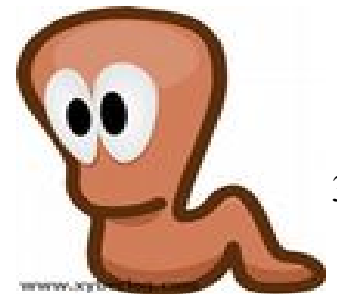
Email best practices

- Use the BCC field when sending to large distribution lists.
 - Protects recipients email addresses
 - Prevents Reply to All issues
- Avoid use of large distribution lists unless legitimate business purpose.
 - E.g., All Faculty/Staff list
- Beware of Reply to All button
- Don't forward chain email letters.



Cloud

- Cloud computing is a new resource that is enables convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned.
- It has great scalability and cost-modulation advantages.
- **However it brings about new security concerns since documents are not physically controlled within the user enterprise.**



Storage of Data in Multiple Jurisdictions

- Mirroring data for delivery by edge networks and redundant storage without real-time information available to the customer of where data is stored.
- Data may be stored and/or processed in high risk jurisdictions where it is vulnerable to confiscation by forced entry.

Protect your data in transit

- If you need to exchange sensitive or confidential information between a browser and a web server, configure TLS on your server instance.
- Create a Virtual Private Cloud by making a few command line calls. This will enable you to use your own logically isolated resources within the cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPSec VPN connections.
- You can also setup an OpenVPN server on a cloud instance and install the OpenVPN client on all user PCs.

Protect your data at rest

- If you are concerned about storing sensitive and confidential data in the cloud, you should encrypt the data (individual files) before uploading it to the cloud.
- For example, encrypt the data using any open source or commercial PGP-based tools before storing it as cloud objects and decrypt it after download.
- Cloud instances running Linux can mount volumes using encrypted file systems using variety of approaches.

Unable to Process Data in Encrypted Form

- Encrypting data at rest is easy but problem is the processing.
- No matter which operating system or technology you choose, if you lose the keys, you will lose your data forever and if your keys become compromised, the data may be at risk.
- Therefore, **key management is** important.



Homomorphic Encryption

(Gentry, 2009)

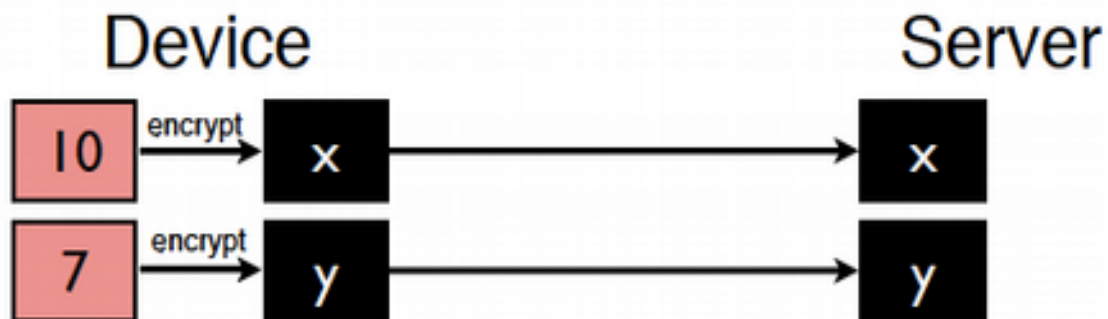
- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

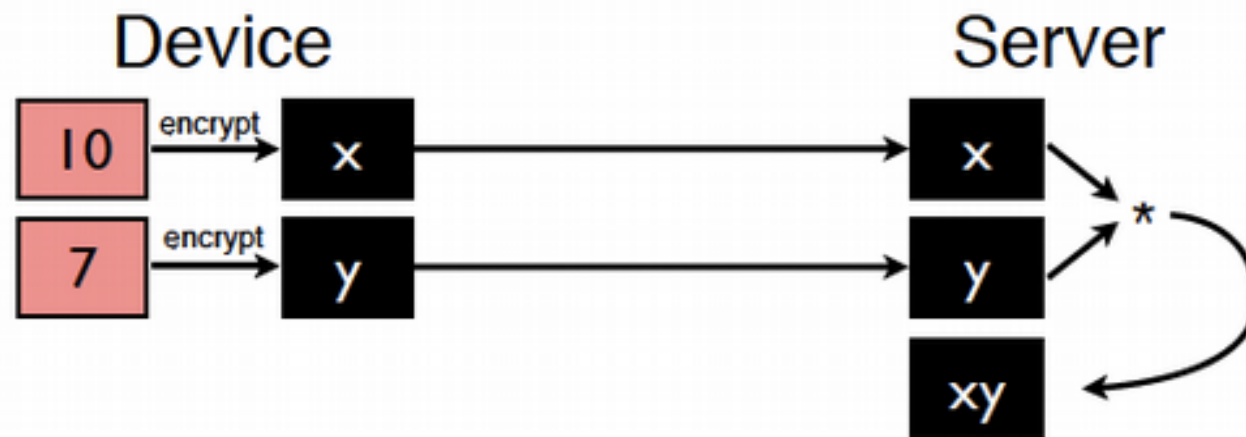
- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

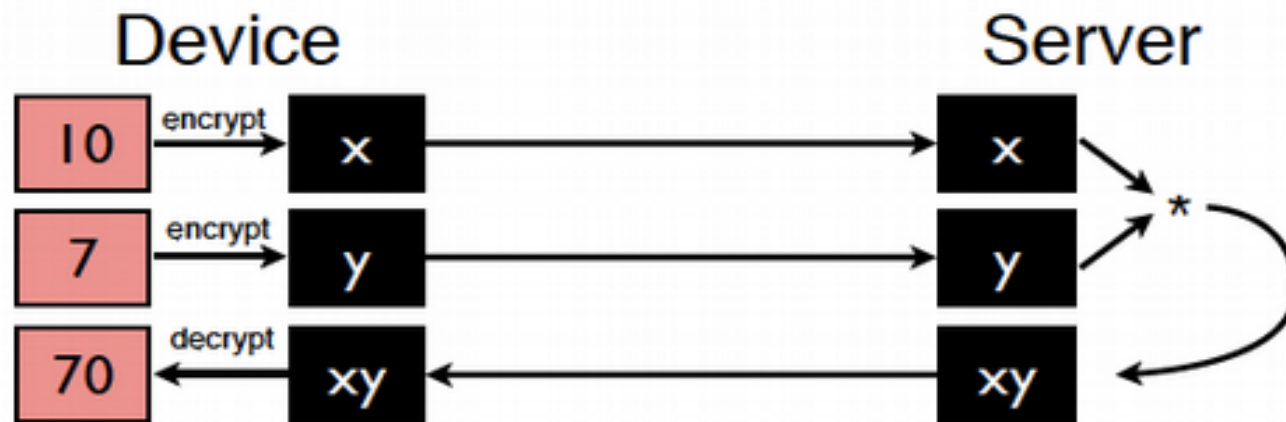
- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

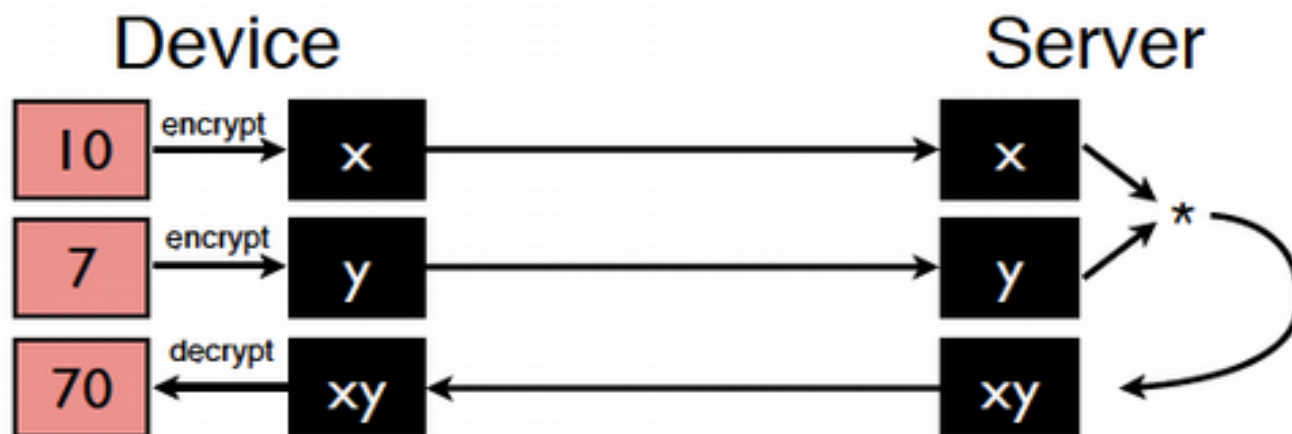
- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



- So confidential analytics possible, but not yet practical
 - Computations on S_e are 1,000,000 slower than computations on S
- But can be fast for *specific* computations (e.g., $*$)

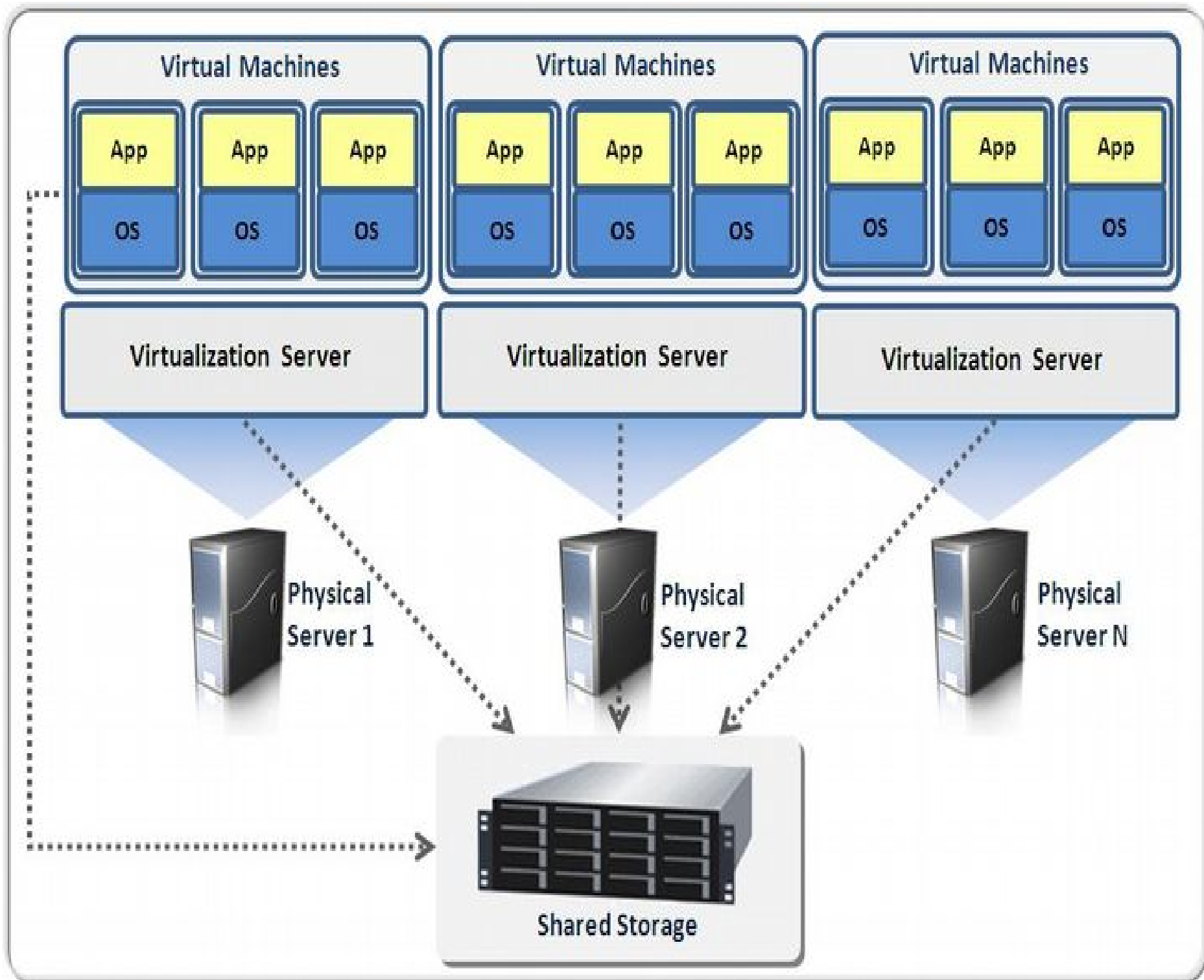
Before the dawn of time.....

- Each application was housed in servers like these!
- Each box housed “a” database, “a” service (eg web, mail, etc).
- When you wanted to start a new database, you bought one of these (or cleaned one up)

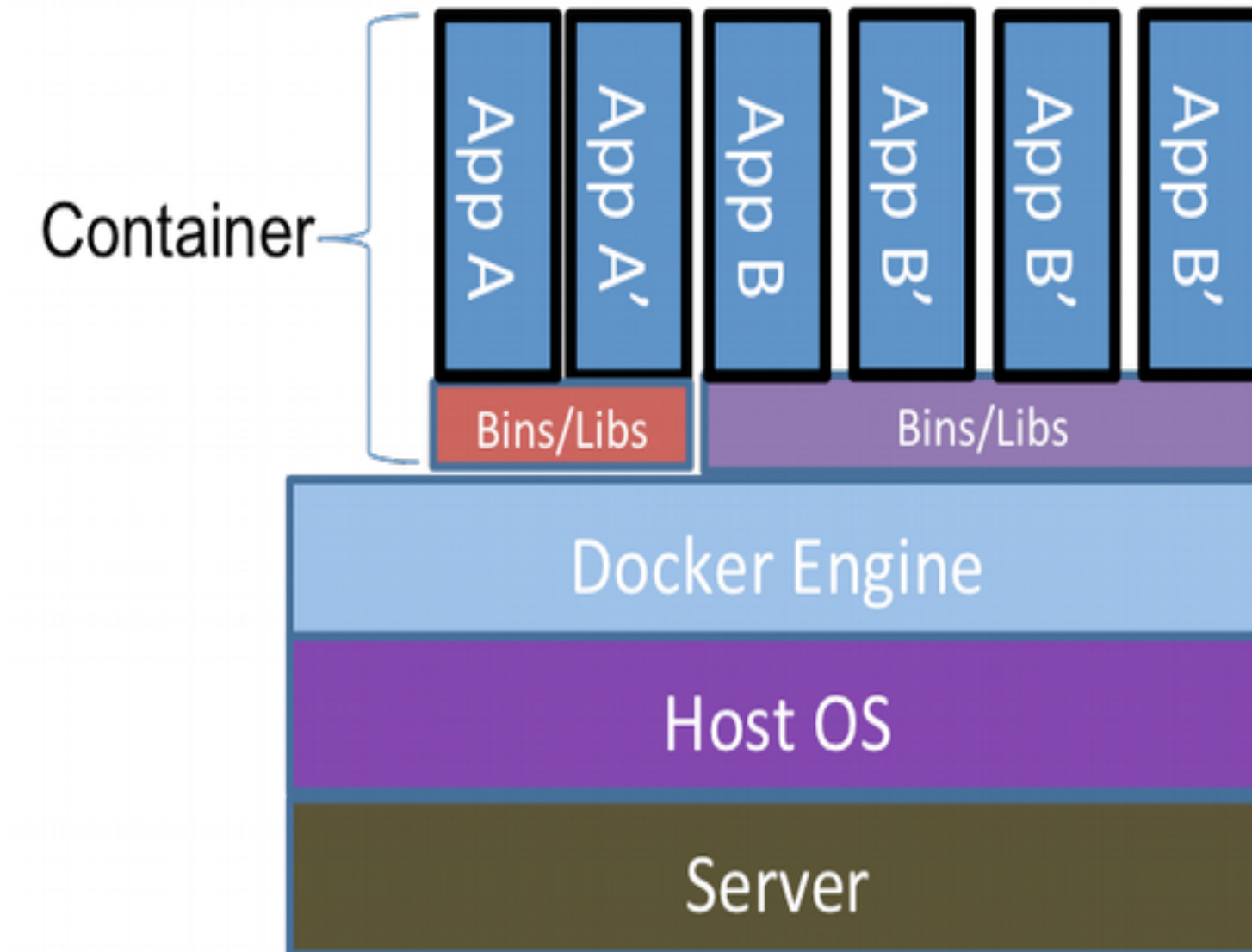


Then came the Age of Virtualization

- The process of creating logical computing resources from available physical resources
- Layer of abstraction between workloads and the underlying physical hardware
- Many virtual servers living and breathing on one physical server!

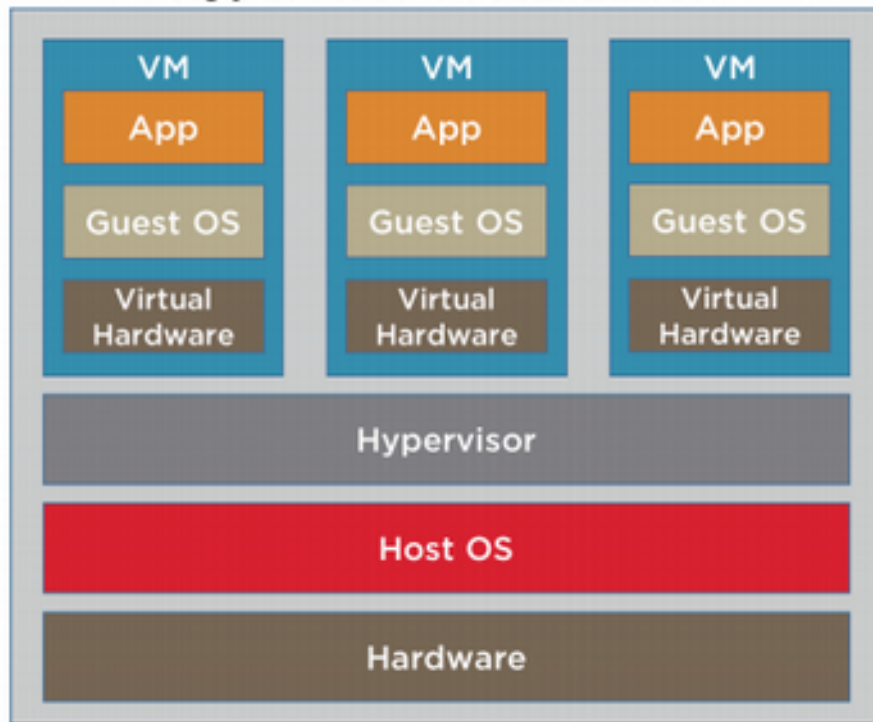


Now comes the.... Age of Containerization



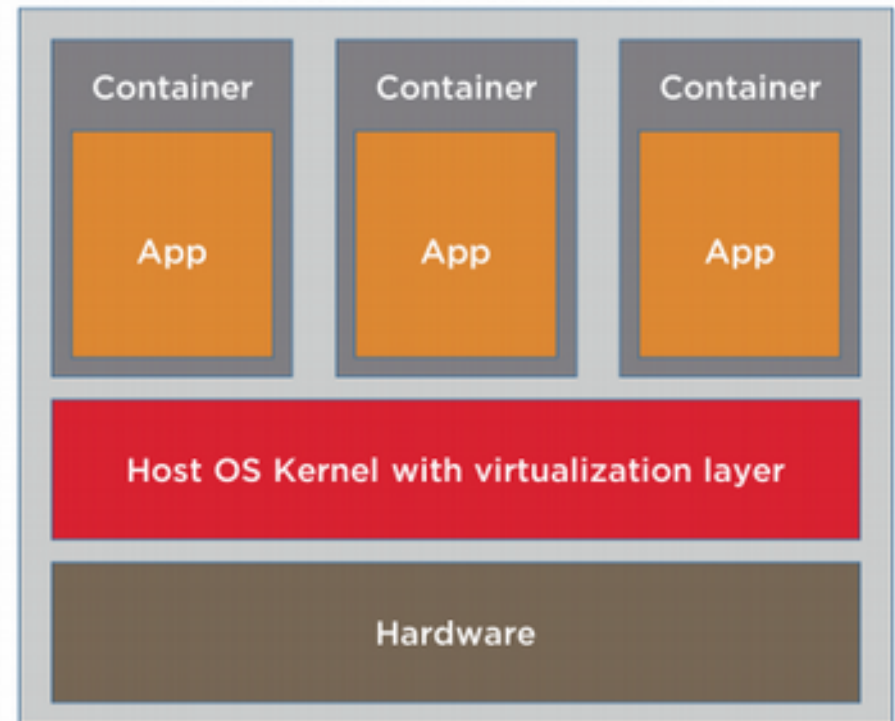
Containers versus VMs

Hypervisor virtualization



- Traditional
- Resource-intensive
- More than one OS

Container virtualization



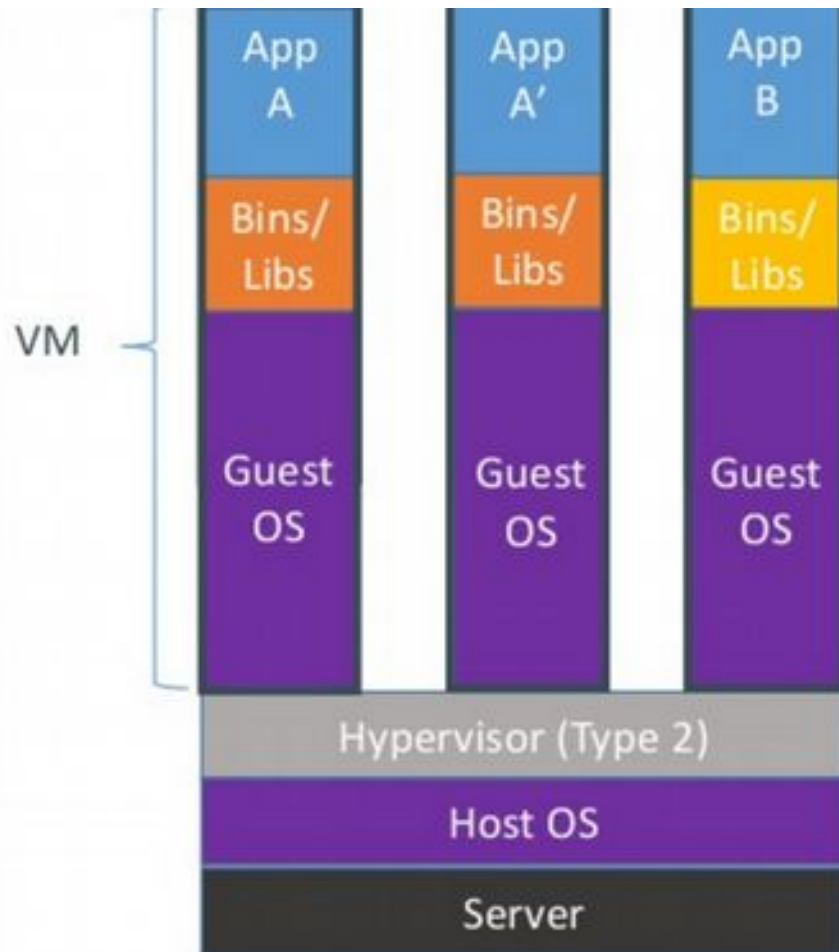
- Lower costs
- High elasticity
- More revenue

What is Docker?

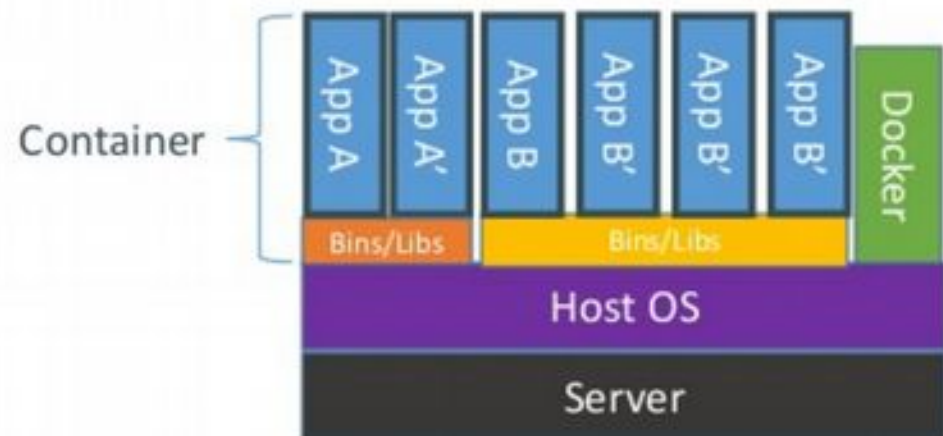
Docker is an open-source project that automates the deployment of applications inside software containers, by providing an additional layer of abstraction and automation of operating system–level virtualization on Linux.

[Source: en.wikipedia.org]

How does Docker containers work?



Containers are isolated, but share OS and, where appropriate, bins/libraries



Docker supported in many Cloud platforms



Security in Docker = Complicated!

- Why? Because containerisation is not piecemeal virtualisation!
 - VMs: isolated virtual **machines**!
 - Containers: packaged & somewhat isolated **minimal instances**!
 - Cnames + Namespaces + Kernel + libs + aufs
 - Containers were built with packaging + deployment + run convenience in mind!
 - Convenience dictates the terms, not security.
 - Containers are comprised of, and have, too many moving parts!
 - Lego
 - Therefore any approach we take to secure them has to take this into account.
 - Layered security, as usual, then!

“Containers are not necessarily a "security" boundry, there are many "leaks" across it, and you should use it only as a way to logically partition off users/processes in a way that makes it easier to manage and maintain complex systems.”

(Greg Kroah-Hartman, Linux Kernel Developer)

Discussion

