Administrarea Bazelor de Date
Managementul în Tehnologia Informaţiei

Sisteme Informatice şi Standarde Deschise (SISD)

2009-2010

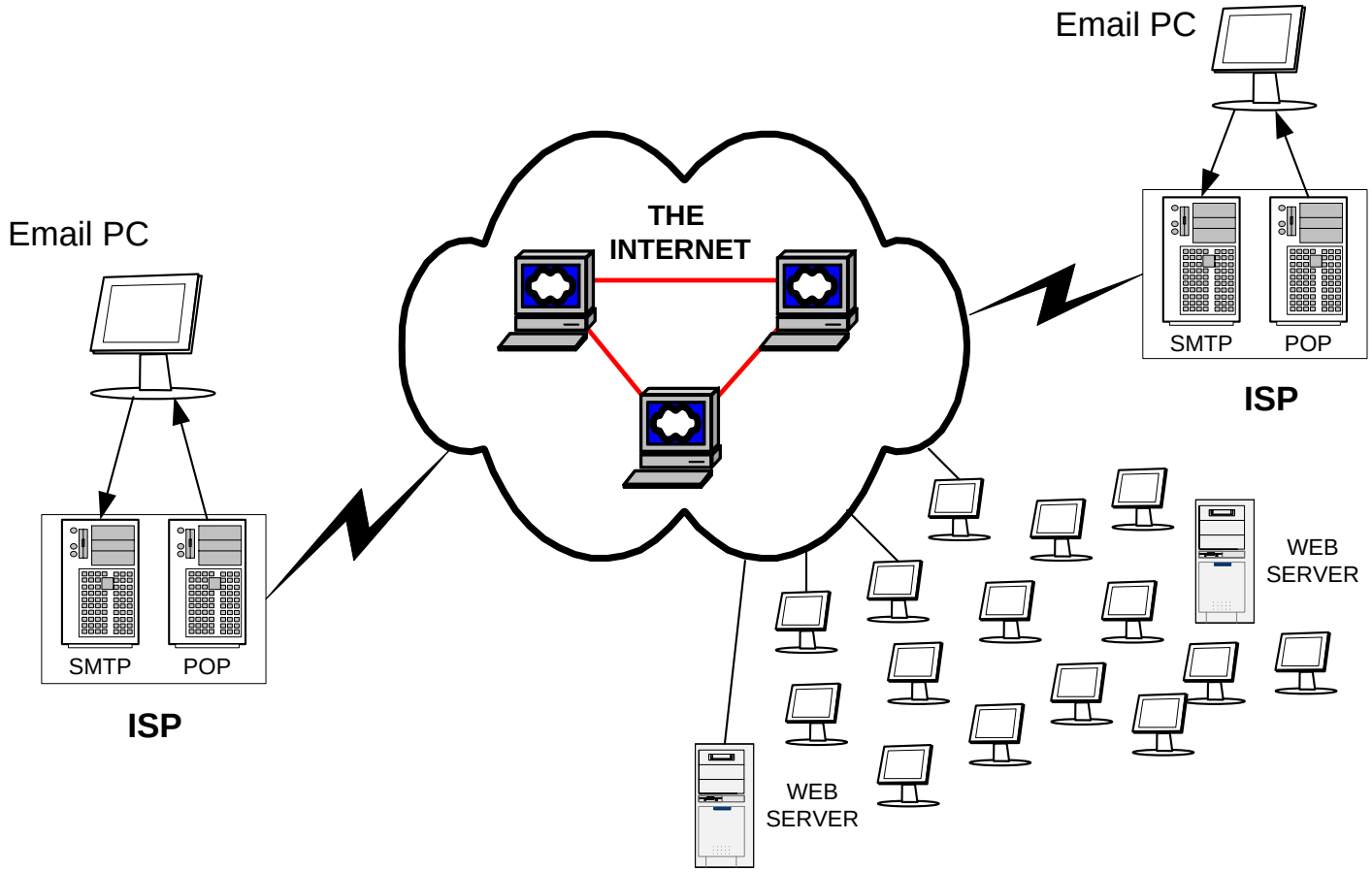
Curs 5
Standarde pentru poştă electronică

Components of an Email System

- Mail Transport Agent (MTA)
- Mail User Agent (MUA)
- Local Delivery Agent (LDA)

- …others??

How Does Email Work



Types of Internet Communications

- **Synchronous**
  - Senders and receivers communicate in “real time”.
  - Examples: Instant Messaging, Chat Rooms.
- **Asynchronous**
  - Senders and receivers communicate at different times.
  - Examples: Email, Discussion Groups

Common Email Protocols

- Sending Mail:
  - SMTP (Simple Mail Transport Protocol)
    Servers include Sendmail, Postfix, Exim, Qmail
- Receiving Mail
  - IMAP (Internet Message Access Protocol)
  - POP3 (Post Office Protocol v3)
    Servers Include Dovecot, Courier, Qmail

SMTP Design

- Delivers a message from one machine to another
- Became popular in the 1980's (as complement to UUCP)
- Used for outgoing messages from a sender to their outgoing mail server
- Communication between mail servers on the Internet
- Typically listens on TCP Port 25
  and also on 587 and 465

SMTP Servers

- Sendmail
  - Widely available, complicated to configure (M4 macros, etc)
  - The term ‘sendmail’ is used in multiple contexts
- Postfix
  - Widely available, semi-straightforward
- Exim
  - Generaly available, semi-complicated to configure
- Qmail
  - Generally available, completely different than most other *nix servers

- (These are my opinions - your mileage may vary)

SMTP Uses

If ever configuring a mail server, try to separate these two types of services

- Outgoing Mail Server
  - Should have some kind of authentication
  - Queue messages when receiving server is unavailable
  - Sends bounce message to sender after retrying delivery

- Incoming Mail Server (or MX server)
  - Receives incoming messages from the Internet
  - Delivers message to a mailbox
  - (Should never send a bounce)

Weaknesses and Extensions

- No Sender Authentication
  - SMTP Auth
- Unencrypted
  - SSL and TLS
- Text-Only
  - MIME
- Bounces ☹
- SPAM ☹☹☹
  - SPF and DKIM

POP3 Protocol

- Retrieves messages from a mail server
- Typically, messages are downloaded to your mail client, and deleted from the server
- Designed for use with dial-up connections when people were intermittently connected
- Listens on Port 110 (with Secure POP generally on port 995)

IMAP Protocol

- Listens on port 143 (IMAP/SSL on port 993)
- Mail stays on the server. Mail Client caches information locally
- Extremely useful for multiple users, multiple machines, Webmail, etc
- Searches are done on the server

POP3/IMAP4 with SMTP

- Uses SSL to secure POP or IMAP connection
- Does not authenticate at front end
- Requires SMTP at front-end to send mail OR separate SMTP relay (watch for relay spam)
- Removes much of the rich functionality
- Public Folder access can be tricky
- Don’t enable unless you absolutely have to

Types of Email Accounts

- **PC-Based**
  - Outlook, Outlook Express, Netscape Mail
  - Uses PC program
  - Connection to Internet not needed except when sending & receiving
  - All messages stored on PC
  - Unsent messages can be viewed using Web
- **Web-Based**
  - Hotmail, Yahoo Mail, Google Mail, many others
  - Uses browser
  - Must be connected to Internet
  - All messages stored on Web
- **Hybrid (AOL Mail)**

SPAM & Phishing

- SMTP has no built-in way to verify the legitimacy of the message
- Anybody can say they are anybody else
- SMTP is far too prolific to try to replace it

- (demonstrate sending an email as PayPal)

Fighting Spam

- Greylisting
- Content Filtering
  - This can get to be incredibly CPU intensive
- DNS-based Blacklists

- Consider Appliances and Outsourced Services

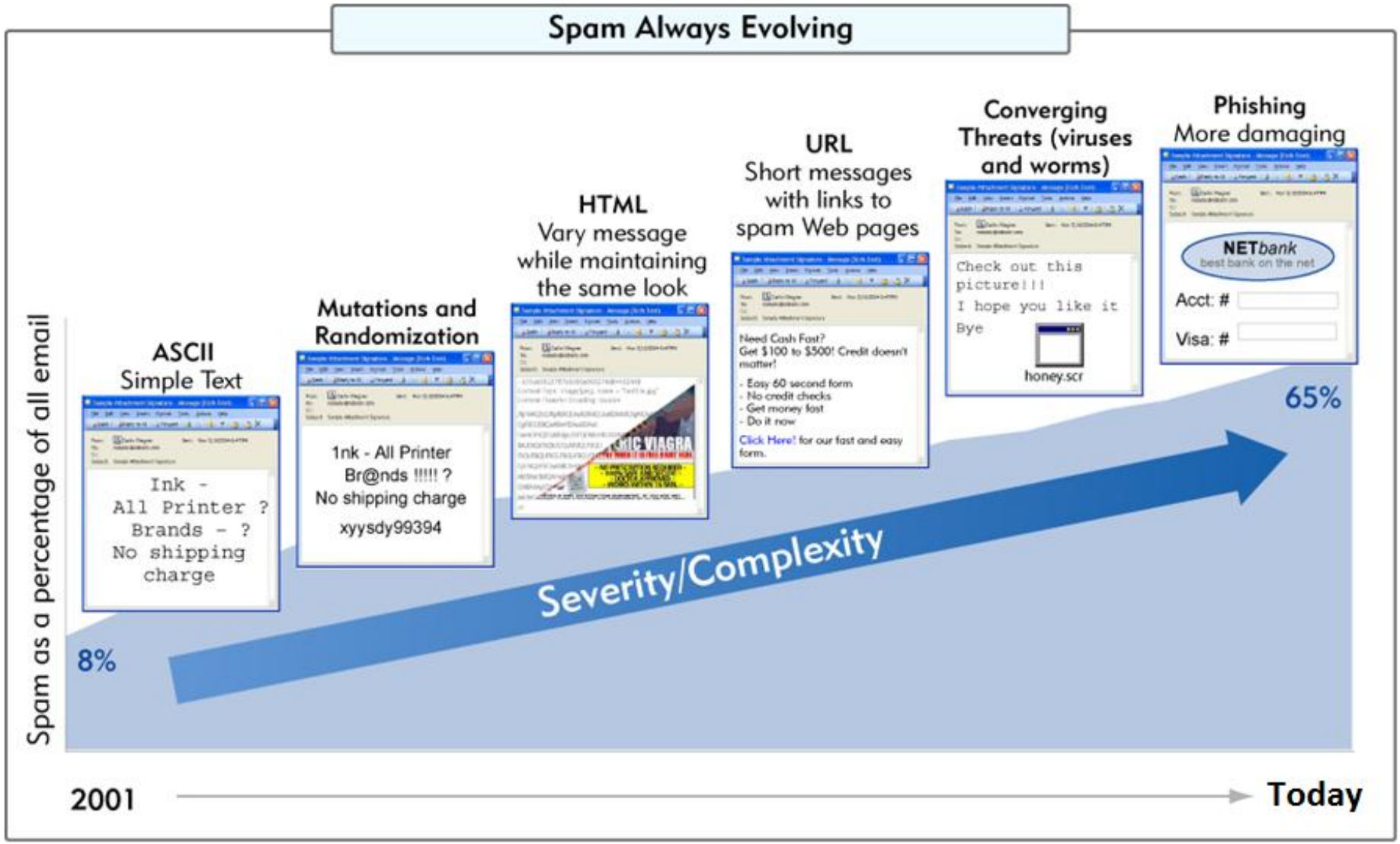
SPF and SenderID

- Concept is to validate the path the message took
- **SPF** (Sender Policy Framework) Record published in DNS gives a list of the servers authorized to send email for a given domain
- Fairly Simple to create
- SPF Record Looks Like:

  v=spf1 a a:mail.domain.com ~all

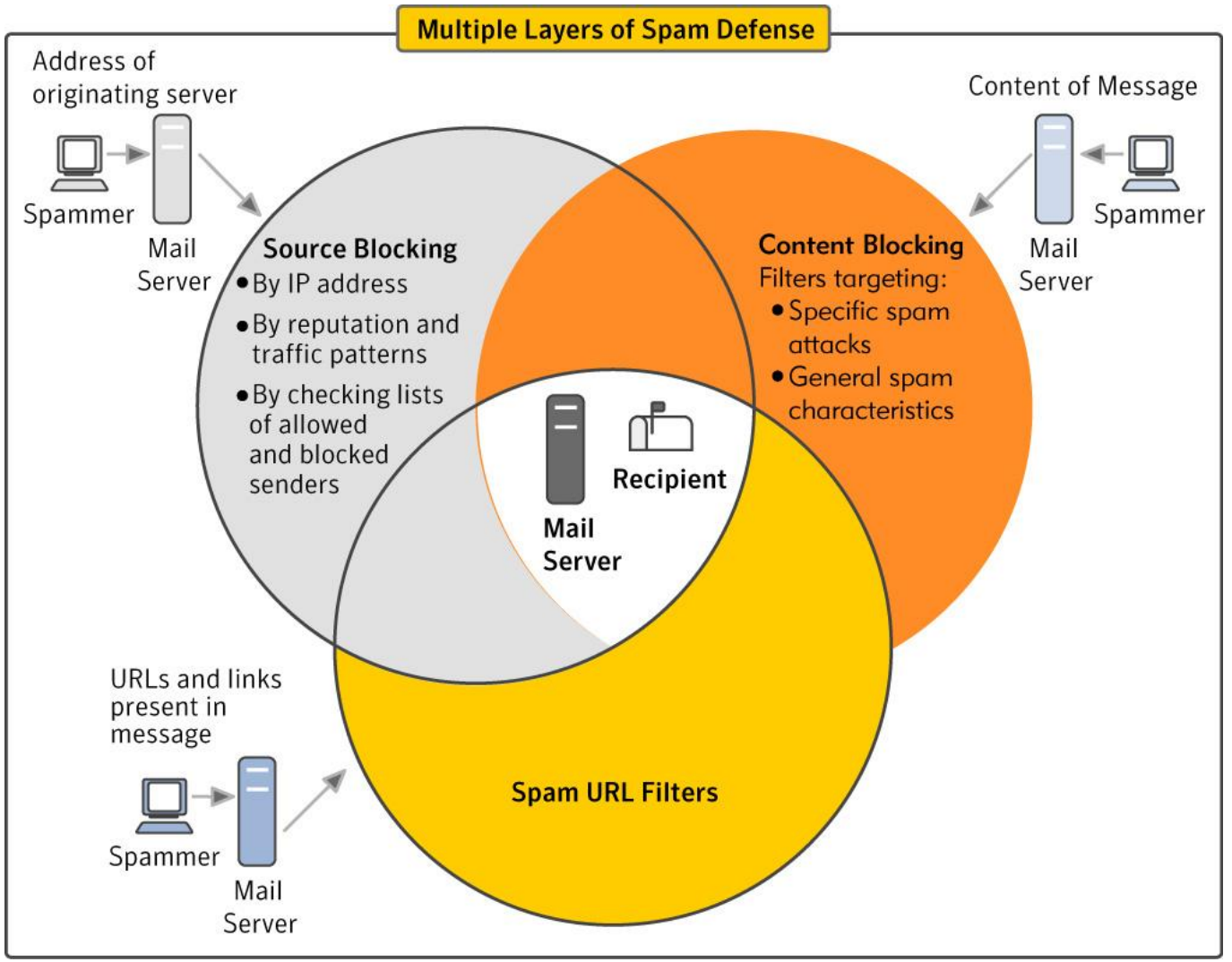
SPF Wizard at http://www.openspf.org/

Spam Continues to Grow and Evolve



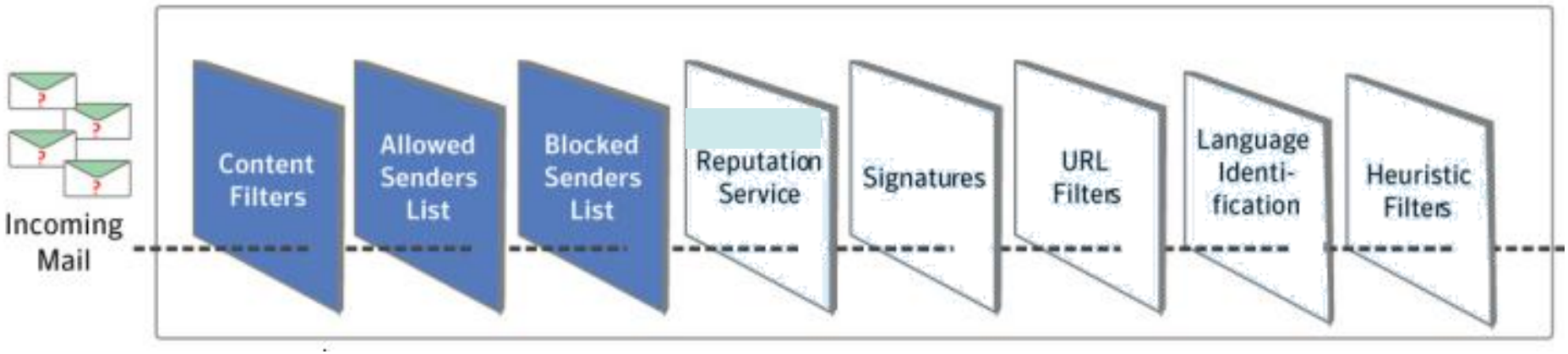
AntiSpam Technology Approach

- **Examine the source**
- **Examine the content**
- **Examine the call to action (URL filters)**



Solutions Need Multi-Layered Defences

- Multiple technologies creates a comprehensive defence
- Force spammers to contend with each layer



Phishing

- Theft of financial information and/or identity
- Growing problem both in terms of magnitude and awareness
- Targets expanding from Financial Services to all organizations with financial information online
  - Banks, ecommerce sites, phone companies, government agencies, etc.
- Global problem – US, UK, Europe, Australia, South America

	Spam	Fraud
Range of Damage	Internal	External
Asset Attacked	IT Resources	Brand
Group Targeted	Employees	Customers and potential customers
Key Threat	Ability to use email as a communication medium	Ability to do business online

Email security

- Email security is important
- If messages are not secure,
  - They may be viewed in transit on the network
  - Viewed by suitably privleged users on destination systems (e.g. sys admins)
  - Easy to masquerade as someone
    - There are emailers you can use to send emails claiming you are Bill.Gates@microsoft.com
  - Message integrity upon reception is not guaranteed

DomainKeys / DKIM

- **DKIM** - DomainKeys Identified Mail
- Cryptographic Hash to sign messages
- Public Key and policy information is distributed via DNS
- Private key is used to sign the message, and certain headers (From, To, Subject, etc)
- Recipients use public key to verify authenticity of the message
- Verifies a legitimate sender, and is not concerned about the path it took to get there.
- Fairly complicated to set-up

Current Email Security and PGP

- Currently email programs are not secure
  - Especially web based email
  - Programs such as Outlook and Eudora do offer encryption
    - But no maintenance of others' public keys
- PGP can be used for email security
  - It stands for Pretty Good Privacy
  - It is a software application created by Phil Zimmermann
  - Public-key rings is the main feature
- PGP
  - It is based on the best available crypto algorithms
    - Considered very strong and secure
  - Mainly used for email and file storage applications
  - Independent of governmental organizations
  - Messages are automatically compressed

Setting up PGP

- PGP is a crypto management module
  - Should tie it to your email client
- Use GnuPG which is free
  - www.pgp.com only has free trial
- Better yet, download WinPT
  - Comes packaged with GnuPG + GUI for key management
- Then tie GnuPG to your email client using plugins
- Example:
  - Mozilla Thunderbird client for pop/smtp email
  - Enigmail plugin for tying GnuPG to Thunderbird
- Other email clients (Outlook, Eudora etc.) have respective plugins.

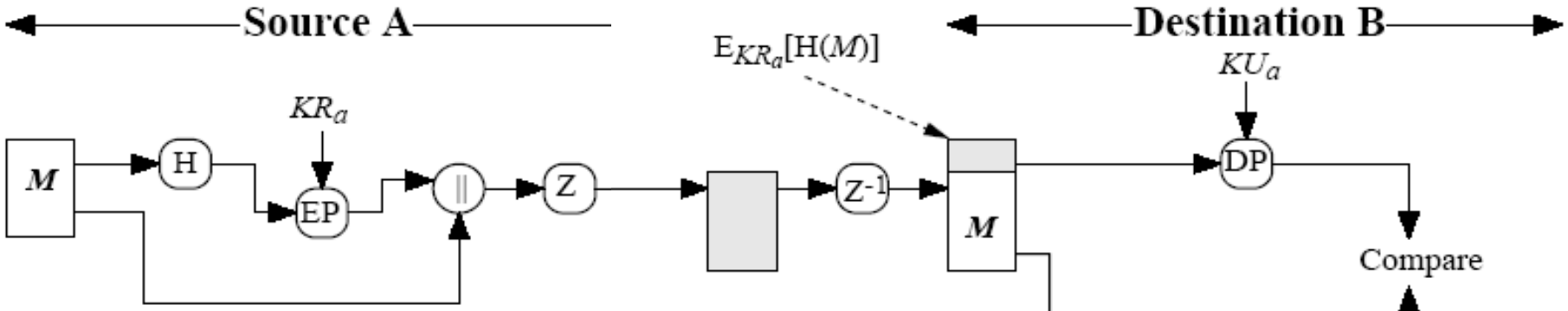
PGP Components

- There are **five** important services in PGP
  - Authentication (Sign/Verify)
  - Confidentiality (Encryption/Decryption)
  - Compression
  - Email compatibility
  - Segmentation and Reassembly

- The last three are **transparent** to the user

PGP: Authentication steps

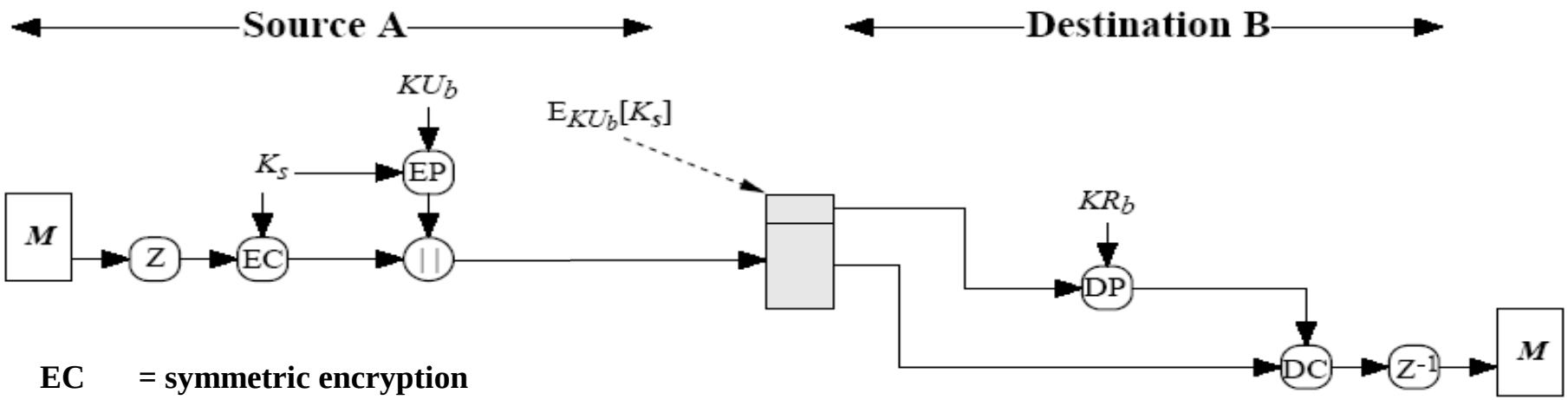
- **Sender:**
  1. Creates a message
  2. Hashes it to 160-bits using SHA1
  3. Encrypts the hash code using her private key, forming a signature
  4. Attaches the signature to message
- **Receiver:**
  1. Decrypts attached signature using sender's public key and recovers hash code
  2. Recomputes hash code using message and compares with the received hash code'
  3. If they match, accepts the message



M	**= original message**	**EP**	**= public key encryption**
H	**= hash function**	**DP**	**= public key decryption**
||	**= concatenation (join)**	**KR_a**	**= A's private key**
Z	**= compression**	**KU_a**	**= A's public key**
Z^{-1}	**= decompression**		

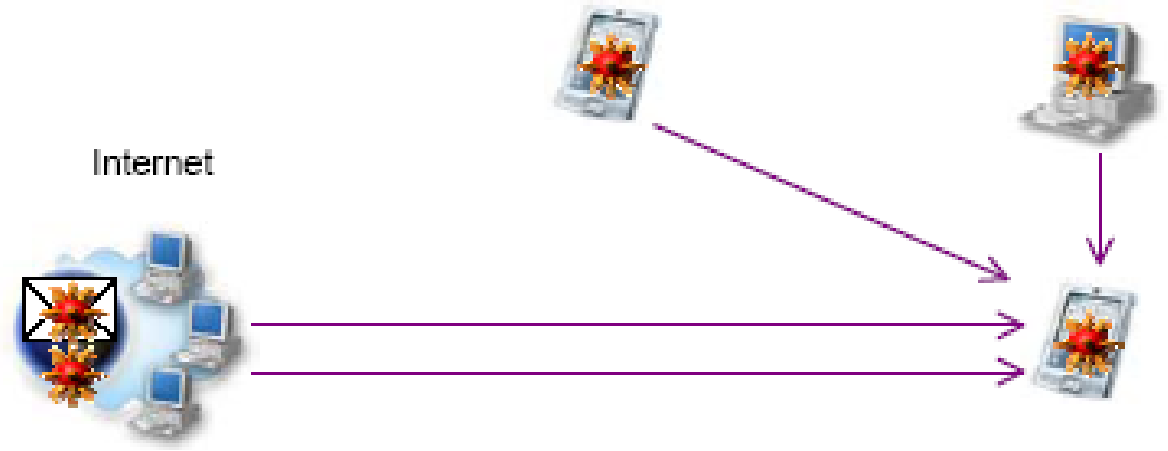
PGP: Confidentiality

- **Sender:**
  1. Generates message and a random number (session key) only for this message
  2. Encrypts message with the session key using AES, 3DES, IDEA or CAST-128
  3. Encrypts session key itself with recipient's public key using RSA
  4. Attaches it to message
- **Receiver:**
  1. Recovers session key by decrypting using his private key
  2. Decrypts message using the session key.



EC = symmetric encryption
DC = symmetric decryption
K_s = session key

Handheld Virus Propagation



- **Through infected e-mail when using a PDA over a wired or wireless Internet connection**
- **When synching with an infected PC**
- **Via an infected file transferred from another PDA via infrared (IR) or Bluetooth**
- **By downloading infected files from the Internet**

Vectors of Delivery

- Synching with a PC
- Peer to Peer Connectivity
  - Bluetooth
  - Infrared
- Telephony
  - GSM
  - GPRS
  - UTMS
- Data Transfer
  - SMS
  - MMS
  - WAP
- Network Connectivity
  - WLAN (802.11)
  - PCMCIA Network Cards

Indirect SMS Worm

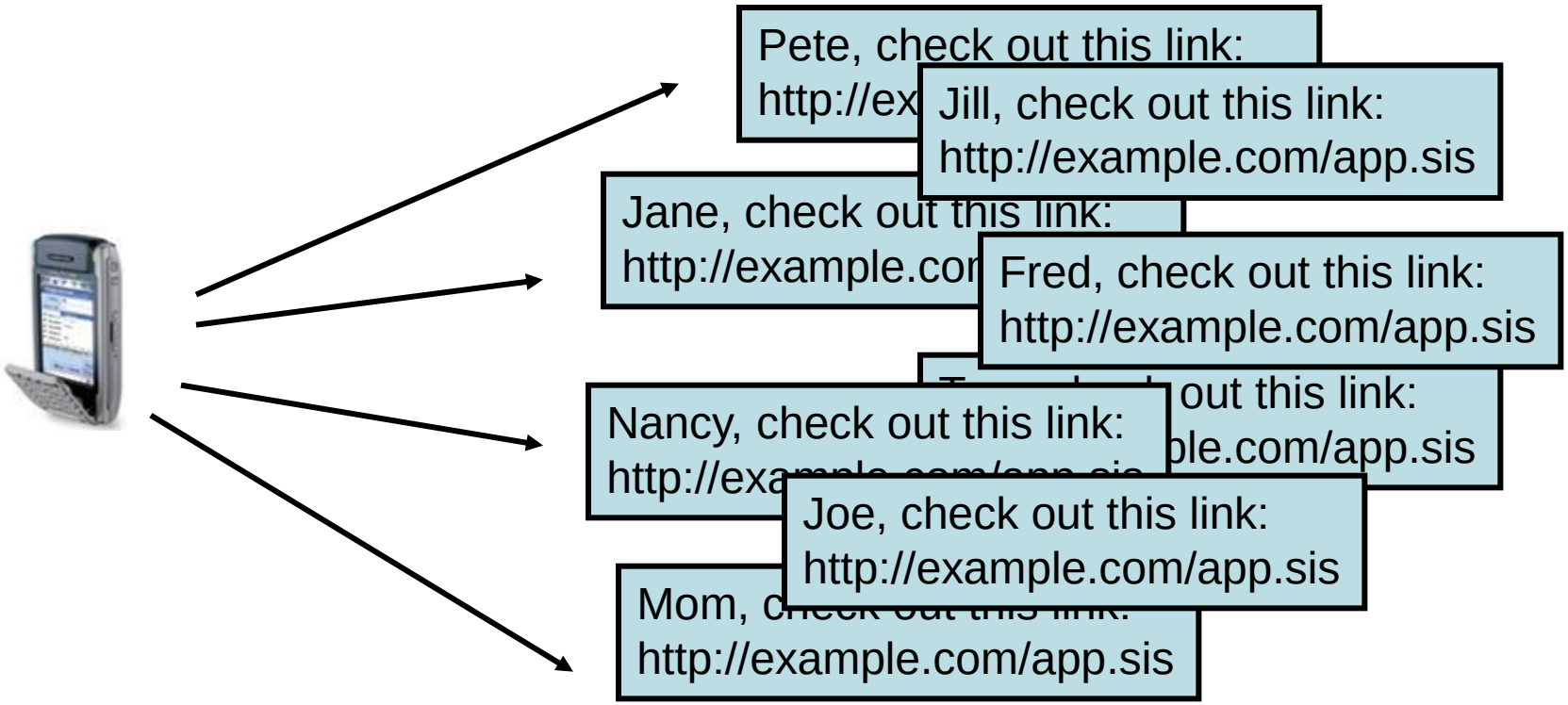
- John receives an incoming SMS from his friend

John, check out this link:
http://example.com/app.sis

- John browses the site and downloads the application

Indirect SMS Worm

- John runs the application and unknowingly sends SMSes to everyone in his contact book



Legal & Regulatory Measures: Government

- International cooperation
- Appropriate legislation (data protection, fraud, consumer protection, unfair competition)
  - Transposition of existing directives
  - Technological neutrality
- Clear allocation of responsibilities between national authorities
- Stronger enforcement of data protection rules
- Tough penalties for individuals
  - Spammers should pay for the spam
  - Rules for evidence collection

Legal & Regulatory Measures: Industry

- Distinguishing Spam from legitimate marketing
- Using clear opt-out procedures
- Use of clear codes of conduct
- Cooperation with government
- Implementation of best-practice technology

Policy and technology

- Technical solutions exist
  - No silver bullet
  - Insufficient/improper implementation
  - Lack of holistic approach
    - Security is a process not a just product
    - Lack of security in specific areas may mean inadequate overall security
  - Lack of awareness
    - Businesses
    - Consumers
    - Policy makers
- Technology is not the only solution
  - Coherent legal framework
  - Co-operation between the different actors
    - Governments – security professionals – communications industry

Awareness & Education

- Role of government in promoting understanding
- Role of business as employers
- Role of ISPs
- Role of the individual

Tips for Managing Email in the Workplace

- Create email file folders for easy reference and processing

- Manage email each day by:
  - Step1: process and organize
  - Step 2: archive or delete

Step 1: Process

- Delete? Does the message even need to be read?
- Do not reply to heated, angry emails. Talk to the person – in person instead.
- Respond now? If it takes less than two minutes, reply now. If it takes more than two minutes, respond later.
- SCHEDULE time to respond and place in a “to do” folder.

Step 2: Replying or Sending Messages

- Archive? Or Delete?
- Do you need to save this message?
  - THINK twice
  - if you need it, organize in folders
- Delete whenever possible

Limit Inflow and Outflow

- Ask to be taken off distribution lists that you don't need
- Process email at least 2-3 times each day
- Think before sending – do you really need to send a message?

Things to keep in mind

- Email is NOT private
- Do not treat it casually – poorly written emails create a negative work image
- Manage your email

Sending Me Email: Protocol

- Write: SISD in the subject line (first word) and your first and last name at the end of the message
- Be specific and concise (about a screen full of information)
- Be professional
- Students are invited to send me their
- project ideas through email for feedback

Exam's quizzes

- **1.** Descrieți modul de interacțiune POP3/IMAP4 cu SMTP. Care sunt tipurile de conturi pentru poșta electronică.
- **2.** Descrieţi pe scurt noţiunea de SPAM. Care sunt măsurile posibile pentru: a) prevenirea lui; b) eliminarea (distrugerea) lui?
- **3.** Descrieţi pe scurt noţiunea de Phishing. Care este modul lui de acţiune?
- **4.** Ce este PGP? Descrieți modul de funcționare pentru PGP.