- 90 minute version -

E - Banking

University
of Belgrade

Dr. Adgaonkar G.S

Outline

I. Introduction to e-Banking
- What is an e-Bank and why to do e-Banking
- Some facts about e-Banking

II. Security issues
- Overview of the security problems
- Cryptography basics
- Digital Signatures
- Digital Certificates
- Secure Sockets Layer (SSL)

continued...

Outline

...continued

III. Bankers’ Point of View

- E-Bank software architecture
- Application Service Providers (ASPs)
- Required tasks after initial introduction of a new channel
- Searching for financial information on the Web

IV. Conclusion

Part I

E-Banking

Introduction to E - Banking

Introduction

- Banking consumers today have more options then ever before:
  - “brick and mortar” institution
    (has a building and personal service representatives)
  - “brick and click” institution
    (physical structure + Internet bank services)
  - “virtual bank”
    (no public building – exists only online)

What Is an E-Bank?

- Traditional banking business assumes:
  - Customer desk at bank’s building
  - Office hours from 8.00 am to 7.00 pm

- Customers have:
  - Their job during the day
  - Family or other activities after the job

What can we do about it?

What Is an E-Bank?

- Logical answer is to use e-channels:
  - Internet
  - WAP based mobile network
  - Automated telephone
  - ATM network
  - SMS and FAX messaging
  - Multipurpose information kiosks
  - Web TV and others …

- E-channels enable financial transactions from anywhere and allow non-stop working time.

What Is an E-Bank?

- E-Bank is transforming banking business into e-Business through utilizing e-Channels
- Customers' requests are:
  - Non-stop working time
  - Using services from anywhere
- E-channels provide:
  - Working time 0 - 24h
  - Great flexibility

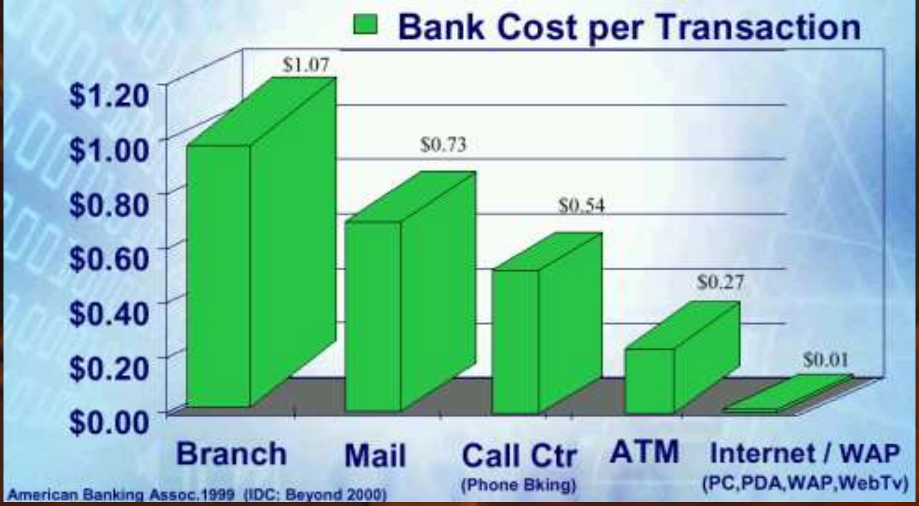
Perfect match!

Other Advantages of E-Banking

- Possibility to extend your market (even out of country)

- Possibility to process more financial transactions

- Possibility to lower your transaction cost



American Banking Assoc.1999 (IDC: Beyond 2000)

Internet Banking ... and E-Banking

- There are two different types of online banking:
  1. Internet banking
  2. Electronic banking

Internet Banking

- Through a PC that connects to a banking website via modem and phone line (or other telecommunication connection) and Internet Service Provider
- Or via wireless technology through PDA or cell phone

Electronic Banking

- By using Automated Teller Machines (ATMs), telephones (not via Internet) or debit cards. (debit cards look like credit card, but using debit card removes funds from your bank account immediately)

Internet Banking

- In this tutorial we shall focus on Internet Banking.
- No need explaining why Internet is so important e-channel:
  - 670 million users worldwide (end of 2001)
  - Almost 1.2 billion users in 2005 (forecasts, worldwide)
  - 54% of U.S. population (143 mil.) is using it (February 2002)
  - Every month 2 million users are going online only in USA

What Internet Banking Offers

- As a consumer, you can use Internet banking to:
  - Access account information
  - Review and pay bills
  - Transfer funds
  - Apply for credit
  - Trade securities
  - Find out if a check was cleared
  - Find out when a bill is due
  - Apply for mortgage
  - Search for the best loan rates
  - Compare insurance policies and prices

- Many consumers also like the idea of not waiting in line to do their banking, and paying their bills without shuffling papers and buying stamps.

Some Facts

- More then 12 million Internet bank consumers in Europe
- In Germany 51% of the online population use online banking services (average for Europe is 10%; expected to be 15% by the end of 2003)

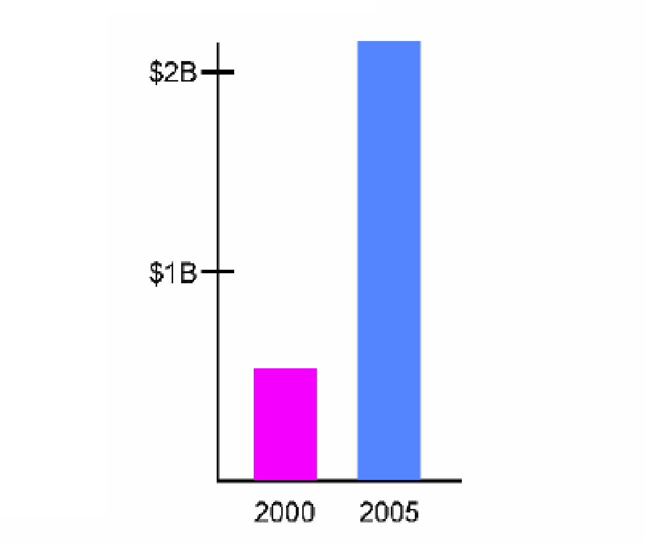


Figure 1. E-Banking Technology Investments

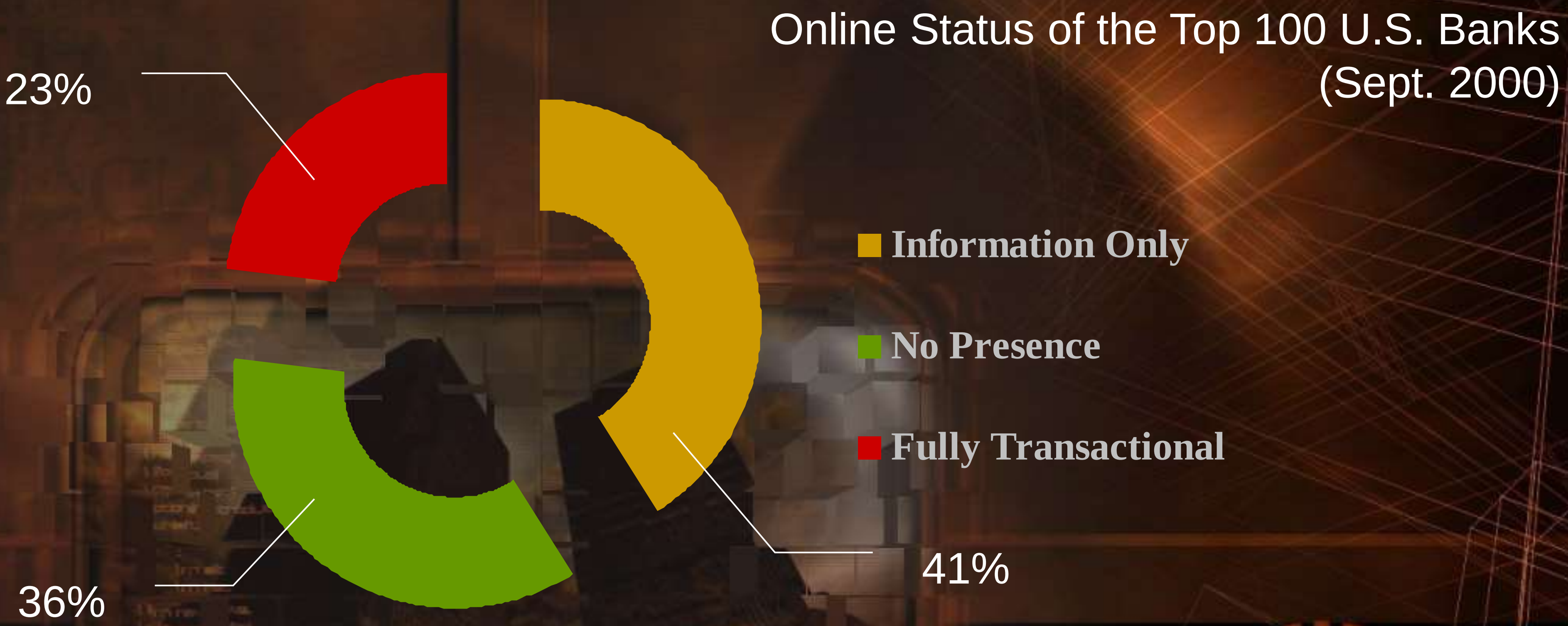
- Structural change in the new economy (USA)
- More then $2B investments in 2005 planned.

E-Banking in the USA

- Powerful banks are more present

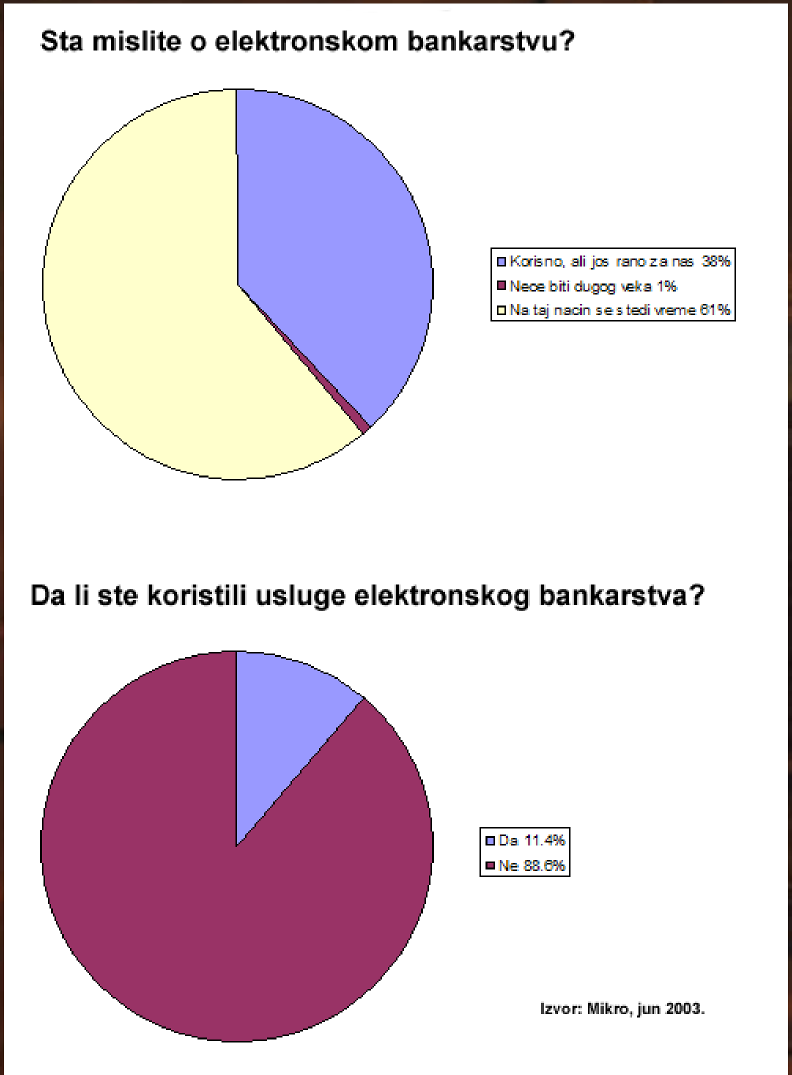
Assets	Number of Banks	Online Presence
Less then $100M	5,912	5%
$100M to $500M	3,403	16%
$500M to $1B	418	34%
$1B to $3B	312	42%
$3B to $10B	132	52%
More then $10B	94	84%

E-Banking in the USA



- Today about 1,100 U.S. banks, large and small, provide full-fledged transactional banking on-line
- In next two years additional 1,200 transactional on-line banks are expected
- By 2005, the number of such banks should increase to more than 3,000

E-Banking in Serbia


Sta mislite o elektronskom bankarstvu?

Da li ste koristili usluge elektronskog bankarstva?

Izvor: Mikro, jun 2003.

- Mali procenat korisnika
- Prilično veliko interesovanje

E-Banking in Serbia

- Elektronski promet Delta banke:
  6.5 milijardi dinara u prva tri meseca
- 25% naloga u Raiffeisen banci stižu elektronskim putem
- U HVB banci svaki drugi nalog je elektronski
- 35% prometa Nacionalne štedionice obavlja se kroz elektronske usluge
- 30% klijenata Atlas banke koristi elektronsko bankarstvo

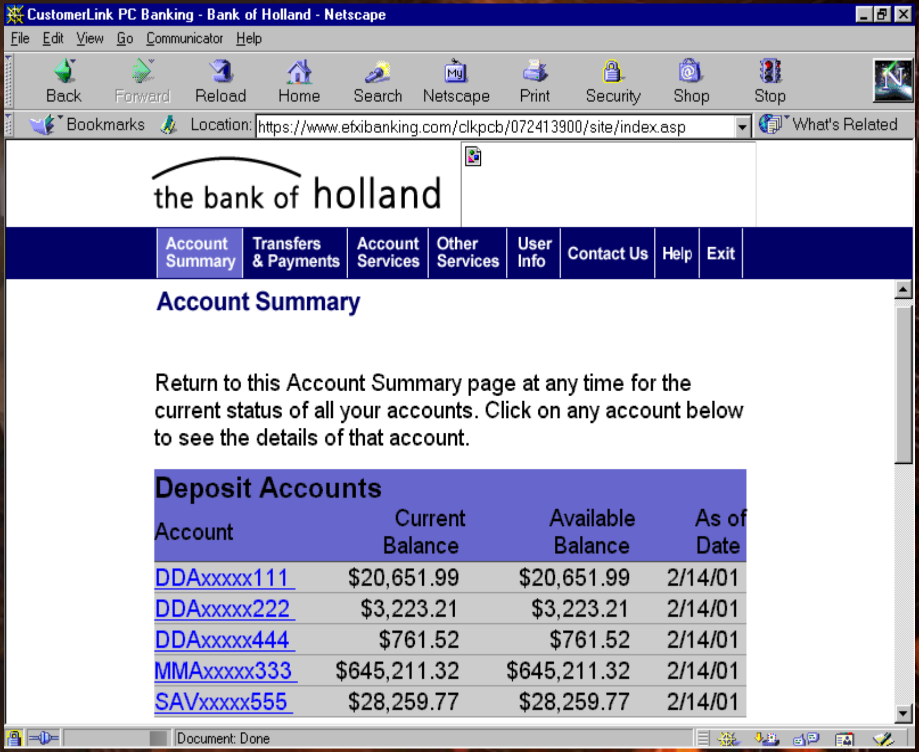
Izvor: Mikro, jun 2003.

Internet Banking

- Using Internet as an e-Channel makes financial services available to wide population

- WWW service

- In this tutorial we shall focus on the Internet banking


CustomerLink PC Banking - Bank of Holland - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks
Location: https://www.efxibanking.com/clkpcb/072413900/site/index.asp
What's Related
the bank of holland
Account Summary
Transfers & Payments
Account Services
Other Services
User Info
Contact Us
Help
Exit
Document: Done

Account Summary

Return to this Account Summary page at any time for the current status of all your accounts. Click on any account below to see the details of that account.

Deposit Accounts

Account	Current Balance	Available Balance	As of Date
DDAxxxxx111	$20,651.99	$20,651.99	2/14/01
DDAxxxxx222	$3,223.21	$3,223.21	2/14/01
DDAxxxxx444	$761.52	$761.52	2/14/01
MMAxxxxx333	$645,211.32	$645,211.32	2/14/01
SAVxxxxx555	$28,259.77	$28,259.77	2/14/01

Part II

E-Banking

Security Issues

Security problems

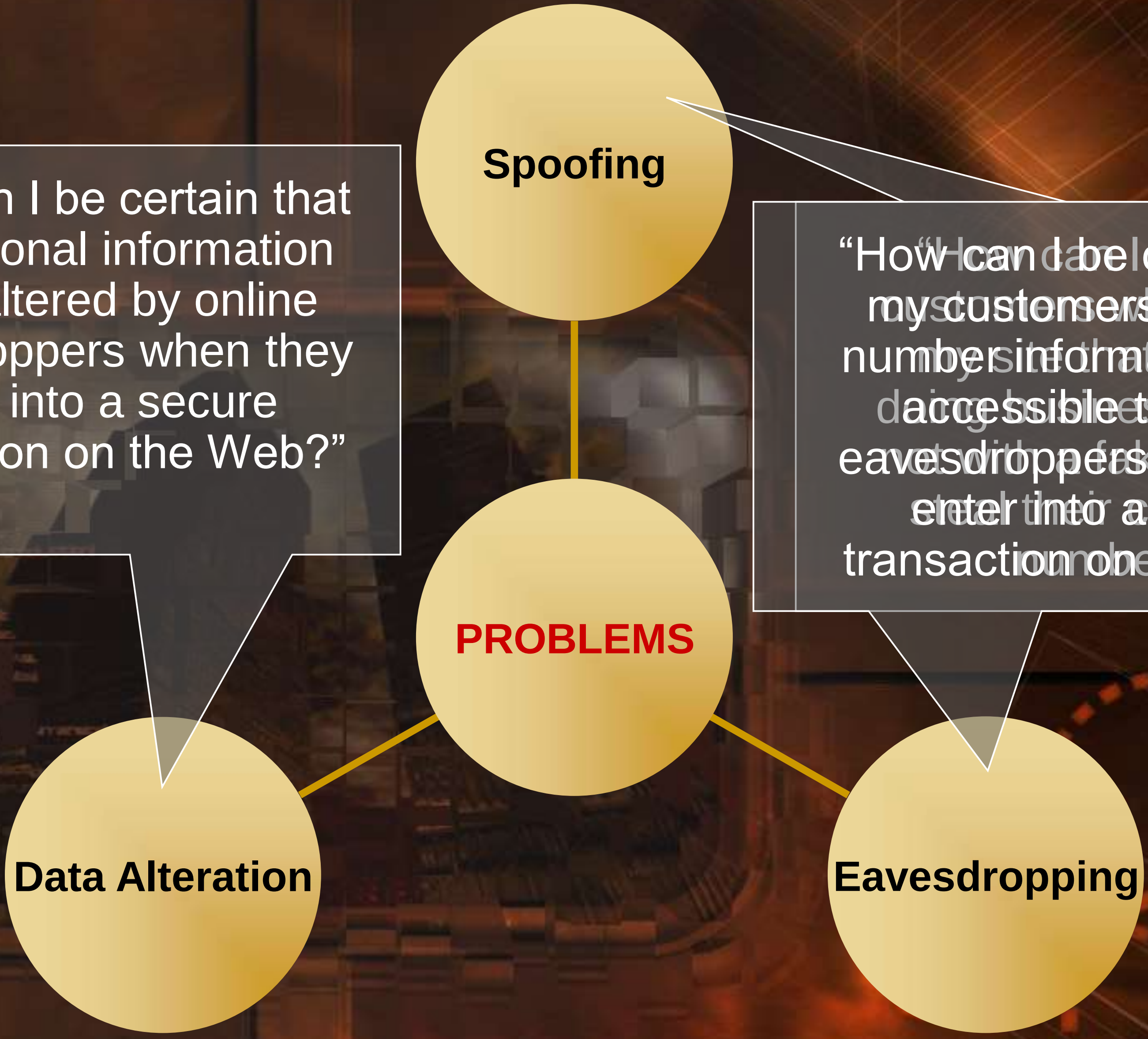
- Online banking relies on a networked environment.
- Network access can be performed through a combination of devices (PC, telephone, interactive TV equipment, card devices with embedded computer chips, ...)

- Connections are completed primarily through telephone lines, cable systems, in some instances even wireless tech.
- All these systems improve efficiency, speed and access but also present some privacy and security issues.
- Worth noting:
  Internal attacks are potentially the most damaging!

Security Problems

- Internet is a public network and open system where the identity of the communicating partners is not easy to define.
- Communication path is non-physical and may include any number of eavesdropping and active interference possibilities.
- *“Internet communication is much like anonymous postcards, which are answered by anonymous recipients.”*
- Although open for everyone to read, and even write in them, they must carry messages between specific endpoints in a secure and private way.

Security Problems

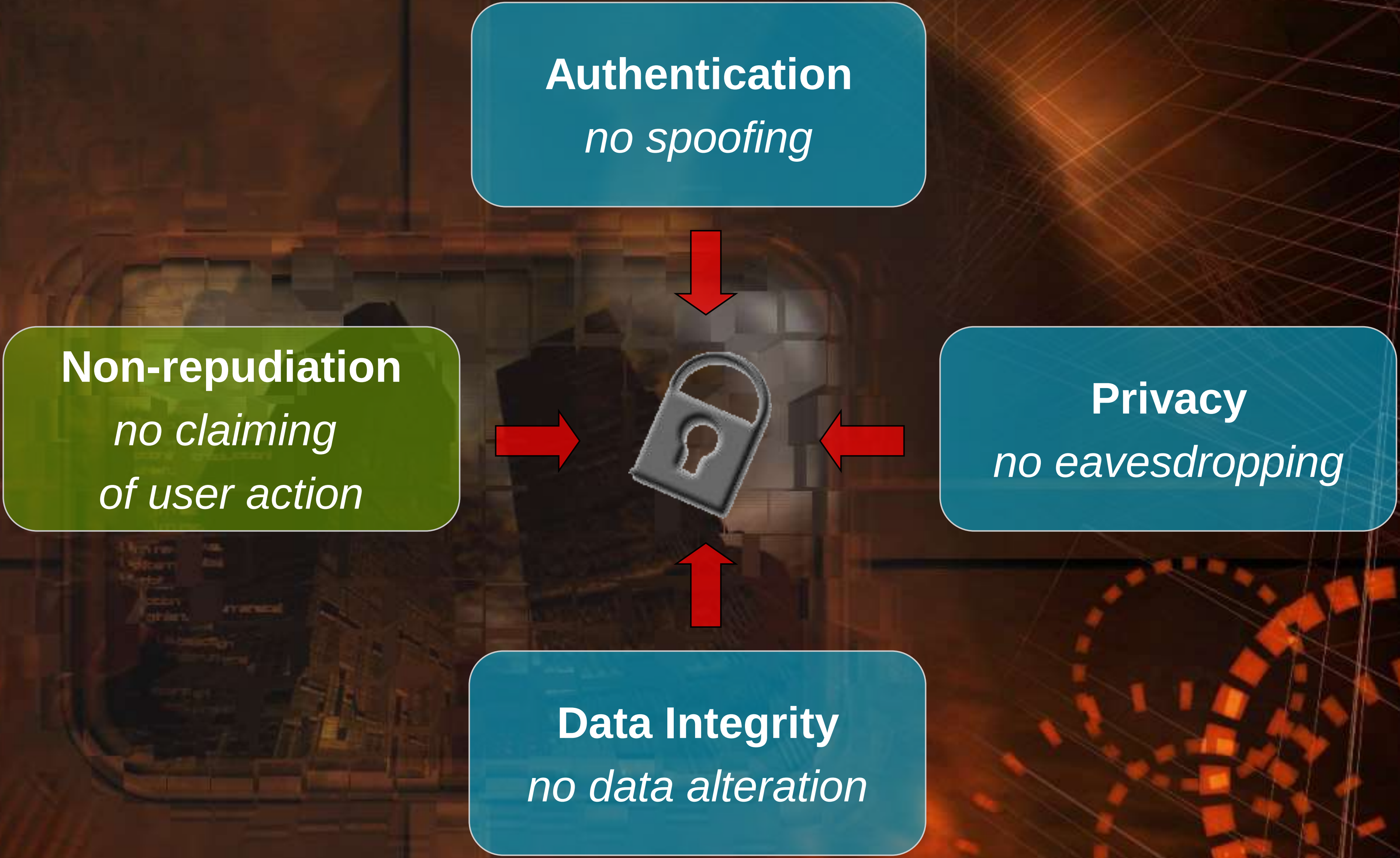


“How can I be certain that my personal information is not altered by online eavesdroppers when they enter into a secure transaction on the Web?”

“How can I be certain that my customers’ account number information is not accessible to online eavesdroppers when they enter into a secure transaction on the Web?”

“How can I reassure customers who come to my site that they are doing business with me, not with a fake set up to steal their credit card numbers?”

What Do We Have to Achieve



Authentication
no spoofing

Non-repudiation
no claiming
of user action

Privacy
no eavesdropping

Data Integrity
no data alteration

How to Achieve It?

- Cryptography algorithms to provide privacy.
- Digital Certificates and Digital Signatures
  for Web servers, to provide authentication.
  data integrity, and non-repudiation service.
- Secure Sockets Layer (SSL) uses all these techniques
  to achieve trusted communication.

  When URL begins with *https* it identifies the site as “secure” (meaning that it encrypts or scrambles transmitted information)

Few Security Tips 1/3

- Protect yourself from potential pitfalls and make your Internet banking more safe, productive and enjoyable by following these advices *(given by Federal Reserve Bank of Chicago)*

  - Make sure your transmissions are encrypted before doing any online transactions or sending personal information.
  - E-mail is usually *not* secure. Do not send sensitive data via e-mail (unless you know it is encrypted).
    Change all passwords and PIN codes received via e-mail that is not encrypted.
  - Make sure you are on the right website.

continued...

Few Security Tips 2/3

...continued

- Make sure that the financial institution is properly insured.
- Be “password smart”
(use mix of letters and numbers; change pw regularly; keep your pw and PIN codes to yourself; avoid easy to guess pw like first names, birthdays, anniversaries, social security numbers...)
- Keep good records. Save information about banking transactions. Check bank, debit and credit card statements thoroughly every month. Look for any errors or discrepancies.

continued...

Few Security Tips 3/3

...continued

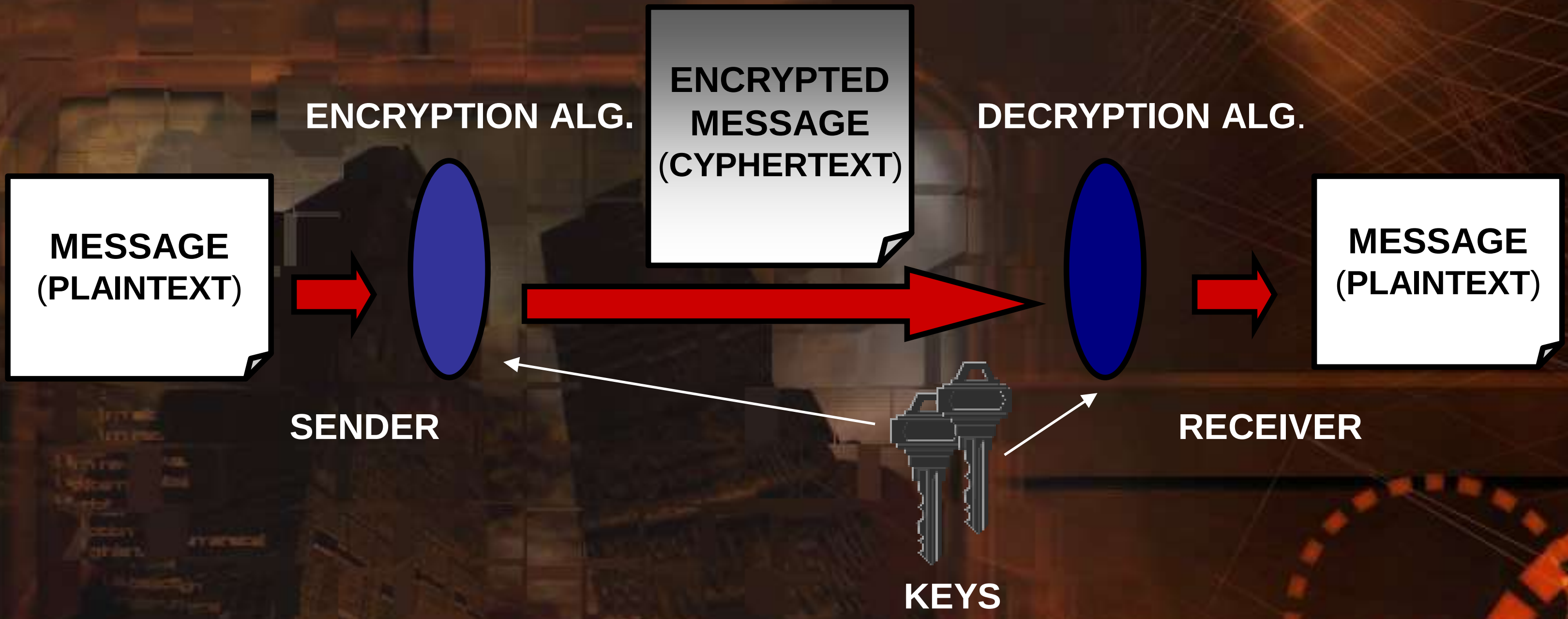
- Report errors, problems or complaints promptly
- Keep virus protection software up-to-date.
  Back-up key files regularly.
- Exit the banking site immediately after completing your banking.
- Do not have other browser windows open at the same time you are banking online.
- Do not disclose personal information such as credit card and Social Security numbers unless you know whom you are dealing with, why they want this information and how they plan to use it.

Know Your Rights

- There are regulations against unauthorized transactions (Including Internet banking, ATM and debit card transactions)
- A consumer's liability for an unauthorized transaction is determined by how soon the financial institution is notified (max. 60 days upon receipt of statement)
- When making purchases via the Internet it is smart to use a credit card instead of a debit card (liability should be no more than $50 if properly reported, plus you do not have to pay disputed amount during investigation).

Cryptography Basics

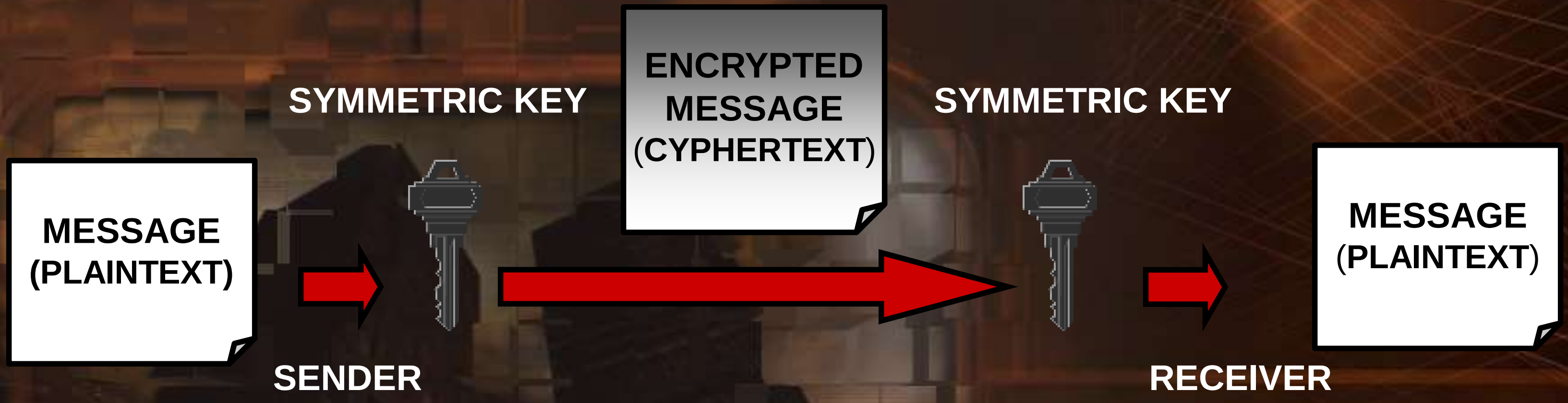
- Cryptography provides privacy



- Symmetric approach
- Asymmetric approach
- Hybrid approach

Symmetric Approach

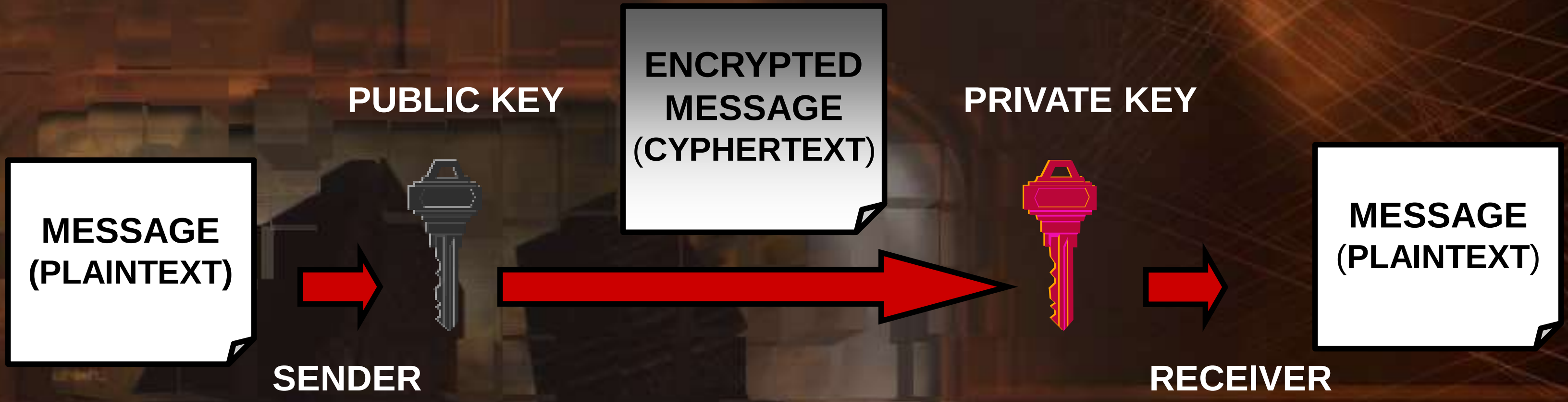
- Both sides use the same key for encryption and decryption



- Convenient for bulk data encryption (computationally faster then other methods)
- Problem: key distribution
- Examples: **DES** (Digital Encryption Standard, IBM & National Bureau of Standards, 1977, braking record 22h15m), 3DES (enhanced DES), AES (Joan Daemen & Vincent Rijmen, 2000)

Asymmetric Approach

- Sender uses public key for encryption, receiver uses private key for decryption



- Convenient for short data encryption (computationally slower then other methods)
- Problem: binding the public key and its owner.
- Examples: **RSA** (Ronald Rivest, Adi Shamir & Leonard Adleman, 1977), basics given by Whitfield Diffie & Martin Hellman (1976), …

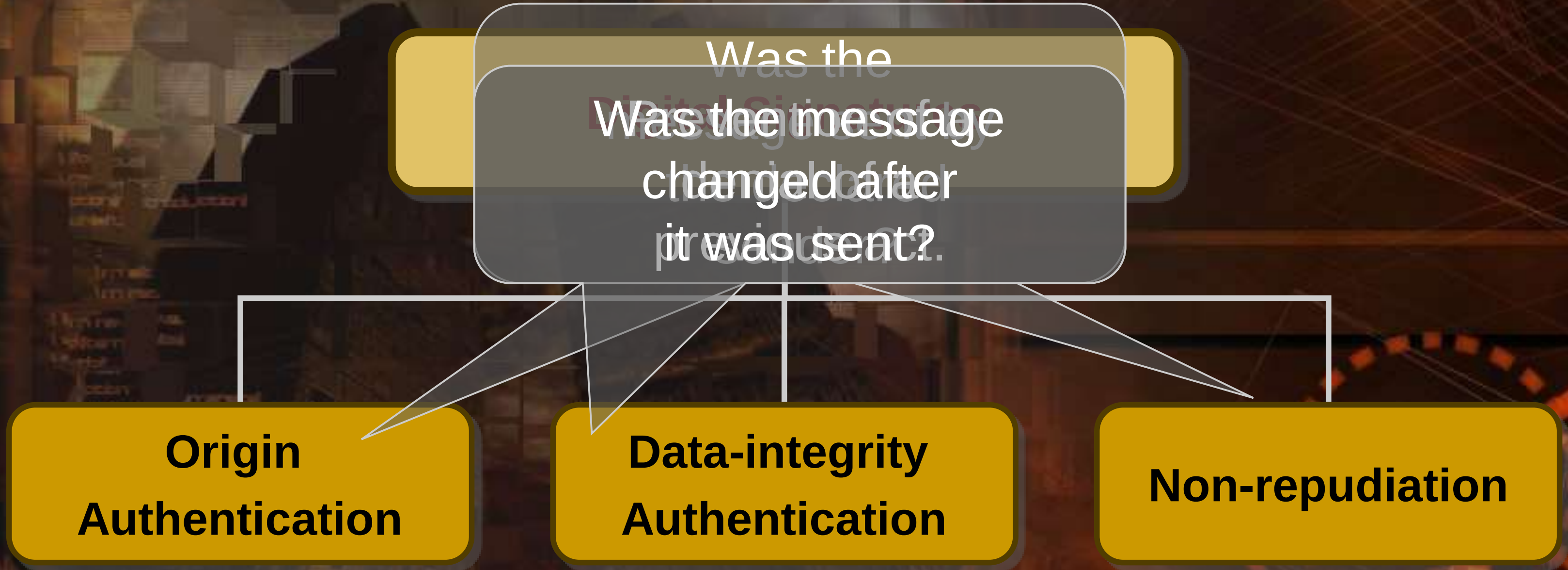
Hybrid Approach

- Uses asymmetric approach for passing the symmetric key
- Uses symmetric approach for data encryption

This approach is applied in SSL

Digital Signatures

- Cryptography provides privacy, but what about security?
- As mentioned before, from a security point of view, we have to achieve three important things:



Digital Signature

Was the

Was the message changed after it was sent?

Origin Authentication

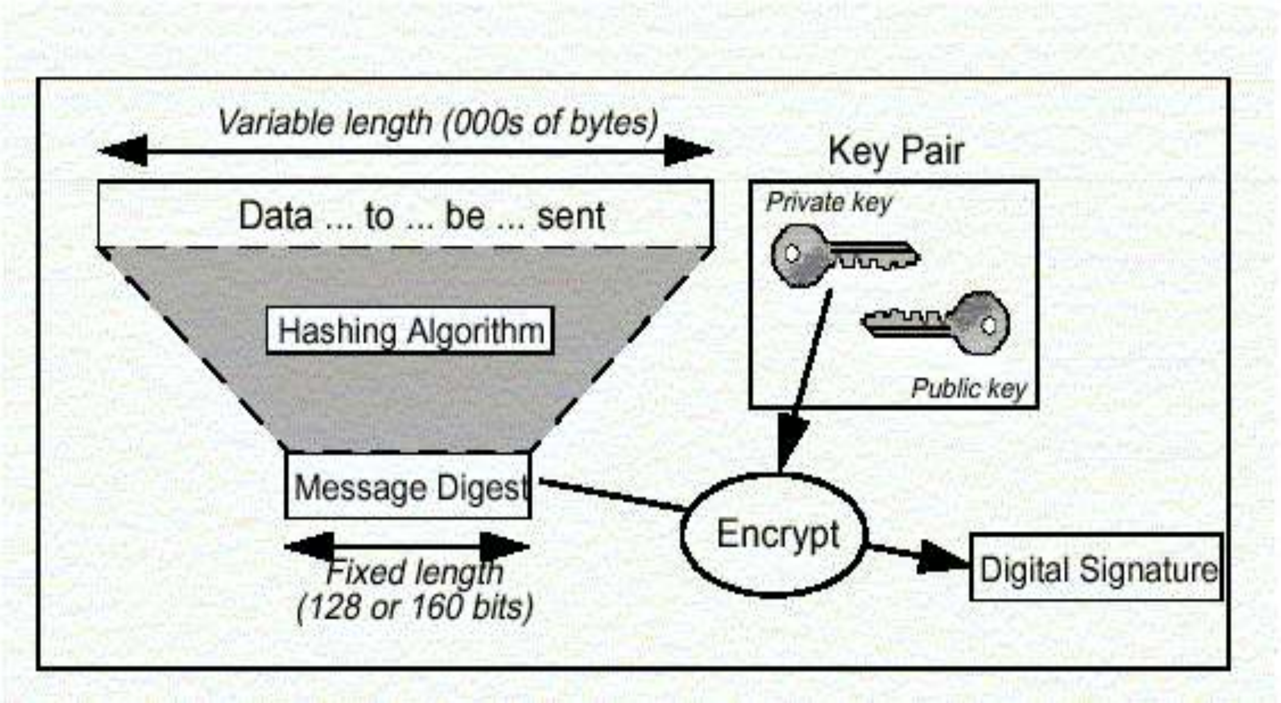
Data-integrity Authentication

Non-repudiation

- This is all accomplished through the Digital Signatures.

Digital Signatures

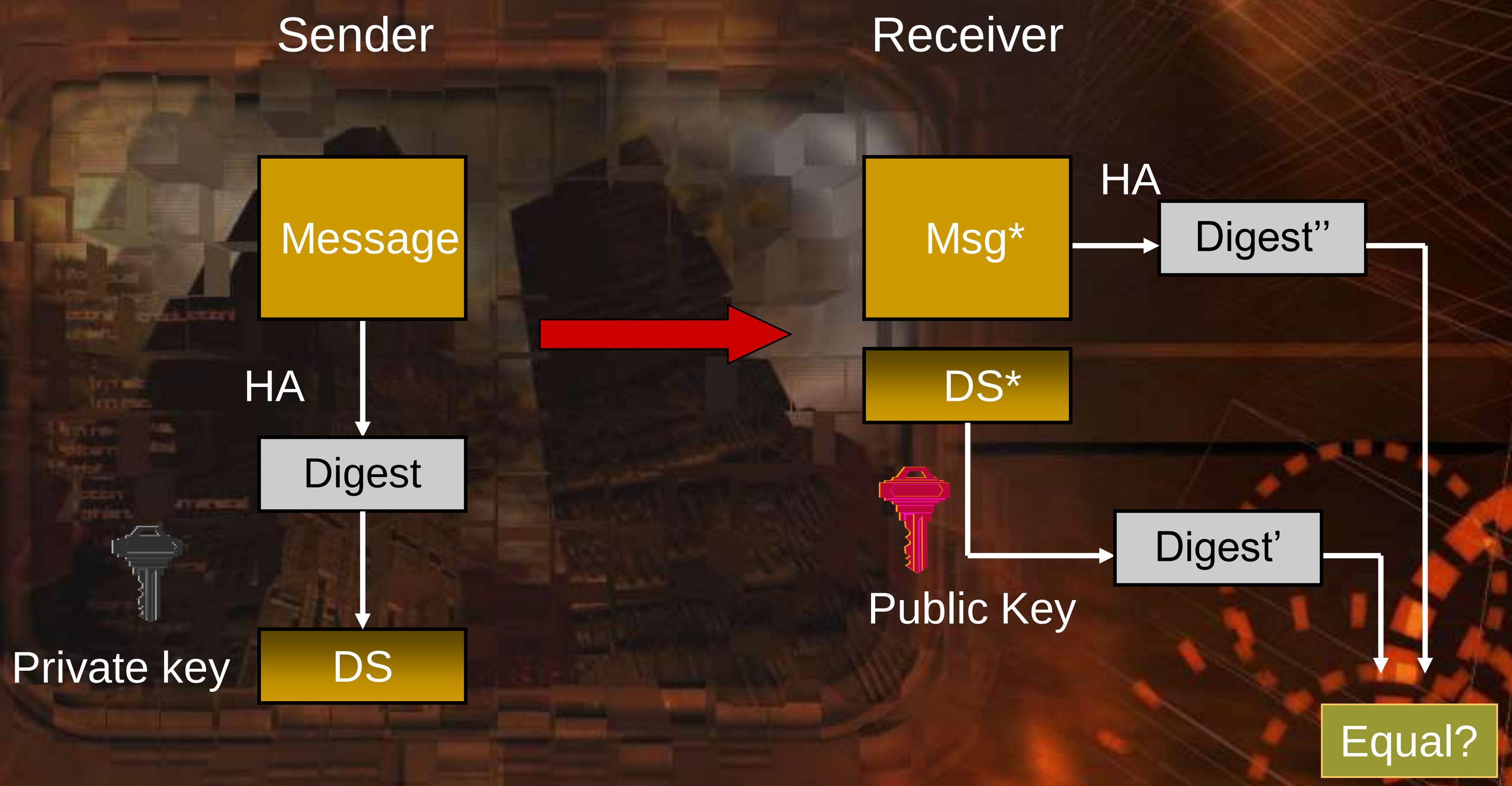
- Process of generation of Digital Signatures:



- Creating message digest using one way hashing algorithm (MD5 from RSA, SHA-1 from NIST…)
- Encrypting digest with private key

Digital Signatures

- Authentication of the message using Digital Signature:



Digital Signatures

“***Non-repudiation****: a service that prevents the denial of a previous act.”*

A. Menezes – “Handbook of Applied Cryptography”

- Non-repudiation service provides proof of the integrity and origin of data – both in an unforgeable relationship which can be verifiable by any third party at any time.

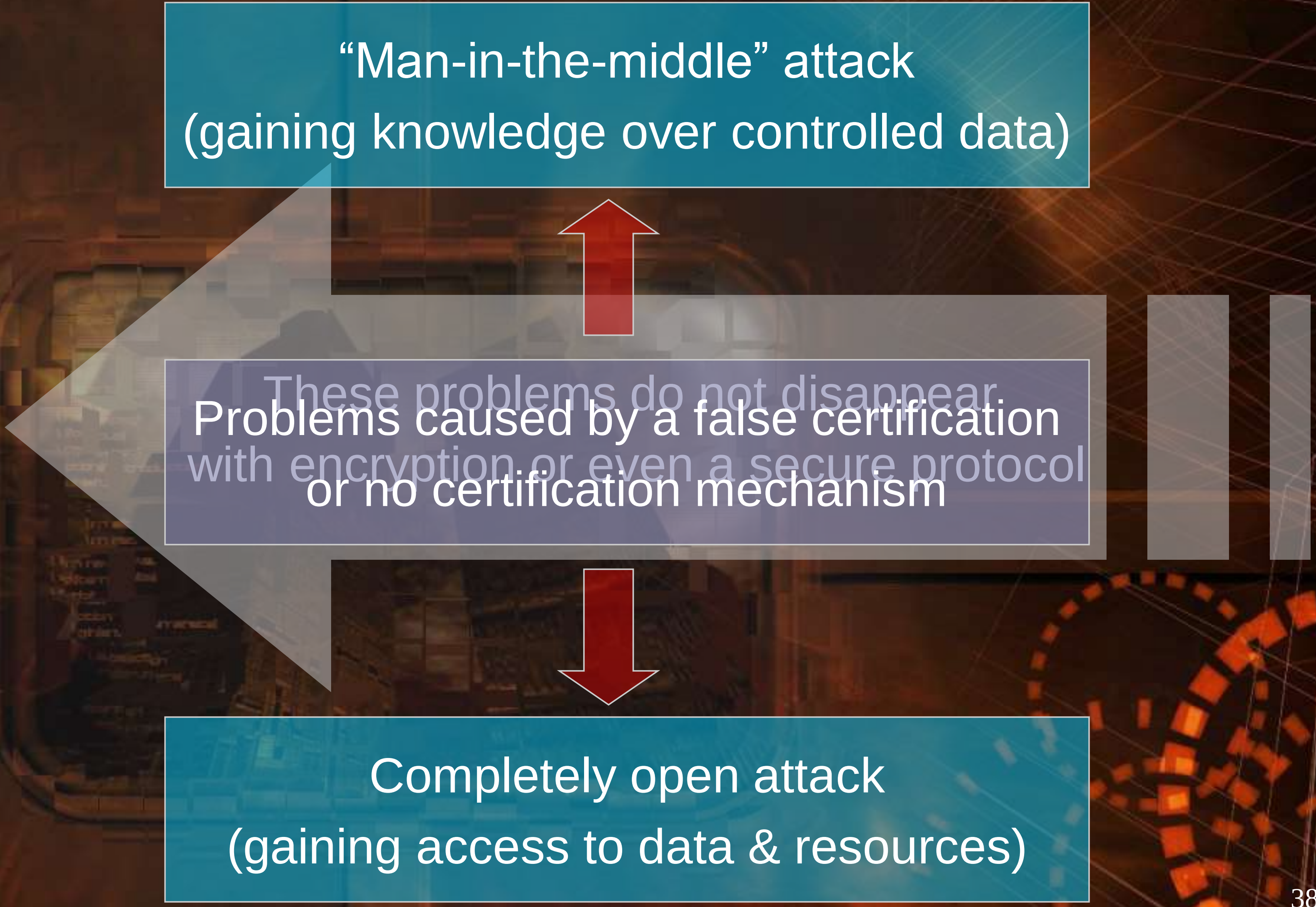
Key Management Problem

- The whole system of Digital Signatures relies on the capability to securely bind the public key and its owner.

  - Q1: “How can I be sure that the public key my browser uses to send account number information is in fact the right one for that Web site, and not a bogus one?”
  - Q2: “How can I reliably communicate my public key to customers so they can rely on it to send me encrypted communications?”

- The solution is to use Digital Certificates.

Digital Certificates



“Man-in-the-middle” attack

(gaining knowledge over controlled data)

Problems caused by a false certification or no certification mechanism

Completely open attack

(gaining access to data & resources)

These problems do not disappear with encryption or even a secure protocol

Certification

- Certificates provide strong binding between the public-key and some attribute (name or identity).

- Certificates introduce tamperproof attributes used to help someone receiving a message decide whether the message, the key and the sender’s name are what they appear to be...

  without asking the sender.

Certainly the administration sees you as more than just a number, Miss...uh...
Phil Frank

©CREATIVE MEDIA SERVICES Box 5955 Berkeley, Ca. 94705

Absolute certification methods are logically impossible because a certificate cannot certify itself.

Digital Certificates

- An electronic file that uniquely identifies communication entities on the Internet.
- Associate the name of an entity with its public key.
- Issued and signed by Certification Authority.

DN=Bill Davis
CA

Everybody trusts CA, and CA is responsible for entity name – public key binding.

ITU-T Recommendation X.509

X.509 defines framework for provision of authentication services under a central control paradigm represented by “Directory”

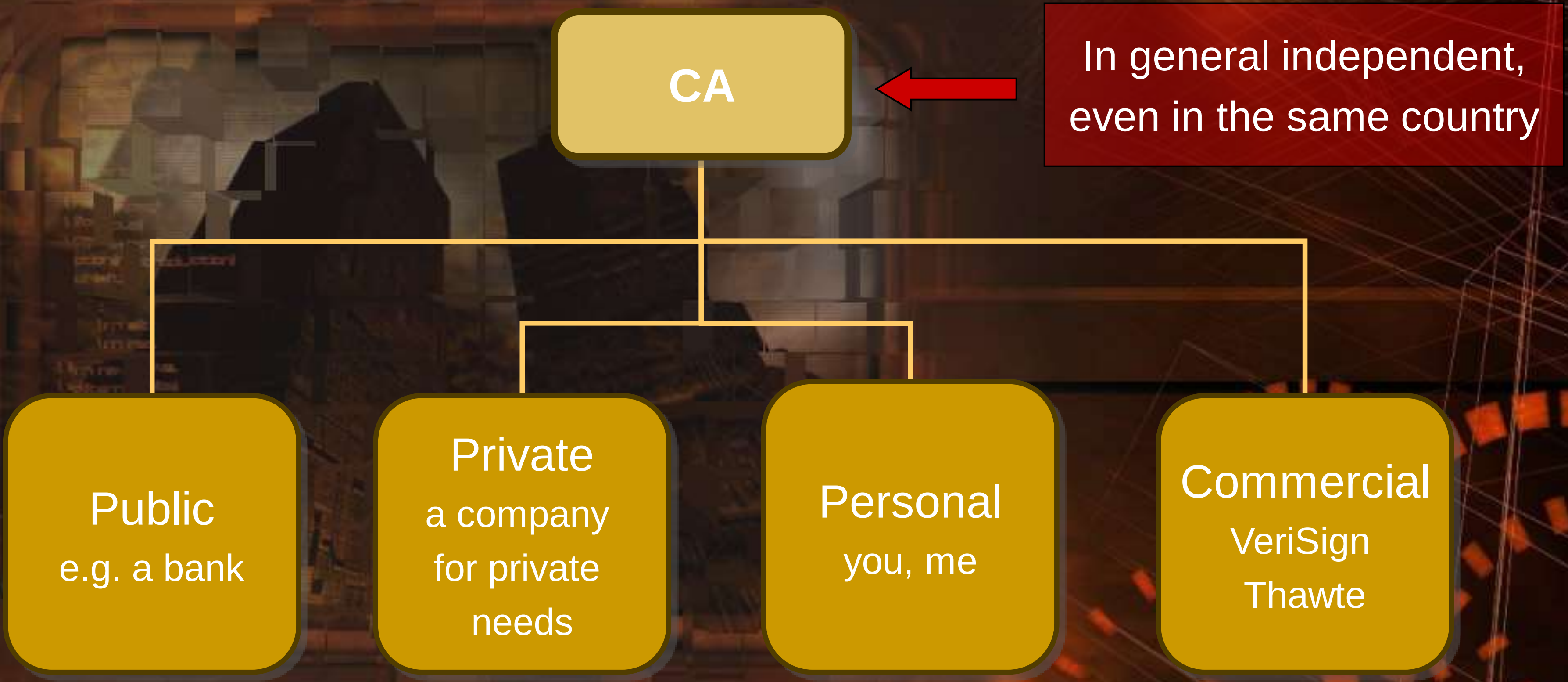
De facto standard

There are three main entities recognizable in X.509 certification procedures

The “Directory” is implemented by **CA**, which issues certificates to **subscribers** (CA clients) in order for such certificates to be verifiable by **users** (the public in general).

Certification Authority

- **CA** is a general designation for any entity that controls the authentication services and the management of certificates (also called **issuer**)


CA
In general independent, even in the same country
Public
e.g. a bank
Private
a company for private needs
Personal
you, me
Commercial
VeriSign
Thawte

X.509 Naming Scheme

- A certificate associates the public key and unique distinguished name (**DN**) of the user it describes.
- Authentication relies on each user possessing a unique distinguished name.
- The DN is denoted by a NA
  and
  as u
  whe

Maybe it has streamlined the information system but I still don't like it!
33017 001
17 00112
Berkeley, Ca. 94705

It's interesting to note that the same user can have different DNs in different CAs, or can have the same DN in different CAs even if the user is **not the first** to use it in any of the CAs.

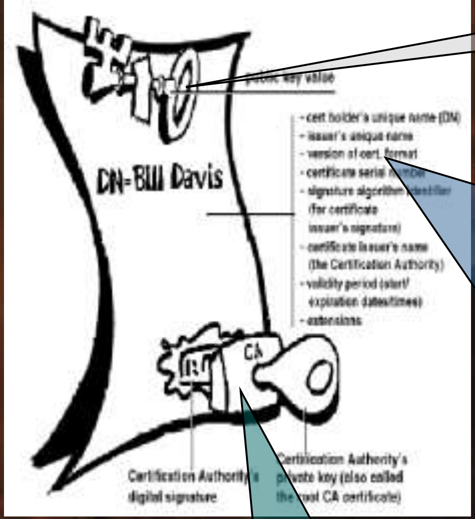
How X.509 Certificate Is Issued

Section 3.3.3 of X.509v3 defines a certificate as:

user certificate; public key certificate; certificate:

> *the public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.*

Contents of X.509 Certificate

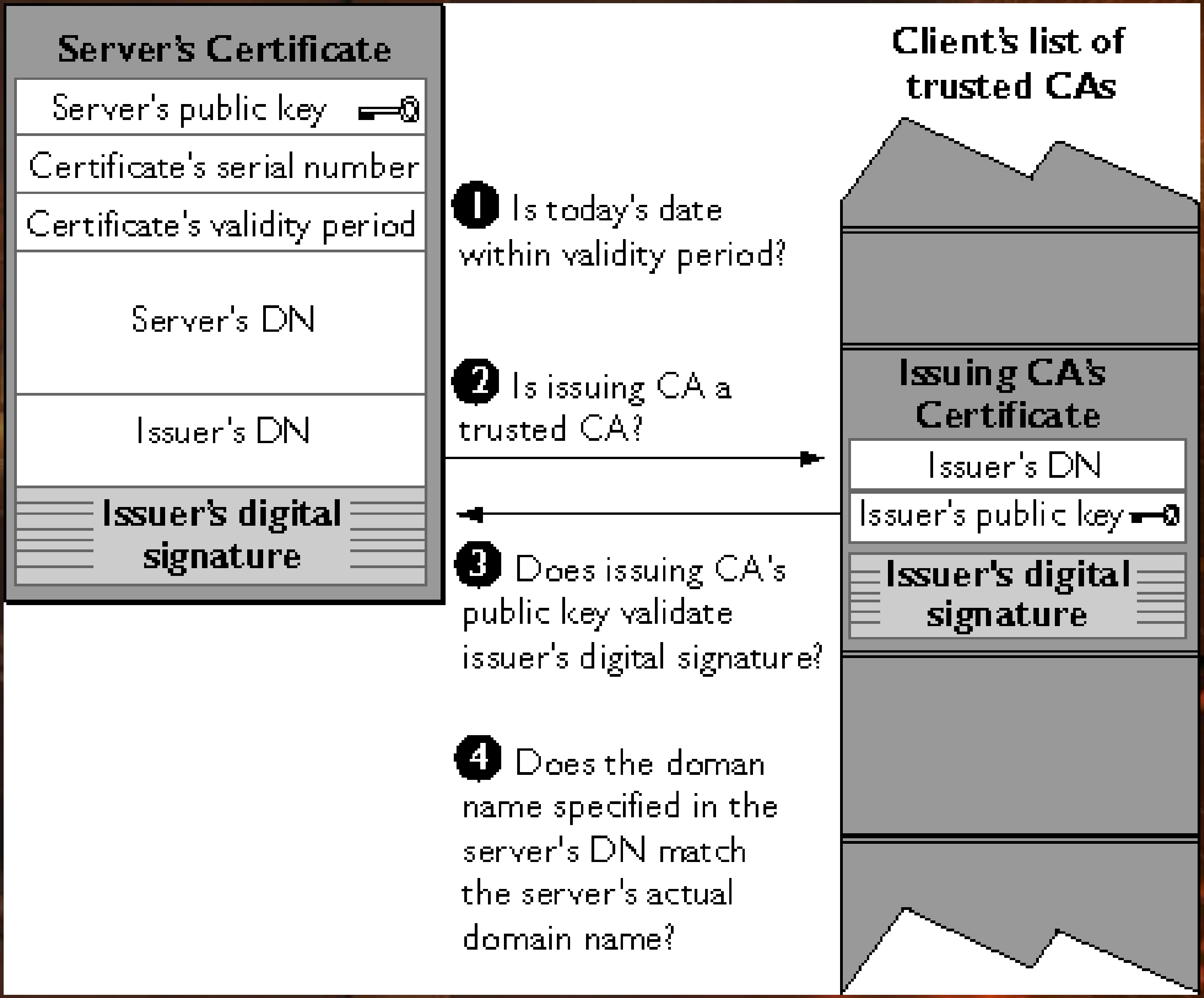

public key value
- cert holder's unique name (DN)
- issuer's unique name
- version of cert. format
- certificate serial number
- signature algorithm identifier (for certificate issuer's signature)
- certificate issuer's name (the Certification Authority)
- validity period (start/ expiration dates/times)
- extensions
DN=Bill Davis
CA
Certification Authority's digital signature
Certification Authority's private key (also called the root CA certificate)

The certificate holder's public key value

- The certificate holder's unique name (DN)
- Version of the certificate format
- Certificate serial number
- Signature algorithm identifier (for certificate issuers signature)
- Certificate issuer's name (the CA)
- Validity period (start/expiration dates/times)
- Extensions

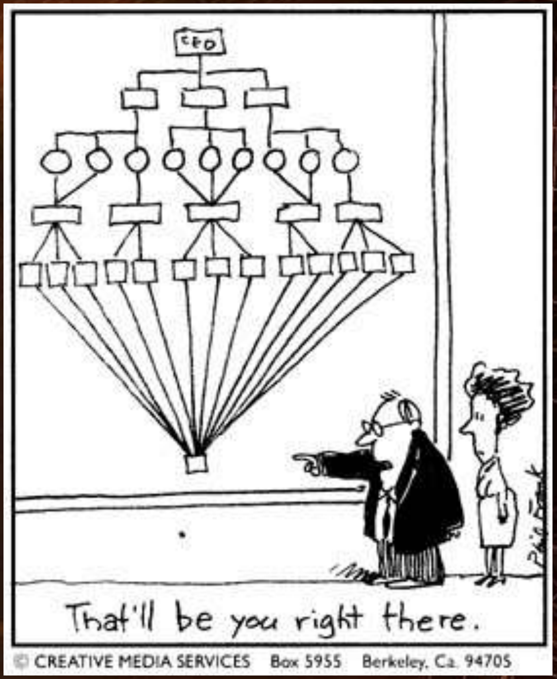
Certificate is signed by the CA with its private key

Verification of DCs in User Browser


Server's Certificate
Server's public key
Certificate's serial number
Certificate's validity period
Server's DN
Issuer's DN
Issuer's digital signature
1 Is today's date within validity period?
2 Is issuing CA a trusted CA?
3 Does issuing CA's public key validate issuer's digital signature?
4 Does the doman name specified in the server's DN match the server's actual domain name?
Client's list of trusted CAs
Issuing CA's Certificate
Issuer's DN
Issuer's public key
Issuer's digital signature

Verification of DCs in User Browser

- Most of the servers that use CA certificates force the client to accept certain CAs’ signatures (for top level CAs), which are “hardwired” into the software, or stored on Smart cards.



© CREATIVE MEDIA SERVICES Box 5955 Berkeley, Ca. 94705

- The CAs’ PK may be the target of an
  e
  –
  a

➲ CAs that may be the most probable targets are the ones that offer the smallest protection level.

➲ Protection, in this case, is an inverse function of worth.

Useful Links to Visit

Two largest commercial CA's:

- www.verisign.com

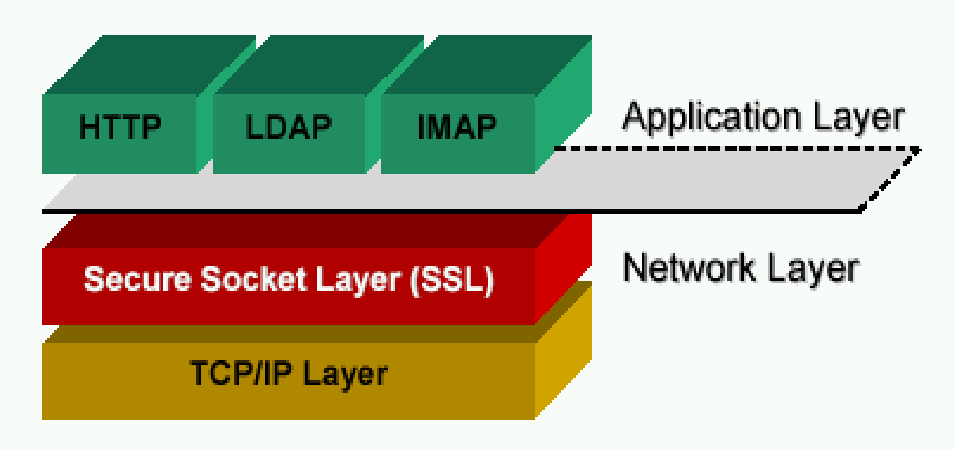
  how to apply for DC, security related stuff

- www.thawte.com

  how to apply for DC, security related stuff

Secure Sockets Layer

- SSL is perhaps the widest used security protocol on the Internet today.



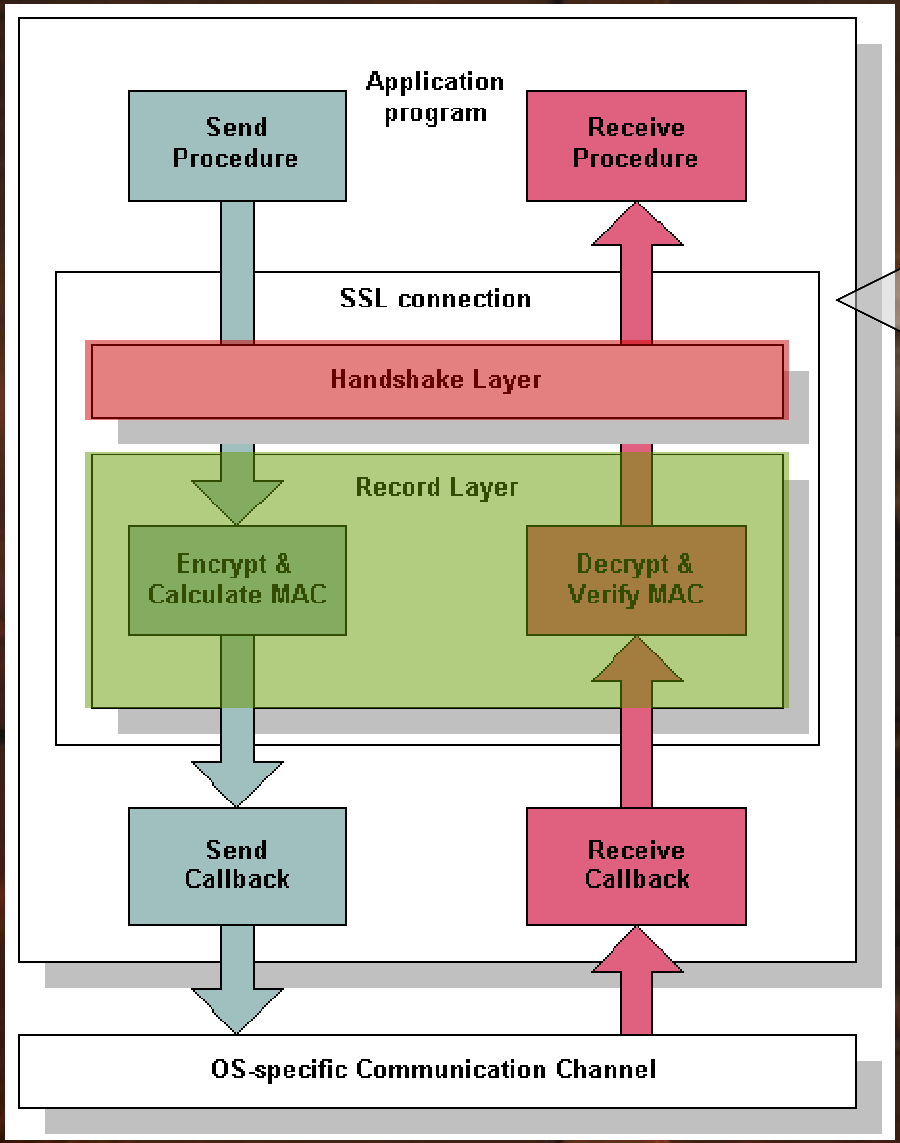
- Together with DC enables secure communication over the TCP/IP network

Common mistake is to regard HTTPS and S-HTTP as identical

HTTPS = HTTP + SSL (part of the Network Layer)
S-HTTP = Secure HTTP (superset of HTTP and part of the App. Layer)

- Higher level protocols can layer on top of the SSL transparently.

SSL Communication Channel



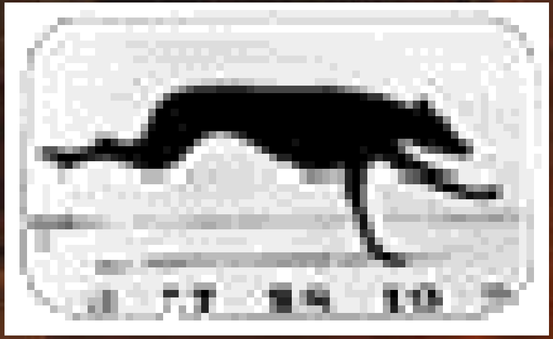
SSL connection is established between application program and OS specific communication channel.

SSL has two layers:

- Handshake Layer
- Record Layer

SSL Record Layer

- At the lowest level, layered on top of some reliable transport protocol (e.g. TCP)
- It provides connection security using data encryption with symmetric cryptography and message integrity check with keyed MAC (Message Authentication Code)
- As a public key for encryption for every SSL session we create a randomly generated temporary master key, SSK (adoption of a SSK is described in Handshake Layer)



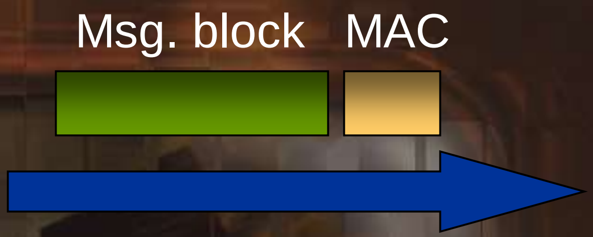
SSL Data Exchange Phase (simplified)

Client

Fragments msg. into blocks (bytes)

Calculates MAC and appends it to msg.

Encrypts data with SSK



Msg. block MAC

Server

Decrypts data with SSK

Calculates new MAC and verifies the old one

Reassembles the msg.

Failures to authenticate, decrypt or otherwise get correct answers result in a close of connection.

SSL Handshake Layer

- A handshake occurs when a machine tries to *use* a SSL connection.
- If connection is opened, but no session exist recently (suggested under 100 sec - SSL, C.8) we have to make a new handshake.
- Other type of handshake occurs when client authentication is desired.

SSL Handshaking Phase (simplified)

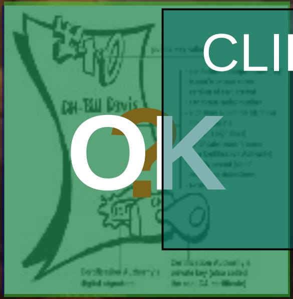
Client

Server

List of supported ciphers

CLIENT-HELLO message
+
Challenge

Strongest cipher supported + DC



SERVER-VERIFY message
+
Responding challenge (encrypt. with SWK)

SERVER-HELLO message
+
Connection ID

SSK generated and encrypted with SPK

CLIENT-MAST KEY (ncrypt. with SPK)

Decrypts SSK with own SK and sends ack.

From now use SSK!

CLIENT-FINISHED message (encrypt. with CWK)

SSL Handshaking Phase

- If client authentication is in use there are three more steps:

1. REQUEST-CERTIFICATE message challenge’ + means of authentication desired
2. CLIENT-CERTIFICATE message client certificate’s type + certificate + bunch of response data
3. SERVER-FINISHED message

SSL Keys

- There are number of keys used over the course of a conversation:
  - Server’s public key (SPK)
  - Master key (SSK) – randomly generated
  - Client-read-key also called Server-write-key (CRK/SWK)
  - Client-write-key also called Server-read-key (CWK/SRK)

- CWK & CRK are derived via a secure hash from the master key, the challenge, and the connection ID.
- Only master key is sent encrypted (with SPK)
- The master key is reused across sessions, while the read- & write- keys are generated anew for each session.

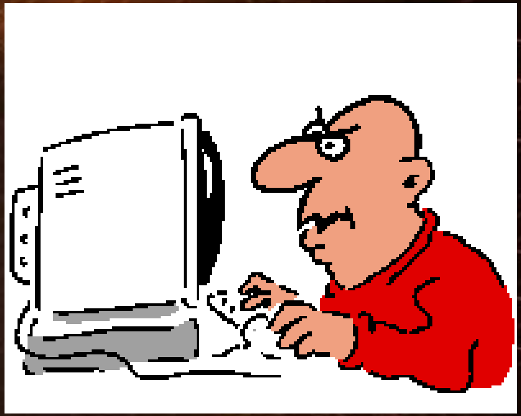
SSL Data Exchange Phase

- Once the handshaking is complete,
  the application protocol begins to operate,
  as described in the Record Layer.
  (this is also called the data-exchange phase, as noted before)

- SSL specification is not clear at what point the SSL connection is consider to be done with a connection, or what to do with the keys at that point.

- Implicitly, the session is done when the TCP connection is torn down, and the keys should be kept for roughly 100 sec after that (although that is not explicitly defined)

About SSL Strength



- Two variants of SSL:

  40-bit and 128-bit
  (refers to master key length)

- According to RSA labs it would take a trillion trillion years to crack 128-bit SSL using today's technology!

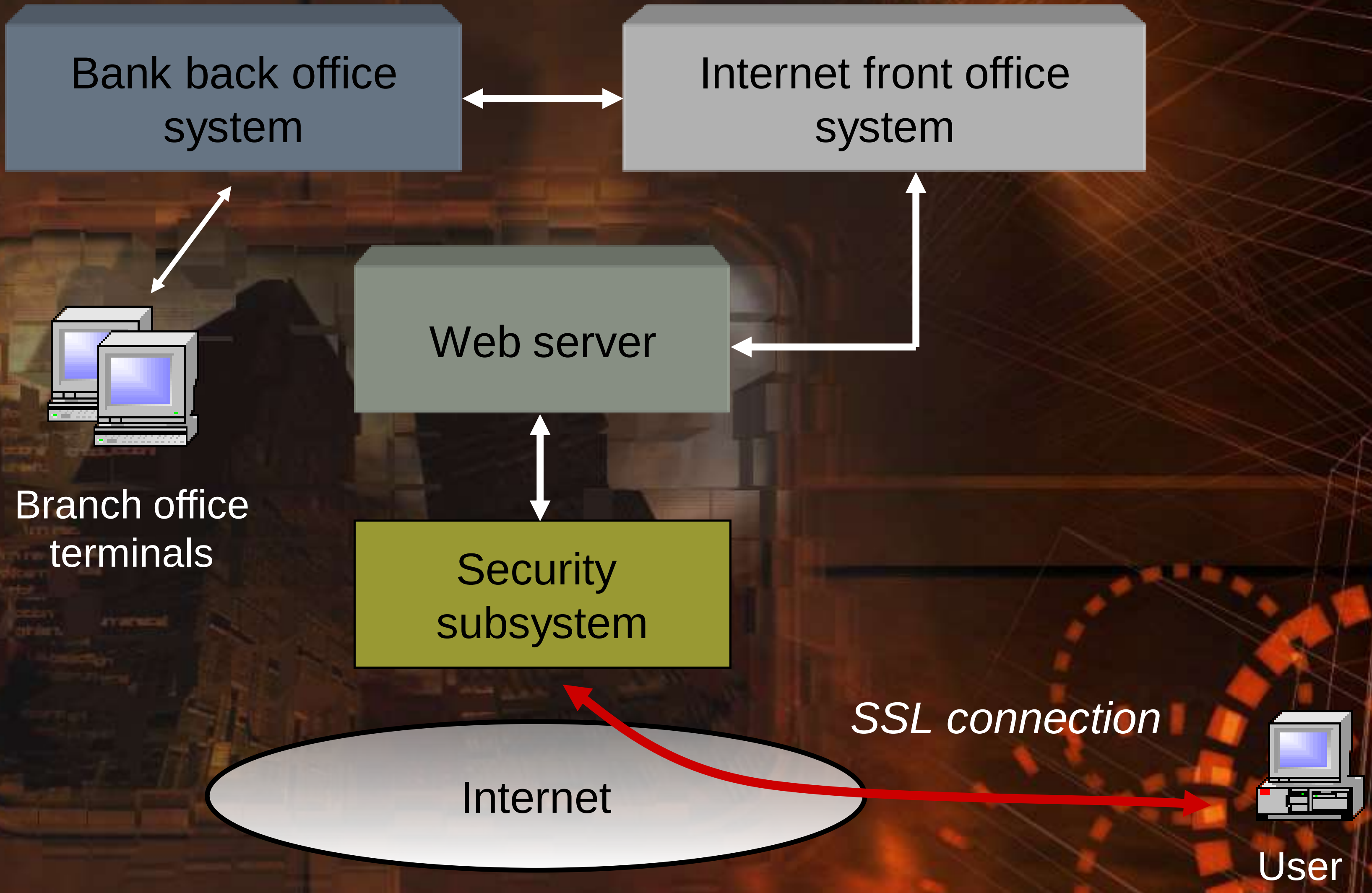
- However, SSL, being a low level protocol, does little to protect you once your host is compromised.

Part III

E-Banking

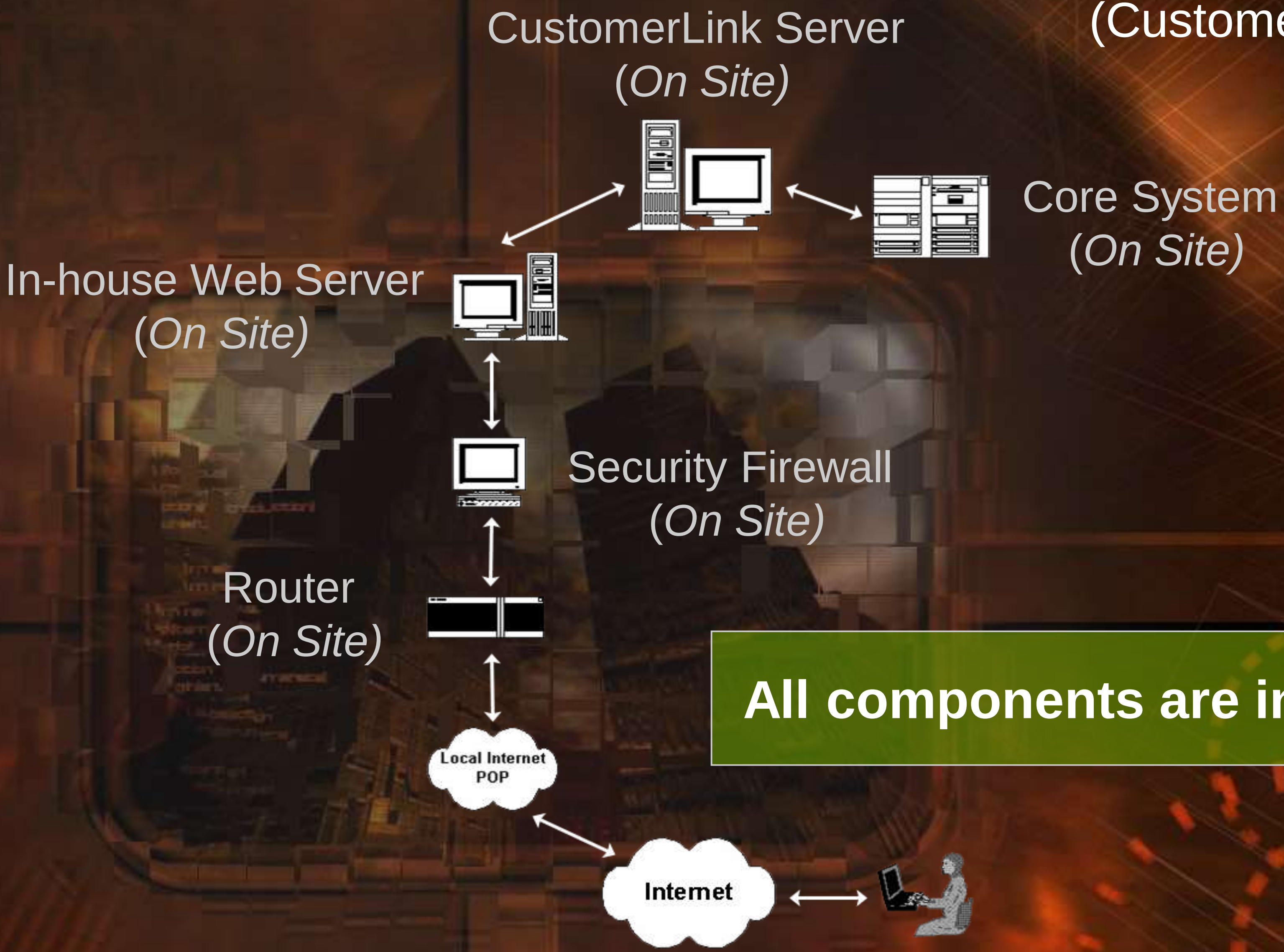
Bankers' Point of View

Internet Bank Architecture



In-house Architecture

(CustomerLink Primer)



CustomerLink Server *(On Site)*

Core System *(On Site)*

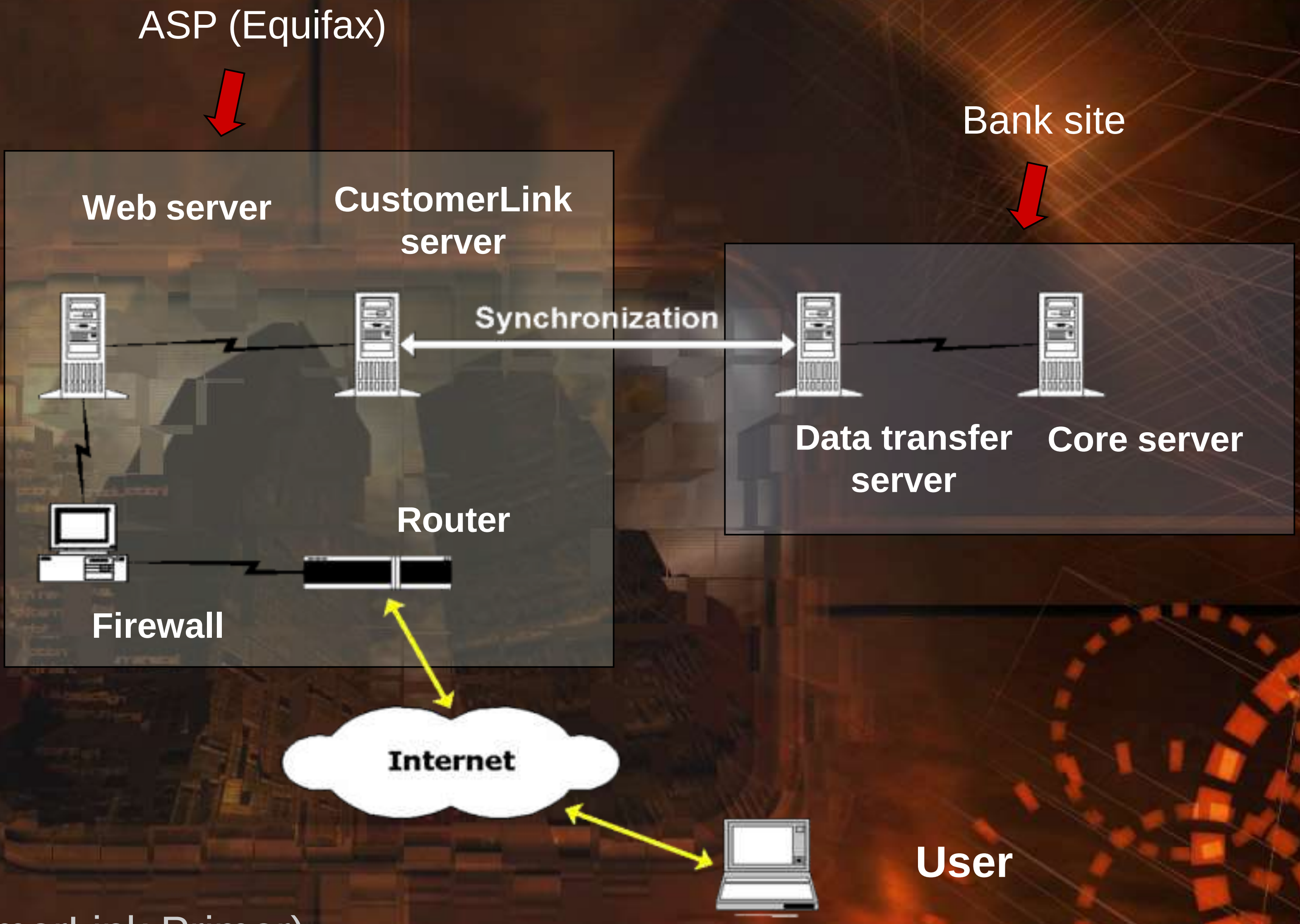
In-house Web Server *(On Site)*

Security Firewall *(On Site)*

Router *(On Site)*

All components are in the bank

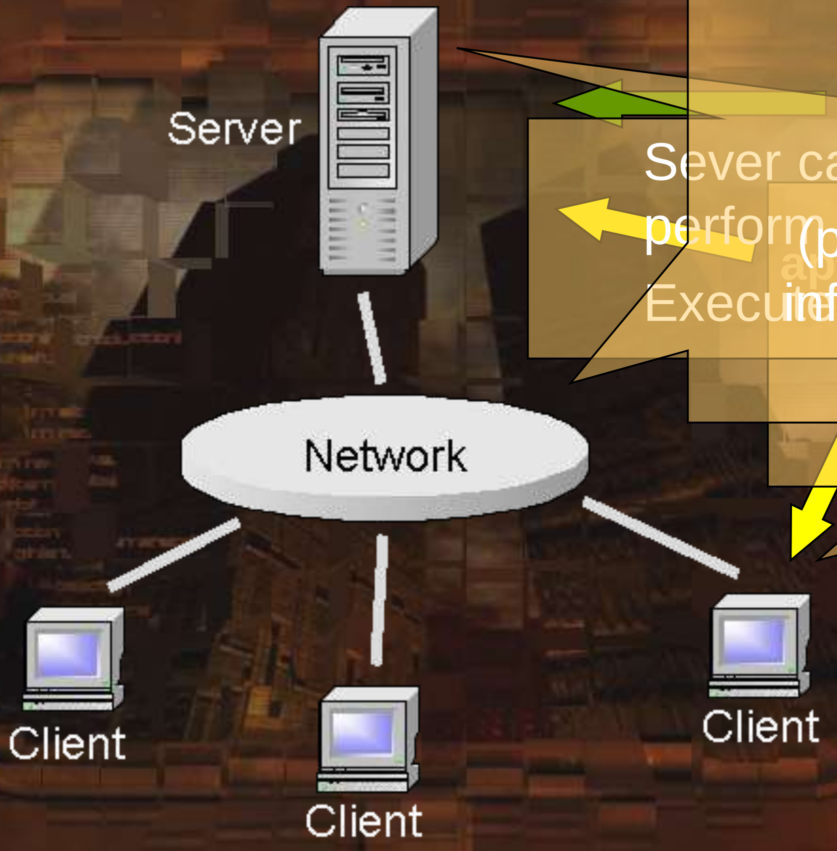
Out-of-house Architecture



(CustomerLink Primer)

Banking Software Architecture

- Before Internet revolution, banking software systems were dominantly of client-server type



CLIENT-SERVER

The network configuration where the work potential (processing abilities & accessible information) is distributed between several machines.

Sever can access huge databases and perform searches on behalf of the client. Executes Back-end application.

Clients demand information from other machines – servers. Executes Front-end App.

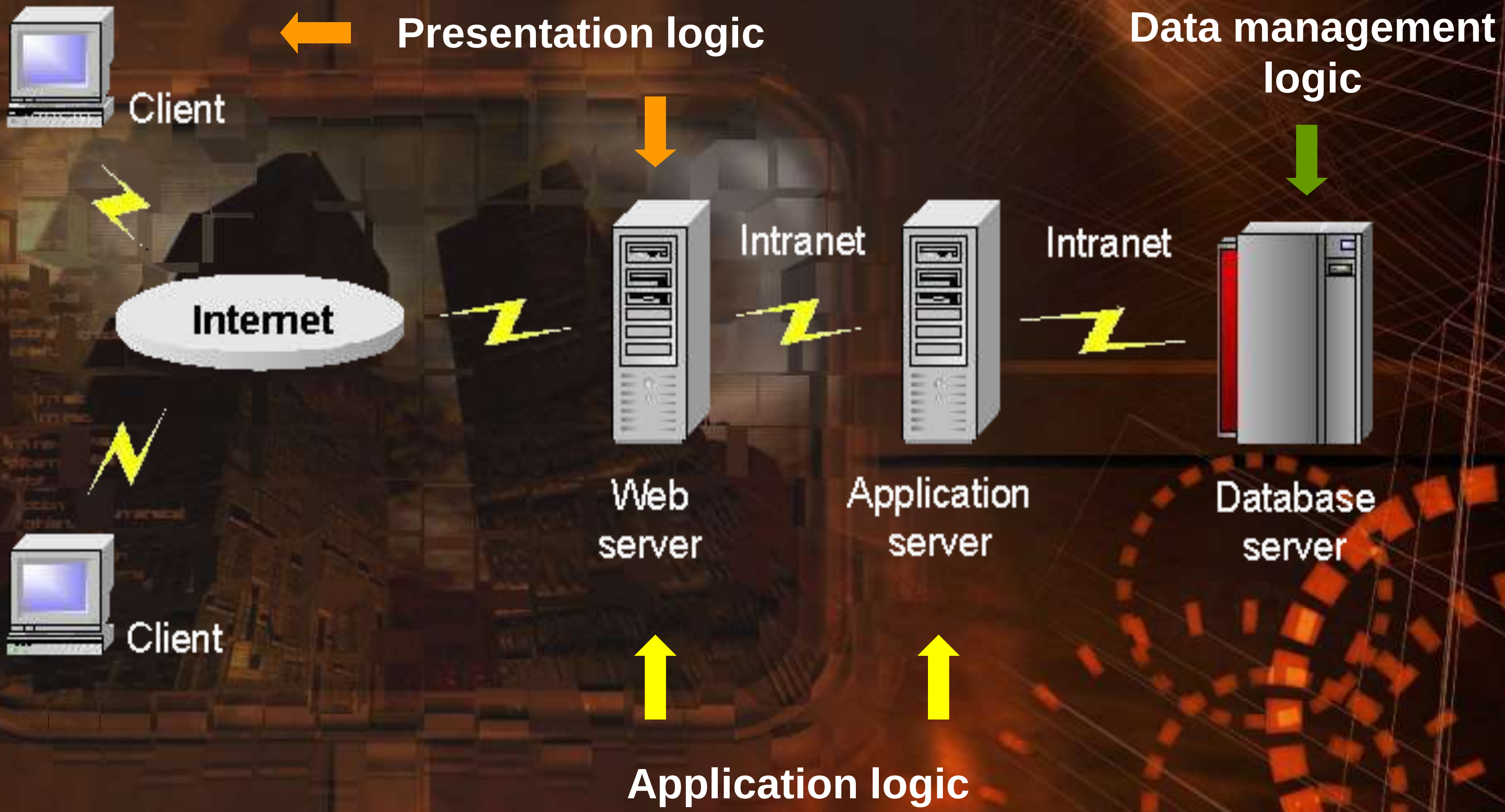
data management

application logic

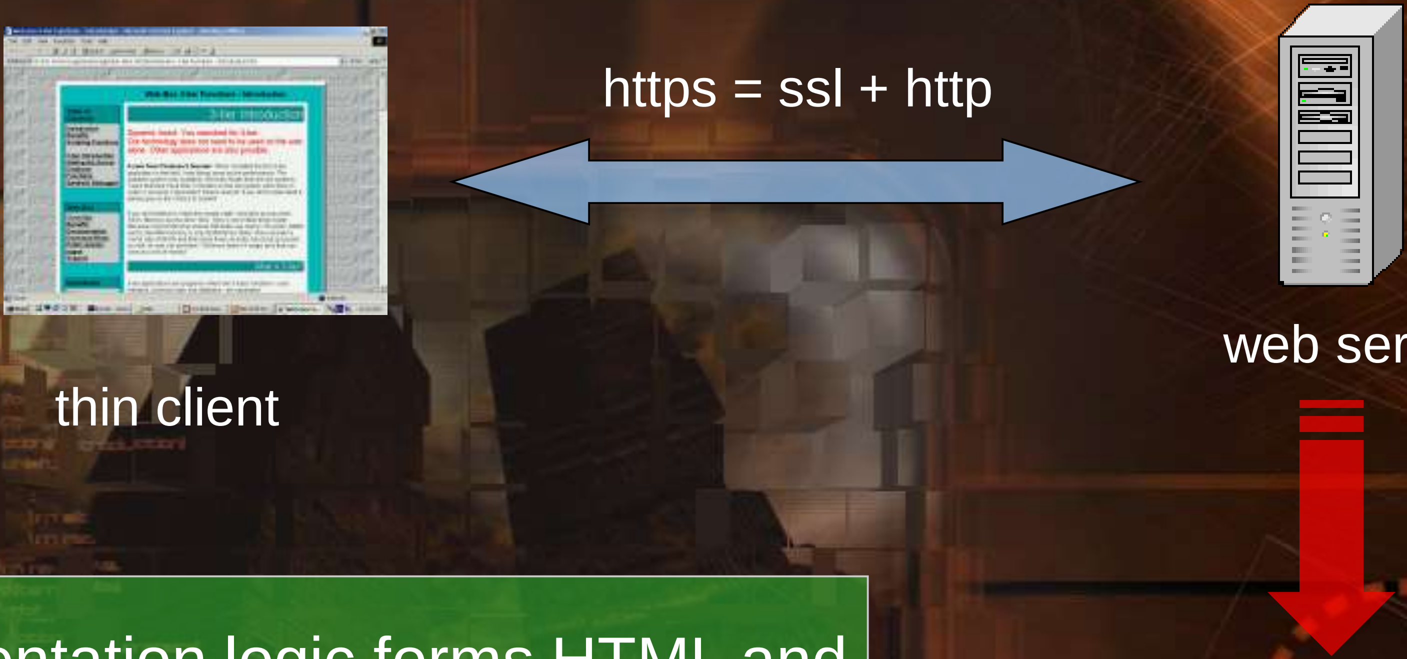
presentation logic

Banking Software Architecture

- In the Internet era banking software systems are n-tier (n > 2)



Presentation Logic



https = ssl + http

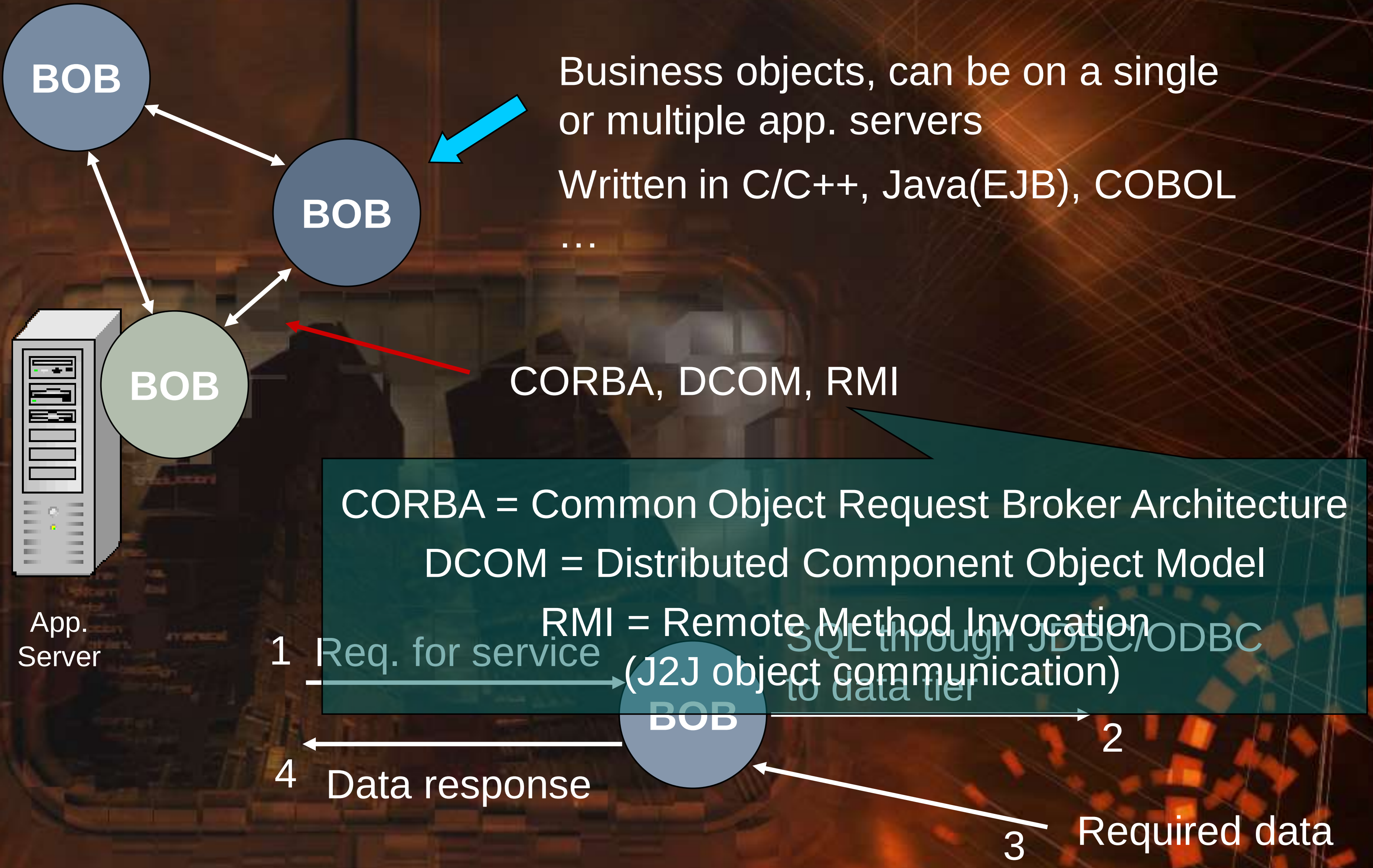
web server

thin client

Presentation logic forms HTML and interacts with application tier

Java Server Pages/Servlets
Active Server Pages
PHP …

Application Logic



Business objects, can be on a single or multiple app. servers

Written in C/C++, Java(EJB), COBOL …

CORBA, DCOM, RMI

CORBA = Common Object Request Broker Architecture

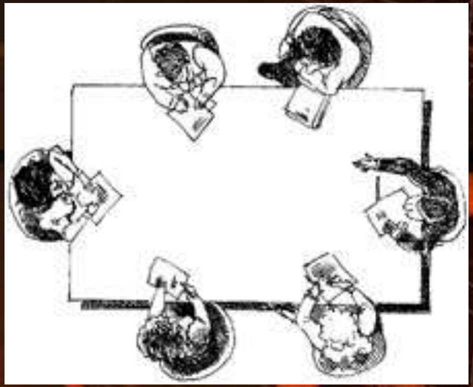
DCOM = Distributed Component Object Model

RMI = Remote Method Invocation (J2J object communication)

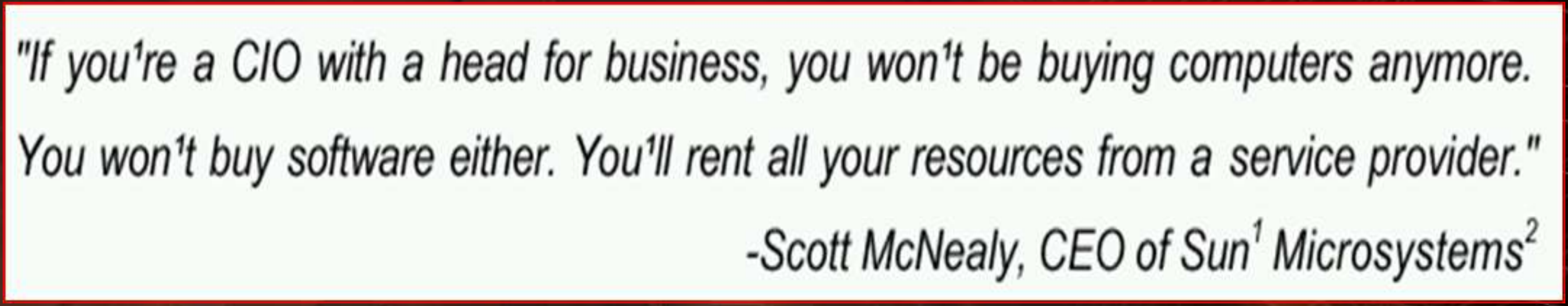
Application Service Providers

First step in the setup process is making a plan.

1. What are the services to be installed?
2. What services we (bank) could implement in-house?
3. What services we could implement through ASPs (out-of-house)?
4. Who are technology partners?



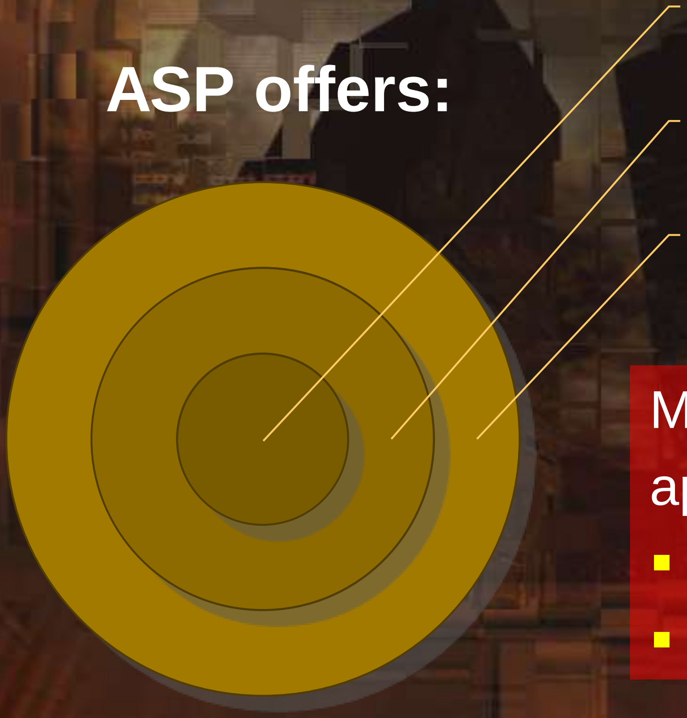
Application Service Providers



"If you're a CIO with a head for business, you won't be buying computers anymore. You won't buy software either. You'll rent all your resources from a service provider."

-Scott McNealy, CEO of Sun[1] Microsystems[2]

ASP offers:



Standardized packages of applications

Necessary infrastructure

Certain degree of service

Main characteristic of ASPs is that they offer applications that are already purchasable.

- ASP → one-to-many solution
- Classic IT outsourcing → one-to-one solution

ASPs – Pros and Cons

Advantages:

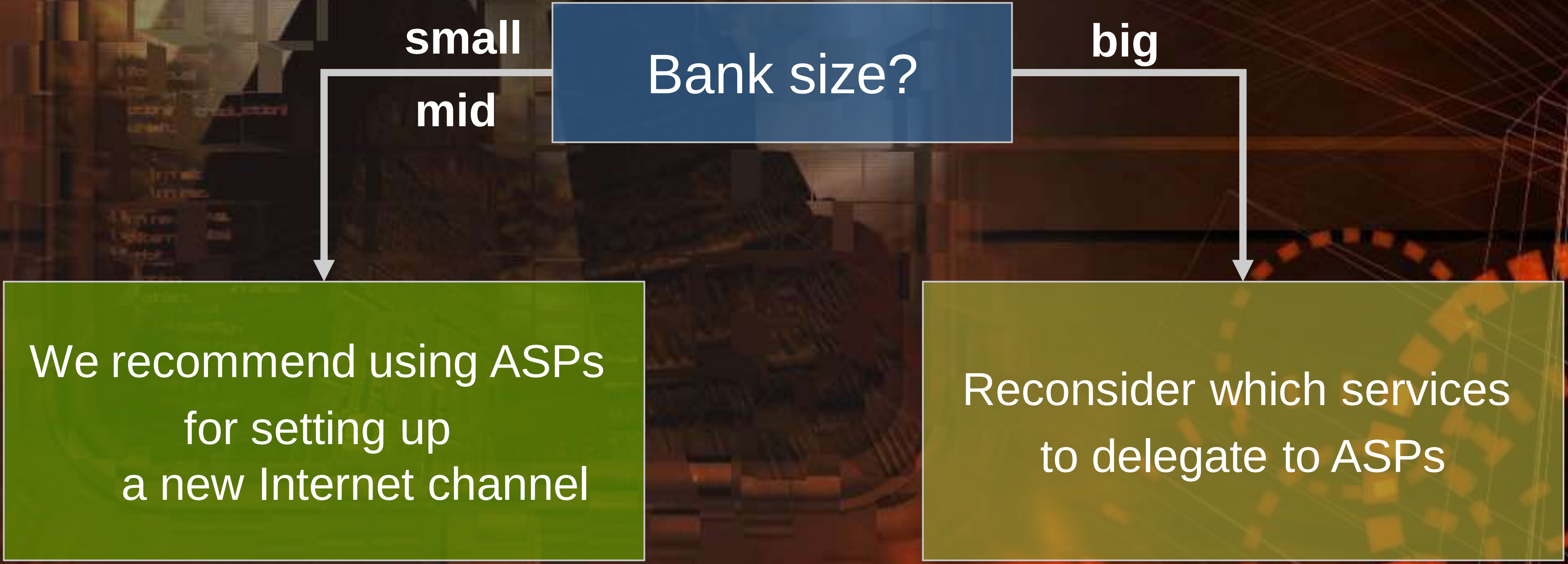
- Thin client
- Renting instead of buying
- Only effective using time charged
- Cost planning more reliable
- Total cost of ownership decreased
- Less IT workforce needed
- Installation / upgrading time saved
- Reaction time reduced
- One single business partner

Disadvantages:

- Every workstation needs Internet access
- Broad bandwidth necessary
- Doubtful data security on the Internet
- Not all applications have Internet compatible surfaces yet
- Loss of company's independence

Planning Phase in the Setup Process

- Complexity of a problem
  - Telecommunications infrastructure
  - Security
  - Multi-tier software infrastructure
  - Maintenance



Bank size?

small

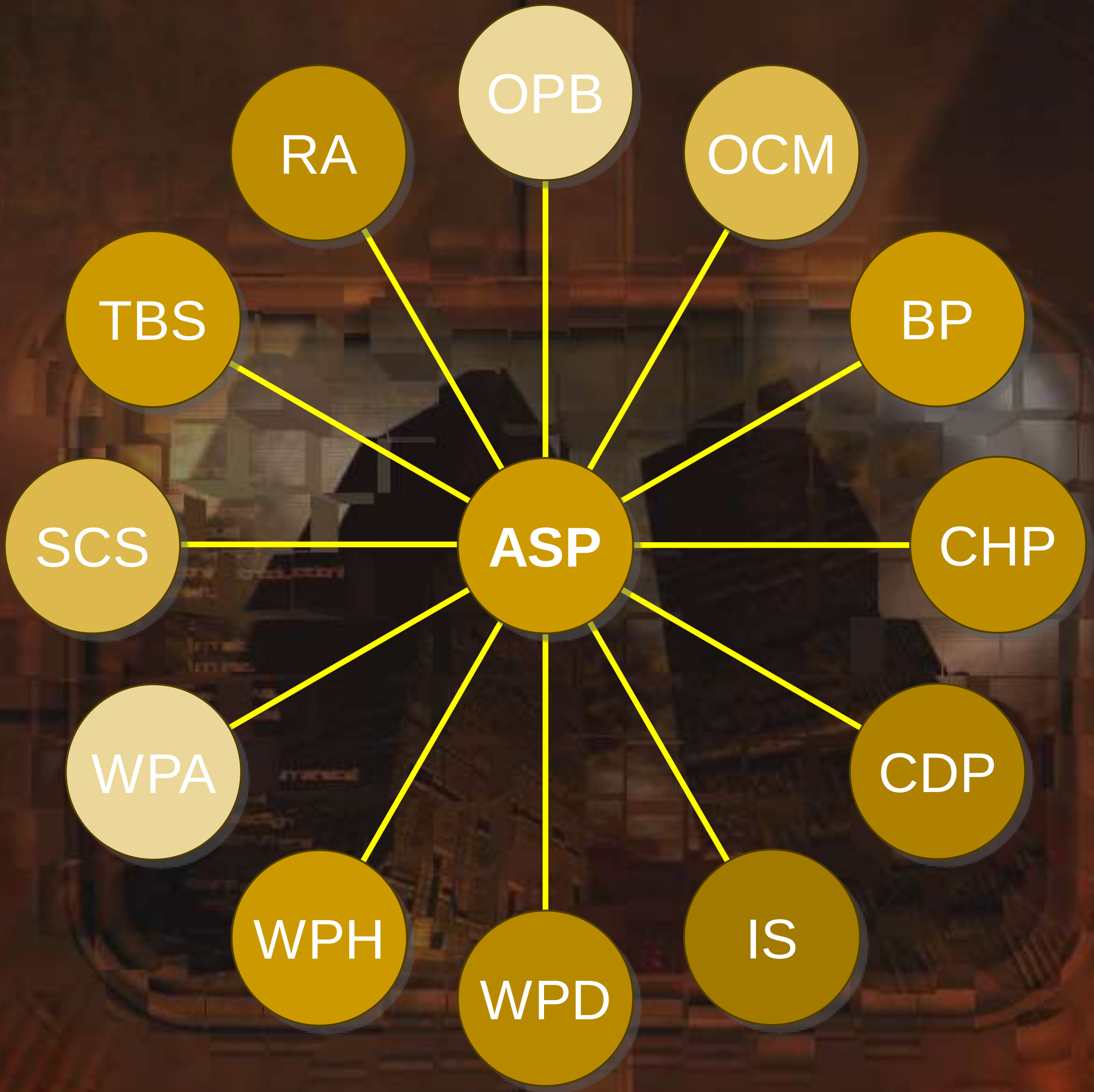
mid

big

We recommend using ASPs for setting up a new Internet channel

Reconsider which services to delegate to ASPs

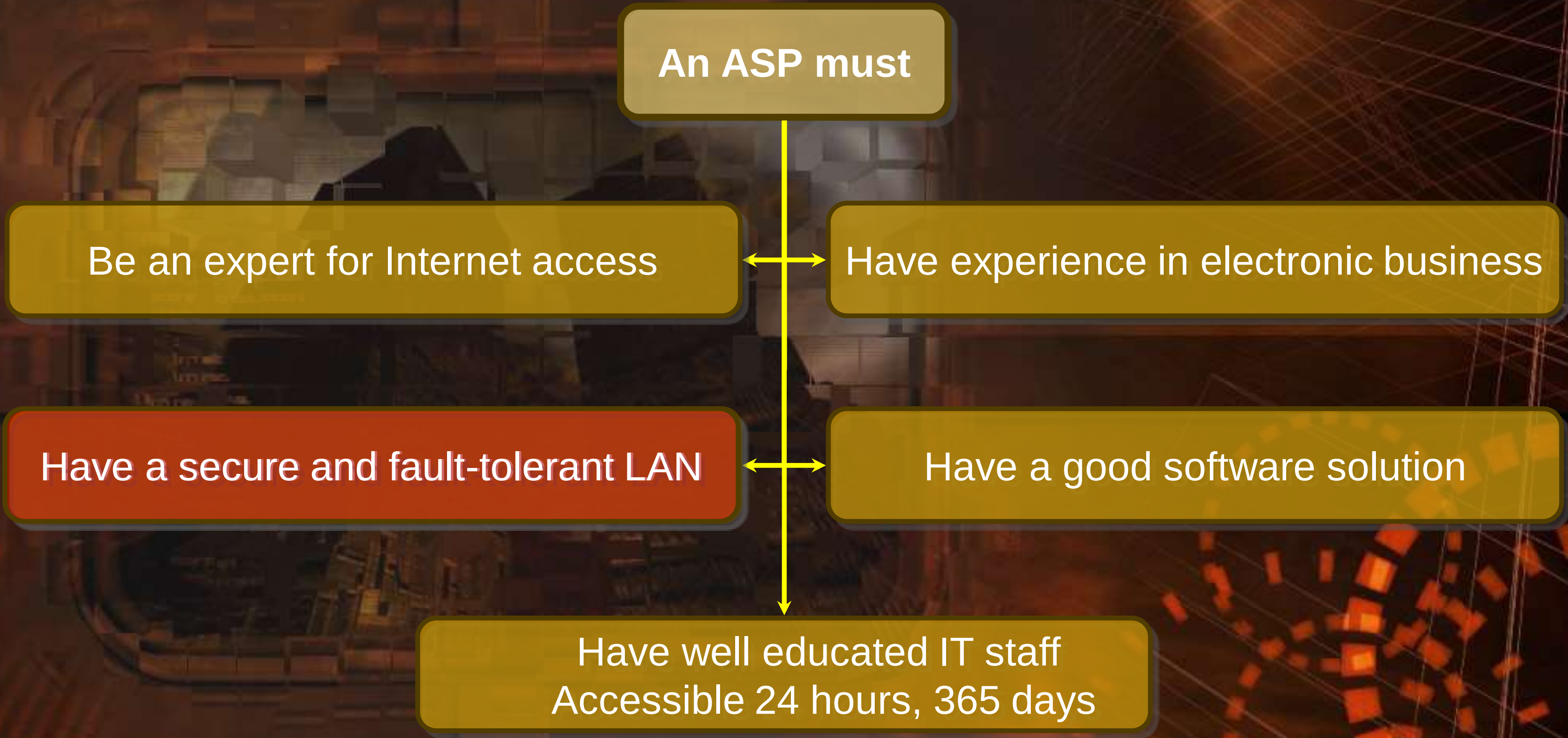
Services offered by ASPs



- Online personal banking *(account information, transfers, deposits, …)*
- Online cash management for companies
- Bill payment
- Check payment
- Card payment solutions
- Insurance services
- Web presentation design, hosting, administration
- Security services
- Testing of electronic business software
- Remote administration

Choosing Strategic and Tech Partners

Choosing the right ASP is the most important task in the setup procedure



An ASP must

Be an expert for Internet access

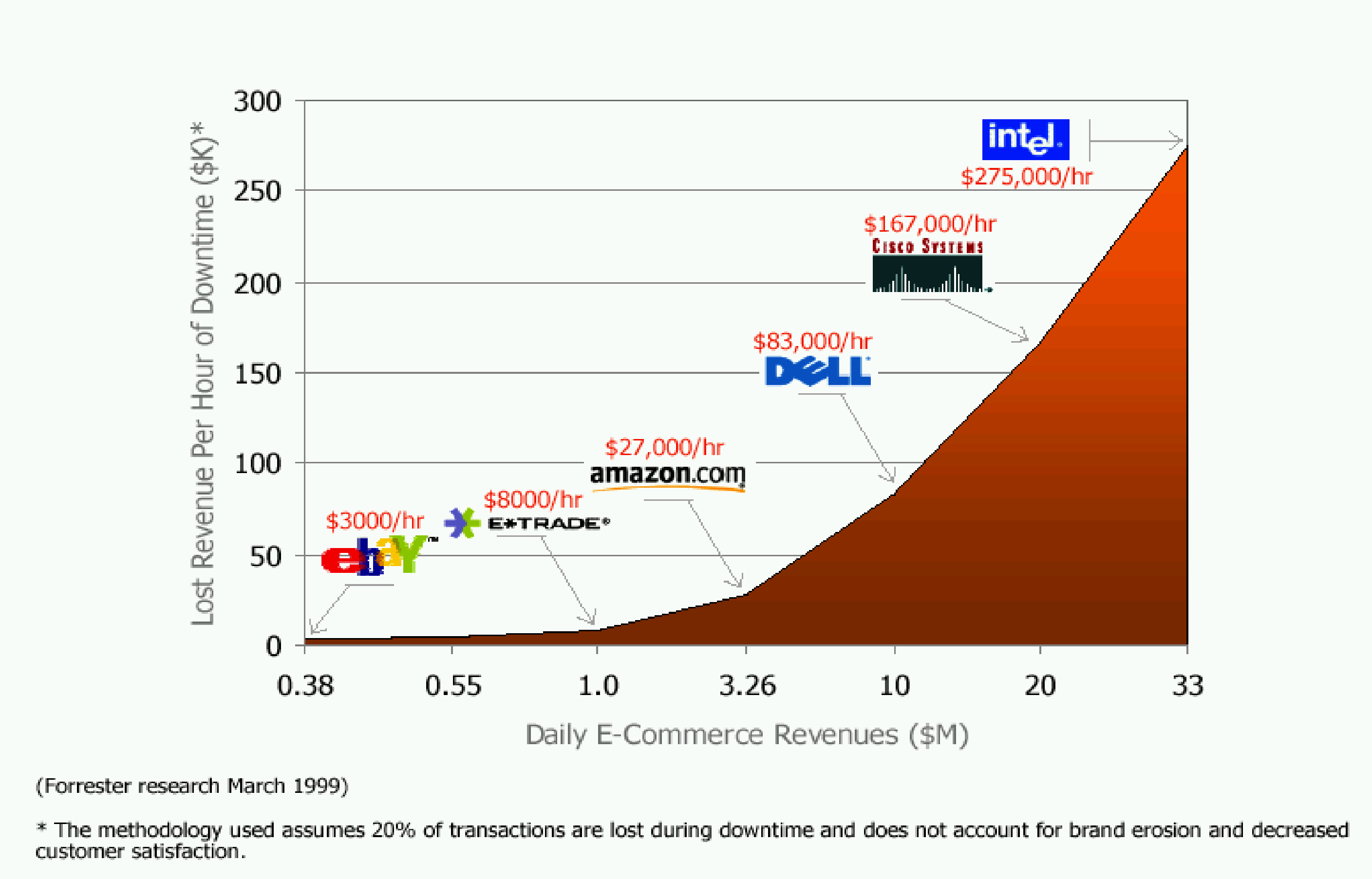
Have experience in electronic business

Have a secure and fault-tolerant LAN

Have a good software solution

Have well educated IT staff
Accessible 24 hours, 365 days

ASPs – The Cost of Downtime



(Forrester research March 1999)

* The methodology used assumes 20% of transactions are lost during downtime and does not account for brand erosion and decreased customer satisfaction.

99.9% uptime is still nearly 10h of downtime per year!

Choosing ASPs - International

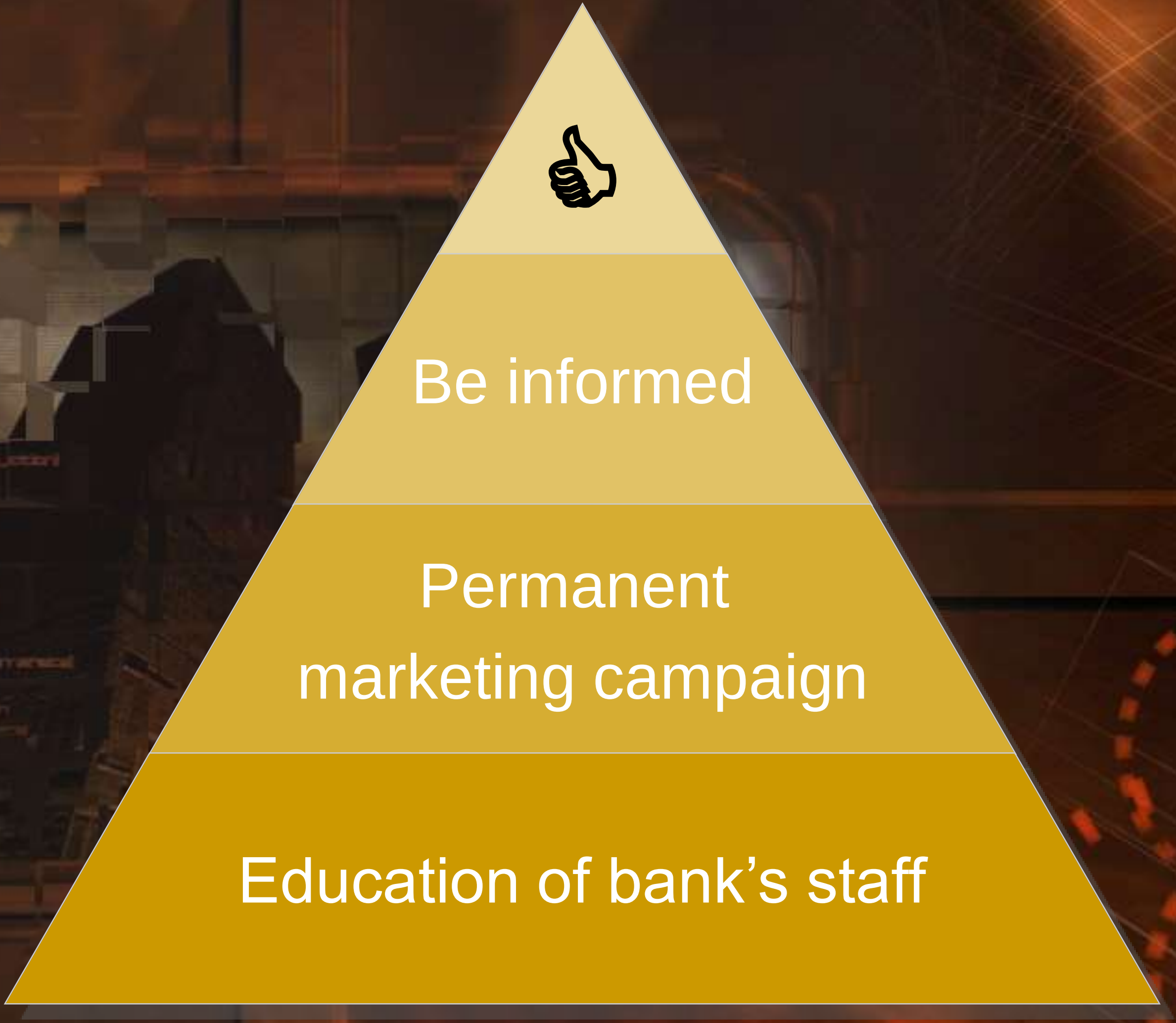
- **Personal Banking & Cash Management:**
  - Equifax, www.equifax.com; CustomerLink, www.efx-ebanking.com
  - Digital Insight, www.digitalinsight.com, AXIS
  - Vifi, www.vifi.com, InternetBanker
- **Bill Payment:**
  - CheckFree, www.checkfree.com
- **Card Payment:**
  - RS2 Software Group, www.rs2group.com, BankWorks
- **Web Hosting and Web Design:**
  - Digex , www.digex.com
  - DiamondBullet, www.diamondbullet.com, www.bankingwebsites.com

Choosing ASPs - Serbia

- **PEXIM** (Nacinalna Štedionica, Delta banka)
  - Web pristup
  - Namenska aplikacija
- **HALCOM** (HVB, Vojvođanska banka)
  - Isključivo namenska aplikacija
- **SAGA** (Atlas banka, Raiffeisen banka)
  - Isključivo Web pristup

After Initial Introduction of a New Channel

- Required tasks after initial introduction of a new channel:



👍

Be informed

Permanent marketing campaign

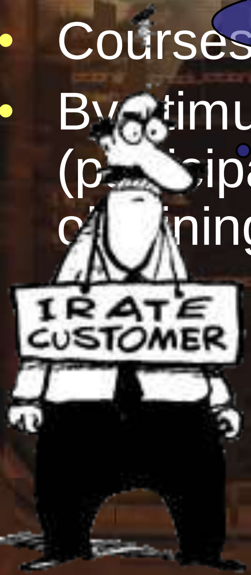
Education of bank’s staff

Education of Staff

- Studies show that education of bank's staff in using the Internet channel is often incomplete.
- Staff should provide answers to FAQ about using the Internet channel to their customers.
- Education process can be done through:
  - Courses after the job
  - By stimulating staff to use Internet Banking from home (participating in PC purchase, obtaining discounts from local ISP)

You do it (Internet Banking) because everyone does it.

You do it but you don't think it is important to you.



Conclusions deduced from incompetence of the staff...

Permanent Marketing

We have a good solution for Internet banking
but number of online users is very low after initial setup.

What’s wrong?

The answer is:

We need a permanent marketing campaign!

- Customers who were not ready for new service at the moment of initial introduction will be ready after few months.

to involve customers that became ready
in the meanwhile

- **Key of success – enthusiasm**, especially among the management

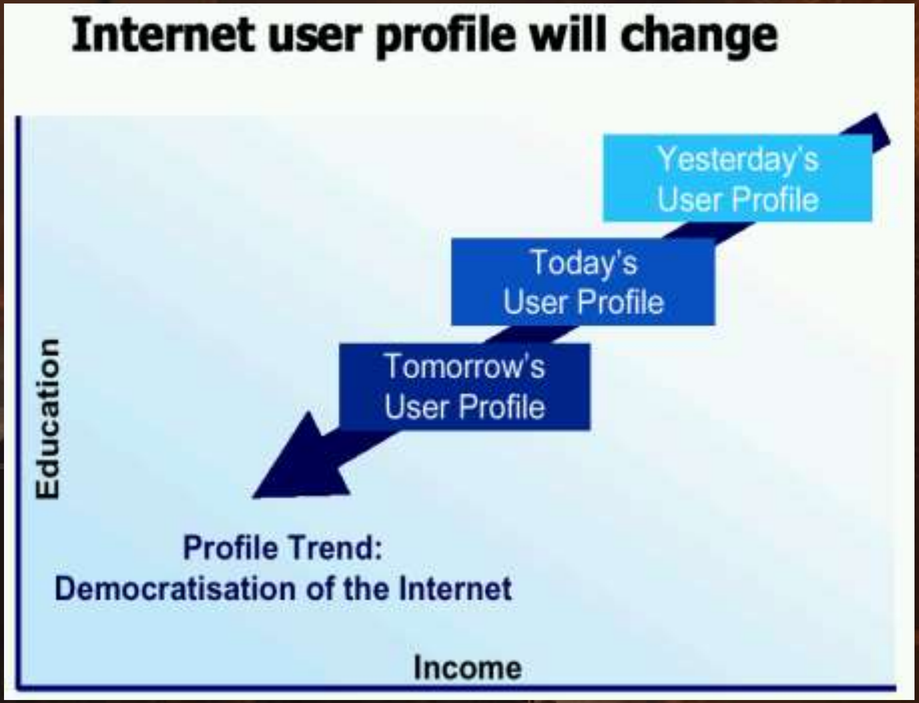
How To Do Marketing

- Spreading enthusiasm among staff
- Utilizing common media for advertising (professional agencies).
- Organizing education
  about Internet technologies
  and new banking services
  among customers.
- Agreements with local ISPs and resellers of PC equipment.

Would you excuse me a moment?.. Someone's trying to get my attention.

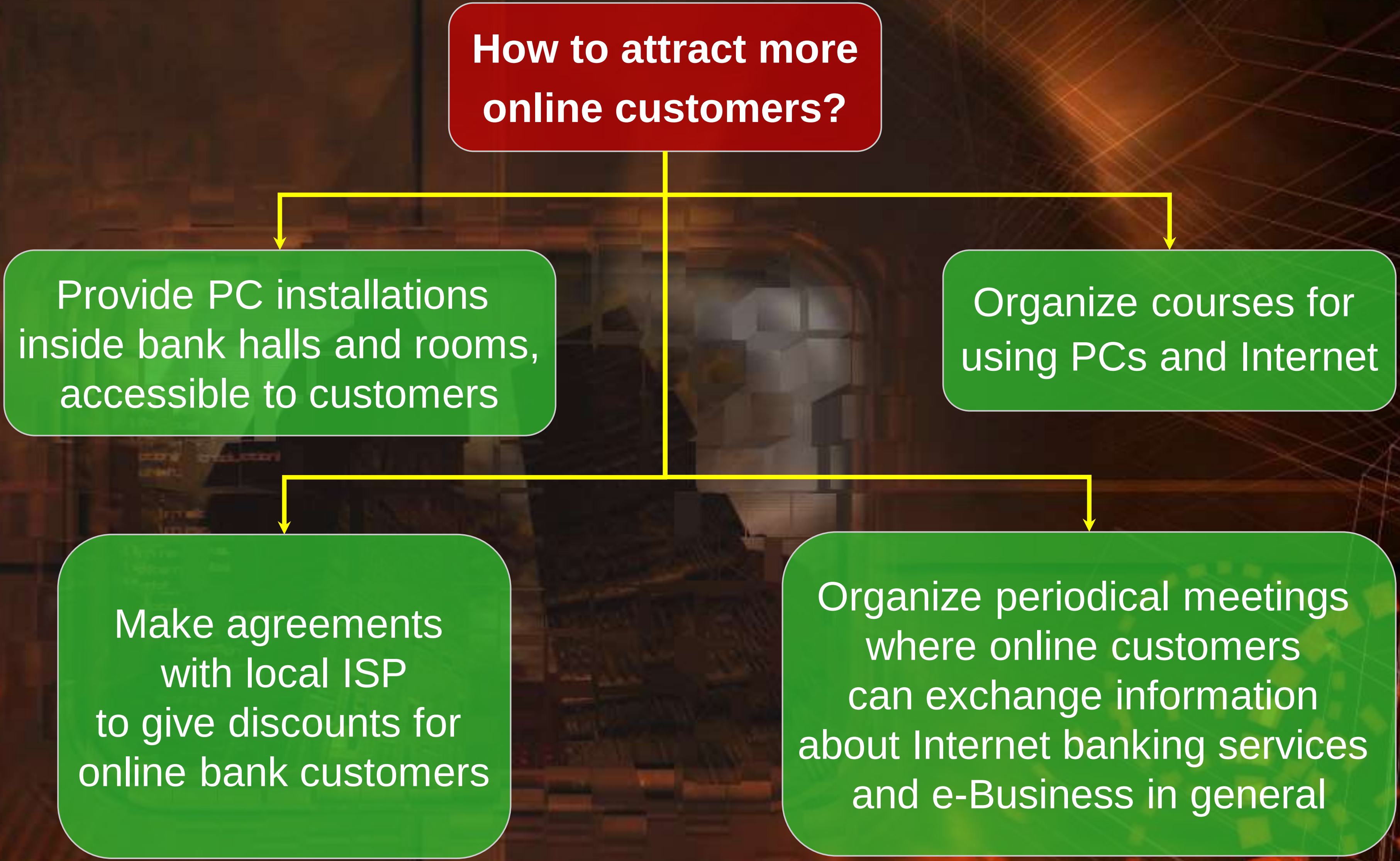
©CREATIVE MEDIA SERVICES Box 5955 Berkeley, Ca. 94705

Education of Customers



- Studies show that:
  - 7% of bank users are technically advanced
  - 25% is open to new banking services
    but they lack technical experience

Education of Customers



How to attract more online customers?

Provide PC installations inside bank halls and rooms, accessible to customers

Organize courses for using PCs and Internet

Make agreements with local ISP to give discounts for online bank customers

Organize periodical meetings where online customers can exchange information about Internet banking services and e-Business in general

Monitoring Activity on Internet Channel

- In order to react fast we should gather information about channel use
- Different statistics should be made:
  - Number of visitors
  - Number of transactions
  - Which services are most/least used
  - Average time spent at Web site by common user
- Feedback support
  - customers forms
  - e-mail for additional questions/services

Be Informed!

- To be successful in any business
  (including banking services)
  you constantly need information about:
  - Competition
    (what they offer, what are the complaints of their customers)
  - Potential customers
- Among other ways for obtaining information,
  it is useful to monitor the Web and Web activity
  using search engines.

Financial Data on the Internet

- Huge amount of financial data publicly available on the Internet
- Among 660 largest companies from 22 countries (30 from each) 62% had some form of financial data on their Web sites (IASC Report for 1999)
- The role of outsiders:
  - DigiTRADE
  - EDGAR
  - Wall Street City.Com
  - Yahoo! Finance

Nature of the Financial Data on the Internet

Among others, we can find information about:

- Quarterly and annual financial report
- Financial history
- SEC filings
- Stock quotas
- Press releases
- Information request forms
- Other shareholder information

Searching Services on the Web

We can generally search the Web using three types of searching services:

Subject directories

Search Engines

Meta crawlers

Subject Directories

- Links to Web sites are collected according to topics they treat
- Links are collected by humans who evaluate them
- Useful when searching for some topic in general
- Not effective when trying to find something specific
- Examples:
  Yahoo!, Lycos, LookSmart, Excite…

You know...you're right! The dollar does look stronger today!
Phil Frank
©CREATIVE MEDIA SERVICES Box 5955 Berkeley, Ca. 94705

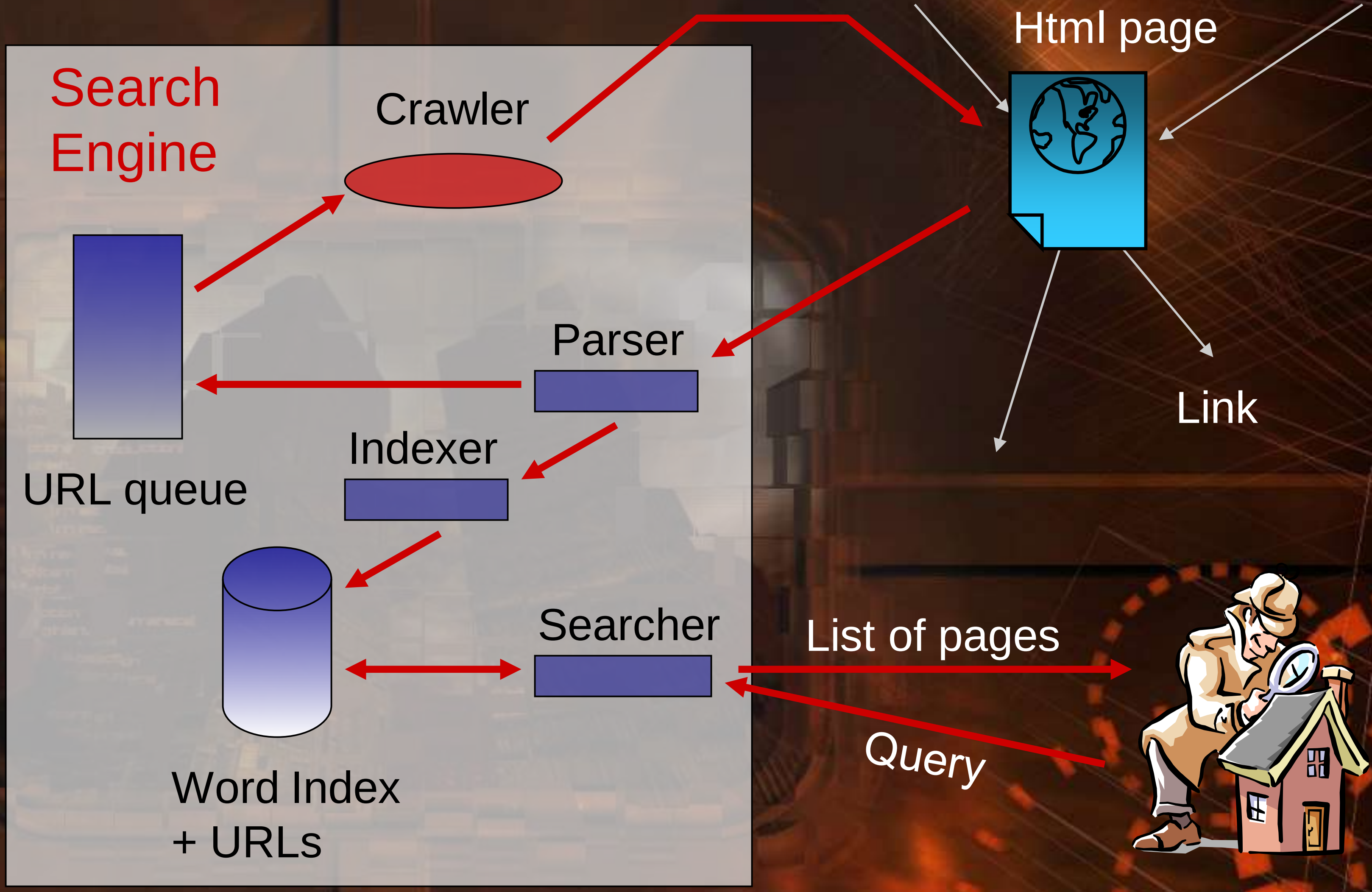
Search Engines

- They try to collect as many as possible pages from the Web and store them locally for later keyword search.
- Pages are collected by using crawlers (SW components).

- Good for search on specific query
- Result pages are sorted by relevancy
- Results can be out of date (currency problem)

- Examples:
  Google, AltaVista, Fast, Northern Light, ...

Search Engines – How Do They Work?



Meta-crawlers

DOGPILE®
All results, no mess.

- They utilize other search engines concurrently by sending user’s request to them.

- Good for queries about exotic topics.

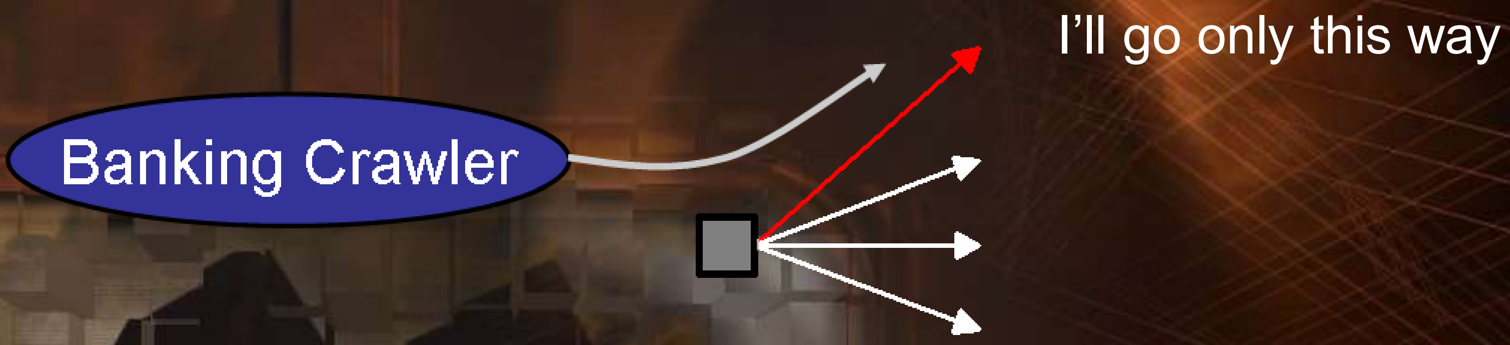
- Queries have to be simple because of different formats among search engines.

®HOTBOT

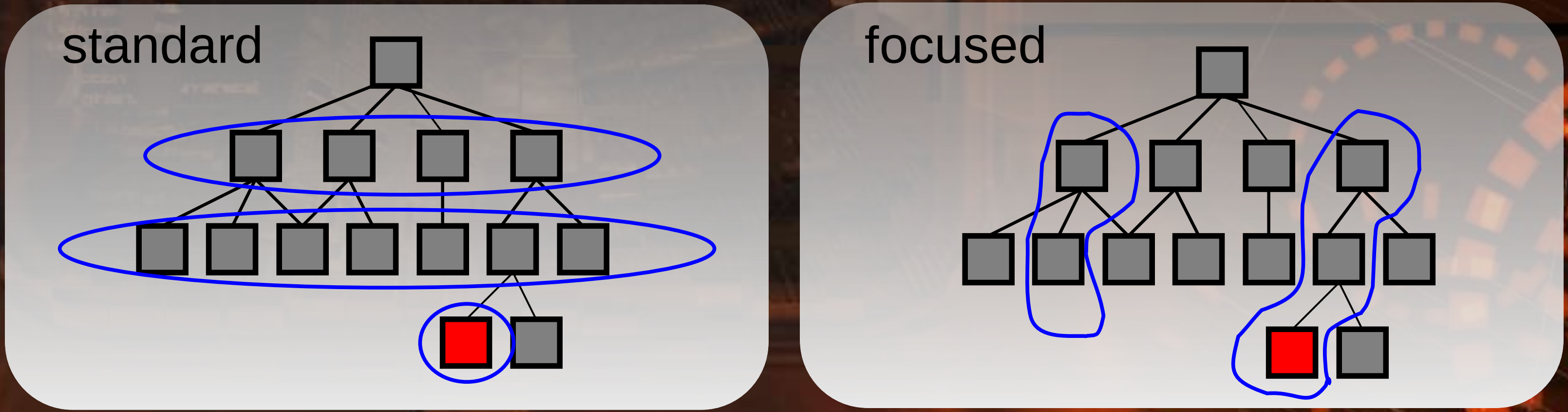
- Examples:
  MetaCrawler, Dogpile, HotBot, …

Focused Crawling

- Focused crawlers visit only topic-specific pages.



- Focused crawlers versus classic crawlers (solve currency problem)



Search Engines - Comparison

- Recent extensive comparison (September 2001) of search engines conducted by PC World’s staff can be found on the following URL:

  http://find.pcworld.com/11060

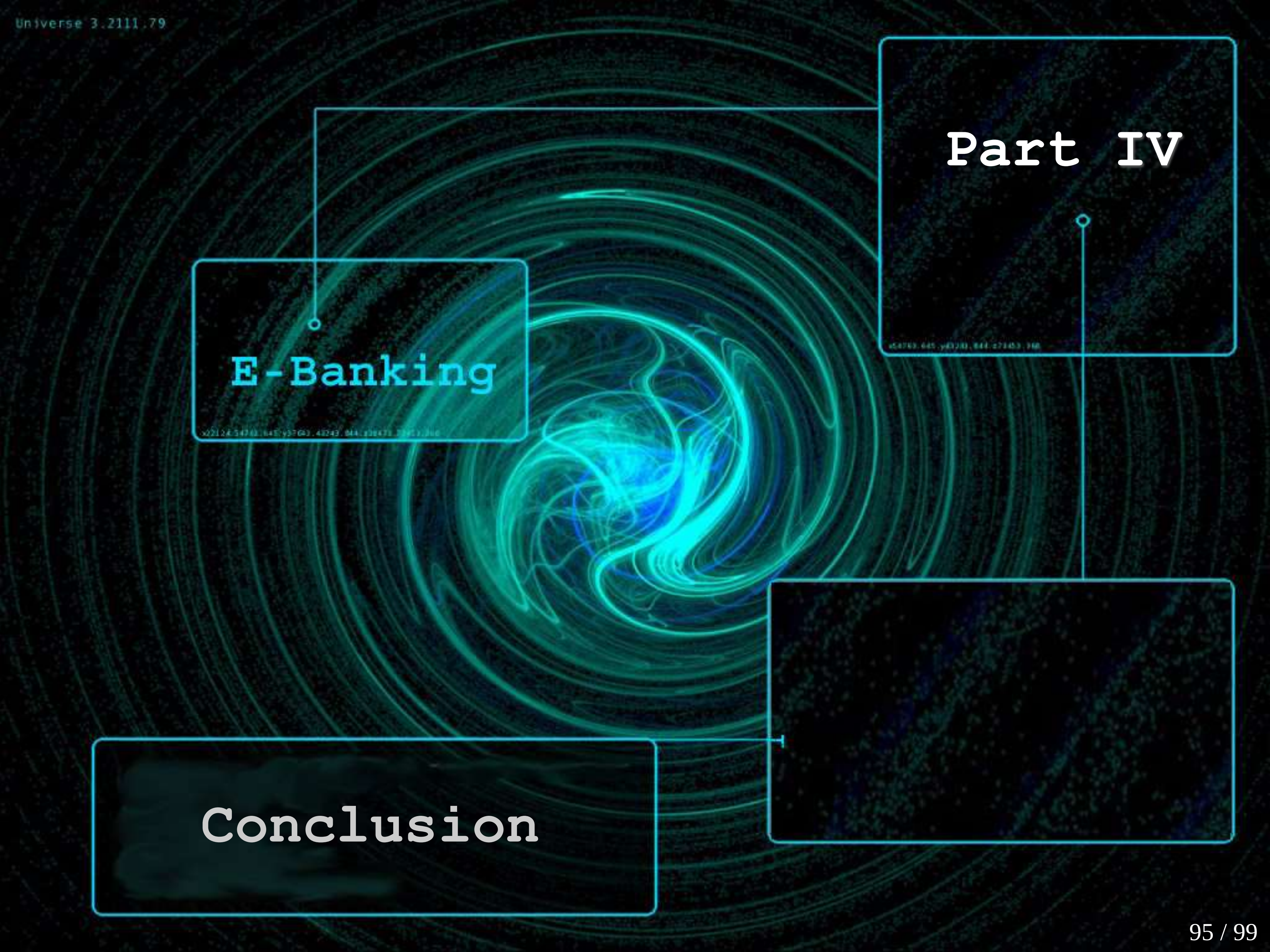
- Leaders are:
  - Google – www.google.com
  - Fast – www.alltheweb.com
  - Yahoo – www.yahoo.com
  - Lycos – www.lycos.com
  - Northern Light – www.northernlight.com

Search Engines - Comparison

- Directories of search engines can be found on following URLs:
  - Search Engine Guide – www.searchengineguide.com
  - Argus Clearinghouse – www.clearinghouse.com
  - BeauCoup – www.beaucop.com
  - Search Engine Watch – www.searchenginewatch.com
- There is even directory of directories of search engines
  - SearchAbility – www.searchability.com
- You can also try with public databases not accessible to search engines.
  - Lycos Searchable Databases Directory http://dir.lycos.com/reference/searchable_databases

Other Useful Links to Visit

- www.streeteye.com/cgi-bin/allseeingeye.cgi, financial data meta-crawler
- www.moneysearch.com, finance specific directory search
- www.dailystocks.com, excellent financial portal for investors
- www.companysleuth.com, excellent financial portal for investors



Part IV

E-Banking

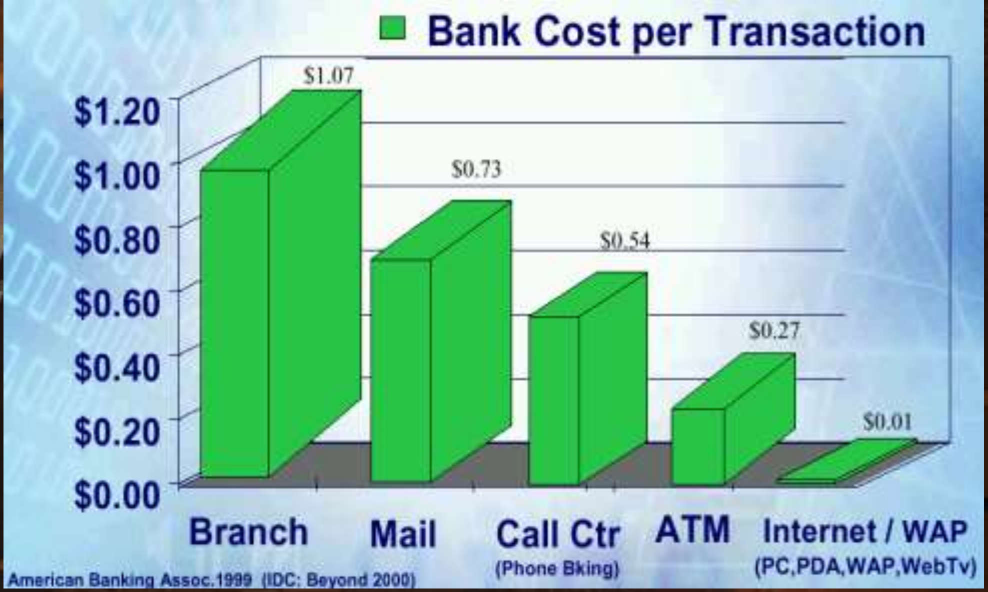
Conclusion

Conclusion

- In this tutorial on e-Banking we covered many of its aspects:
  - You learned what an e-Bank is, and what the benefits of e-Banking are
  - You familiarized yourself with the structure of the e-Bank
  - You learned how to implement your own Internet channel and how to afterwards search for financial information on the Web in order to improve your business
  - And you have also learned what possible security problems can occur and how to fight those problems

Conclusion in 40 Words

- Every bank should implement its Internet channel (reduced cost of transaction, global connectivity).



American Banking Assoc.1999 (IDC: Beyond 2000)

- Small and mid sized banks could benefit from using Application Service Providers for different kind of service (and choosing the good ASP is the most important step).

Final Words…

Some Internet Myths

(from “European ECM momentum”, Maria Luisa Rodriguez, San Jose State University)

Myth:	Fact:
The Internet requires little upfront investment.	You get what you pay for.
The Internet will drive transactions from other channels.	Channel behavior is additive (channel adoption has always been additive).
The Internet is borderless.	Brand, marketing and consumer behavior is local.

~ The End ~

Authors:

Nikola Skundric
nikolas@galeb.etf.bg.ac.yu

Prof. Dr. Veljko Milutinovic
vm@etf.bg.ac.yu

Milos Kovacevic
milos@grf.bg.ac.yu

Nikola Klem
klem@grf.bg.ac.yu