CS155b: E-Commerce

Lecture 6: Jan. 25, 2001

Security and Privacy, Continued

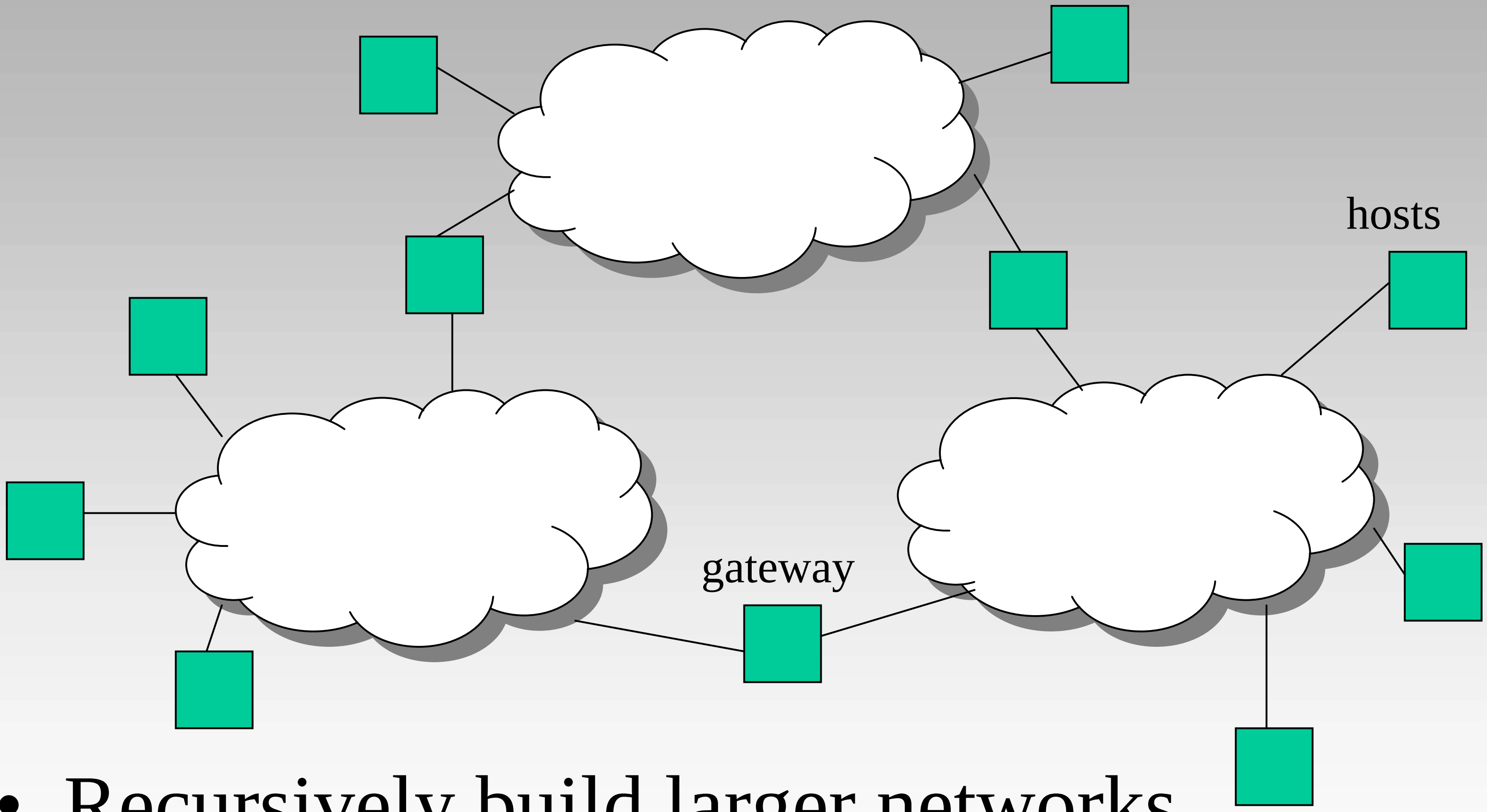
FIREWALL

- A barrier between an internal network & “the Internet”
- Protects the internal network from outside attacks
- Executes administrator-defined security policy
- Decides whether a datastream is allowed to pass through or not
- Main Components:

  - packet filter

  - proxy

Interconnection of Networks



- Recursively build larger networks

PACKET FILTER

- Works at IP layer
- Rule-table-driven
- Forwards, refuses, or drops a packet according to the rules
- An example rule table

Rule#	Source	Destination	Port	…	Action
1	128.*.*.*	130.*.*.*	Any		Fwd
2	61.*.*.*	130.*.*.*	23		Refuse
3	61.*.*.*	Any	21		Drop

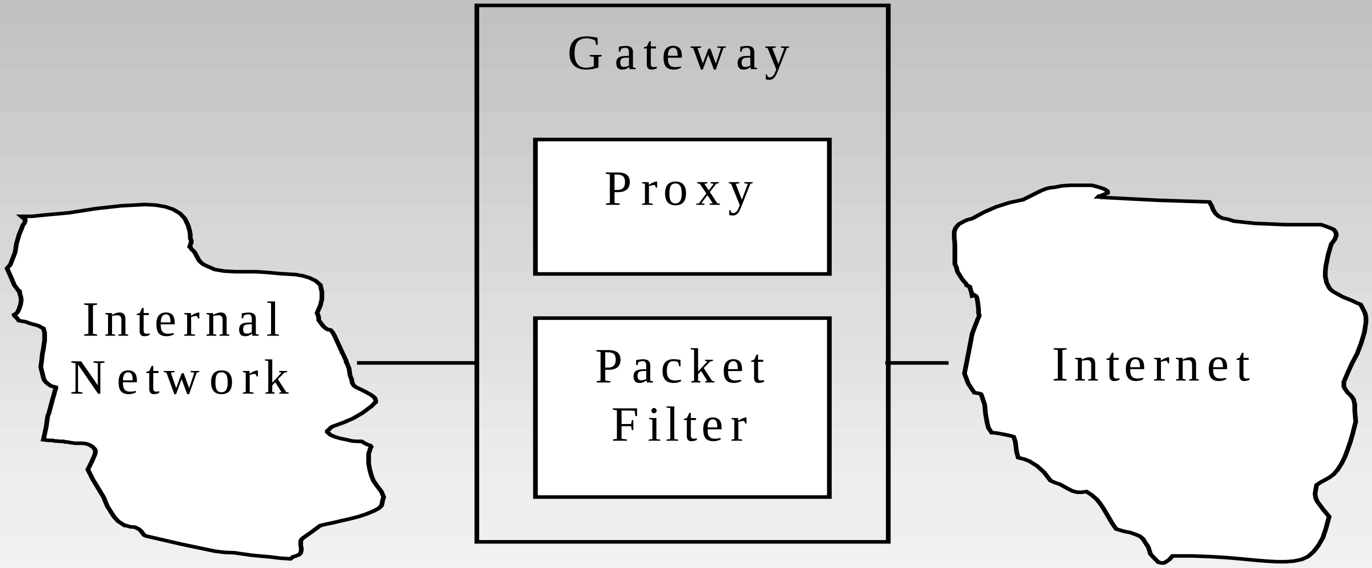
PROXY

- Works at application layer
- One proxy per (application layer) protocol

  - HTTP proxy, FTP proxy, …
- User authentication required
- Different users can have different privileges
- Can be made transparent to users

SEVERAL CONFIGURATIONS POSSIBLE

- A Sample Configuration: Dual-home Host



- Trade-offs: Security vs. Accessability, Security vs. Cost

CHECKPOINT

- Full Name: Check Point ™ Software Technologies Limited
- Employees: 1000 +
- Stock Price: $146.5 (Jan 22, 2001)
- Revenues in 2000: $425.3 million
- Business Area: Internet Security

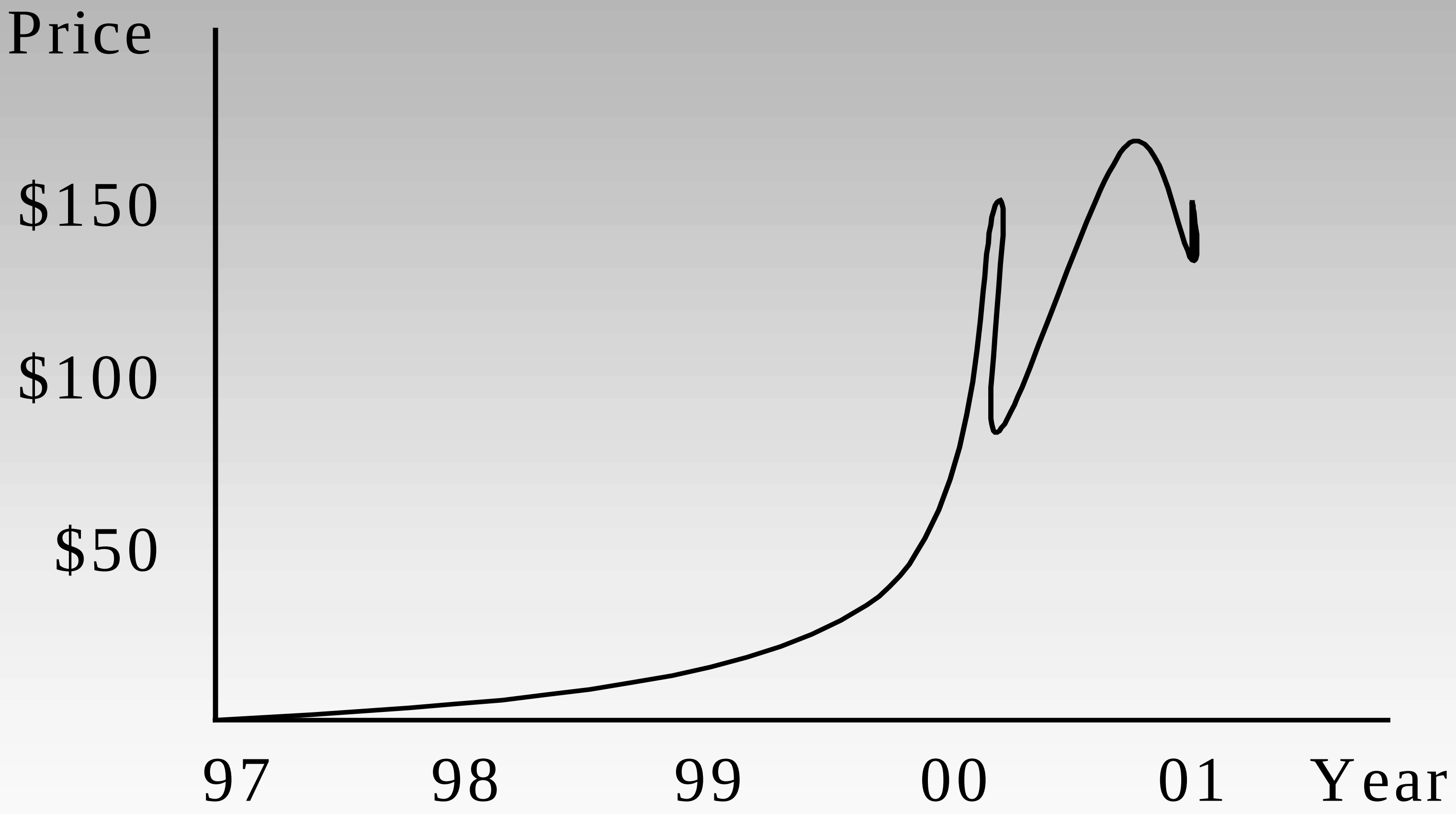
MAIN PRODUCTS

- **FireWall-1® :** a popular firewall product
- **Open Platform For Security (OPSEC):** an enterprise-wide framework for security policies extending FireWall-1®
- **VPN-1:** a family of virtual private networking solutions
- **Provider-1™:** a security management solution

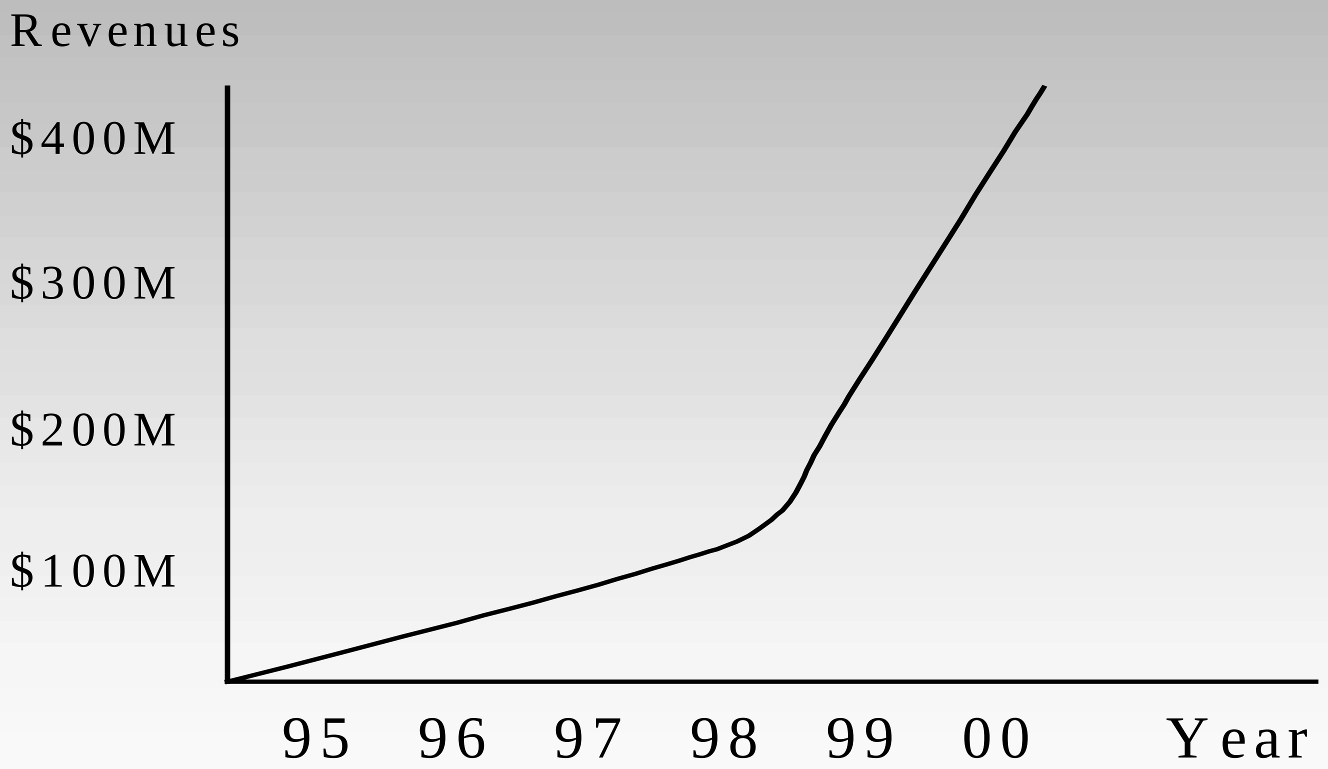
BRIEF HISTORY

- 1993 Founded
- June 1996 Initial Public Offering
- 1998 Annual Revenues More than $100M
- June 2000 Stock Price More than $100
- Q3, 2000 Quarterly Revenues More than $100M

STOCK PRICE CHART



REVENUES CHART



Discussion Point

- Firewalls aren’t perfect
  E.g., “Address spoofing” is a problem

- Why is CheckPoint so successful?
  Importance of “feeling secure”?
  “Knee-high protection?”

Symmetric Key Crypto

$D(E(x, k), k) = x$

(decryption, encryption, plaintext, key)

- Alice and Bob choose k_{AB}
- Alice: y < -- $E(x, k_{AB})$ (ciphertext)
- Alice --> Bob: y
- Bob: x < -- $D(y, k_{AB})$

(Eve does not know k_{AB})

Well Studied and Commercially Available

  - DES
  - IDEA
  - FEAL-n
  - RC5
  - AES

- Users must deal with
  - Government (especially export)
  - Key management

Public Key Crypto

$D(E(x, PK_u), SK_u) = x$

(user's Secret Key, user's public key)

Bob generates SK_{bob}, PK_{bob}

Bob publishes PK_{bob}

Alice: Lookup PK_{bob}

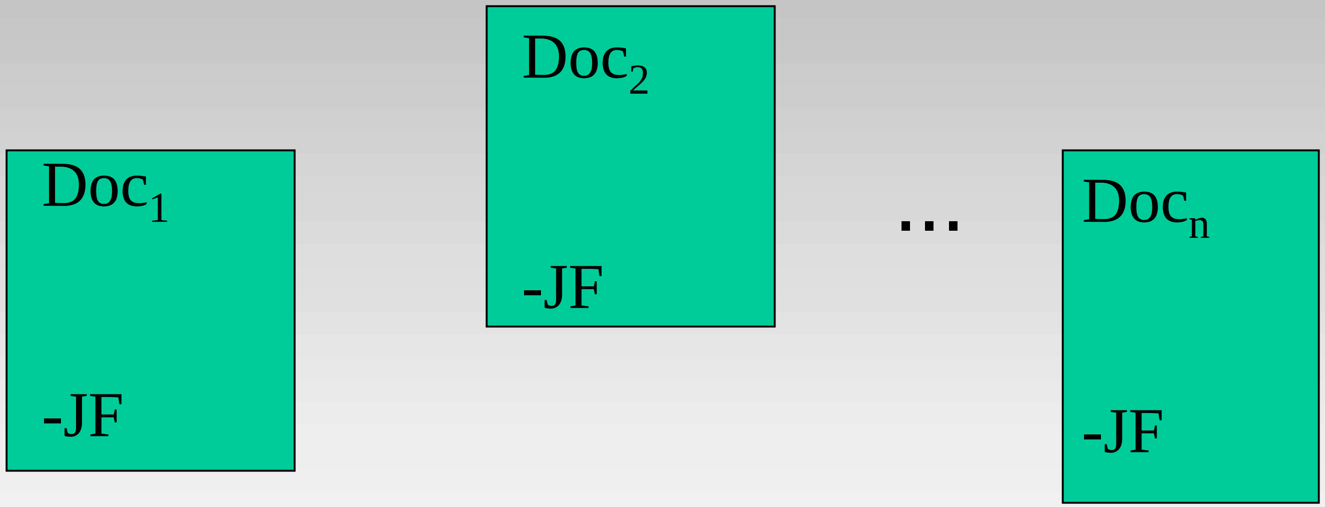
y < -- $E(x, PK_{bob})$

Alice --> Bob: y

Bob: x < -- $D(y, SK_{bob})$

(Eve does not know SK_{bob})

Digital Signatures



Doc_1

-JF

Doc_2

-JF

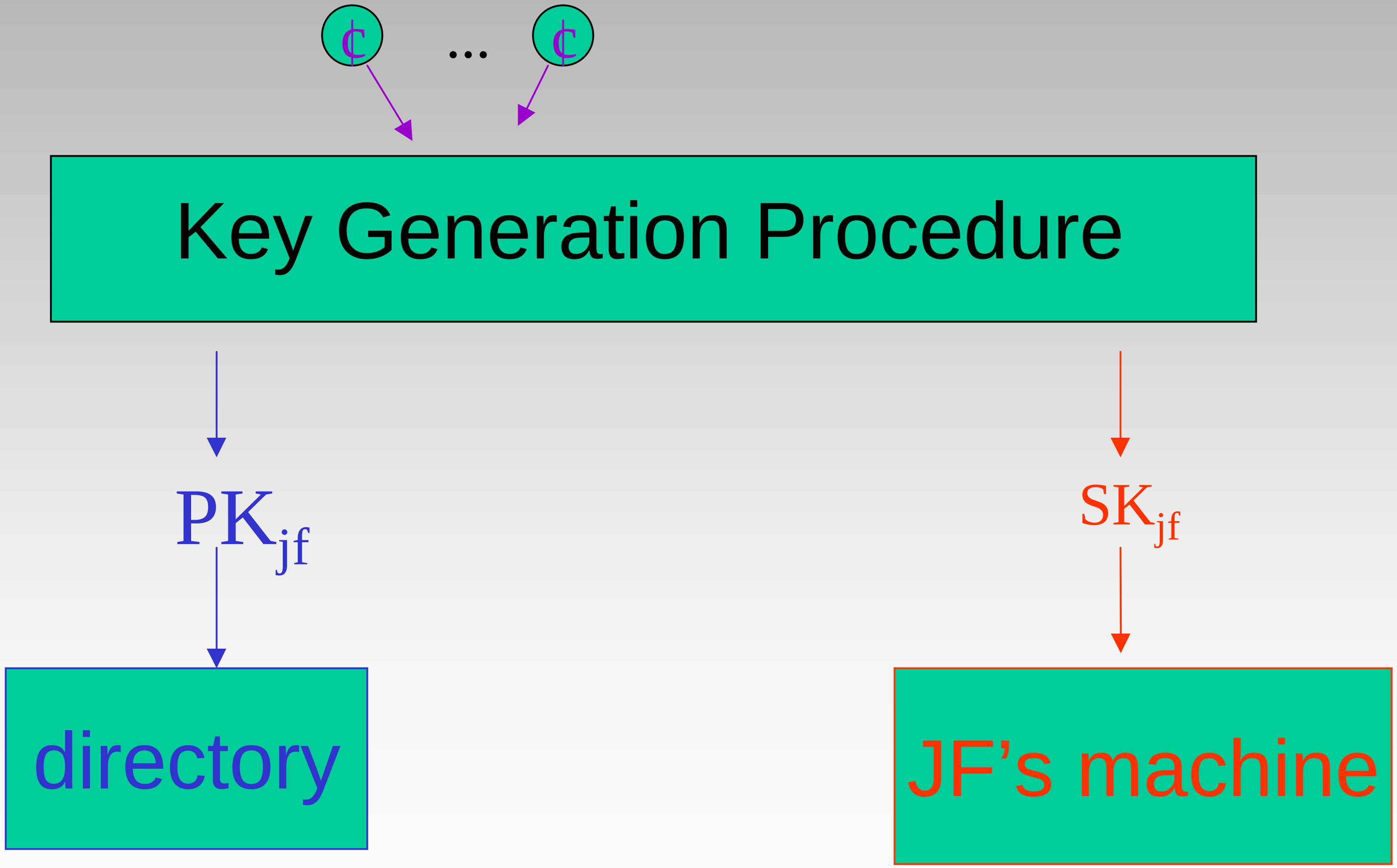
…

Doc_n

-JF

Trickier than the paper “analogue”

3-part Scheme



¢ … ¢

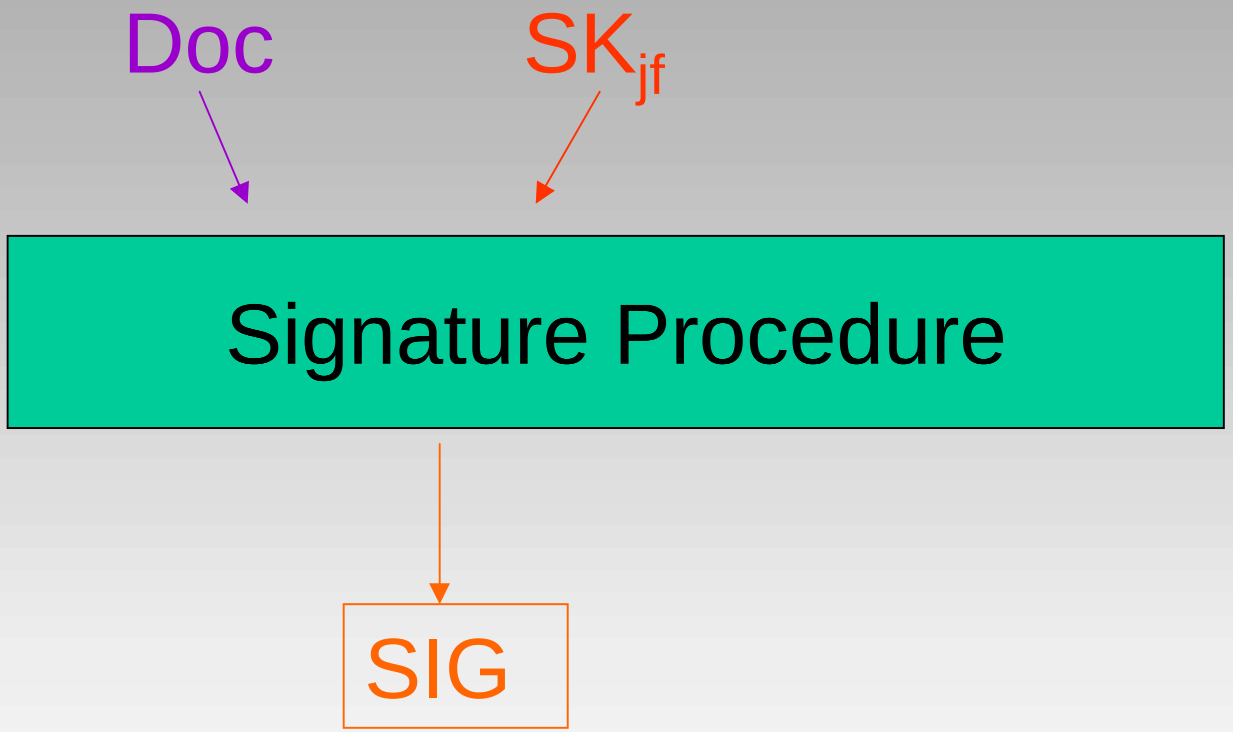
Key Generation Procedure

PK_{jf}

SK_{jf}

directory

JF’s machine

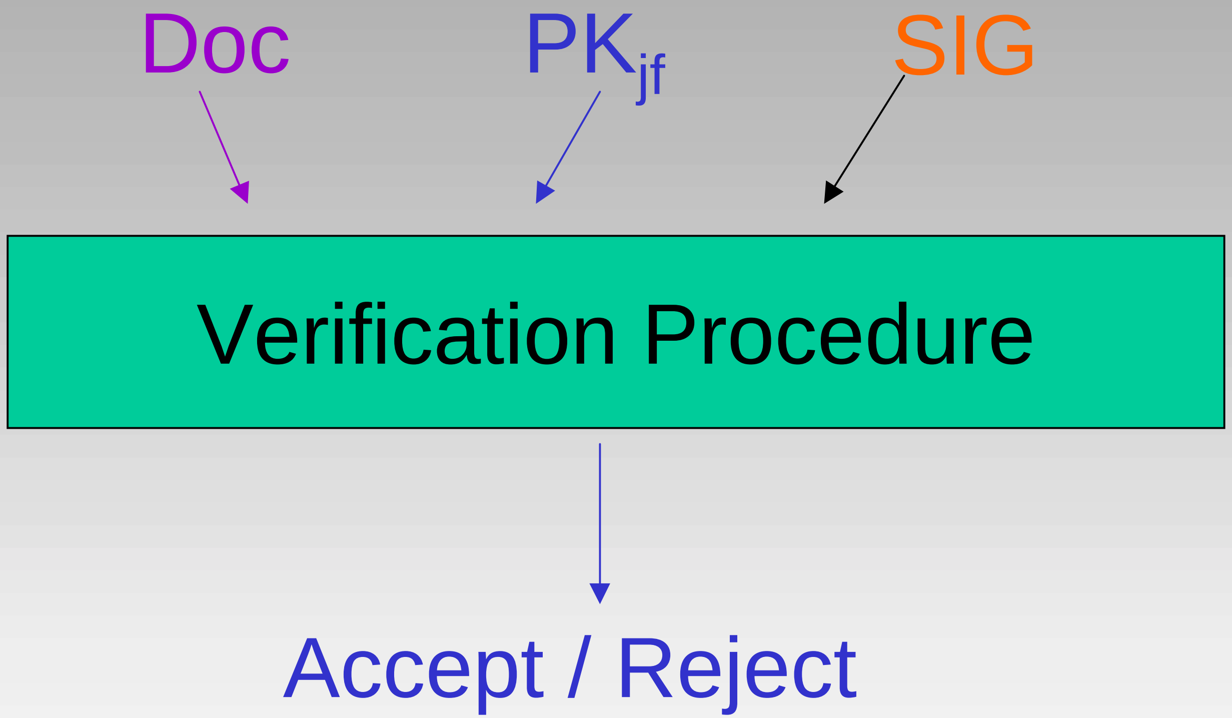


Doc

SK_{jf}

Signature Procedure

SIG



Doc

PK_{jf}

SIG

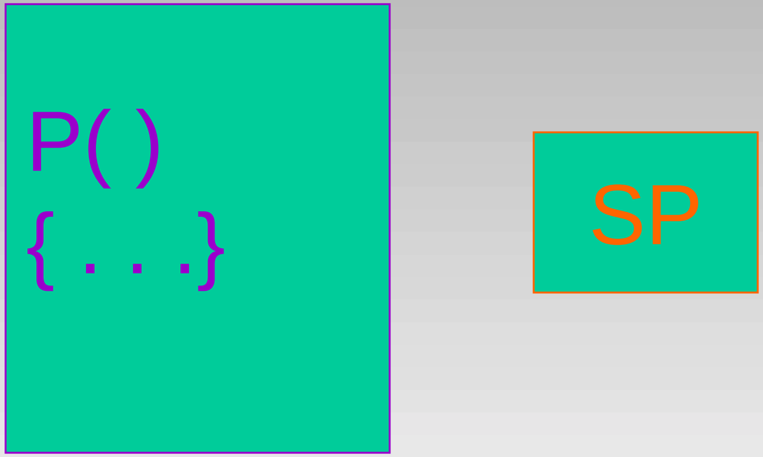
Verification Procedure

Accept / Reject

Examples

- RSA
- El Gamal
- DSA
- McEliece

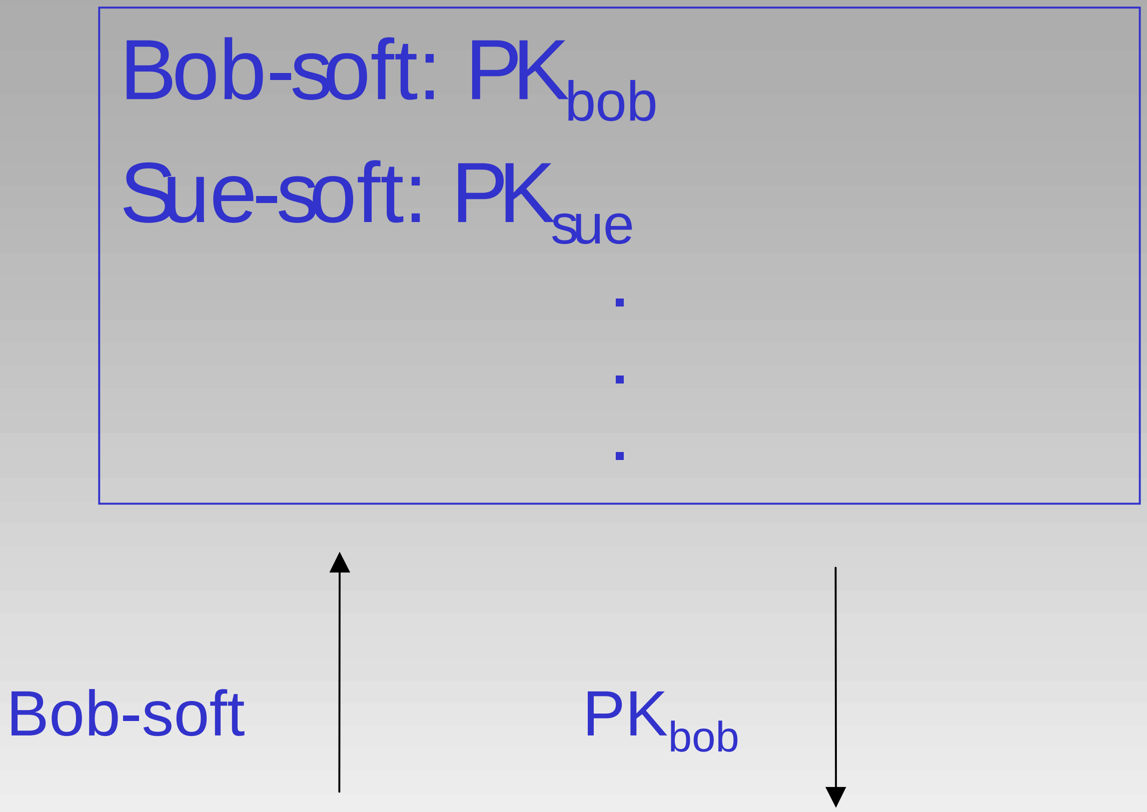
http://www.bob-soft.com



P( )
{ . . .}

SP

$SP = \text{signature}(P, SK_{bob})$



Bob-soft: PK_{bob}

Sue-soft: PK_{sue}

.

.

.

Bob-soft

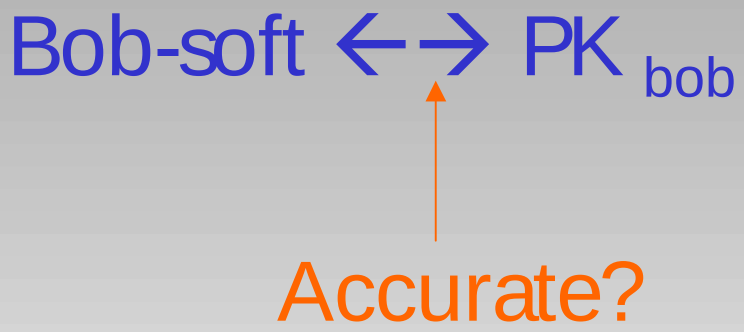
PK_{bob}

Alice: Verify (P, PK_{bob}, SP)

New Potential Problem

- Is PK_{bob} the “Right Key”?
- What does “Right” mean?

Traditional Meaning



Bob-soft ←→ PK_{bob}

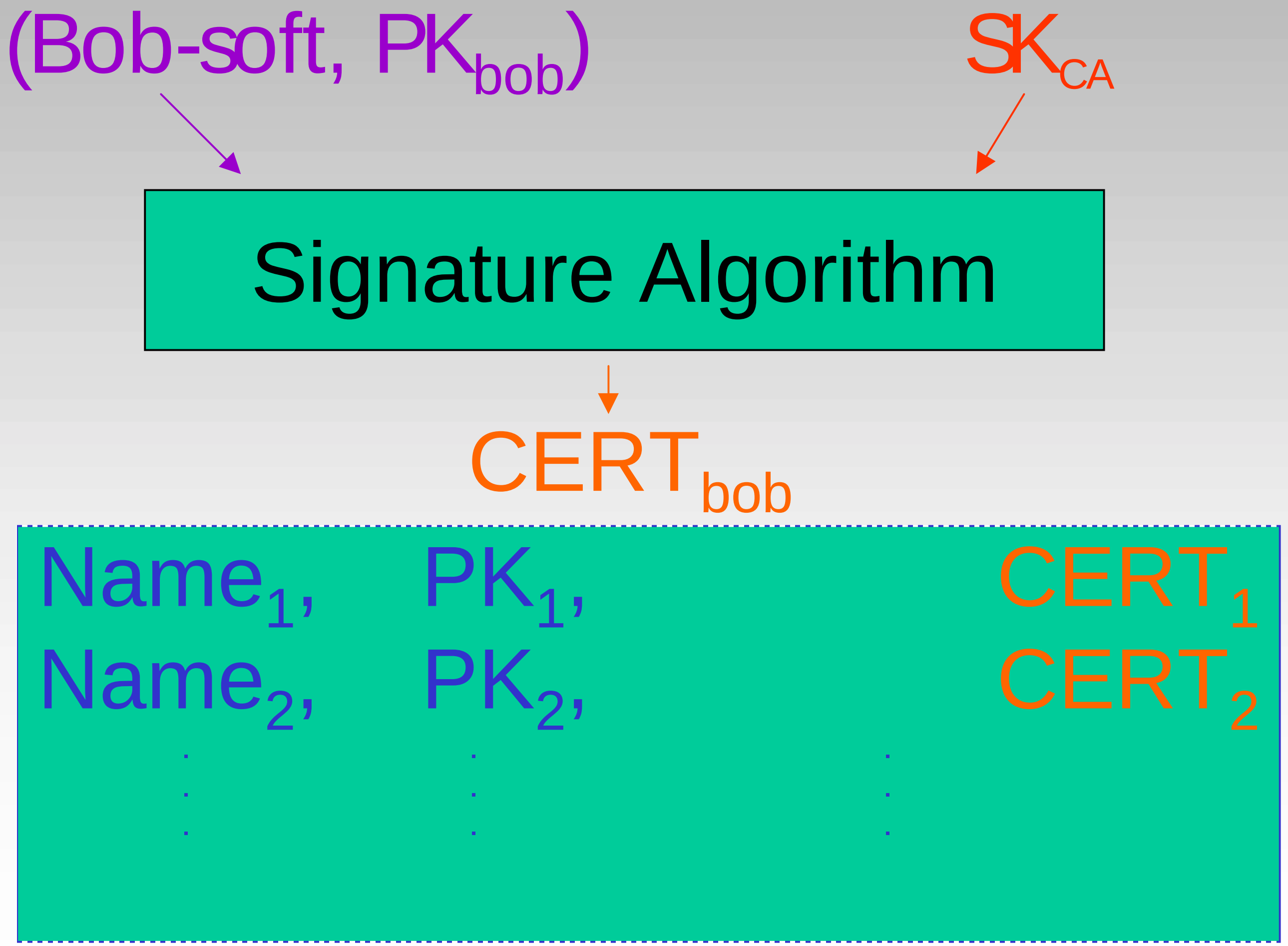
Accurate?

Traditional Solution

Alice's Computer

PK_{CA}

Bootstrapping Trust



(Bob-soft, PK_{bob})

SK_{CA}

Signature Algorithm

$CERT_{bob}$

$Name_1$, PK_1, $CERT_1$

$Name_2$, PK_2, $CERT_2$

. . .

- Technical Question: Is this the right PK?
- Business Question: Can you make money selling public-key certificates?
- Political Question: Crypto export
- Legal Question: Do we have a right to use encryption? To some form of “electronic privacy”?

VeriSign:
Enable everyone, everywhere to use the Internet with confidence

- Through its acquisition of Network Solutions, VeriSign serves as the gateway to establishing an online identity and Web presence, with more than 24 million domain name registrations in *.com*, *.net* and *.org* .
- As the leader in the Web site security market, VeriSign provides Internet authentication, validation and payment services.
- Through VeriSign Global Registry Services, VeriSign maintains the definitive directory of over 24 million Web addresses and is responsible for the infrastructure that propagates this information throughout the Internet. VeriSign Global Registry Services responds to over 1.5 billion DNS look-ups daily.

History

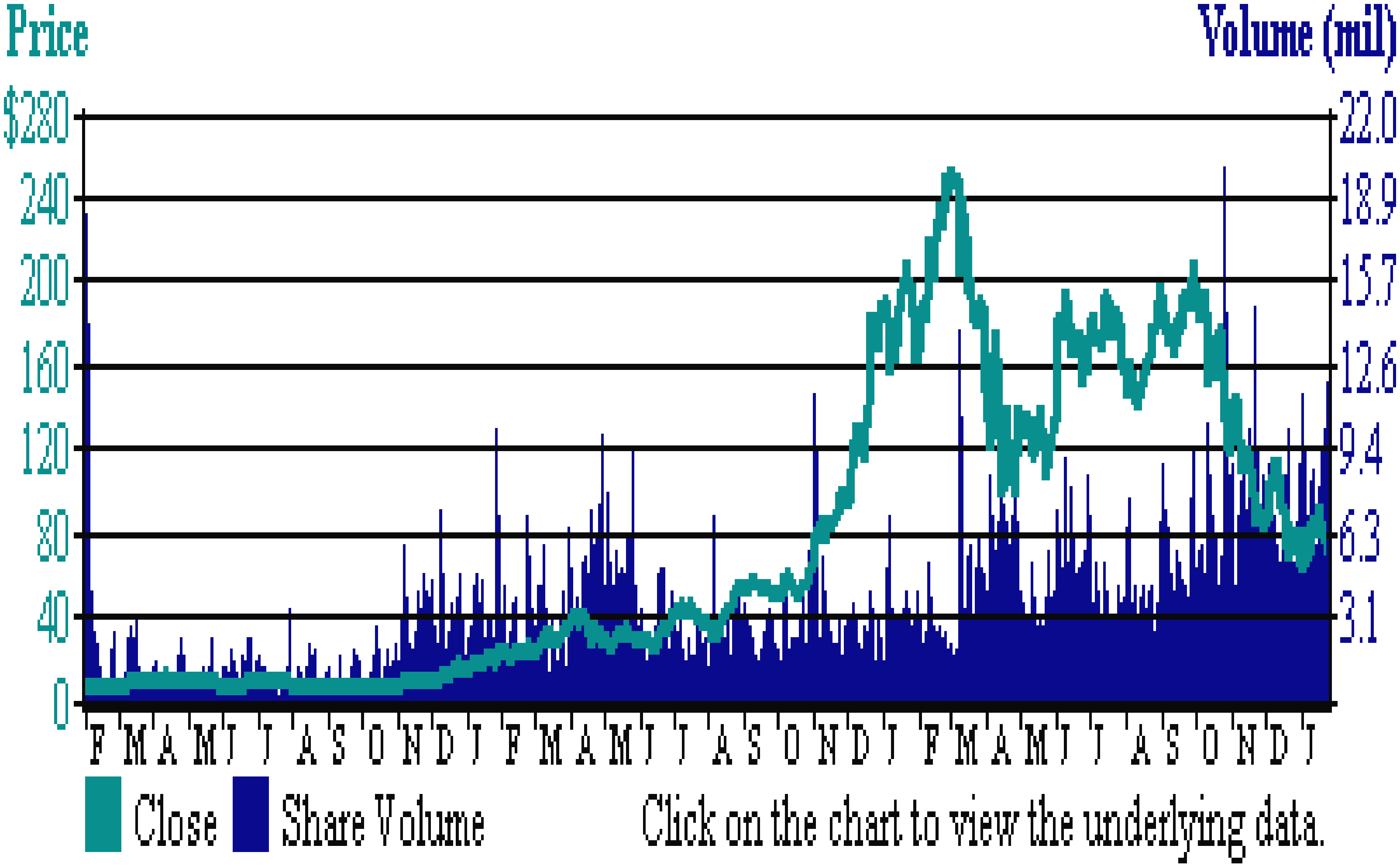
- VeriSign opened HQ in Mountain View: April 1995
- IPO: January 1998
- Aquired Network Solutions: June 9, 2000
- Currently: 2000+ employees

Product Line

- **Web Site Trust Services**
  Authenticate your site to customers and protect Internet transactions with SSL encryption.
- **Payment Processing**
  Securely accept, process, and manage credit card and other payment types for B2B, B2C, and person-to-person purchases on your site.
- **Code Signing**
  Digitally sign software and macros for safe online downloading to your customers.
- **Secure E-Mail**
  Digitally sign and encrypt your e-mail to safeguard it from intrusion and alteration online.
- **Web Identity**
  Register for and manage Web addresses (domain names).

- **Web Authoring**
  Build a professional-looking Web site and then enhance and promote it with business features
- **Enterprise Trust Services**
  Protect your intranet, extranet, e-mail systems, and Virtual Private Networks as well as B2B transactions with PKI and Internet infrastructure solutions.
- **Network Security**
  Protect information with firewalls, VPNs, network appliances, consulting resources, and security management.
- **Global Registry Services**
  Domain name registrars: take advantage of registry services and Domain Name System (DNS) support.
- **Wireless Trust Services**
  Carriers, service providers, manufacturers, and developers: enable a secure wireless commerce environment through an array of standards, devices, and applications.

36 Month Price and Volume as of 1/23/2001



Click on the chart to view the underlying data.

“Internet Identity” ⟷ “Real-World Identity”

- Expertise? Liabilty?
- Suppose you are “Purely” Internet Business? (Recall bob-soft.com)
- Authorization vs. Authentication
- Importance of “Feeling secure”