

ECE 646 - Lecture 1

Security Services

1

Need for *information security*

- widespread use of data processing equipment:
computer security
- widespread use of computer networks and distributed computing systems:
network security

2

Computer Security

- Virus attacks cause greatest financial losses
 - Unauthorized access
 - Loss of Laptops
 - Loss of proprietary information
- Little outsourcing
- Cyber insurance low
- Reporting computer intrusion low but increased
- Data protection is most critical (e.g. through identification, encryption, etc.)

3

Who provided the data

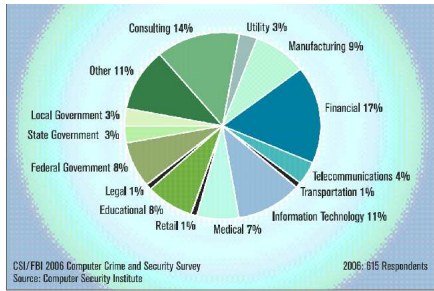


Figure 12. Unauthorized Use of Computer Systems Within the Last 12 Months

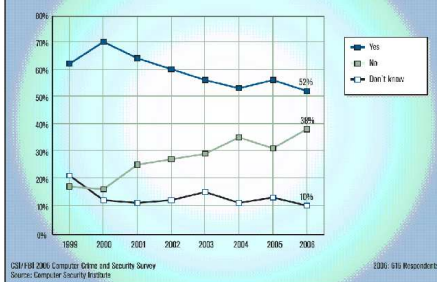
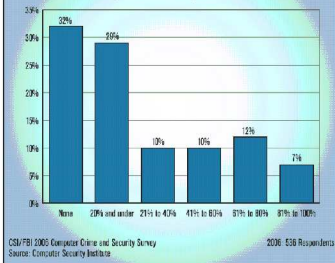
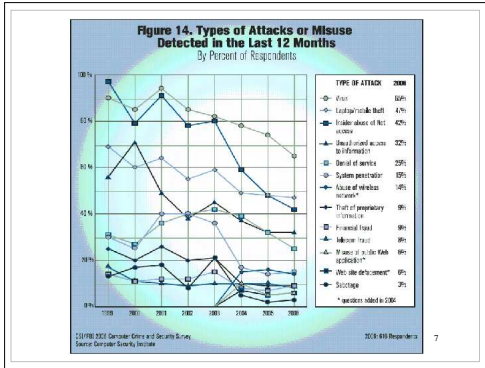
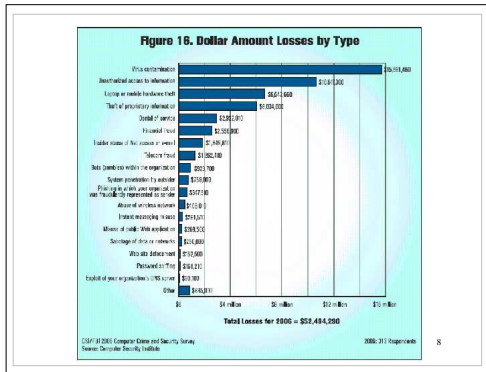


Figure 13. Percentage of Losses That Come from Insider Threats By Percent of Respondents





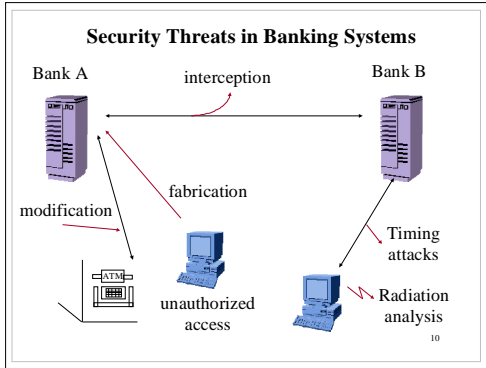


Cryptography is Important

- Algorithms and Usage
- User Education

Table 2. Respondents Identify the Most Critical Issues for the Next Two Years

Most critical computer security issues in next two years	# of respondents
Data protection (e.g., data classification, identification and encryption) and application software (e.g. Web application, VoIP, or financial) security	73
Policy and regulatory compliance (Sarbanes-Oxley, HIPAA)	63
Identity theft and leakage of private information (e.g. proprietary information, intellectual property etc.) business secrets	58
Viruses and worms	52
Management involvement risk management, or support services (human resources, capital budgeting and expenditures)	47
Access control (e.g. passwords)	45
User education, training and awareness	43
Wireless infrastructure security	41
Internal network security (e.g. insider threats)	38



Electronic Commerce

<p>ELECTRONIC FUND TRANSFER - EFT</p> <ul style="list-style-type: none"> • intra-bank fund transfers • inter-bank fund transfers • home banking • electronic cash 	<p>ELECTRONIC DATA INTERCHANGE - EDI</p> <ul style="list-style-type: none"> • financial transactions among companies
--	--

HOME-SHOPPING

- non-digital goods (e.g., books, CDs)
- services (e.g., travel reservations)
- digital goods (e.g., software, music, video)
- micropayments (e.g., database access)

11

Electronic Data Interchange

- transactions between computers
- human participation in routine transactions limited or non-existent
- paper records eliminated
- less time to detect and correct errors

12

Other types of data needing security

- financial records
- medical records
- commercial secrets
- business and private correspondence
- technical specifications
- your computer

13

Potential attackers

- hackers
- industrial competitors
- spies
- press
- government agencies

14

Security on the Internet

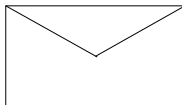
E-MAIL

≡

Alice, Alice
Love you, Smurftown,
Bob SL 22030
Smurfland

**SECURE
E-MAIL**

≡



15

NSA

National Security Agency
 (also known as “**N**o **S**uch **A**gency”
 or “**N**ever **S**ay **A**n~~Y~~thing”)

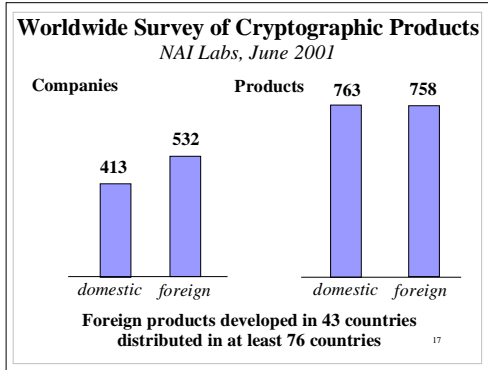
Created in 1952 by president Truman

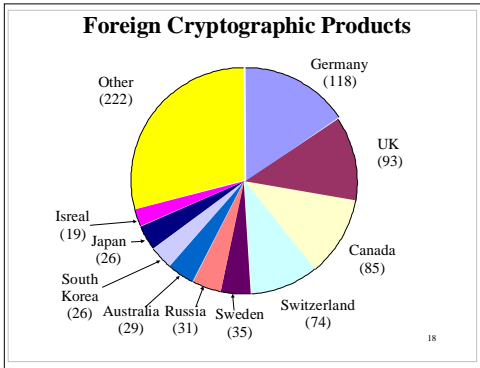
Goals:

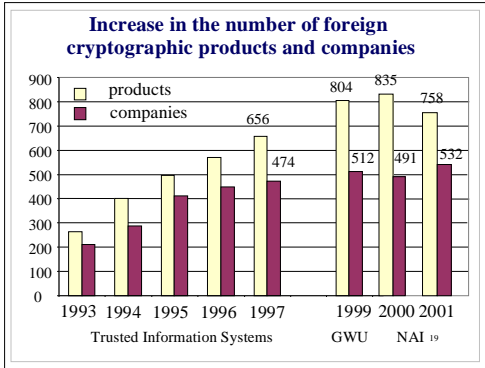
- designing strong ciphers (to protect U.S. communications)
- breaking ciphers (to listen to non-U.S. communications)

Budget and number of employees kept secret
 Largest employer of mathematicians in the world
 Largest purchaser of computer hardware

16



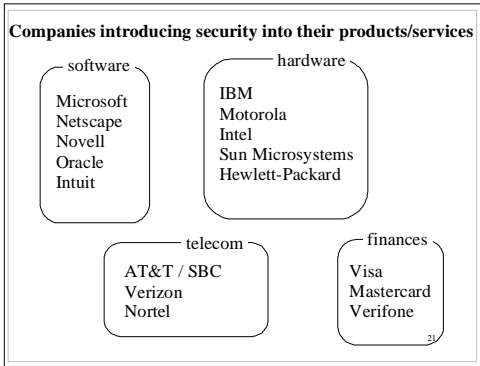


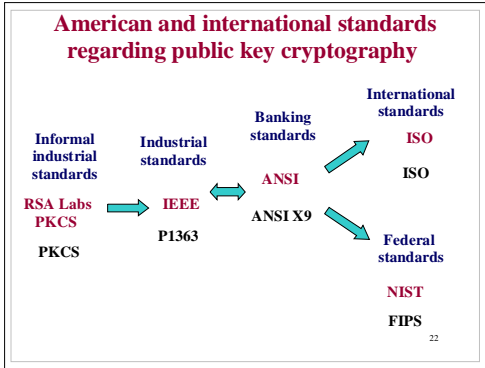


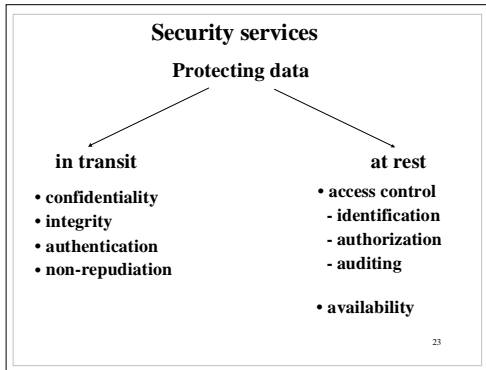
RSA Security Inc.

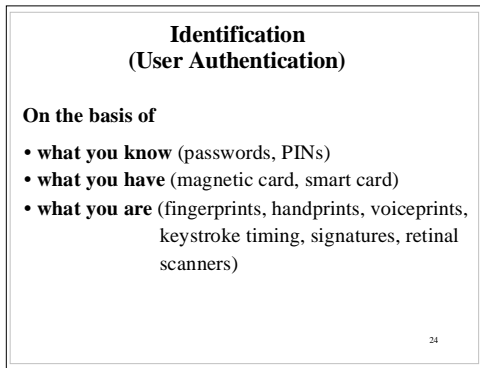
- patents for RSA, RC5, RC6 and other
- over 1 billion users of crypto library BSAFE
- RSA Laboratory
- RSA Conference
- spin-off companies
 - VeriSign (1995) – Public Key Infrastructure
- acquired by EMC² (2006)
 - EMC² Data storage solutions

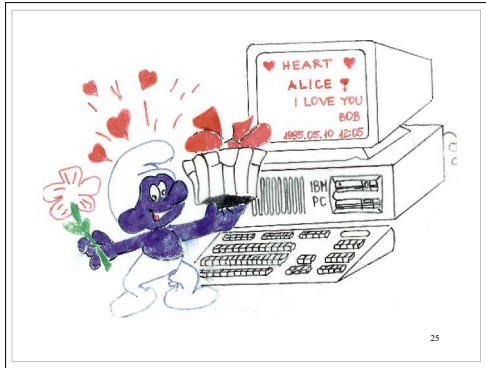
20



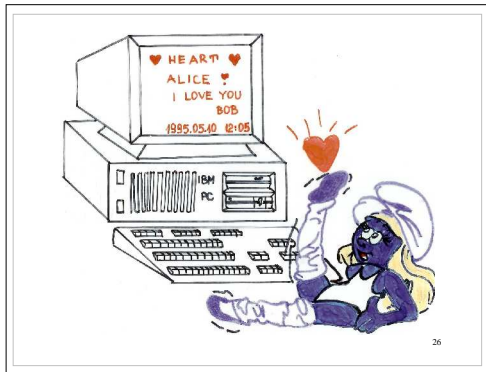




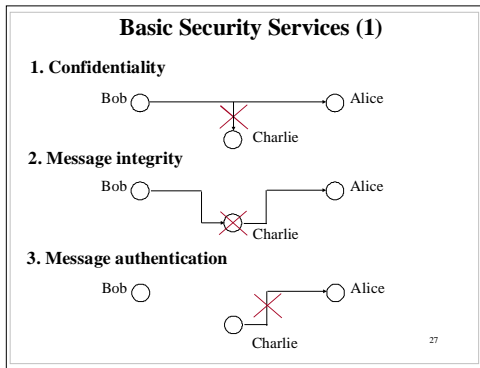




25



26



Basic Security Services (2)

4. Non-repudiation
- of sender - of receiver - mutual


Technique: *digital signature*

DIGITAL

A6E3891F2939E38C745B
25289896CA345BEF5349
245CBA653448E349EA47

Signature

HANDWRITTEN



Main Goals:

- unique identification
- proof of agreement to the contents of the document

28

Handwritten and digital signatures
Common Features

Handwritten signature	Digital signature
<ol style="list-style-type: none"> 1. Unique 2. Impossible to be forged 3. Impossible to be denied by the author 4. Easy to verify by an independent judge 5. Easy to generate 	

29

Handwritten and digital signatures
Differences

Handwritten signature	Digital signature
6. Associated physically with the document	6. Can be stored and transmitted independently of the document
7. Almost identical for all documents	7. Function of the document
8. Usually at the last page	8. Covers the entire document

30

