Litchko & Associates, Inc.

Practical and Acceptable Authentication

Jim Litchko
Litchko & Associates
301-493-0001
jim@litchko.com

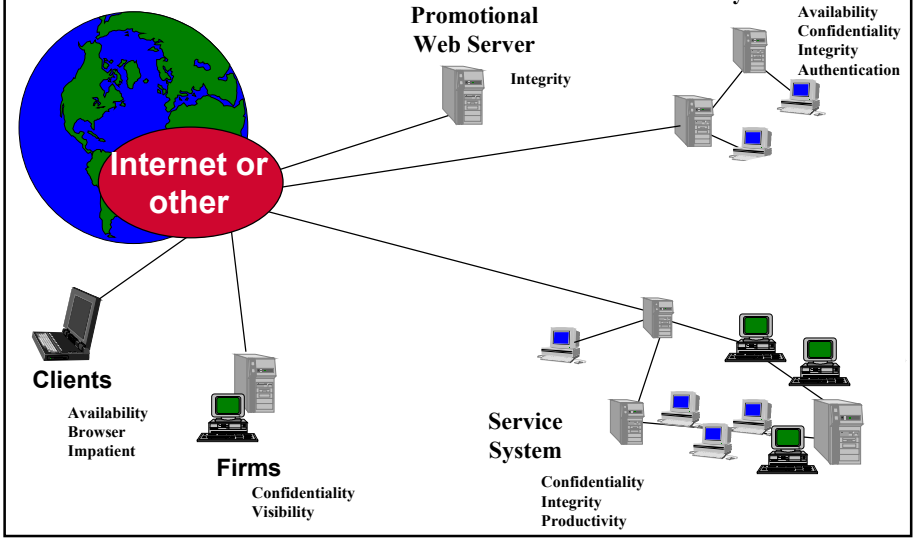
Presentation

- Basics
- Solutions
- Problems
- Applications
- Conclusions

Basics are . . .

- Solutions are based on:
  - "Business" requirements first,
  - Customer acceptance second,
  - Affordability third, and
  - Technical security fourth.

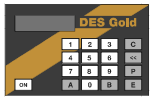
Requirements



Authentication Basics

- Something that you <u>know</u>:
  - PIN or combination
  - Password
  - Procedure

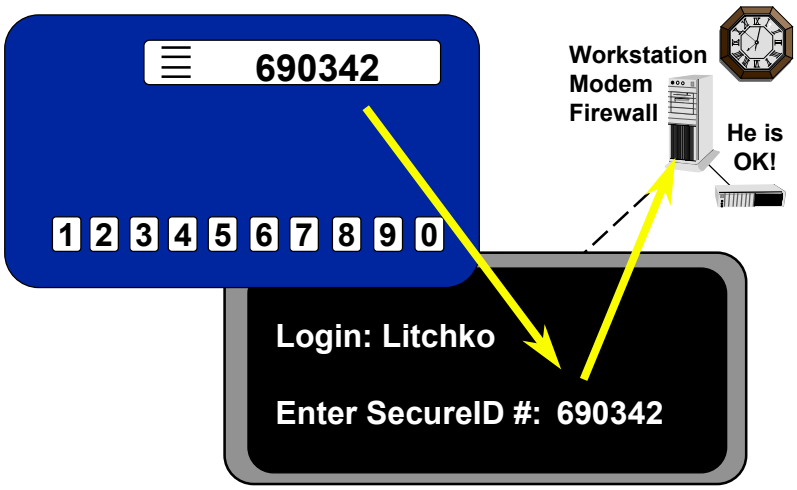
R-38
L-13
R-41



- Something that you <u>have</u>:
  - Badge or ID
  - ATM or Credit card
  - Token

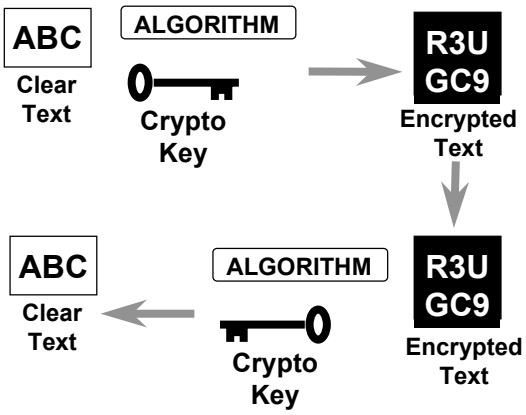
- Something that you <u>are</u>:
  - Finger prints and retina patterns
  - Voice pattern and weight
  - Signature

Password Token ..... time based.



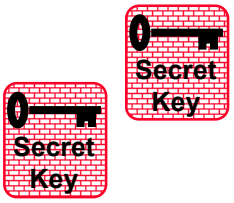
Components and Process

- ENCRYPT
- DECRYPT



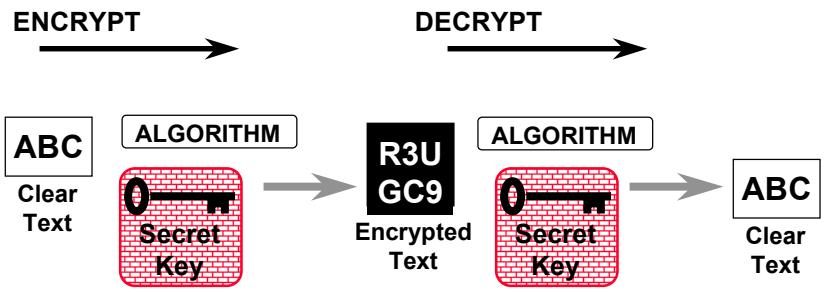
Algorithms

- **Symmetric**
  - Called "secret-key encryption"
  - Shared "Secret Keys"
  - Data Encryption Standard (DES)



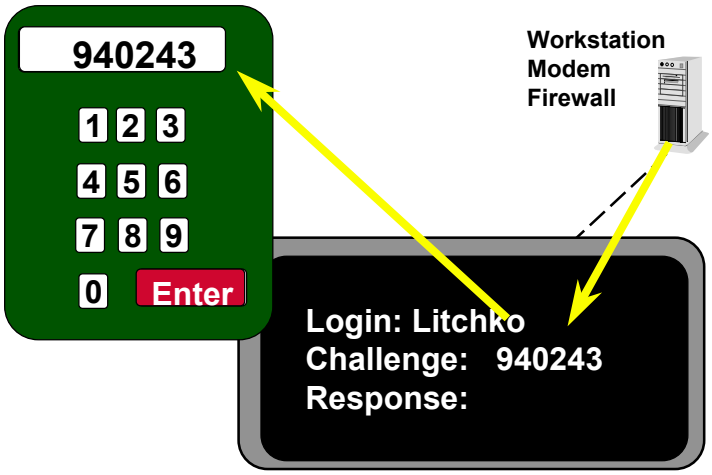
- **Asymmetric**
  - Called "public-key encryption (PKE)"
  - A "Private Key" and a "Public Key"
  - Rivest, Shamir, and Adleman (RSA)

Secret-Key Encryption

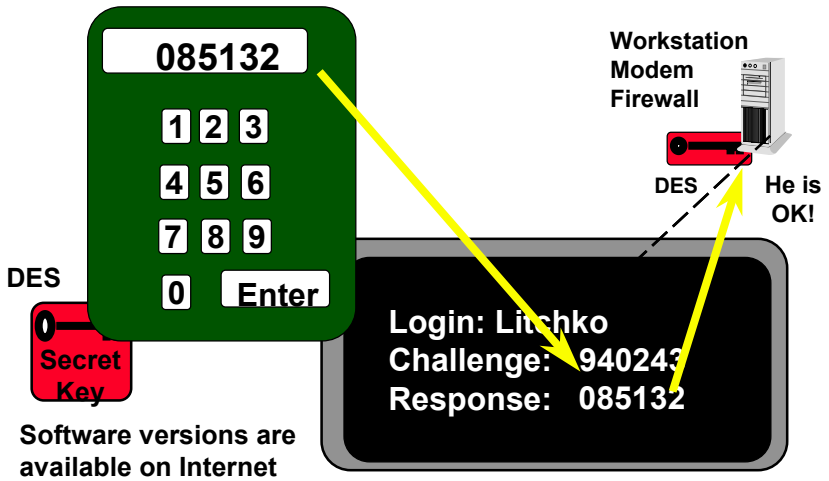


Confidentiality?
Authentication?
Integrity?
Non-repudiation?

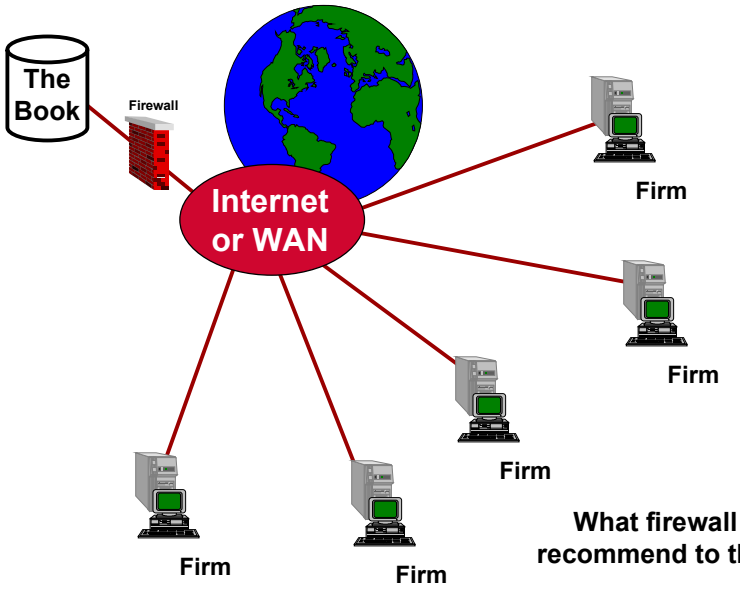
Challenge-Response . . . in a token.



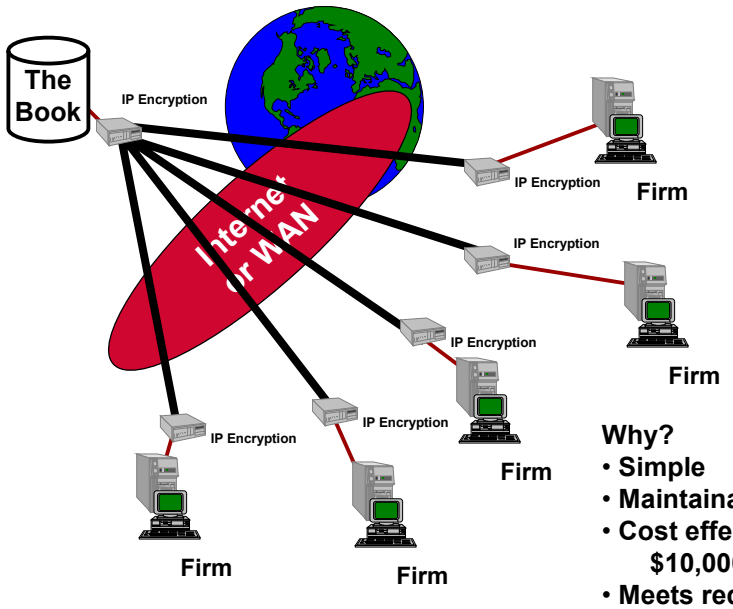
Challenge-Response . . . in a token.



Software versions are available on Internet and from vendors.

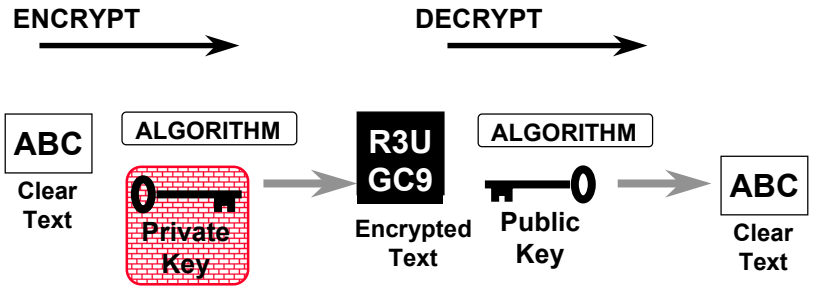


What firewall shall I recommend to the firms?



Why?
- Simple
- Maintainable
- Cost effective
  $10,000US/site
- Meets requirements

Public-Key Encryption



Confidentiality?
Authentication?
Integrity?
Non-repudiation?

Authentication Solutions

• Smartcards

• PCMCIA Card
Spyrus
Fortezza

• Tokens
SecureID
Challenge-Response

• SmartDisk
Fischer International

• Computer Chip
DataKey
iKey
iButton

Smartcard Deployment

PCMCIA Card

Token Reader

Smart Disk

Card Reader

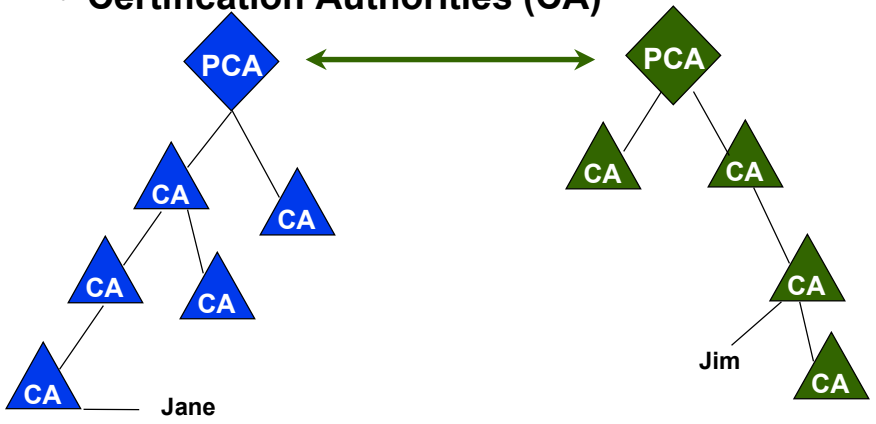
Certificate Format

- X.509 Standard Certificate
- Format:
  - Version Number
  - Serial Number
  - Signature Algorithm Identifier
  - Certificate Issuer
  - Validity Period
  - Subject (owner)
  - Subject's Public Key

  Issuer's Signature

Certificate Hierarchy

- Principle Certification Authorities (PCA)
- Certification Authorities (CA)

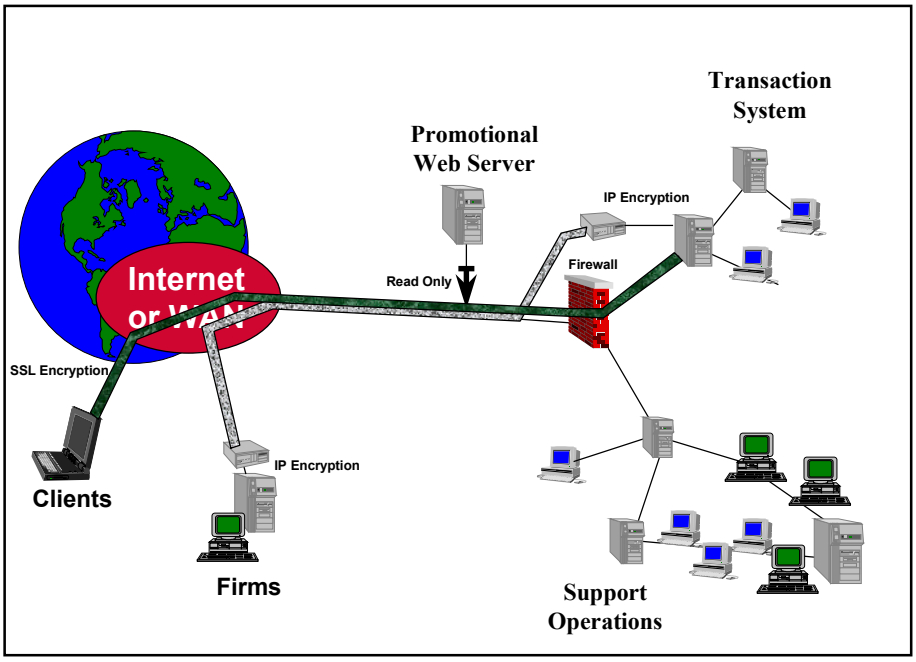


Biometrics

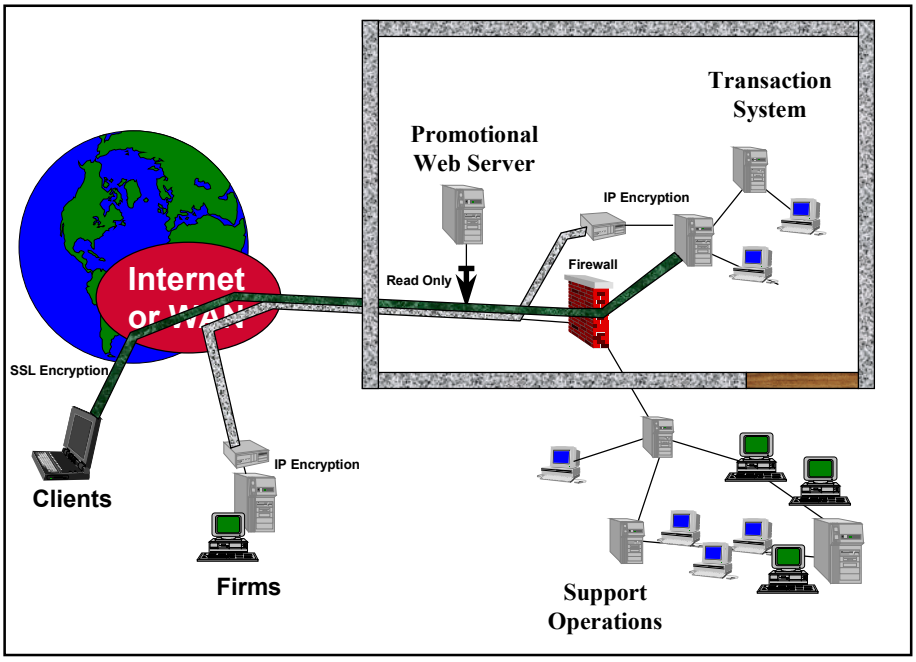
http://www.identix.com/itsecurity/products/index.html

Security and Business Math

	Before	After	Better Idea?
Gross:	$ 50B	$ 50B	$ 40.0B
Loss:	$ 4.5B	$ 1.0B	$ 0.0B
Net:	$ 45.5B	$ 49.0B	$ 40.0B



MID/jpl 12/19/2001 21



MID/jpl 12/19/2001 22

The Lone Ranger and Tonto

- Tonto, “Look up and tell me what you see.”
- “I see millions of stars, Tonto.”
- ”And what does that tell you, Kemo Sabi?”
  - Astronomically speaking . . . .
  - Astrologically . . . .
  - Time wise . . . . .
  - Theologically . . . .
  - Meteorologically . . . .
- “What it tell you, Tonto?”

Summary

- Business requirements “First!”
- Keep solutions “minimal”
- Think “user acceptance”
- Sometimes the “stone arrow” is more effective and affordable then the “silver bullet”.

Jim Litchko's Bio:

Mr. Litchko is a senior information systems security specialist with over twenty-five years experience assessing and developing information system security (INFOSEC) solutions for computer and network systems. He has held senior executive positions for special projects and business development at the two largest commercial INFOSEC companies, Secure Computing Corporation and Trusted Information Systems and the enterprise integrator, Telos, all internationally known for advance INFOSEC research and development, consulting, and network security products. During his twenty-year career as a Navy cryptologist, Mr. Litchko spent his first six years supporting operations on naval combatants and air reconnaissance platforms in the Atlantic, Pacific, and European theaters. Mr. Litchko's last five years in the Navy were in staff and technical positions in the National Security Agencies (NSA) INFOSEC Directorate and the National Computer Security center (NCSC). His last position was Staff Chief for the Director of the NCSC. Since 1988, he has been an instructor for systems and network security for Johns Hopkins University, MIS Training Institute and the National Cryptologic School. He has also given INFOSEC presentations to Congressional staffs, Gartner Group, Conference Board, Price Waterhouse, Exxon, Freddie Mac, National Industrial Security Association, Computer Security Institute (CSI), National Computer Security Association (NCSA), Defense Intelligence University, and Armed Forces Communications and Electronic Association (AFCEA). Mr. Litchko has chaired panels and provided INFOSEC presentations at national, international, and executive conferences. He holds a Masters degree in Information Systems from John Hopkins University and a Bachelors degree in Industrial Technology from Ohio University. He is currently an independent systems and network security consultant.

jim@litchko.com (301) 493-0001phone (503) 961-8391fax
4604 Saul Road, Kensington, Maryland 20895

