



# Practical Authentication:

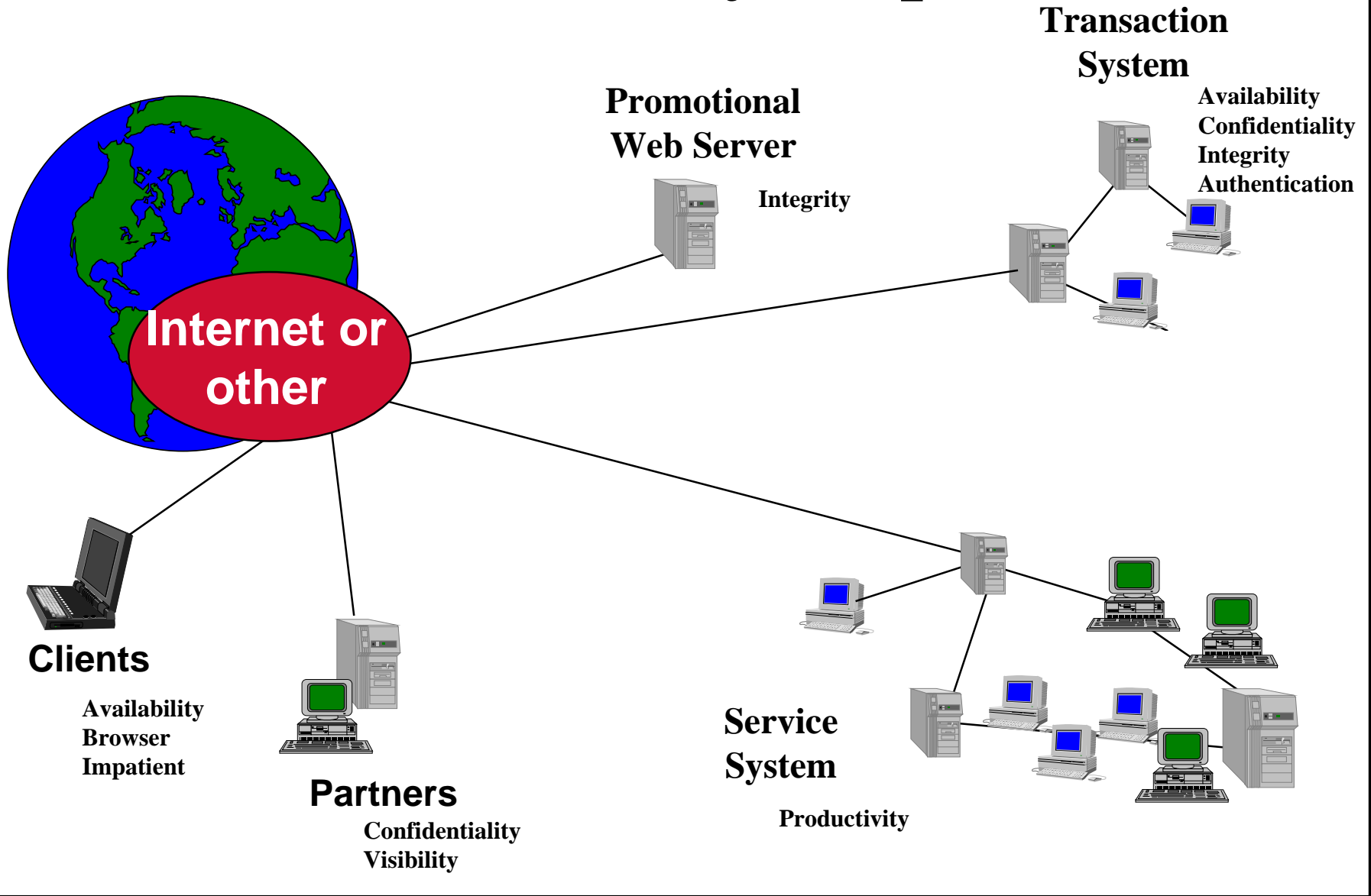
## The right way and the wrong way.

**Jim Litchko**  
**Litchko & Associates, Inc.**  
**301-493-0001**  
**[jim@litchko.com](mailto:jim@litchko.com)**

# Presentation

- **Security Requirements**
- **Authentication Solutions**
- **Issues and Opinions**
- **Questions**

# Business/Security Requirements



# The Cuckoo's Egg by Cliff Stoll

- **West German Cracker**
- **Attacks**
  - Exploited known security holes
  - Guessed weak passwords



# Internet Worm by Robert Morris, Jr.

- **Automated Attack**
  - Exploited known security holes
  - Guessed weak passwords - list of 350

# Authentication

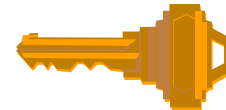
- **Something that you know:**

- PIN or combination
- Password
- Procedure

R-38  
L-13  
R-41

- **Something that you have:**

- Badge or ID
- ATM or Credit card
- Token

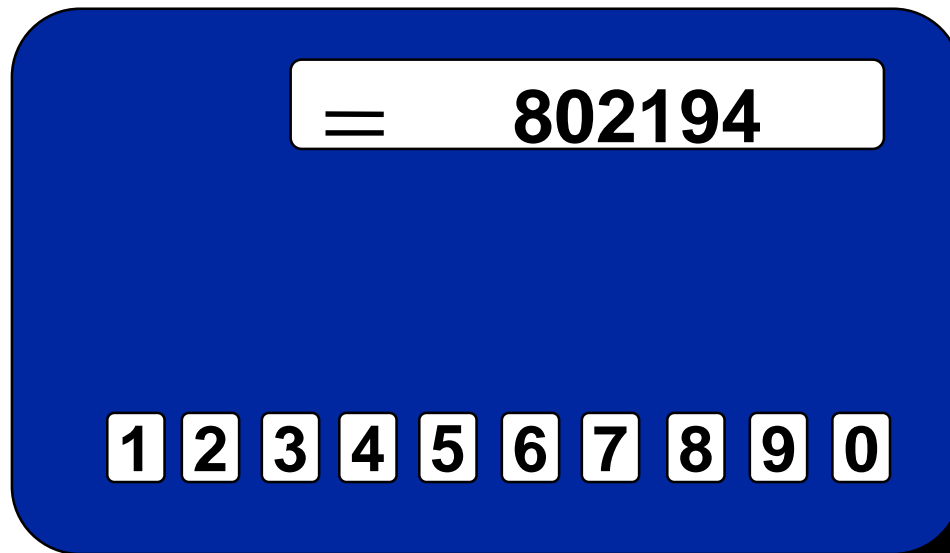


- **Something that you are:**

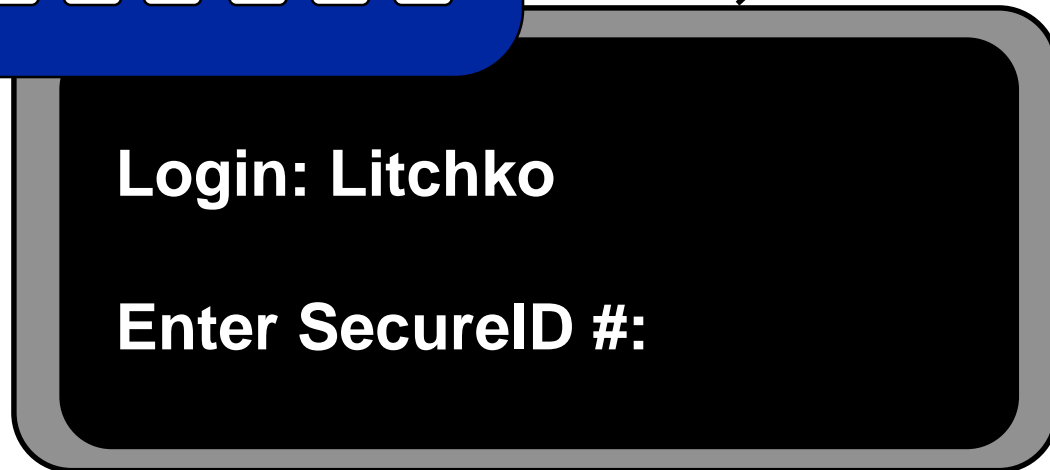
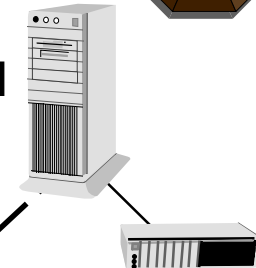
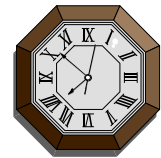
- Finger prints and retina patterns
- Voice pattern and weight
- Signature



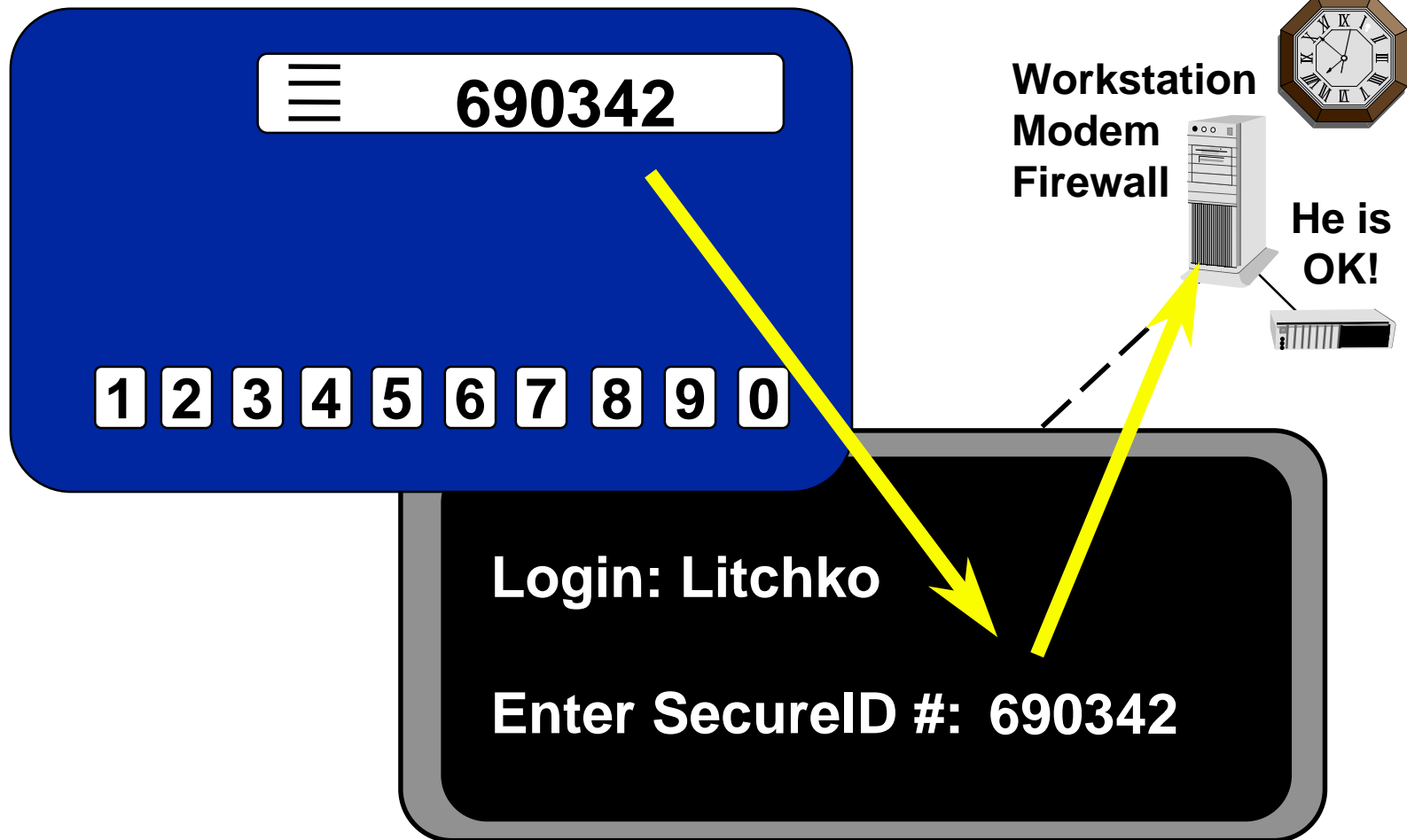
# Password Token..... time based.



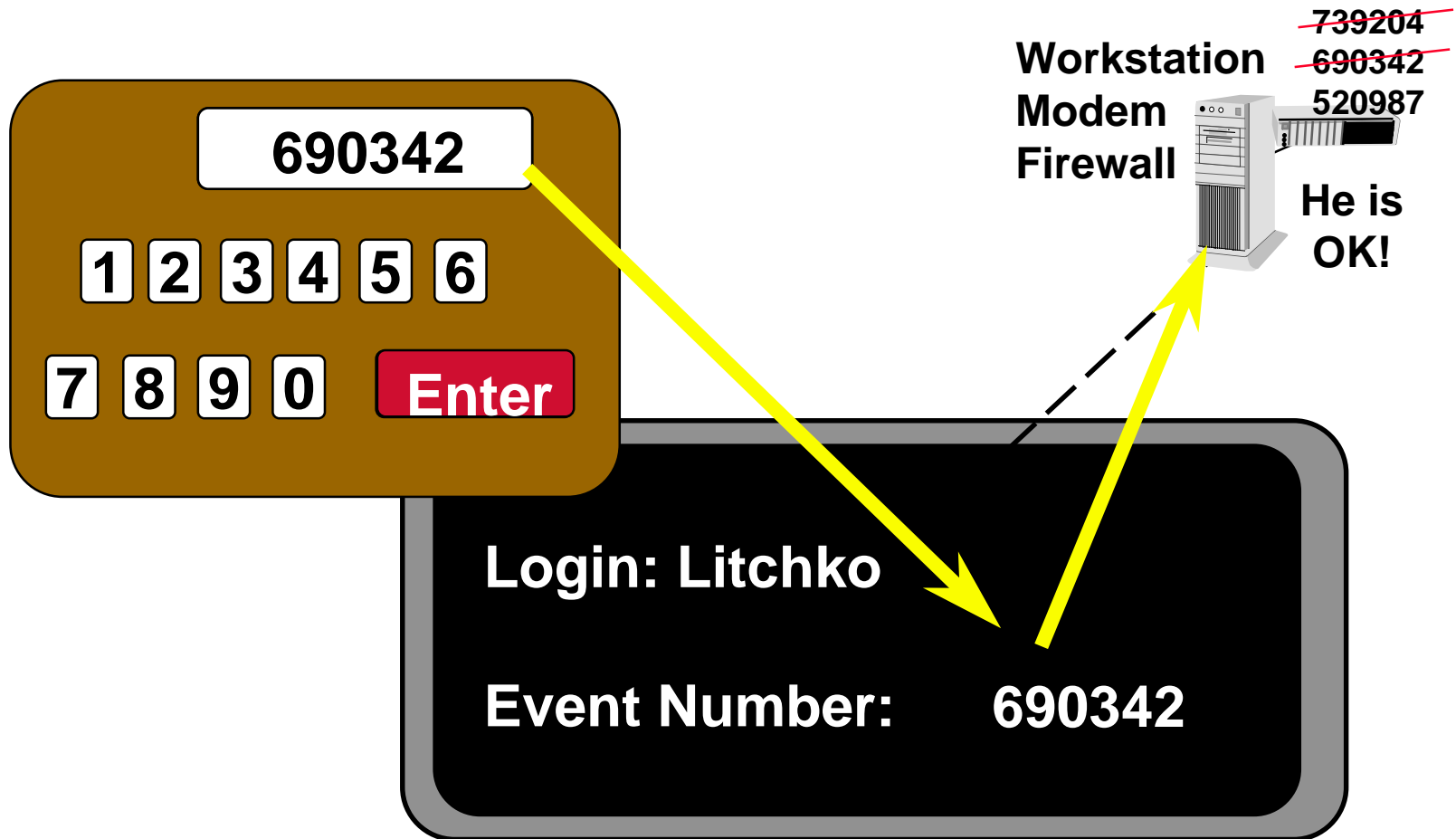
Workstation  
Modem  
Firewall



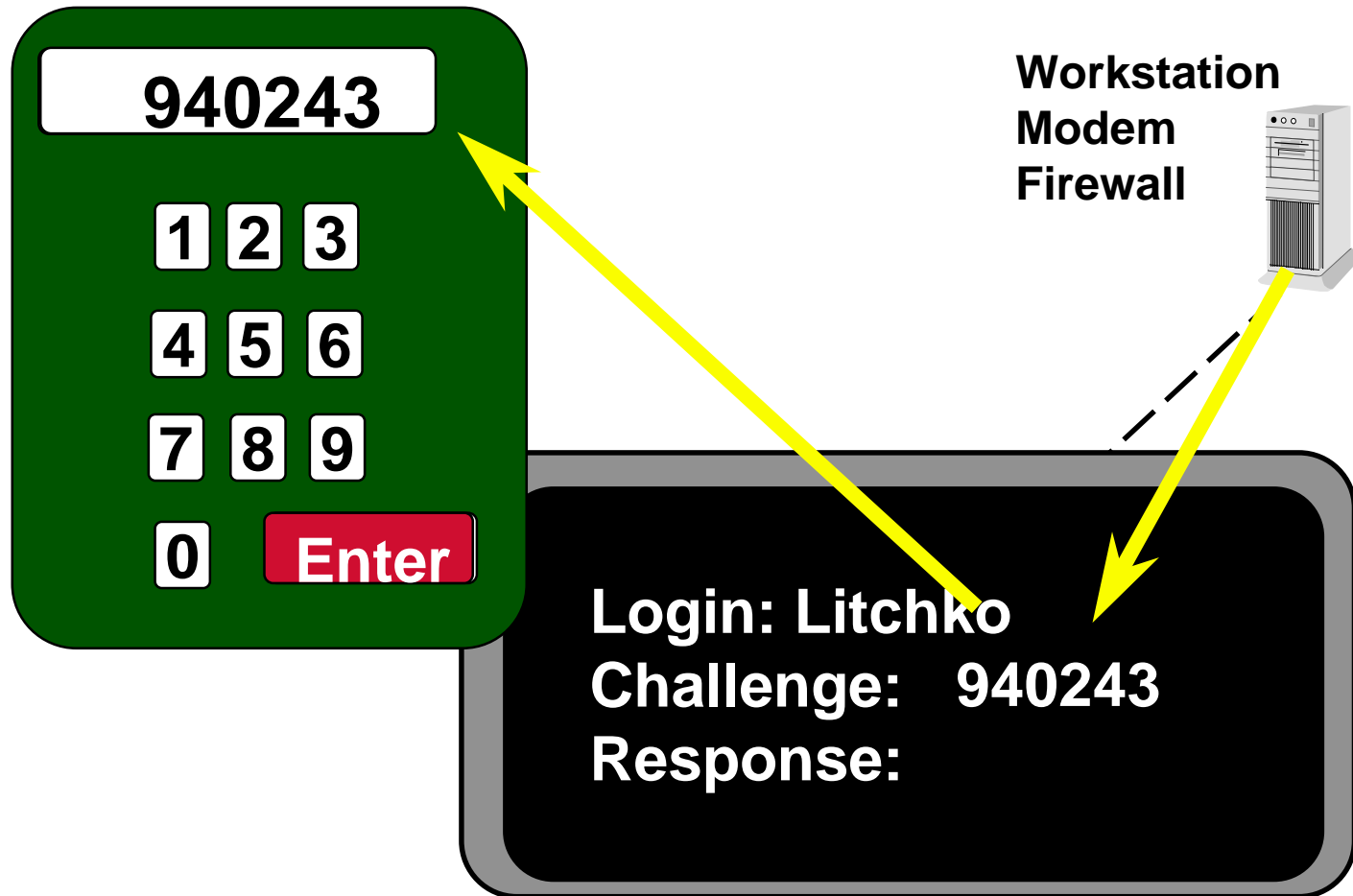
# Password Token..... time based.



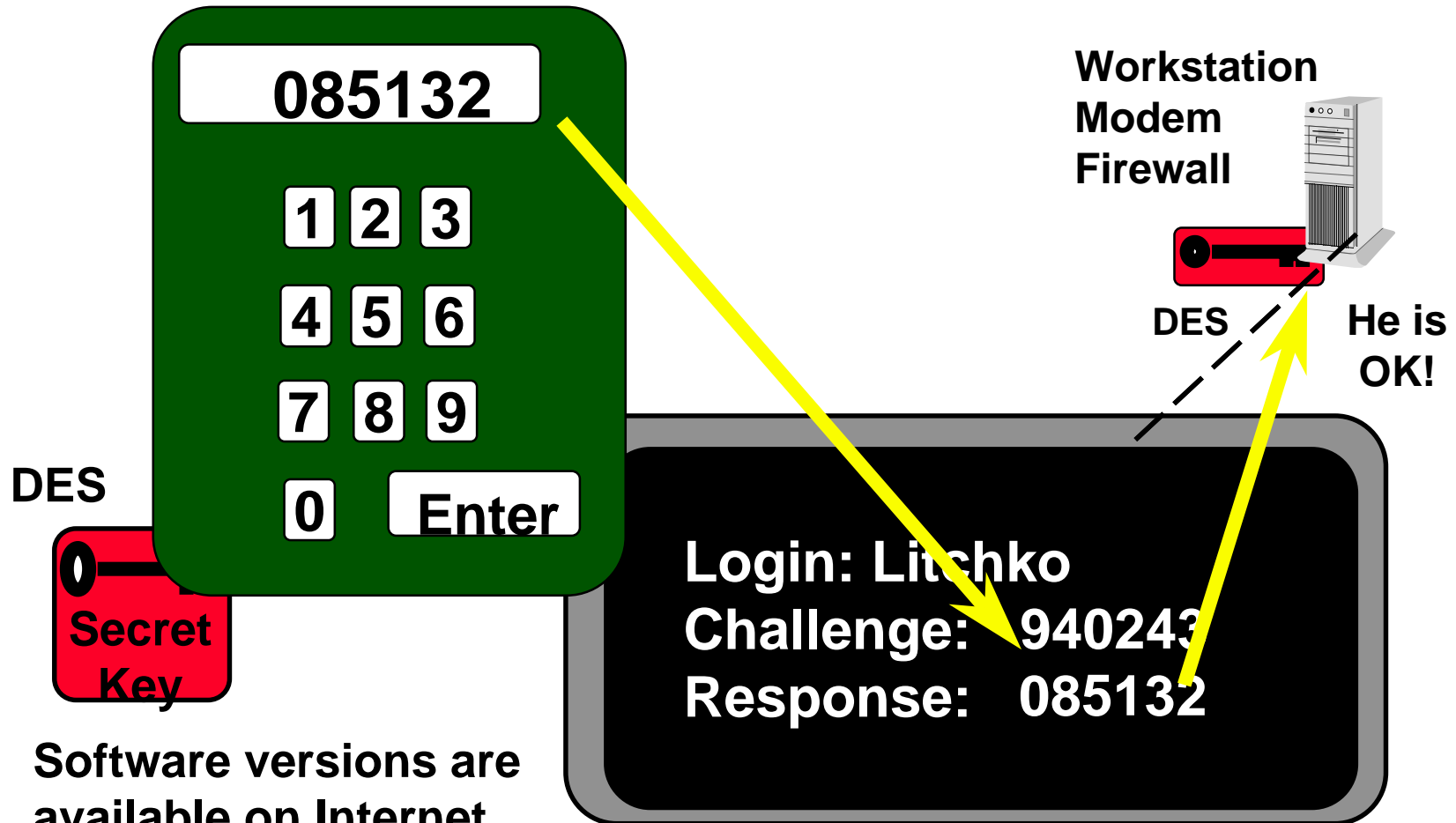
# Password Token..... event based.



# Challenge-Response . . . in a token.

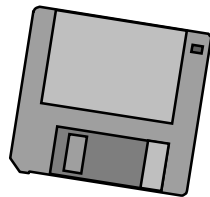


# Challenge-Response . . . in a token.



Software versions are available on Internet and from vendors.

# Crypto Deployment



- Software  
PGP  
Netscape



- PCMCIA Card  
Spyrus  
Fortezza



- SmartDisk  
Fischer International



- Computer Chip  
DataKey  
iKey  
iButton



# Crypto Deployment

- Smart Cards



**Serial Reader**



**Smarty**



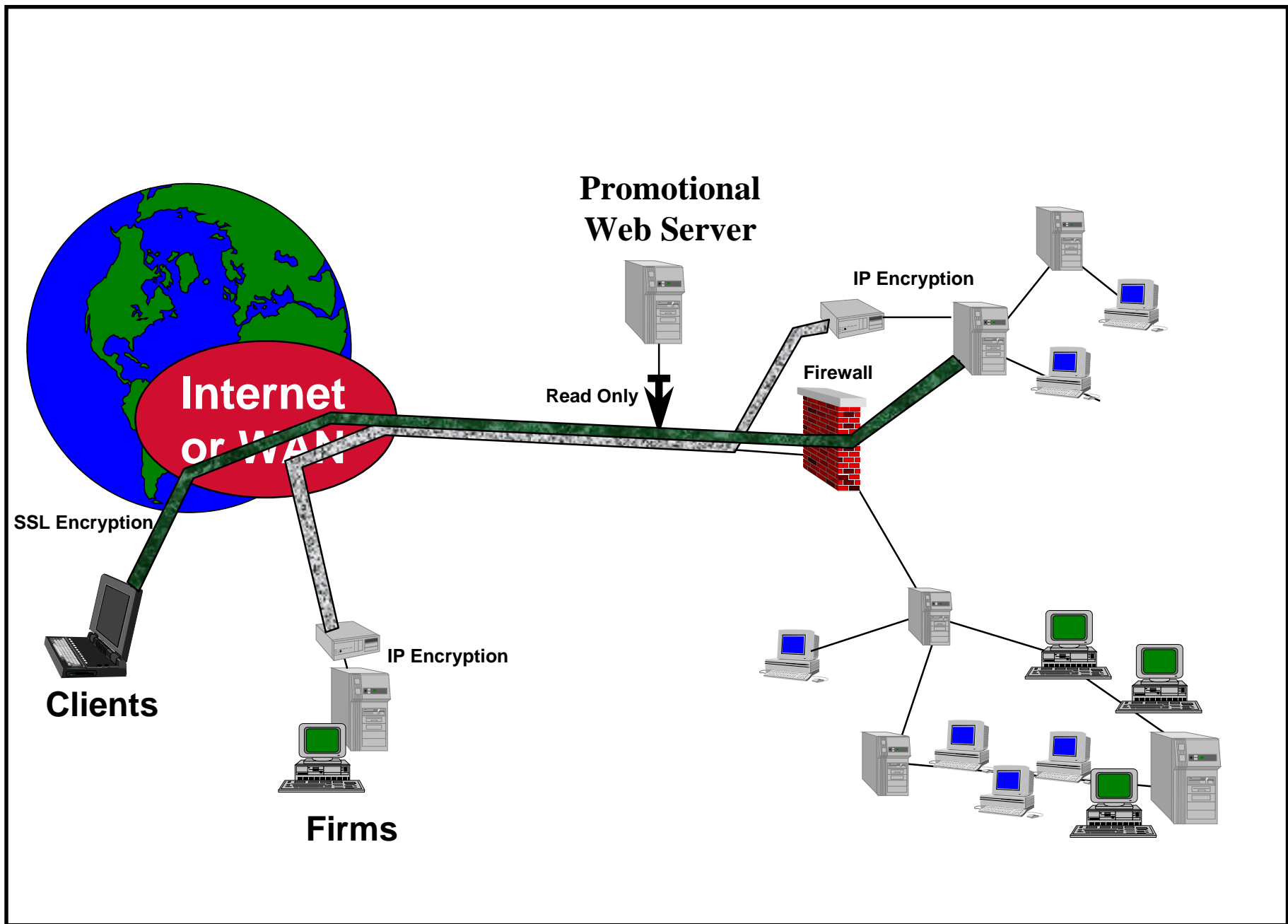
**PCMCIA Reader**

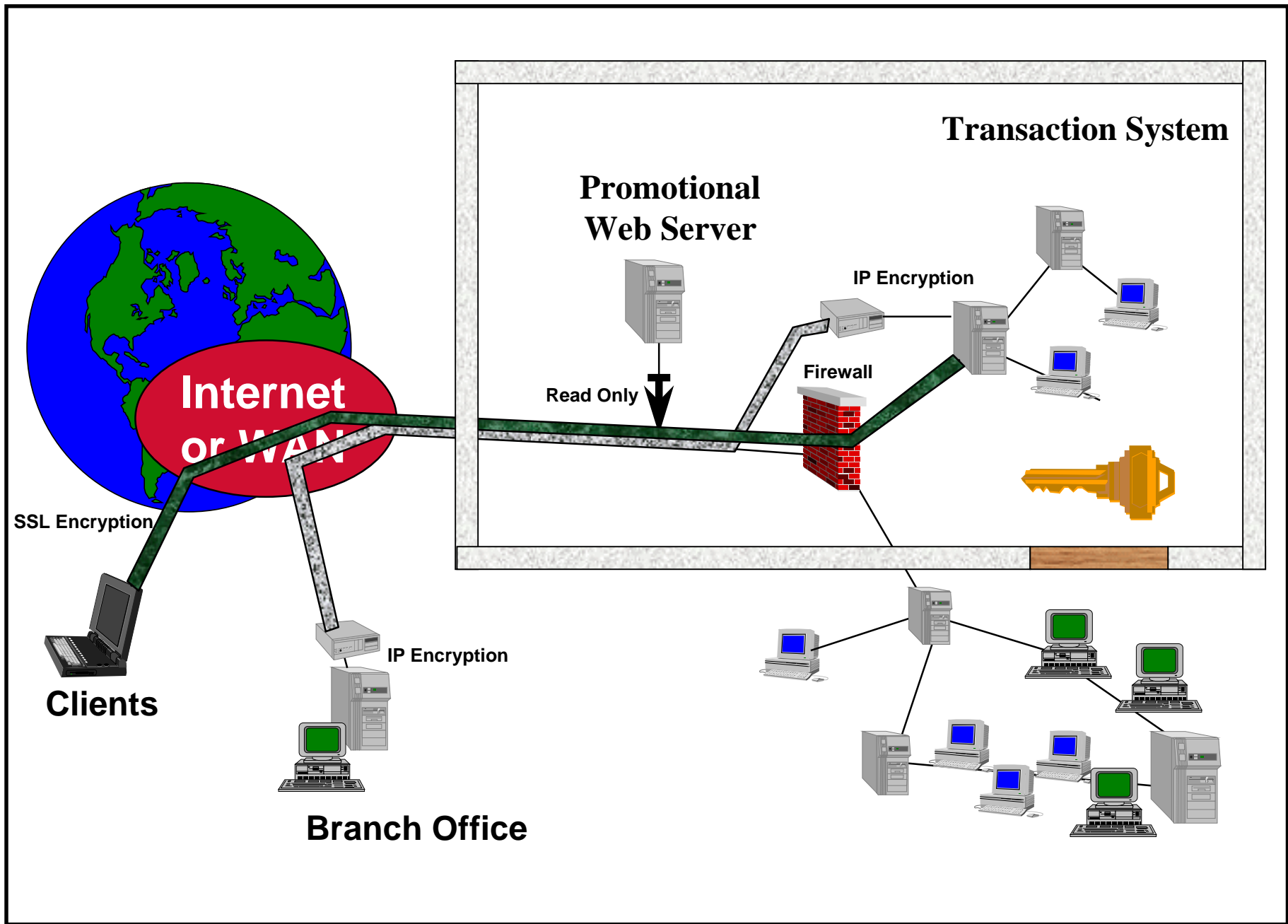
# Access Problem

- Odds Projection Web-site
- Subscription
- Sharing passwords
- \$40,000/month losses
- Solution?

# Security and Business Math

	<u>Before</u>	<u>After</u>	<u>Better Idea?</u>
<b>Profit:</b>	\$ 50B	\$ 50B	\$ 40B
<b>Loss:</b>	\$ 4.5B	\$ 1.0B	\$ 0
<b>Net:</b>	\$ 46.5B	\$ 49.0B	\$ 40B





## **Practical and Acceptable Authentication:**

### **The right way and the wrong way.**

You have identified the need to authenticate and now must decide on what authentication solution you should use. The “good news” is that you have over 300 product options, the “bad news” is that you have over 300 options. Which one will support your needs and more importantly will be acceptable by your clients and employees?

This presentation will review the generic options, will discuss the variables that you should consider when selection a solutions, and will provide real-world business examples of successful and unsuccessful deployments. Generic options that will be covered are: static passwords, challenge-and-response, time-based, one-time pads, public-key cryptography, biometrics, and post-it notes. The variables are very business and end-user dependent and include: corporate culture, costs, practical, environment, acceptable, etc. The business examples will include government, commercial and personal case studies. This presentation is a must for anyone designing an information system.



## 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**