Weak links in e-commerce security: examples from the field

Gary McGraw

Reliable Software Technologies

Sterling, Virginia

gem@rstcorp.com

http://www.rstcorp.com

As if we didn’t know...

“We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even immaginable today, opening up a new world of economic possibilities and progress.”

- *Vice President Albert Gore, Jr.*

“The Wild West of the global economy…make sure that it’s safe and stable terrain for those who wish to trade on it.”

- *President William J. Clinton*

Deja vu all over again

Software Engineering and E-commerce

- Developing a solid specification is hard and errors are common
  - diagrams and formal methods are underutilized
  - crucial design decisions are often not justified
- The best specification in the world has to be implemented
- Complex systems are very hard to get a handle on
- Testing of final systems is overlooked

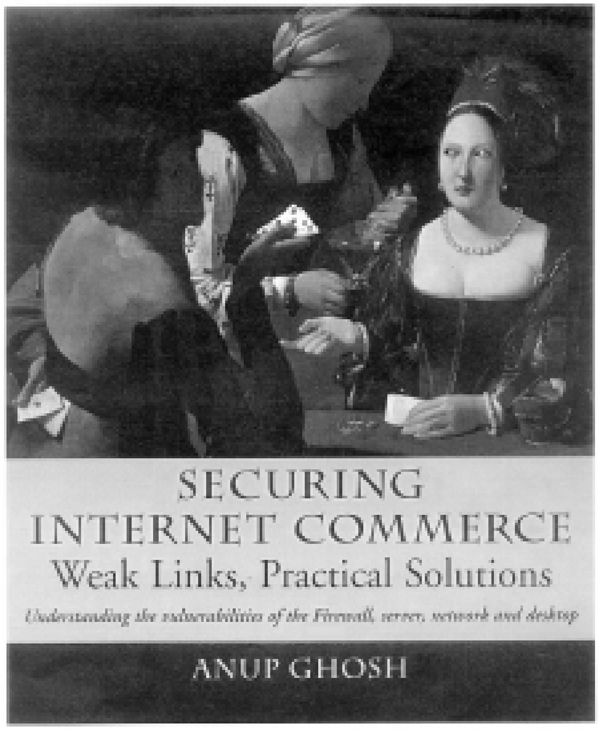
Errors in the real world

Specification errors	Examples
● Beginning with an old system and bolting things on	● Taking an existing stored-value system and “Internet”-ing it
● Mis-using encryption – key management	● Double and triple encryption
● Underspecification and clarity	● No use of formalism for protocols
● Error handling	● Exception propagation

Errors in the real world (2)

Implementation errors	Examples
● Weaknesses in crypto systems	● Data integrity hashes that are easily broken ● DES-based key management weakness
● Not enough testing for security	● Functional testing does not simulate attacks

EC security RST


SECURING
INTERNET COMMERCE
Weak Links, Practical Solutions
Understanding the vulnerabilities of the Firewall, server, network and desktop
ANUP GHOSH

- How can we certify the security of a software component for e-commerce?
- What impact do smart cards (especially Java Cards) have on security?

http://www.rstcorp.com/EC-security.html