Quality, Security and Privacy: Independent or Interlocked Issues?

Gregory A. Rondot

CISSP, NSA-IAM, CCNA, MCP, CNE,
Certified Network Analyst

January 14, 2004

rondotech CONSULTING INC

Core Questions

- Can you have a secure system without it being a high quality system?
- Can you have true assurances of privacy without known level of security and quality?

Premise

- Privacy
  - Protect ourselves from misuse of personal information
- Security
  - Data integrity, availability, and confidentiality
- Quality
  - Improve systems

Is Privacy Important?

- Virtual Society
  - Less in-person interaction
  - Rely on other authentication mechanisms
- Commercially known by computerized identity
  - Credit report, Driving record, Financial records / accounts
- Health information
  - Anti-discriminatory measures

Congressional Opinion Polls

- Americans have great concerns about their privacy being compromised – privacy seen as a “landmine issue”
- Different people mean different things when they are talking about privacy – examples:
  - Privacy means absolute anonymity
  - Privacy means absolute confidentiality.
  - Privacy means security;
    - ***More than two-thirds of Internet users worry that hackers will steal their credit card information.***
- Americans are most anxious about sensitive information that might be used to cause them harm.

Opinion Surveys: What Consumers Have To Say About Information Privacy
Subcommittee on Commerce, Trade, and Consumer Protection, May 8, 2001

State & Federal Privacy Regulations

- Gramm Leach Bliley Act
  - Applies to Federally chartered financial institutions – banks, securities firms, etc
- HIPPA
  - Medical Privacy - National Standards to Protect the Privacy of Personal Health Information
- California Financial Information Privacy
  - Addresses Identity Theft and Data Collection and Use Limits

rondotech CONSULTING INC

Privacy & Security

- So Privacy is important to society…
- How does security apply?

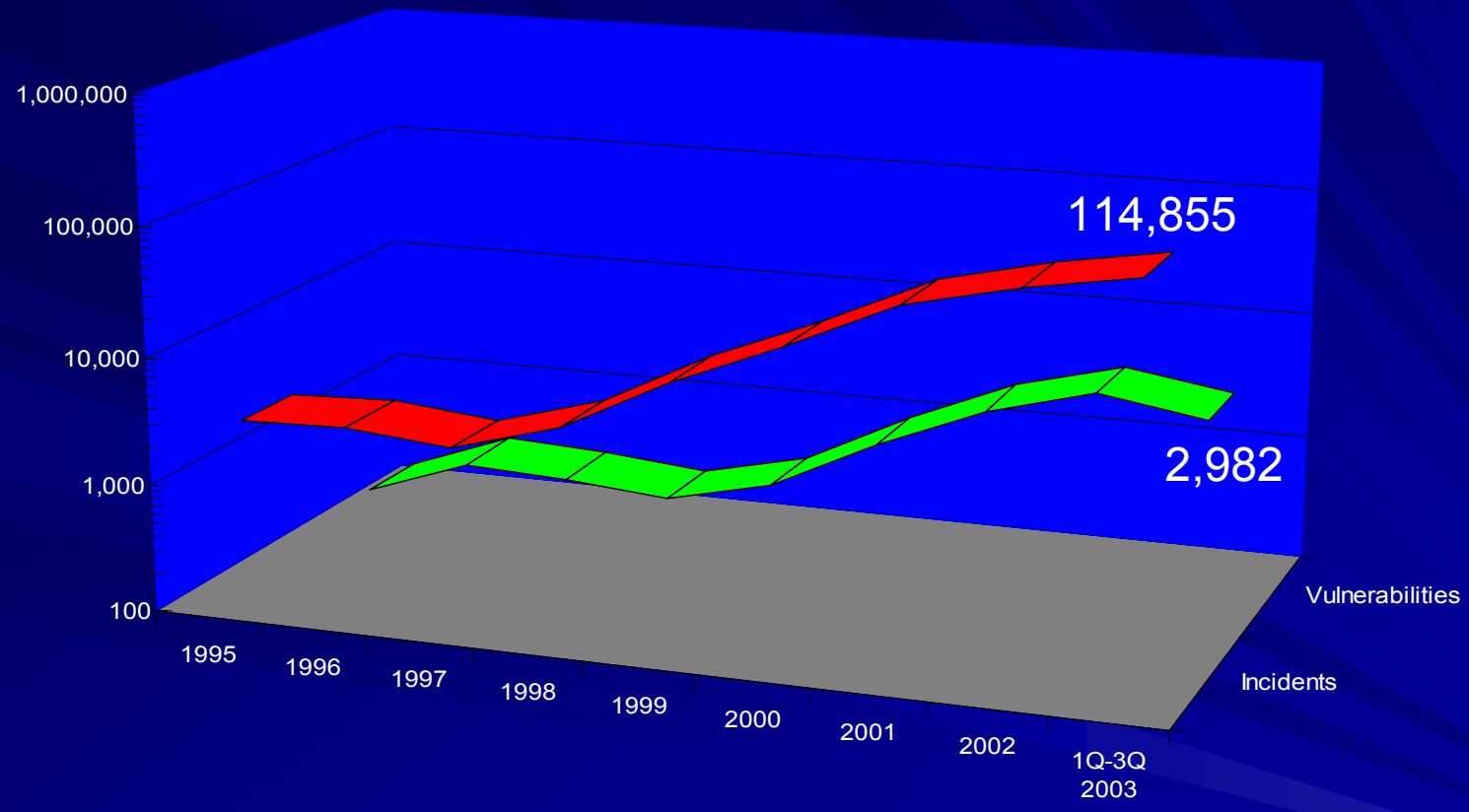
Computer Security

- Common definition
  - Protect electronic information, applications, and systems from unauthorized access
  - Preserve the confidentiality, availability and integrity of electronic information

Vulnerabilities Reported

- CERT Statistics - 2003
  - Most vulnerabilities threaten confidentiality
    - Implant rogue applications
    - Permit unauthorized remote access
    - Obtain and send sensitive data out
  - ***Majority of non-virus vulnerabilities result from programming errors or mishandling unanticipated input***

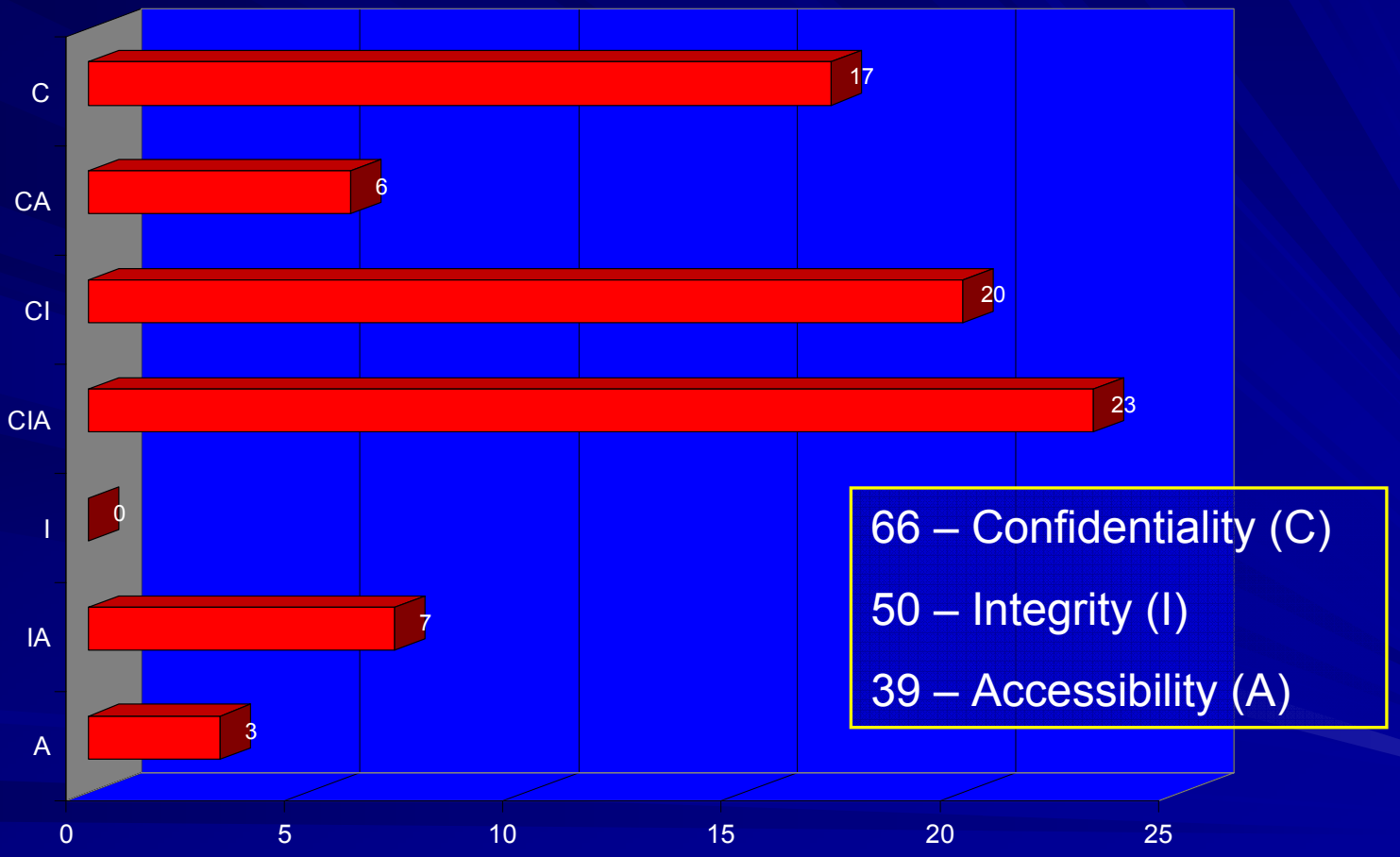
Vulnerabilities & Incidents



	1995	1996	1997	1998	1999	2000	2001	2002	1Q-3Q 2003
Incidents	2,412	2,573	2,134	3,734	9,859	21,756	52,658	82,094	114,855
Vulnerabilities	171	345	311	262	417	1,090	2,437	4,129	2,982

CERT/CC Statistics 1995-2003 www.cert.org/stats/cert_stats.html

Attack Types



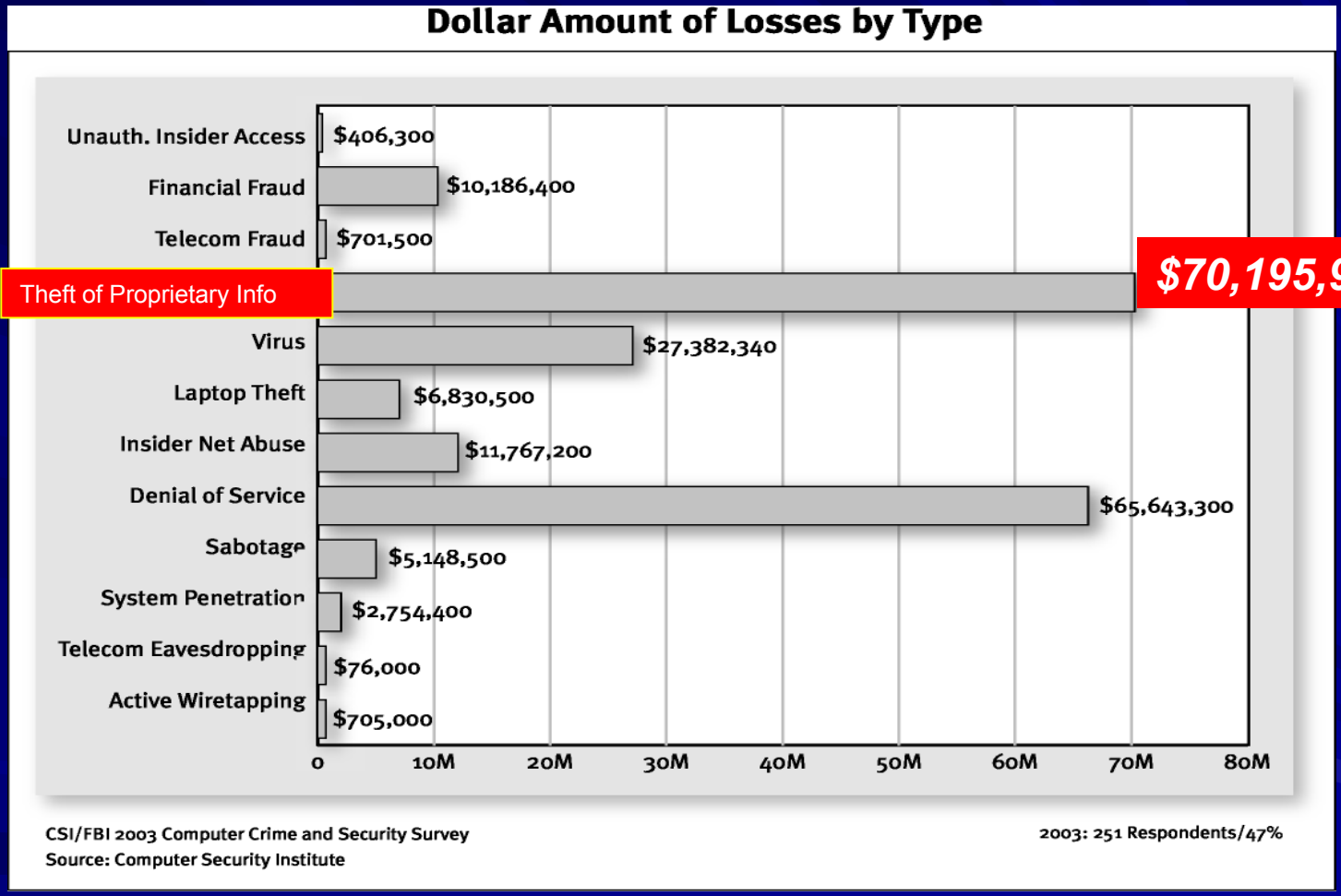
66 – Confidentiality (C)

50 – Integrity (I)

39 – Accessibility (A)

US Department of Justice, Computer Crime and Intellectual Property Section – from 76 cases profiled on the DoJ CCIPS web site, 1988 - 2004

Losses from Attacks



rondotech CONSULTING INC

Seminal Works in Security

- Department of Defense
  - First significant user of computers for sensitive work
  - First developed concept of securing computer systems
  - Long-term driver of high-security environments
- So how do they do it?

DoD System Classifications

- **DIVISION C: DISCRETIONARY PROTECTION**
  - Provides for discretionary (need-to-know) protection
  - Provides for *subjects' accountability and actions* through audit capabilities
- **DIVISION B: MANDATORY PROTECTION**
  - Preserves sensitivity label integrity, *uses labels to enforce mandatory access control rules*
  - Must carry the sensitivity labels with major data structures
  - Developer provides security policy model and furnishes a specification of the Trusted Computer Base
- **DIVISION A: VERIFIED PROTECTION**
  - Uses *formal security verification* methods to assure that mandatory and discretionary security controls employed effectively protect classified / sensitive information in the system
  - Requires extensive documentation to demonstrate that the TCB *meets security requirements in all aspects of design, development and implementation*

DoD Security Criteria – Division B

Medium Security Environment

- Security Policy
  - Discretionary Access Control
  - Object Reuse
  - Labels
    - Label Integrity
    - Exportation of Labeled Information
    - Subject Sensitivity Labels
    - Device Labels
    - Mandatory Access Control
- Accountability
  - Identification and Authentication
  - Audit
- Assurance
  - Operational Assurance
    - System Architecture
    - System Integrity
    - Covert Channel Analysis
    - Trusted Facility Management
    - Trusted Recovery
  - Life-Cycle Assurance
    - Security Testing
    - Design Specification and Verification
    - Configuration Management
- Documentation
  - Security Features User's Guide
  - Trusted Facility Manual
  - Test Documentation
  - Design Documentation

rondotech CONSULTING INC

Quality

- Software Development focus
- Definition
  - System complies with requirements
  - Design and implementation include handling abnormal input and situations

Benefits? Benefits!

- Documented
  - Repeatable, reliable, and maintainable processes reduce the cost of execution
  - Predictable processes provide transparency
- The earlier an exception is identified, the less it costs to bring it into compliance

rondotech CONSULTING INC

Quality Processes & Security

- NIST –
  - NIST SP800-26 IT Security Self-Assessments
  - NIST SP800-27 Engineering Principles for IT Security
  - Security included in development life cycle
    - NIST SP800-64 Security Concerns in Information SDLC
- **ASQ Docs**
  - EDP Audit / Quality Assurance Perspective for Preventing Security Exposure in a Large Scale Environment

rondotech CONSULTING INC

Core Questions Answered

- Can you have a secure system without it being a high quality system?

  NO!!

- Can you have true assurances of privacy without known level of security and quality?

  NO!!

rondotech CONSULTING INC

Tie It All Up

- Impossible to guarantee privacy and security in the real world
- Penalties for private information getting out has increased and will continue to increase
- Higher quality, better engineered, more reliable systems reduce a firm's vulnerabilities

Thank You!

Gregory A. Rondot

greg@rondotech.com
www.rondotech.com

703-830-4800

rondotech CONSULTING INC

Resources

- Gramm Leach Bliley Act - http://www.ftc.gov/privacy/glbact/
  - http://www.senate.gov/~banking/conf/
- HIPPA - http://www.hhs.gov/ocr/hipaa/
- US Congress Hearing on Consumer Privacy Opinions- www.house.gov
- California Office of Privacy Protection – www.privacy.ca.gov
- Computer Security Institute – www.gocsi.org
- CSI/FBI Computer Crime and Security Survey - www.gocsi.com/awareness/fbi.jhtml;jsessionid=D0PQ5KYDQ51VQQSNDBGCKHY
- Carnegie Mellon Software Engineering Institute, CERT® Coordination Center - www.cert.org Statistics www.cert.org/stats/cert_stats.html
- National Cyber Security Response System - www.us-cert.gov
- Federal Computer Incident Response Center - www.fedcirc.gov
- Internet Security Alliance - www.isalliance.org
- Department of Justice, Computer Intrusion Cases - **www.usdoj.gov/criminal/cybercrime/cccases.html**
- Department of Defense Trusted Computer System Evaluation Criteria - www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html#HDR3.2.1.3.2.3

rondotech CONSULTING INC