Carnegie Mellon
Software Engineering Institute

CERT Coordination Center

Vulnerability Disclosure: Why It Matters To You

APRICOT 2005
Asia Pacific Regional Internet Conference on Operational Technologies

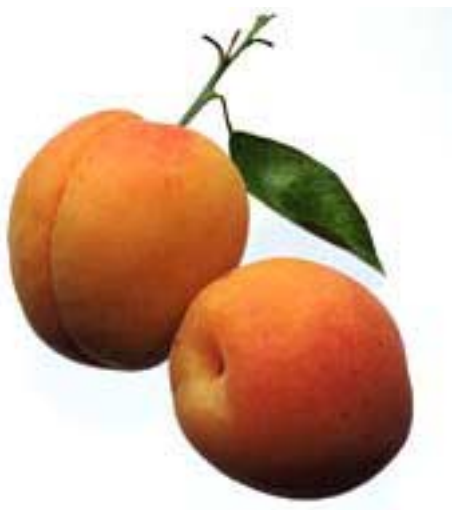
CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Overview

Stakeholders

Why Disclosure Process Matters

Future Challenges



Vulnerabilities Affect Everybody

Consumers

Businesses

Economies

Global critical infrastructure

Stakeholders

Researchers / Reporters

Vendors / Software developers / engineers
- OEMs / Integrators (staged disclosure)

Coordination bodies / CSIRTs

Government / Consumer
/ Public interest

Historical Record

Limited disclosure

Full disclosure

Responsible disclosure

All of the above

Why Disclosure Process Matters

Disclosure creates trust

Trust creates opportunity

Cooperative Disclosure Framework

Discovery ("I Know A Secret")

Validation

- **Expectation setting**
- **Credibility**

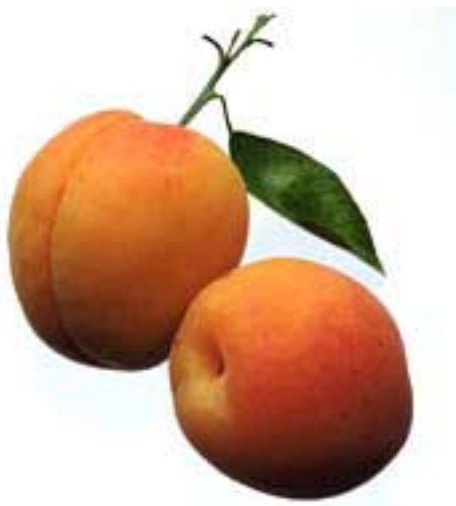
Communication

Remediation

Education

Tradeoffs (1)

Immediate Disclosure versus Coordinated Disclosure



Tradeoffs (2)

Full Disclosure versus Measured Disclosure

Future Challenges

Technology
- **Legacy (infrastructure, protocol, HTTP)**
- **Emerging (mobile, telecom, high-performance)**

Anti-Security
- **Economy of non-disclosure**
- **Philosophic differences**

Laws and Policy
- **DMCA, Anti-trust, etc**

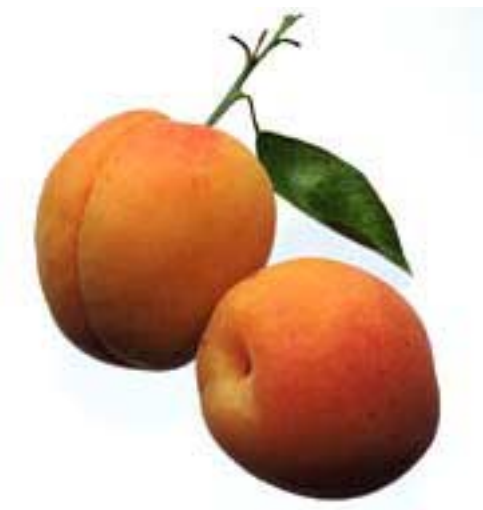
Mission Goals
- **When disclosing,**
  who needs to know?
- **Software assurance**

Further Reading (1)

CERT/CC Vulnerability Disclosure Policy, **CERT Coordination Center**
http://www.kb.cert.org/vuls/html/disclosure

Vulnerability Disclosure Framework, **U.S. National Infrastructure Advisory Council (NIAC)**
http://www.dhs.gov/interweb/assetlibrary/vdwgreport.pdf

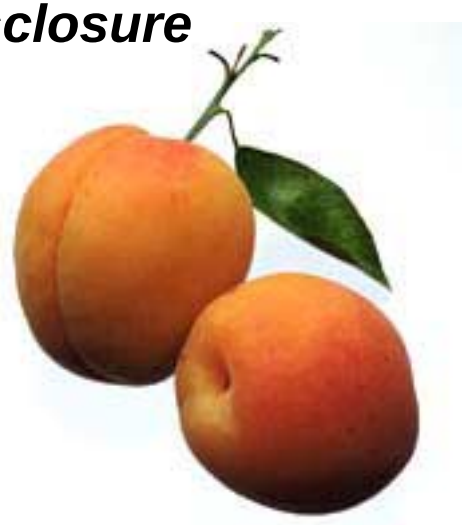
Vulnerability Disclosure Publications and Discussion Tracking,
University of OULU
http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/



Further Reading (2)

Economic Analysis of the Market for Software Vulnerability Disclosure
http://csdl.computer.org/comp/proceedings/hicss/2004/2056/07/205670180a.pdf

Optimal Policy for Software Vulnerability Disclosure
http://www.dtc.umn.edu/weis2004/xu.pdf



CERT®/CC Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA

Hotline: **+1 412 268 7090**

CERT/CC personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: **+1 412 268 6989**

Web: **http://www.cert.org**

Email: **cert@cert.org**