Towards Trustworthy Computing: Security Strategy
Scott Charney
Chief Trustworthy Computing Strategist
Microsoft Corporation
RIETI BBL
September 9, 2003
Our Long Term Commitment

Trustworthy Computing

Security

Privacy

Reliability

Business Integrity
Trustworthy Computing

**Security**
- Resilient to attack
- Protects confidentiality, integrity, and availability of data and systems

**Privacy**
- Individuals control personal data
- Products and Online Services adhere to fair information principles

**Reliability**
- Dependable
- Available when needed
- Performs at expected levels

**Business Integrity**
- Open and transparent interaction with customers
- Address issues with products and services
- Help customers find appropriate solutions
The Security Framework: SD³+C

Secure by Design
- Mandatory training
- Built threat models
- Conducted code reviews and penetration testing
- Used automated code tools
- Redesigned IIS 6.0 architecture

Secure by Default
- 60% less attack surface area by default compared to Windows NT 4.0 SP3
- 20+ services changed to be off by default
- Service install in a secure state (IIS 6.0 Lockdown)

Secure by Deployment
- New patch management tools
- 7 Microsoft Official Curriculum courses available at launch
- Official security configuration guides
- Integrated security tools

Communications
- Writing Secure Code 2.0
- White papers
- Configuration guides
- Consumer bulletins
- Training and education
Protection and Prevention Strategy

Windows Update

Fixes, patches, updates, etc.

Solutions

Government

Partners

Communities

Customers

Intern

Education

Recovery and Prevention

Problems, crashes, annoyances

Reporting 7x24

Microsoft

Investigations
TwC Commitment in Japan

- Trustworthy Computing is a global initiative and Japan is an integral part
- Commitment to work with partners
  - 40 STPP (Strategic Technology Protection Program) partners in Japan
  - Security partners (OEMs, TrendMicro, Symantec, etc)
  - Communities (MVPs, etc)
  - Universities (Shared Source, Curriculum)
  - Government (NPA, JPCERT/CC, IPA/ISEC, NIRT, Telecom-ISAC, etc)
The Future of TwC: Information Rights Management

- Digital intellectual property protection: To protect information from unauthorized access and reuse
- Information privacy, control, and integrity: To help prevent unauthorized actions such as forwarding, pasting, or printing confidential or sensitive information
- Product offerings: Windows Server 2003, Office 2003, IE, etc.
The Future of TwC: NGSCB

- NGSCB built on four key features:
  - Strong Process Isolation
  - Sealed Storage
  - Secure path to and from the user
  - Attestation (to authenticate officially)

- The first three are needed to protect against malicious code
- Attestation breaks new ground in distributed computing
  - “Things” (SW, machines, services) can be securely identified