Establishing End to End Trust
Creating a more trustworthy Internet

Scott Charney
Corporate Vice President, Trustworthy Computing
Microsoft Corporation
The Internet Revolution

Beneficial change

- Social: Enabling a global village
- Economic: Easier, faster, cheaper commerce
- Political: Freer exchange of ideas

Undesirable change

- Loss of data subject control over information
- Rise in identity theft
- Targeted attacks against businesses & governments
- Increases in other types of online and tech-facilitated crimes

Now required: End to End Trust

- Users must be empowered to make informed trust decisions (including accepting the risks of anonymity)
- Strong identity claims and reputation must be available to enhance security, privacy, and trust
- Better accountability must be created to deter crime and facilitate responses
Exponential Growth of IDs
Identity and access management challenging

Increasingly Sophisticated Malware
Anti-malware alone is not sufficient

Source: Microsoft Security Intelligence Report (January - June 2007)

Crime On The Rise

National Interest
Large segment by $ spent on defense
Largest area by $ lost

Personal Gain
Spy

Personal Fame
Thief

Curiosity
Trespasser

Fastest growing segment
Largest area by volume

Author

Largest segment by volume

Largest area by volume

Number of variants from over 7,000 malware families (1H07)

Pre-1980s 1980s 1990s 2000s

Num. of Digital IDs


Client/Server

Mainframe

Internet

mobility

Attacks Getting More Sophisticated
Traditional defenses are inadequate

Examples
- Spyware
- Rootkits
- Application attacks
- Phishing/Social engineering

User

GUI

Applications

Drivers

O/S

Hardware

Physical

Script-Kiddy

Amateur

Expert

Specialist

Exponential Growth of IDs

Internet


Client/Server

Mainframe

mobility

National Interest

Largest segment by $ spent on defense

Largest area by $ lost

Personal Gain

Spy

Thief

Personal Fame

Trespasser

Curiosity

Vandal

Author

Fastest growing segment

Largest area by volume

Source:

Microsoft Security Intelligence Report (January - June 2007)

Attacks Getting More Sophisticated

Traditional defenses are inadequate

Examples

Spyware

Rootkits

Application attacks

Phishing/Social engineering

User

GUI

Applications

Drivers

O/S

Hardware

Physical

Script-Kiddy

Amateur

Expert

Specialist
Microsoft's Commitment to TwC

Trustworthy Computing

Security
- Secure against attacks
- Protects confidentiality, integrity & availability of data & systems
- Manageable

Privacy
- Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles

Reliability
- Dependable, Available
- Predictable, consistent responsive service
- Maintainable
- Resilient, works despite changes
- Recoverable, easily restored
- Proven, ready

Business Practices
- Commitment to customer-centric Interoperability
- Recognized industry leader, world-class partner
- Open, transparent

Launched in January 2002
A Microsoft company-wide mandate
Security And Privacy Progress

SDL and SD3
- Security Development Lifecycle process
  - Engineered for security
  - Design threat modeling
- SD3:
  - Secure by Design
  - Secure by Default
  - Secure In Deployment
- Automated patching and update services

Defense in Depth
- Malware Example
  - Consumer Education
  - Laws
  - Firewalls
  - Antivirus Products
  - Antispyware Products
  - Malicious Software Removal Tool
  - Memory Management (ASLR)
  - Law Enforcement

Threat Mitigation
- Microsoft Security Response Center (MSRC)
- Microsoft Malware Protection Center (MMPC)
- Windows Live OneCare and Forefront Client Security, powered by the Microsoft Malware Protection Center
- SPAM (Sender ID, Phishing Filters)
- Network Access Protection (NAP/NAC)
Building a Trusted Stack

Core Security Components

Identity Claims
Authentication
Authorization
Access Control Mechanisms
Audit

“I+4A”

Secure Foundation

Integrated Protection

SDL and SD3
Defense in Depth
Threat Mitigation
Benefits

- Reduce types and severity of threats (e.g., de-value PII and reduce ID Theft)
- Create accountability for online crime
- Enable greater, safer personal Internet usage
- Enter new markets, expand Internet presence, and collaborate with partners and customers while reducing costs and risks
- Improve public safety and national security efforts, including disaster response (e.g., priority routing)
Building Alignment

- Successful end-to-end trust needs solutions aligned with
  - Societal values
  - Market forces
  - Regulatory environment

- These ideas, raised by many before, have not been implemented, in part because of misalignment

- We must come together to change the status quo, and find ways to address international barriers to implementation
End To End Trust

Economic Forces

Political/Legislative

Core Security Components

Identity Claims
Authentication
Authorization
Access Control Mechanisms
Audit

“1+4A”

Trusted Stack

Trusted Data
Trusted People
Trusted Software
Trusted Hardware

Integrated Protection

SDL and SD3
Defense in Depth
Threat Mitigation

Social Requirements
We need a broad dialogue on

- Technology Innovations
- Economic Forces
- Political Standards
- Social Change

www.microsoft.com/endtoendtrust