Information Privacy Protection – The Role of Technology

Purpose: Information
Submitted by: Microsoft
Information Privacy Protection
The Role of Technology

Meng-Chow Kang, CISSP, CISA
Chief Security & Privacy Advisor
Asia Pacific Region, Microsoft

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce
February 20-22, 2006
Horison Hotel, Hanoi, Vietnam
Privacy Invading Technology

- There are often legitimate needs for identifying, tracking, and monitoring capabilities, e.g., safety, security audit, automation, management, which can be misused or abused
- PIT is becoming pervasive
  - Exploiting technology capability
    - "Knowledge is Power"
    - Financial opportunities
  - Exploiting vulnerabilities
    - Financial gains
  - Business/individuals laxes
    - Ignorance or over-enthusiasm (CRM, safety/security concerns)
    - Simply bad practices
- Many forms of PIT
  - User devices (installed software, active contents, browser extensions, toolbars)
  - On the Internet (Internet gateways, email servers, proxies, web sites)
- Some recent cases:
  - Exploiting technology capability
    - "Knowledge is Power"
    - Financial opportunities
  - Exploiting vulnerabilities
    - Financial gains
  - Business/individuals laxes
    - Ignorance or over-enthusiasm (CRM, safety/security concerns)
    - Simply bad practices
- Many forms of PIT
  - User devices (installed software, active contents, browser extensions, toolbars)
  - On the Internet (Internet gateways, email servers, proxies, web sites)

Some recent cases:

- Tracked behavior across sites
- Stored personal information and sold it to various third parties
- RealJukebox unique identifier
- Info on every track ripped or played was returned to RealNetworks along with the ID
- Toolbar purports to enhance searching and purchasing experiences
- Tracks sites, full URLs, IP addresses, emails, search results, products explored
Welcome to ReadNotify.com!

ReadNotify lets you know when email you’ve sent gets read.

Length of Reading
Find out how long they read your email for.

Member Sign-in

email:

password:

Sign-in

Sign up now - Free!

Your existing email address:

GO!

Start here! New: Get the optional Plugin

home

about ReadNotify

business solutions

member utilities

Done

Internet
About ReadNotify.com

What is ReadNotify?

ReadNotify is the most powerful and reliable email tracking service that exists today. In short - ReadNotify tells you when email you sent gets read / re-opened / forwarded and so much more!

How does ReadNotify work?

Sending tracked emails via ReadNotify is incredibly easy: simply add .readnotify.com to the end of your recipients email address (they won’t see this) - or install one of our Active Tracker plug-ins to add the tracking for you. The email is then directed to pass through our server, where we assign it a tracking code, “strip off” the .readnotify.com part and send it on to your recipient. When your recipient opens the email, the assigned tracking code sends our server a message, which allows us to report the details to you.

ReadNotify.com does not use any kind of spyware, nor do we install anything onto your recipients computer in order to track emails.

Can you read my emails?

No. We do not cache or copy the body of your emails. The only time that emails are stored on our server is to enable our ‘ensured’ or ‘self-destructing’ features. (Although once an ensured or self-destructing email expires, no record of it is retained by us)

Is my email address safe with you - will I get spammed?

Your email address is completely safe with us - we never send, allow or support ‘spam’ or unsolicited email of any kind - nor do we publish anything on lists.

How can I contact you?

If you cannot find answers to your queries in our FAQ’s, please email the appropriate department:

- accounts@readnotify.com - for anything relating to accounts and payments
- pr@readnotify.com - for affiliate, reseller or publicity-related assistance
Deceptive Software - Spyware

Spyware and other Potentially Unwanted Software: Programs that perform certain functions without appropriate user consent and control

- Clearly malicious (worm, trojan)
  - Sasser

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innocuous</td>
<td>No potential harm</td>
<td>+ Notepad</td>
</tr>
<tr>
<td>Advertising</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Changes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Activity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exploit Data Analysis – Suspicious List (May~June 2005)

- Gathered 16,190 suspicious URLs through Web search and exploit neighborhood crawling
- Identified 288 of them as exploit URLs → 1.28%
- Expanded into 752 exploit URLs after auto-visit URL analysis → 263%

<table>
<thead>
<tr>
<th></th>
<th># Exploit URLs</th>
<th># Exploit Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>752</td>
<td>288</td>
</tr>
<tr>
<td>WinXP SP1-UP</td>
<td>688</td>
<td>268</td>
</tr>
<tr>
<td>WinXP SP2-UP</td>
<td>204</td>
<td>115</td>
</tr>
<tr>
<td>WinXP SP2-PP</td>
<td>17</td>
<td>10</td>
</tr>
<tr>
<td>WinXP SP2-FP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Evolving Landscape

Past
Broadcast attacks
- Networks worms
- Denial of Service

Present
Financially motivated attacks
- Phishing / Social Engineering
- Botnets
- Rootkits

Future
Specific target attacks
- Technically-oriented social engineering attacks
- Cross-device attacks

- Identity Theft
- Data Leakage/Theft
- DDoS Extortion
- Frauds
- Software Piracy
- Illegal Downloads
- Child Exploitations
- Others
### Recent losses of data

<table>
<thead>
<tr>
<th>When</th>
<th>What</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/15/2005</td>
<td>145,000 addresses and SSNs</td>
<td>Bought data posing as legitimate customers</td>
</tr>
<tr>
<td>2/25/2005</td>
<td>1,200,000 SSNs</td>
<td>Computer backup tapes were lost.</td>
</tr>
<tr>
<td>3/8/2005</td>
<td>1,400,000 credit and debit cards</td>
<td>Hackers stole data from a database from 108 stores</td>
</tr>
<tr>
<td>3/9/2005</td>
<td>310,000 SSNs and driver's licenses</td>
<td>Unauthorized use of customer logins</td>
</tr>
<tr>
<td>3/17/2005</td>
<td>120,000 addresses and SSNs</td>
<td>Intruder hacked into a school computer</td>
</tr>
<tr>
<td>4/14/2005</td>
<td>180,000 credit cards</td>
<td>Employees</td>
</tr>
<tr>
<td>4/19/2005</td>
<td>200,000 items</td>
<td>Backup computer tape was lost in shipping</td>
</tr>
<tr>
<td>5/2/2005</td>
<td>600,000 SSNs</td>
<td>Backup computer tape was lost in shipping</td>
</tr>
</tbody>
</table>

*When Security slacks, Privacy is at Risk*
Expanding threat boundary

- Mphasis Call Center (India)
  - Four bank accounts, defrauding up to US$300,000/- by three BPO’s employees
  - Implication extended beyond security and privacy of outsourcing providers
  - Cost and challenges of restoring trust (many entities)

When Privacy is risk, Trust is at stake
Privacy Is Only As Strong As The Weakest Link

- Technology is neither the whole problem nor the whole solution.
- Privacy enhanced systems depend upon Technology, Processes (including Policies) and People (including Organization).
Privacy enhancing technologies and features

- Privacy statement (short notices)
- Platform for Privacy Protection (P3P) integration
- Privacy settings and centralized management
- Ability to see what’s being transmitted
- Ability to clear tracks and stored information
- Documentation of privacy-related data
- Unsubscribe feature
- Access control
- Encryption

- Anonymizer - proxy
- Mix
  - Anonymous communications
  - Unlink, or remove correspondences between incoming and outgoing messages
  - Mix unrelated messages to remove linkages

... see [www.petworshop.org](http://www.petworshop.org) and [www.cfp.org](http://www.cfp.org)
Privacy enhancing technologies

- **History-clearing tools**
  
  [http://www.historykill.com](http://www.historykill.com)

- **Popup blockers**

- **Anti-spam, anti-phishing**

- **Anti-spyware**
  
  [www.spychecker.com/software/antispy.html](http://www.spychecker.com/software/antispy.html)
  
  [www.microsoft.com/antispyware](http://www.microsoft.com/antispyware)

- **Cookie managers**

- **Secure file deletion**
  
  `cipher.exe /w:directory`

- **Online privacy protection suites**
  
  [http://www.junkbusters.com](http://www.junkbusters.com)
  
# Microsoft PETs

| **BizTalk HIPPA Accelerator** | Permits BizTalk users to protect medical information included in transactions |
| **CryptoAPI** | Data encryption APIs in VisualStudio.NET |
| **EFS** | Protects confidential files at the operating system level |
| **Internet Explorer popup blocker** | Blocks ads and other privacy-invading devices on web sites |
| **RMS and IRM** | Protect and restrict documents (Office 2003) |
| **Internet Explorer** | P3P integration helps for managing cookies |
| **MS-CRM** | Email privacy settings |
| **MSN** | Parental controls; spam protection; email certification and sealing (beta); popup “pusher”; anti-spyware (MSN Premium); Sender-ID |
| **Outlook** | Anti-spam; support for IRM; Secure remote access |
| **Office hidden data removal tool** | Removes metadata from Word, Excel, and PowerPoint documents |
| **Windows Messenger** | Control visibility of state and who can send you messages |
Anti-Phishing in IE7

Privacy Statement

Viator Networks, Inc. has created this privacy statement in order to demonstrate our firm commitment to privacy. The following discloses our information gathering and dissemination practices for this website: Viator Networks Portals.

We use your IP address to help diagnose problems with our server, and to administer our Web site. Your IP address is used to help identify you and your shopping cart. We use cookies to deliver content specific to your interests and to save your password so you don't have to reenter it each time you visit our site.

Our site's registration form requires users to give us contact information (like their name and e-mail address). Users may opt-out of receiving future mailings. Please see the choice/opt-out section below.

This site contains links to other sites. Viator Networks, Inc., this hotel owners, management or employees are not responsible for the privacy practices or the content of such Web sites.
Key Trends in Digital Identity...

Number of Passwords Growing

<table>
<thead>
<tr>
<th>Company</th>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>eBay</td>
<td>john68739</td>
<td>football</td>
</tr>
<tr>
<td>MSDN</td>
<td><a href="mailto:john@home.com">john@home.com</a></td>
<td>gohawks</td>
</tr>
<tr>
<td>WSJ</td>
<td><a href="mailto:john@wsj.com">john@wsj.com</a></td>
<td>gohawks</td>
</tr>
<tr>
<td>My Bank</td>
<td>My Account #</td>
<td>Go#Hawks1</td>
</tr>
<tr>
<td>My Broker</td>
<td>My SS#</td>
<td></td>
</tr>
</tbody>
</table>

Mobile Identities On the Rise

New Threats Emerging

Is the Industry Finished Innovating?

Applications Increasingly Connected
Lessons from Passport & others

- Passport designed to solve two problems
  - Identity provider for MSN
    - 250M+ users, 1 billion logons per day
  - Identity provider for the Internet
    - Unsuccessful
- Identity efforts succeed and fail for reasons both technological and sociological
- Solution must move beyond single technology and single provider
- Solution must withstand the tests of a set of fundamental principles or propositions, i.e., the Laws of Identity.
The Laws of Identity

Established Through Industry Dialogue

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity (public versus private identity)
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Join the discussion at www.identityblog.com

Identity Metasystem whitepaper -
Individual control of personal data
Products, online services adhere to fair information principles
Protects right to be left alone

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

Engineering Excellence
Dependable, performs at expected levels
Available when needed

Open, transparent interaction with customers
Address issues with products and services
Help customers find appropriate solutions

Security
Privacy
Reliability
Business Integrity
Support the Trust Ecosystem through accountable identities

Engineering for Security
Embrace secure coding practices incorporating TwC D3+C

Fundamentally Secure Platforms
Develop products, services, and platforms using standards and best practices

Drive for Simplicity
Customer Trust

Privacy
"Know me & respect my choices"

Confidence
"Give me products that works"

Security
"Protect me from intrusion and loss"

Satisfaction
Loyalty
Leadership

IT
Network
Products

Help realize the potential of Technology

Products
Services
Brand
Microsoft’s Approach to Privacy

- Customers make choices and set preference
- Clearly defined guidelines on information collection and use
- Global Policy meets & exceeds high legal requirements
- Protecting information
- Provide customers experience they expect

Putting Customers in Control of their Information
Privacy Framework

Privacy in Design
- Put users in charge of their information
- Address needs of enterprises and parents
- Comply with corporate policies

Privacy by Default
- Collect only data that is required
- Get appropriate consent
- Protect the storage and transfer of data

Privacy in Deployment
- Privacy deployment guidelines for users
- Offer comprehensive privacy options
- Privacy response team for all products

Communications
- Analyst reviews and white papers
- Content on MS.com, MSN.com privacy sites
- Participation in privacy & tech conferences