

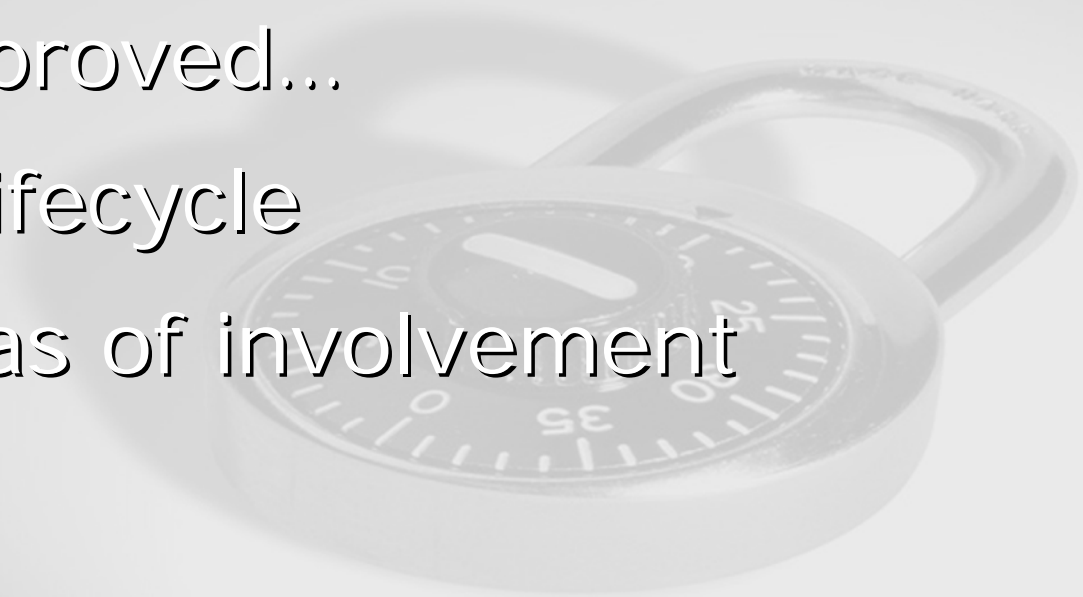
# A look inside Microsoft Security

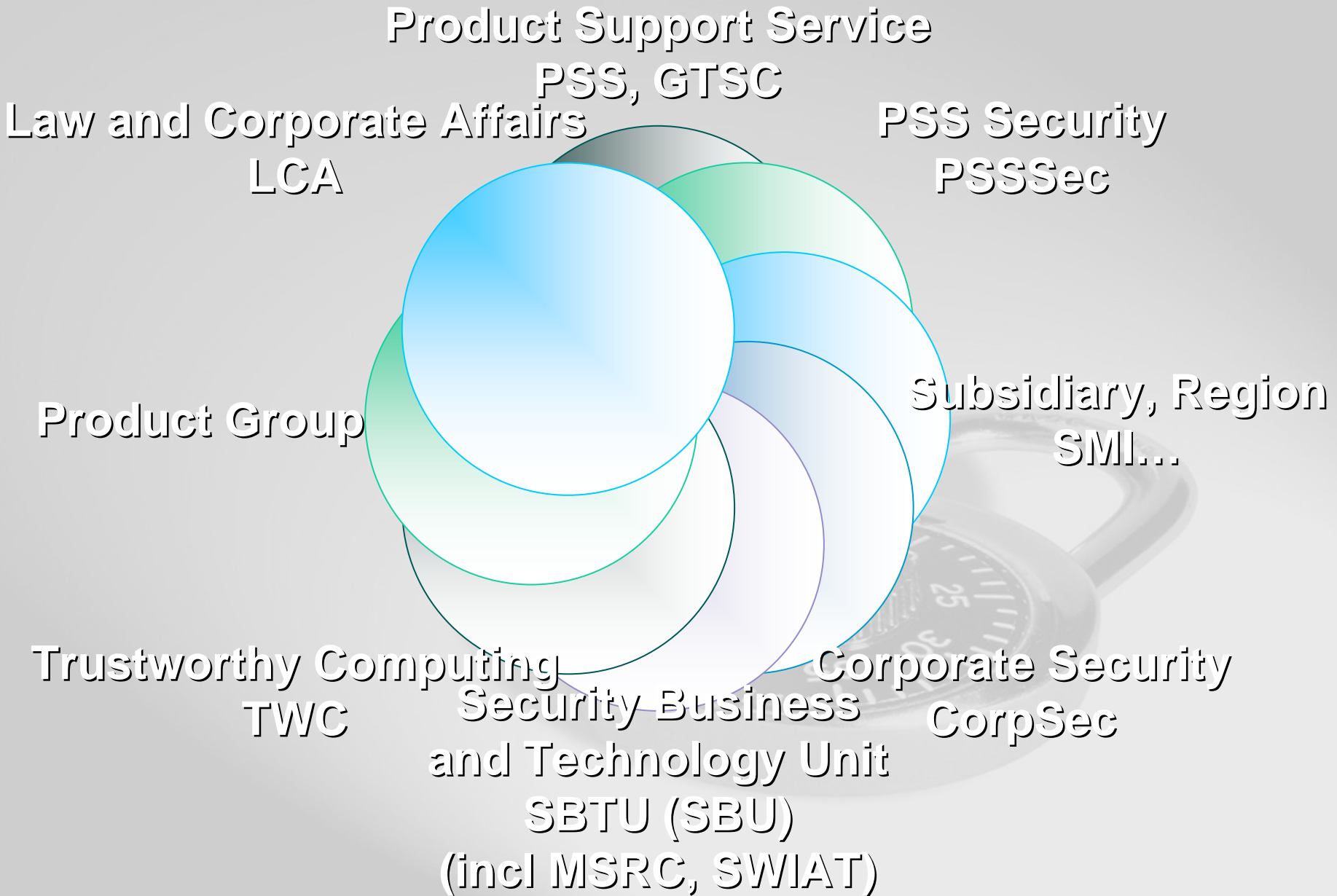


Simon Conant MCSE CISSP  
Security Program Manager  
Microsoft Corporation  
[sconant@microsoft.com](mailto:sconant@microsoft.com)

# Overview

- Who's who
- Lifecycle of a vulnerability
- New & improved...
- Support Lifecycle
- Other areas of involvement





# Who you need to know

- Security Business and Technology Unit (SBTU)
    - Microsoft Security Response Center (MSRC)
      - Handle all vulnerability reports ([secure@microsoft.com](mailto:secure@microsoft.com))
      - Co-ordinate vulnerability response
      - Publish security updates
  - Product Support (PSS)
    - PSS Security (PSSSec)
    - Global Technical Support Centre (GTSC)
      - Handle “real world” part of MS Security
      - Customer interface & support
- 

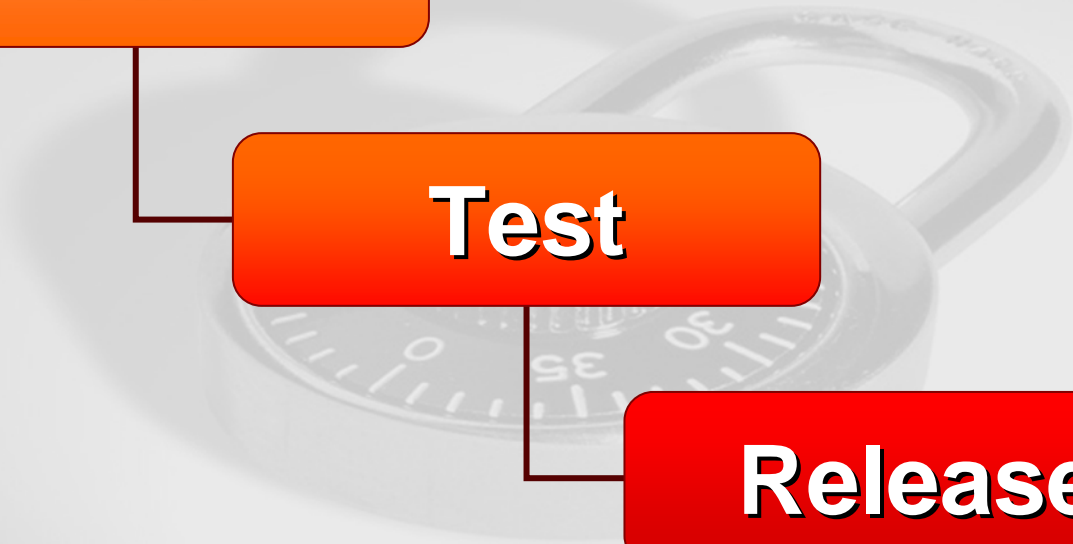
# Lifecycle of a vulnerability

**Investigate**

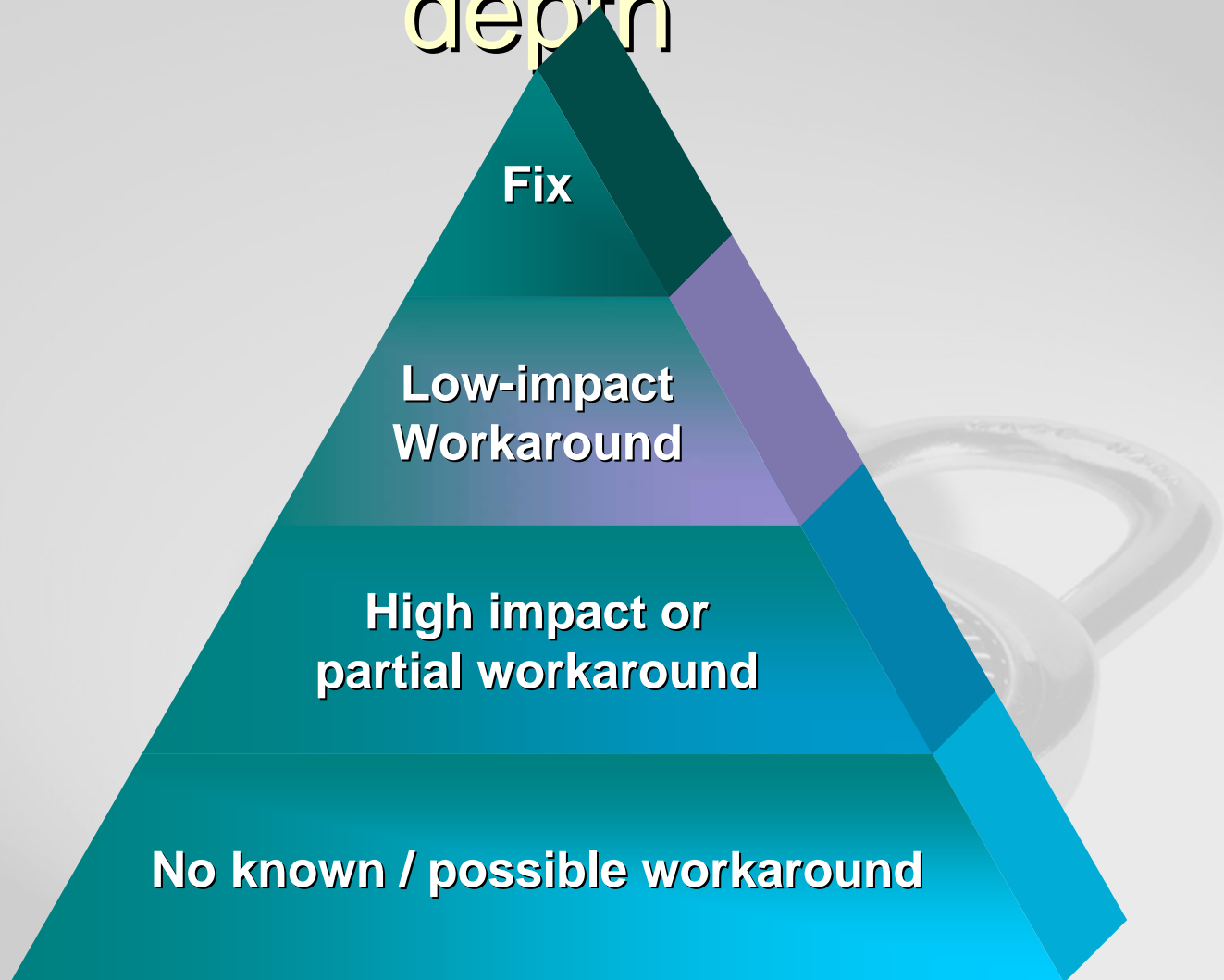
**Fix**

**Test**

**Release**



# Workarounds & Defence-in-depth



# New & improved...

- Public Vulnerability Program
  - Monthly Releases
    - Heads-up
    - Emergency releases
  - Released Software Updates Community
  - Local Security Support
  - XP SP2
  - Patch Improvements
- 

# Patch Improvements

- Speed of release vs. adoption & deployment
- Reduce Complexity
  - Number of installers, consistency in interface
- Reduce reboots
  - Developer
  - "Hot patching"
- Uninstall
- Increased internal testing, RSUC
- Reduce size of patches – Delta compression
- Deployment
  - SUS, SMS, MS Update



# Guidance

- Training, whitepapers, guides
  - <http://www.microsoft.com/practices>
  - <http://www.microsoft.com/technet/security>
  - <http://www.microsoft.com/security>
  - <http://www.microsoft.com/protect>
- How Microsoft secures Microsoft
- Deployment guidance
- Wireless security
- In-depth anti-virus
- Windows XP Security Guide V2.0...



# Support Lifecycle

- Also “New and improved”:
  - <http://www.microsoft.com/lifecycle>
- Limitations:
  - Supporting Service Packs
  - Supporting older versions



# Minimum Guarantees

10 Years is the minimum length of the product support lifecycle

- Policy:
  - Microsoft will provide Mainstream Support for the current release ('N') for the greater of:
    - 5 Years
    - 2 years after the N+1 release ships
  - Microsoft will provide Extended Support for the current release for the greater of:
    - 5 Years
    - 2 years after the N+2 release ships
- Customer Benefit:
  - Improves the predictability of our support offerings by reducing exceptions we need to make as schedules change
  - Ensures that Microsoft's support lifecycles match the way our customers want to manage their product upgrades
- Examples:
  - SQL 2000
    - Mainstream Support for Microsoft SQL 2000 will not end for 2 years after the next release (codenamed 'Yukon') ships
    - Given current ship dates, this will result in more than 5 years of Mainstream Support for SQL Server 2000

# Security Support Policy

★ New

Moving forward, Microsoft will provide security update support for a minimum of 10 years (through extended support phase)

- Security updates will be posted via the Microsoft Update\* site during the mainstream support phase, and the first two years of extended support.
- In the final three years of the extended support period, Microsoft will continue to post important & critical security fixes to the Microsoft Download Center site.
- Should a security vulnerability arise that, in Microsoft's judgment, could be exploited to build a worm or virus that could pose a significant threat to the Internet, Microsoft may post the fix to the Microsoft Update site.
- Older products – such as Windows NT 4.0 – were designed before some security threat models emerged. And, new vulnerabilities may emerge where it would be infeasible for Microsoft to provide fixes for these products. Therefore, to remain as secure as possible, Microsoft advises customers to remain as up-to-date as possible with product releases and service packs.

\* Only applies to products that post patches through an update site

# Service Pack Support

- Microsoft will provide 12 months support after the successor service pack ships.
- Support may be extended to 24 months for those service packs where Microsoft believes customers will need additional time for testing and deployment.
  - XP SP1 will receive 24 months support after XP SP2 releases
  - Windows 2000 SP3 support will now end June 30, 2005 (24 months after SP4 released).
- If support for a service pack is extended, Microsoft will announce that at the time the successor service pack is released

★ New

# Affect on some Key Products

## Windows NT4 (Server and workstation)

- NT4 will not snap to the new policy
  - Workstation support ends June 30, 2004
  - Server support ends Dec 31, 2004
- ★ **New** ▪ Customers with custom support agreements after those dates will receive **critical security updates** at no additional charge.

## Windows 2000 Server

- Mainstream ends March 31, 2005 (no change)
- Extended support now ends March 31, 2010

## SQL 2000

- Mainstream support will end 2 years after Yukon ships.
- ★ **New** ▪ Extended support will now end 5 years after mainstream ends.

## Office 2000

- ★ **New** ▪ Mainstream ends June 30, 2004 (no change)
- Extended support will now end June 30, 2009

# Affect on some Key Products

## Windows XP SP1

- ★ **New** Support will be extended to 24 months after XP SP2 releases

## IE 6 SP1

- ★ **New** Support will follow the lifecycle of the operating system it runs on.

## IE 5.5 SP2

- No change, support continues to follow the lifecycle of Windows Millennium Edition
- Support for IE 5.5 SP2 on all other operating systems ended Dec 31, 2003.

## Windows 98, 98SE and Millennium Edition

- Windows 98/98SE and Millennium Edition are in extended support and will not snap to the revised policy

## Windows Media Player

- Versions of media player that shipped with an operating system will follow the lifecycle of the operating system they shipped with.
- Those versions of media player that shipped outside of an operating system release will follow the already published end of support dates.

## Exchange 5.5

- No change as Exchange 5.5 is already in the extended phase


## SQL 6.5

- No change as support for SQL 6.5 has ended

# More Information on Windows NT4

- Windows NT 4.0 was designed at a time when many of today's security threat models were unknown.
  - That makes it difficult (and sometime impossible) for Microsoft to provide security patches for Windows NT 4.0 for new vulnerabilities.
- Microsoft is concerned that by extending the support period to 10 would imply (1) that there was not the level of urgency to upgrade that we previously had implied, and (2) that we now believe that Windows NT 4.0 is more secure-able than we did only a few months ago.
  - Neither of these is true, so we decided to leave our policy on Windows NT 4.0 unchanged.
- This approach has been endorsed by customers and leading industry analysts.
- Note: we do offer custom support options, for a fee, to customers that need support for a longer period of time.
- While it would be extremely unlikely, Microsoft may release a Windows NT4 security update publicly if we see a serious exploit in the wild targeting NT4 systems.

# Fix it before it breaks

- Security in development:
    - Fundamental
    - Design
    - Default
    - Check, check, check
    - Security as show-stopper
    - Root-cause analysis – learn from mistakes
- 

# Where else we're involved

- Supporting Security patches & tools
  - Virus – VIA, GIAIS
  - Crisis support
  - Privacy
  - Hacking and IR, Proactive support
  - Gov't & Law Enforcement Liaison
    - Spammers, virus authors, hackers, blackmailers
  - Press/PR/outreach/communications
- 

# How to get a hold of someone @ MS

- Via your existing MS contact / relationship
- If you can't get someone, or the right someone, or are dissatisfied:
  - [sconant@microsoft.com](mailto:sconant@microsoft.com)
  - +49-175-584 4290

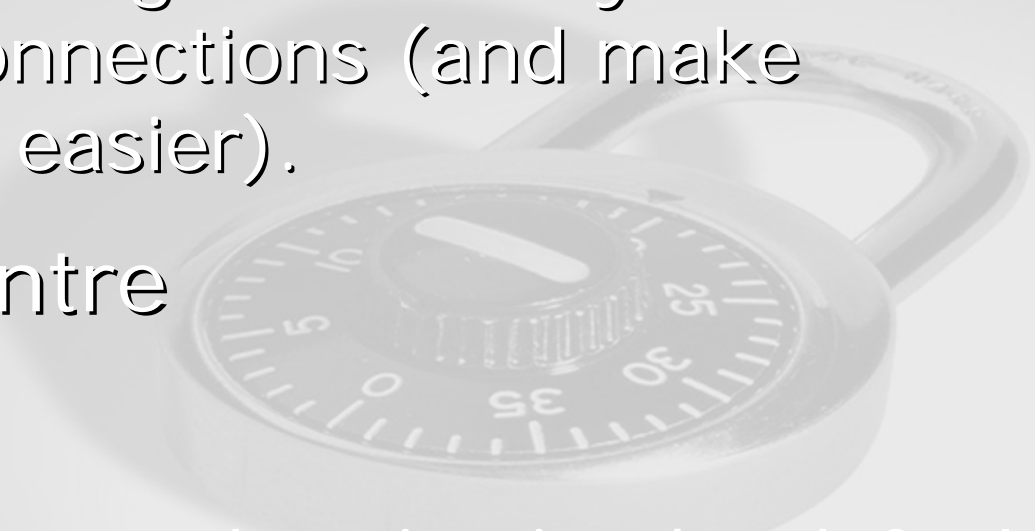
# Windows XP SP2



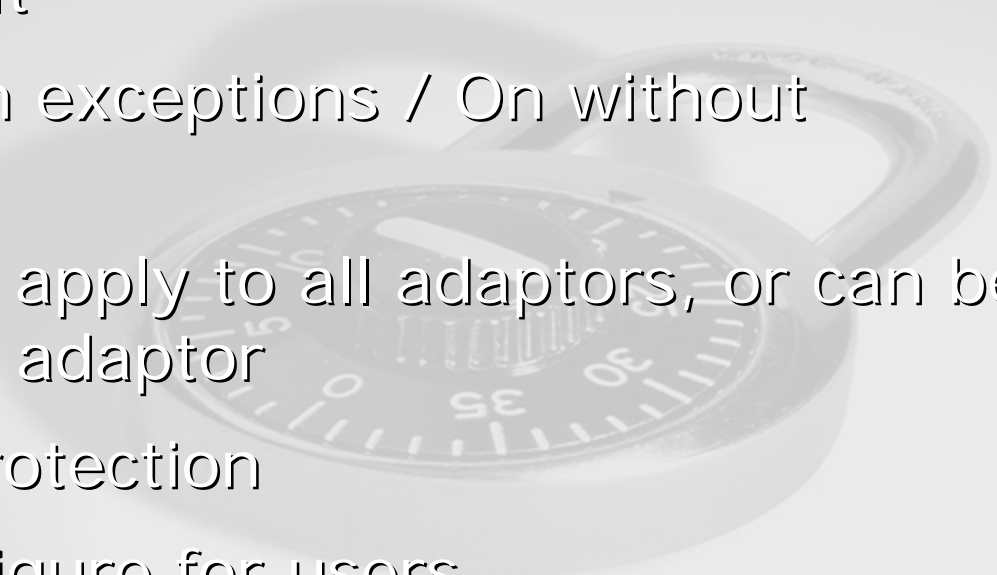
# What's special?

- Departure from usual Service Pack philosophy
    - Usually only patch roll-up, to encourage deployment
    - BillG instructions
  - Important patches
  - Important improvements
  - Broad public push
- 

# Changes – cosmetic to invisible

- Wireless configuration
    - Interface changed to clearly indicate insecure connections (and make connecting easier).
  - Security Centre
  - RPC
    - Now requires authentication by default.
- 

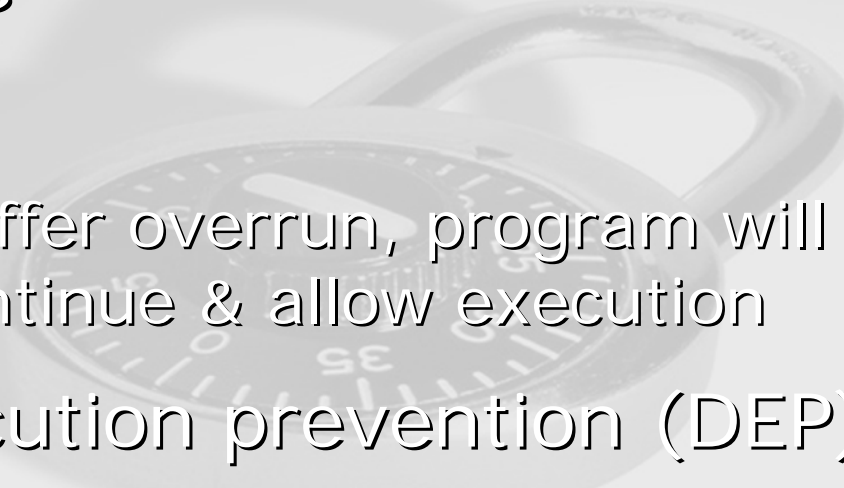
# Changes – trying to match security with usability – users, and admins

- Windows Firewall (formerly ICF)
    - On by default
    - Off / On with exceptions / On without exceptions
    - Settings can apply to all adaptors, or can be different per adaptor
    - Boot-time protection
    - Easy to configure for users
    - Easy to configure, and deploy configurations, for admins
- 

# Speaking of attack surface...

- Block unsolicited inbound – example UPnP
  - Dynamic Opening – example
    - Won't "listen" as 1900 & 2869 are not open by default, for unsolicited inbound traffic.
    - Dynamically opens ports when you use the (optional) UPnP user interface components
    - Need it? Add these to your exceptions list
    - Predefined exceptions, dynamic discovery, manual definition
- Services off by default – including:
  - Alerter
  - Messenger

# Protecting against classes of attack

- RPC, DCOM, WebDAV...
    - Reduce attack surface
  - Buffer overruns
    - /GS Switch
      - In case of a buffer overrun, program will crash rather than continue & allow execution
    - NX ("Data execution prevention (DEP)")
      - Mark memory pages as data – "No execute"
      - Hardware protection – but hardware prerequisite
- 

# User experience – mail & web

- Single API to handle attachments
    - Attachment Execution Service (AES)
    - Outlook, OL Express, Windows Messenger
    - Safe preview, default don't trust, open/execute in least possible privilege
    - Consistent user experience
  - IE – Popup blocker ☺ & UI restrictions
  - Zone lockdown improved (esp. local machine zone)
  - IE binary behaviours
  - Tighter control on scripting
  - Block cross-site, zone elevation attacks
  - Plain-text preview, reading, no HTML download...
- 