

Inspect a Gadget

Rafael Dominguez Vega

FIST Conference
26th October 2007
Barcelona

MWR InfoSecurity

Introduction

MWR InfoSecurity

A little about me…

- My name is Rafael Dominguez Vega and I am a Security Consultant with MWR InfoSecurity in the UK.
- I have approached this subject from the perspective of a security researcher and also as a penetration tester.
- I chose this subject for research based on my interest on new technology and its impact on information security.

MWR InfoSecurity

Intended Audience

This talk is aimed at the following people:

- Windows Vista Users
- Gadget developers
- Security Managers
- Penetration Testers

MWR InfoSecurity

What this talk will cover

- What Sidebar Gadgets are and just how flexible they can be
- The construction and distribution of Sidebar Gadgets
- Examples of Attacks
- Best Practice and Recommendations
- All the research has been conducted against Windows Vista Business Edition. However, it is expected that similar dependencies may be identified in other editions.

MWR InfoSecurity

Why research Vista Sidebar Gadgets?

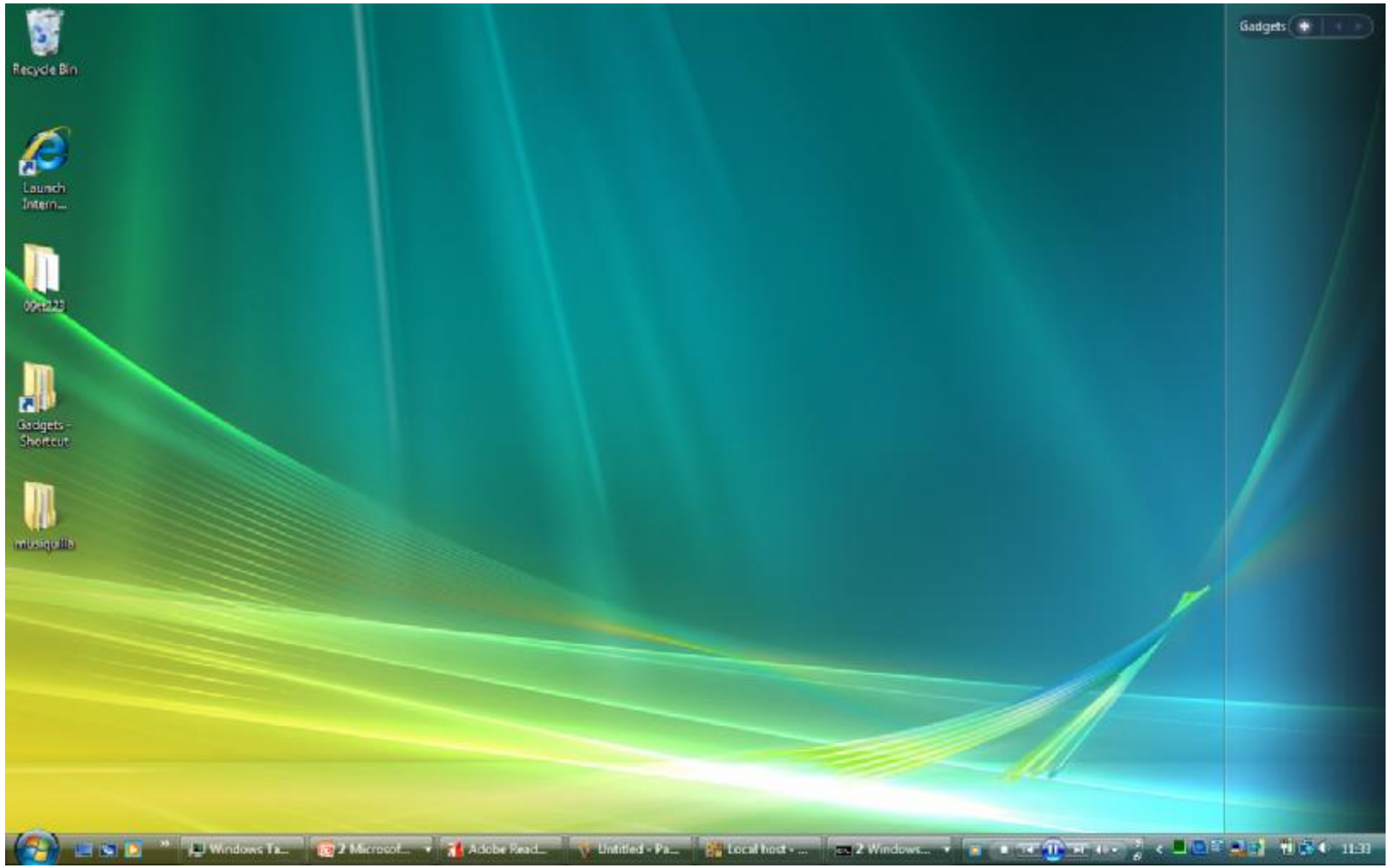
- New technology
- They are seen as "fun“ mini-applications and so there could be a more relaxed attitude to security
- They are intended to be developed by anyone, expected to be used by everyone and to be distributed in very large quantities

MWR InfoSecurity

Technical Background

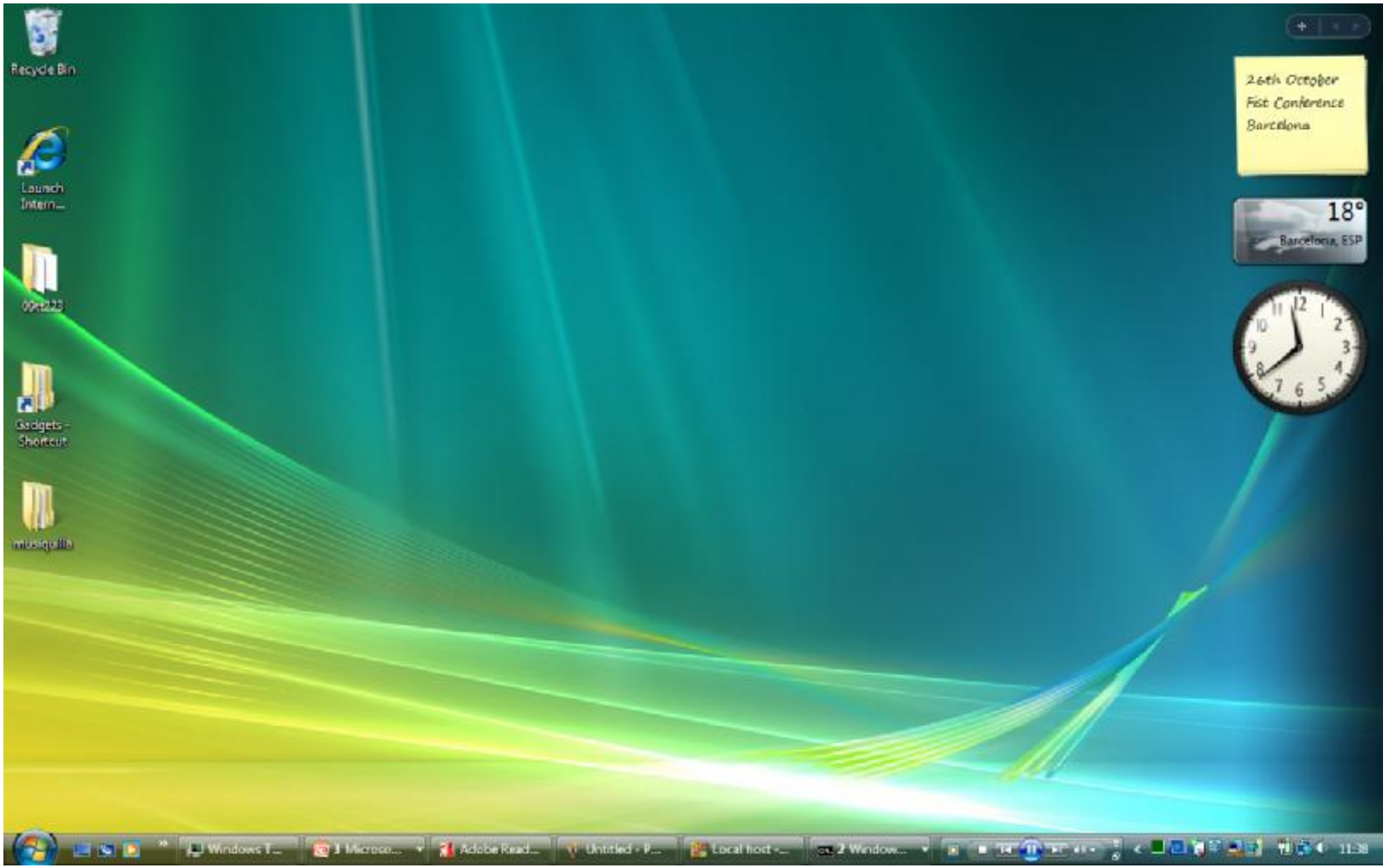
MWR InfoSecurity

What is the Sidebar?



MWR InfoSecurity

What is a Gadget?



MWR InfoSecurity

Characteristics of Sidebar Gadgets

- They are mini-applications
- They can include HTML pages, XML files, CSS, JavaScript or VBScript
- They have the ability to use Active X controls
- Gadgets' APIs
- They run within the context of the currently logged in user
- They cannot interact with the UAC

MWR InfoSecurity

Creating a Sidebar Gadget

A simple gadget consists of at least:

- An HTML file (e.g. Test.html)
  This is the body of the gadget
- An XML file (e.g. gadget.xml)
  The manifest – containing gadget information
- A Gadget folder (e.g. Test.gadget)
  This contains all the gadget's files

MWR InfoSecurity

The HTML File

```
<html>
  <style>
    body { width:125; height:35;}
  </style>

  <body>
      <b>This is your Gadget!</b>
  </body>
</html>
```

MWR InfoSecurity

The Manifest

```
<?xml version="1.0" encoding="utf-8" ?>
<gadget>
<name>Test Gadget</name>
<author name="AuthorName"></author>
<copyright>2007</copyright>
<description>Test Gadget</description>
<version>1.0</version>
<icons>
<icon>gadget_icon.jpeg</icon>
</icons>
<hosts>
<host name="sidebar">
<base type="HTML" apiVersion="1.0.0" src="Test.html" />
<permissions>full</permissions>
<platform minPlatformVersion="0.3" />
</host>
</hosts>
</gadget>
```

MWR InfoSecurity

The Manifest



MWR InfoSecurity

The Test Gadget installed in the Sidebar



MWR InfoSecurity

Distributing and Obtaining Gadgets

The most common distribution methods:

- Downloaded from the Internet
- Sent as an attachment by email

An attacker could take advantage of either of these methods to persuade users to install malicious gadgets.

MWR InfoSecurity

Gadget Packing

For distribution, Gadgets should be packed in the following manner:

- The file must be packaged as a ZIP or a CAB file
- The extension .zip or .cab must be changed to .gadget in order for the Sidebar to open the file when it is double clicked.

The gadget is now ready to be distributed to users who can then deploy it onto their systems by simply double clicking on it.

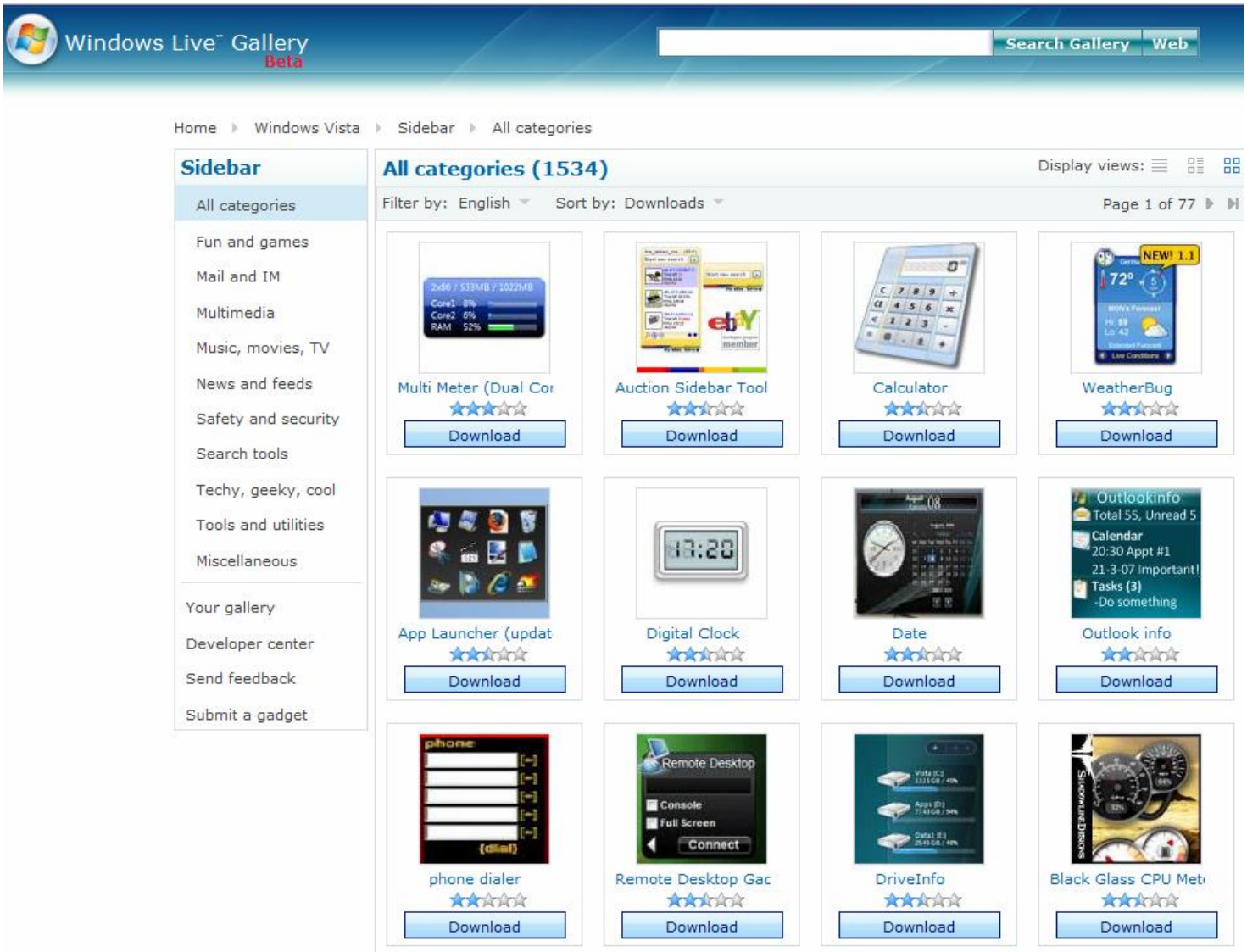
MWR InfoSecurity

Code-Signed Certificates

- Used to provide more information to the user about the source of the gadget before installation
- Code signing certificates are not mandatory
- They are costly to implement and therefore infrequently used
- Even sites such as gallery.live.com are at the present time distributing unsigned gadgets

MWR InfoSecurity

Pick a gadget, any gadget



MWR InfoSecurity

Code-Signed Gadget



MWR InfoSecurity

Unsigned Gadget



MWR InfoSecurity

Downloading Gadgets from a Web Server

Windows Vista implemented “Protected Mode” for IE7:

- Ensures that IE runs as a low integrity process in order to control its level of access
- Protects users from malware running on remote un-trusted web sites

These security measures are not applied to the Sidebar

MWR InfoSecurity

Example Attacks

MWR InfoSecurity

Example Attacks

- Man in the Middle – Script Injection
- Password Gathering
- Remote Command Line
- Denial of Service Attacks
- Persuading Users to Elevate Privileges with the UAC

MWR InfoSecurity

Attacks Characteristics

- Scope of these attacks would only be limited by the creativity of the person performing them
- Most of the attacks described today rely on a human element in order to succeed
- Man in the Middle attacks – gadgets can be vulnerable to script injection
- They do not constitute a compromise of the Windows® Vista™ security model

MWR InfoSecurity

Man in the Middle – Script Injection

MWR InfoSecurity

Man in the Middle – Script Injection

- Affects third party gadgets vulnerable to script injection
- A number of Microsoft gadget have also been reported to be vulnerable to script injection
- A large number of gadgets have already been written, both by amateurs and professional development companies
- Of the gadgets I have tested, roughly 60% are vulnerable to script injection attack
- Approximately 40% of the professionally developed gadgets tested so far are vulnerable
- I am currently coordinating with the vendors of a number of popular Vista gadgets which are vulnerable

MWR InfoSecurity

Man in the Middle – Script Injection

- This code will execute within the context of the currently logged in user
- Script injection could potentially allow remote attackers to execute commands on the target system
- For this attack to be successful, an attacker would need to be able to intercept and modify network traffic between the remote web server and the targeted user

MWR InfoSecurity

Man in the Middle – Script Injection

Example Attack

- A news gadget that provides users with the ability to view the latest news
- The news gadget requests information from a web server, which responds to the gadget with the latest news
- An attacker capable of intercepting the web server response, could modify that response such that a script was injected and then run on the user's system

MWR InfoSecurity

Password Gathering

MWR InfoSecurity

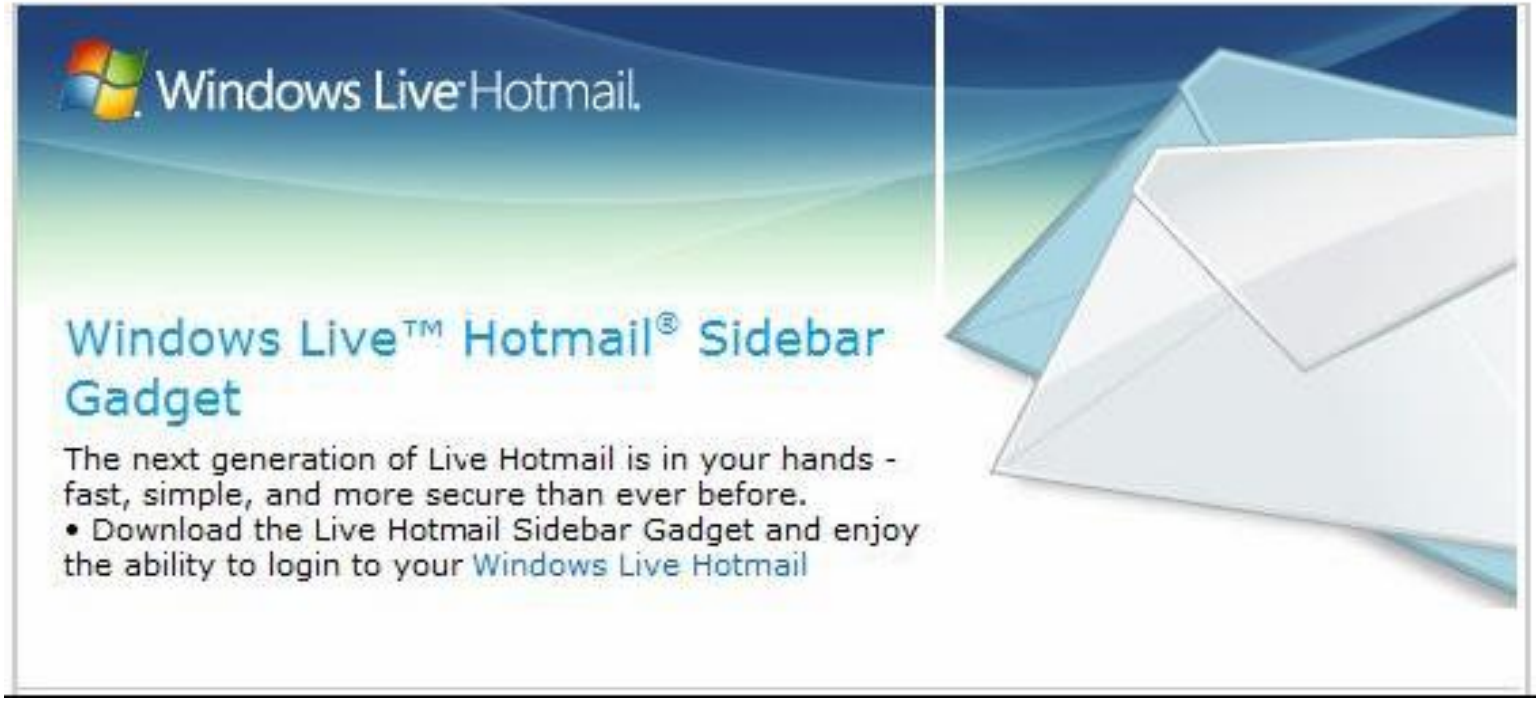
Password Gathering

- Users could be persuaded to provide sensitive information by a phishing attack
- A gadget would be constructed which impersonated a trusted entity
- In the following example, the Windows Live Hotmail service is impersonated

MWR InfoSecurity

Password Gathering - Email

From: [redacted]@live.com
To: [redacted]@hotmail.com
Date: Fri, 3 Aug 2007 07:04:18 +0000
Subject: Get the Windows Live Hotmail Sidebar Gadget



MWR InfoSecurity

Password Gathering – Gadget Running



MWR InfoSecurity

Remote Command Line

MWR InfoSecurity

Remote Command Line

- This attack could be exploited by an attacker to obtain a reverse shell
- The target user would have to be persuaded to download and run the malicious gadget
- The following example uses the FTP service and the Netcat tool

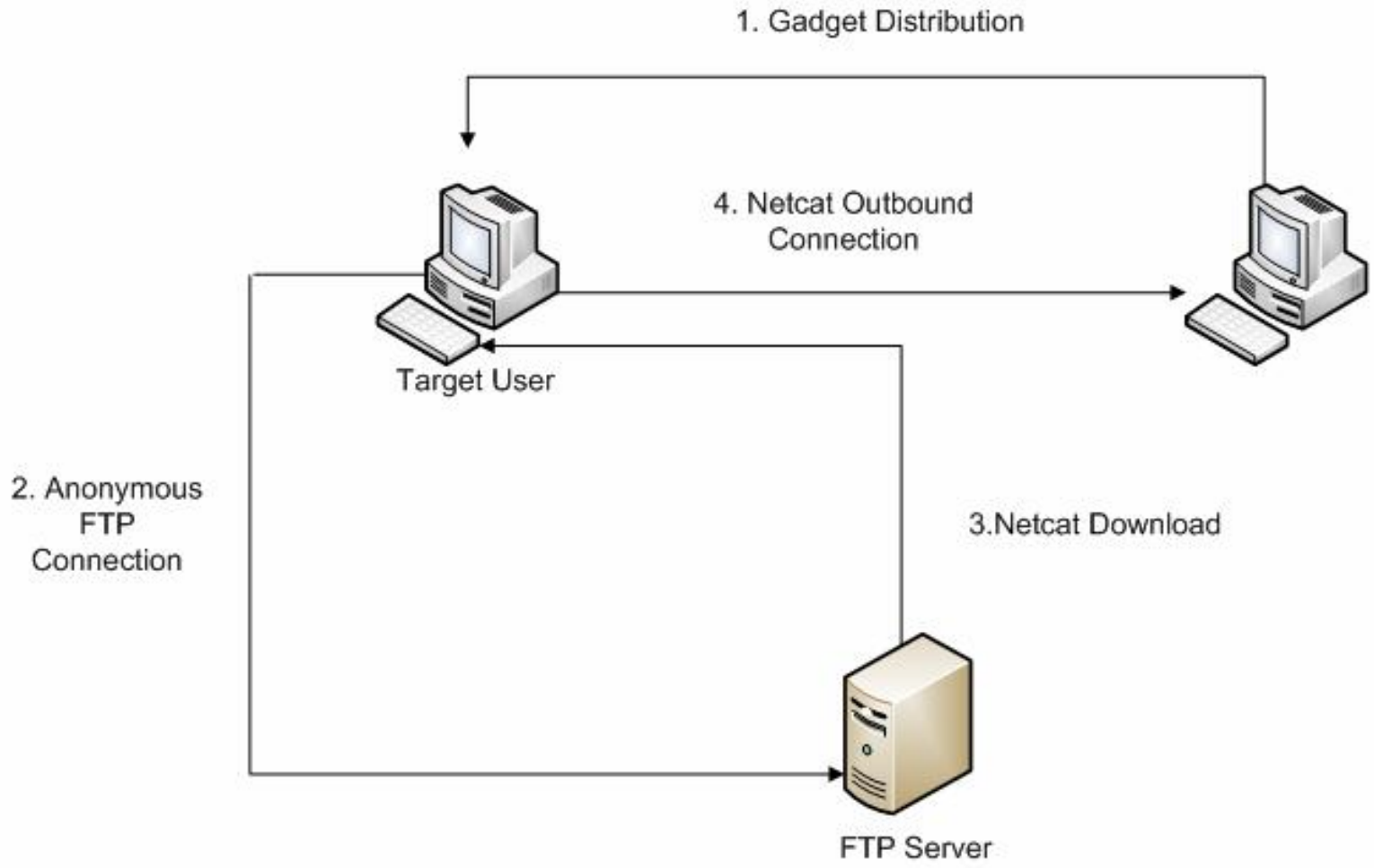
MWR InfoSecurity

Remote Command Line

- Distribute Gadget to target user
- Use FTP to download Netcat to the target system
- Run Netcat to open a cmd.exe socket connection to the attacker's system

MWR INFOSECURITY

Remote Command Line



MWR InfoSecurity

Remote Command Line

To be considered:

- Any malicious Gadget should be sufficiently attractive to persuade a large number of users to install it
- Restarting the computer will rerun a malicious Gadget
- This attack could be performed with no indication to the target user that it was running
- Opportunities for privilege escalation exist

MWR InfoSecurity

Denial of Service Attacks

MWR InfoSecurity

Denial of Service Attacks

- DoS attacks exploit vulnerabilities in order to affect the functionality of services and the reliable and timely access to data and resources either temporarily or indefinitely
- A malicious gadget could delete important files from the user's home directory, permanently removing this data
- Alternatively, it could perform a very simple task in an infinite loop (e.g. constantly sending the input keys "Left" and "Enter")

MWR InfoSecurity

Persuading Users to Elevate Privileges with the UAC

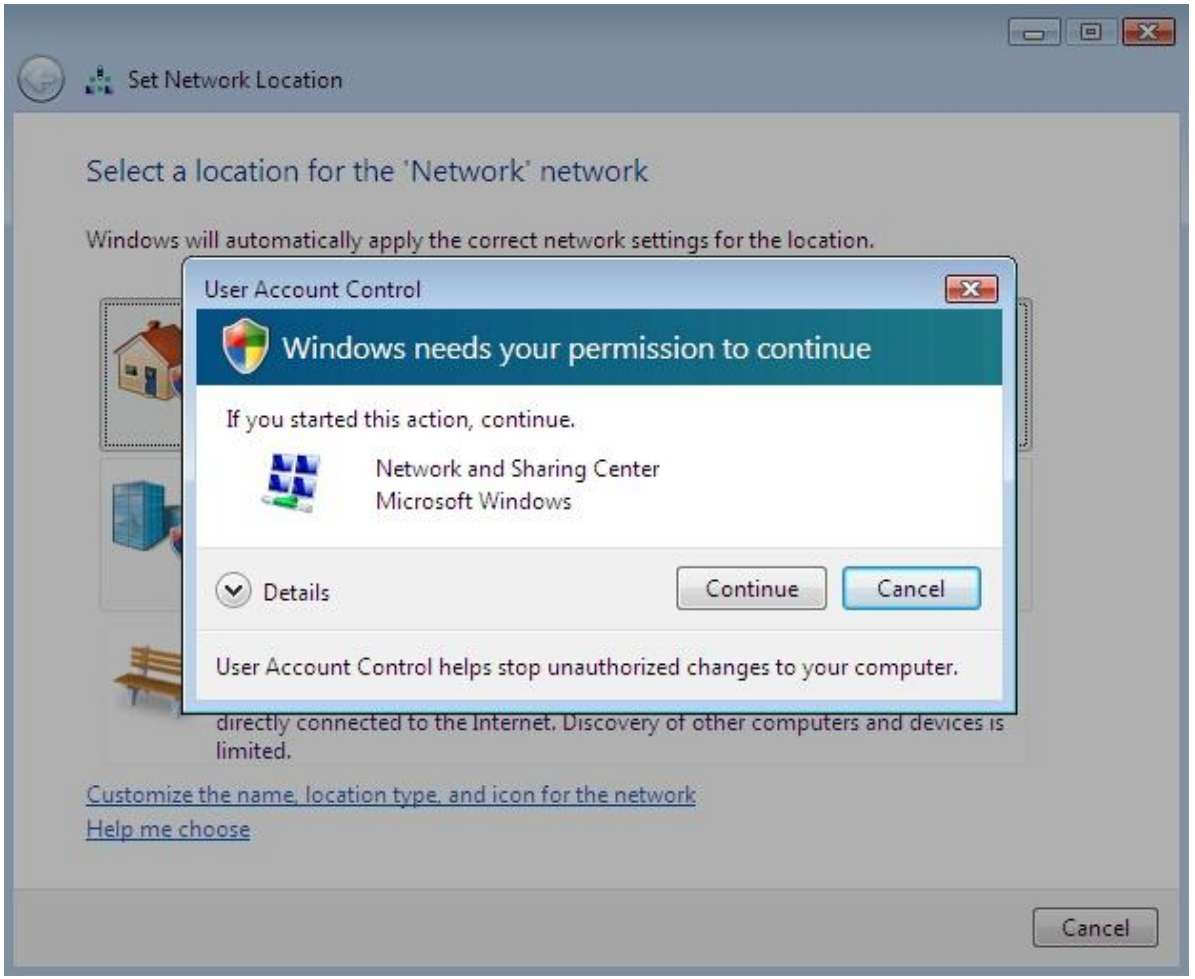
MWR InfoSecurity

Persuading Users to Elevate Privileges with the UAC

- User Account Control (UAC) is a new security measure implemented in Vista
- It is intended to prevent unauthorised changes to a user's system by asking for permission, or for an administrative password to be supplied, before a task is performed
- In this attack, immediately after the targeted user ran the malicious gadget they would be prompted with a UAC dialogue box asking for authorisation

MWR InfoSecurity

Persuading Users to Elevate Privileges with the UAC



MWR InfoSecurity

Best Practice and Recommendations

MWR InfoSecurity

Best Practice and Recommendations

Security Awareness

- Educate users as to the dangers of malicious gadgets
- Educate users not to visit un-trusted sites to download gadgets
- Educate users not to install gadgets however they are received, whether by email or otherwise
- Encourage the use of code-signed certificates

MWR InfoSecurity

Best Practice and Recommendations

Possible Sidebar Gadget Policies

- Only allow the unpacking and installation of code-signed gadgets
- Only allow gadgets located in the Gadget folder and/or in the Shared Gadget folder to be executed
- Modify the link “Get more gadgets online”
- Disable the Windows Sidebar

MWR InfoSecurity

Best Practice and Recommendations

High Level Recommendations

- Transmission channel encryption (certificates)
- Use multiple layers of defence: Firewall and Antivirus
- Secure gadget development
- Gadget source code should be software audited
- Gadgets should be securely tested before being implemented in any environment

MWR InfoSecurity

Conclusion

- The use of new technology should be assessed when it is implemented in any environment
- As the use of Gadgets accelerates security considerations need to be taken
- Sidebar gadgets provide a different opportunity to attack users via established techniques
- Gadgets should be subject to a risk assessment and securely tested before deployment

MWR InfoSecurity

References and Further Reading

Gadgets

http://msdn2.microsoft.com/en-us/library/aa163287.aspx

Gadgets for Windows Sidebar Security

http://msdn2.microsoft.com/en-us/library/bb508510.aspx

Scripting in Windows Vista - Creating Gadgets: Part 1

http://www.microsoft.com/technet/scriptcenter/topics/vista/gadgets-pt1.mspx

Microsoft Developer Network

http://msdn2.microsoft.com/

Inspect Your Gadget

http://msdn2.microsoft.com/en-us/library/bb498012.aspx

MWR InfoSecurity

References and Further Reading

Next Generation Malware – Tim Brown

The Inherent Insecurity of Widgets and Gadgets - Aviv Raff and Iftach Ian Amit

Books:

Windows Vista Security, Securing Vista Against Malicious Attacks.
by Roger A.Grimes and Jesper M. Johansson

MWR InfoSecurity White Paper

"Considerations for the Secure Rollout of Sidebar Gadgets on Windows Vista"
http://www.mwrinfosecurity.com/publications/mwri_sidebar-gadgets_2007-09-25.pdf

Contact Me

MWR InfoSecurity

Question and Answer Session