The future frontier of Hacking - UMTS mobile phone platform
Web intrusions: the best indicator of the vulnerable status of the Internet

Speaker: SyS64738 www.zone-h.org
this is to officially certify that your phone got 0wn3d!

ps: nothing was deleted but everything got stolen!
pps: I see you through the cam, so... smile!!!

The fluffy bunny has owned you.
Zone-H.org: the Internet thermometer?
attacks techniques and tools

By attack method:

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>known vulnerability (i.e. unpatched system)</td>
<td>31.3%</td>
</tr>
<tr>
<td>configuration / admin. mistake</td>
<td>24.2%</td>
</tr>
<tr>
<td>undisclosed (new) vulnerability</td>
<td>21.3%</td>
</tr>
<tr>
<td>brute force attack</td>
<td>16.2%</td>
</tr>
<tr>
<td>social engineering</td>
<td>4.7%</td>
</tr>
<tr>
<td>no method specified</td>
<td>0%</td>
</tr>
</tbody>
</table>

2003 top used vulnerabilities by attackers

- Webdav
- Frontpage extensions
- Openssl
- Samba
- Php nuke
Defacement reasons

- For fun
- Revenge
- Political
- Challenge
- Wannabe
- Patriotism
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related

Zone-H.org
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related

Zone-H.org
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related

Zone-H.org
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related
Zone-H.org
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related

Zone-H.org
CYBER-CRIMES ARE CONVENIENT BECAUSE:
• Lack of IT laws
• Lack of L.E. international cooperation
• ISPs are non-transparent

CYBER-PROTESTS ARE CONVENIENT BECAUSE:
• General lack of security
• No need to protest on streets
• No direct confrontation with L.E.

CYBER-CRIMES WILL NEVER STOP BECAUSE:
• Inherent slowness of the Institutions
• The Internet is getting more complicated
• Software producers are facing a market challenge
Traditional hacker’s limited world

Universal Mobile Telecommunication System

Our every day's life activities
UMTS vs Wi-Fi (P.A.P.) why not?

- 80,000,000,000 USD paid for UMTS licenses and tight development plans will force Telecoms to spread the UMTS service as fast as possible offering connectivity at a very convenient price.
The UMTS 3G platform

- Videoconference
- Full multi-media platform
- Data bank
- Office files
- Mobile computing
- Web browsing

NO LIMITS: they will do whatever a PC currently does as they will be powered by Windows, Linux and other commercial OSs.
The conceptual weaknesses in UMTS

- Weakly built operative system
- Memory stacked application and data

Win pocket PC running memory stack

Win pocket PC storing memory stack
How UMTS works

Wireless node

Radio network controller

ATM network

Mobile switching center

Visiting location register

Telephone network

Encrypted area

128bit Key

USIM

Zone-H.org
How UMTS works

Wireless node

Radio network controller

ATM network

Mobile switching center

Visiting location register

Encrypted area

Telephone network

USIM

128bit Key

128bit Key

Encrypted area


Zone-H.org
How crackers will exploit UMTS

• Using OS security flaws
• Through open ports
• Virus (mail, downloaded prgs)
• Trojan (mail, downloaded prgs)
• Using components flaws (media player browser, active sync etc.)
• Webserver flaws
• Exploiting application level
DIRECT DAMAGES

- Loss of precious information
- Denial of service (received)
- Denial of service (attack), $$$ loss
- Espionage (loss of documents)
- Eavesdropping (audio and video)
- Unauthorized online shopping
- Bank account unauthorized access
Installation

Setup for the SQL Server Dashboard must be run on a web server that database in which to store dashboard and Web Part definitions. Access or a local connection to an instance of SQL Server installed on the same will be prompted to specify the name of your SQL Server, database, and used to connect. If the database does not exist, Setup creates the database you create an account specifically for your SQL Server Digital Dashboard.

You should also check the system requirements before installing any of the SQL Server Digital Dashboard components.

Installation Components

Install the Microsoft SQL Server Digital Dashboard 3.0
Run the Setup program to install the Microsoft SQL Server Digital Dashboard 3.0.

Install the Microsoft Digital Dashboard Offline Replication Client
Run the Pocket PC Client Setup program to install the Microsoft SQL Server Offline Replication application.

Information about the Microsoft Office XP Developer SQL Update Patch
Read about the Microsoft Office XP Developer SQL Update Patch and follow a walkthrough to help you use the new features in your applications.

Zone-H.org
Welcome to the Windows CE Web Server Beta!

© 1999 Microsoft Corporation. All rights reserved.

Note that you must read the attached LEGAL information before using this software.

We are providing an Internet newsgroup at newsgroup microsoft.public.windowsce.beta.webserver to enable peer program. We will attempt to monitor this newsgroup for issues, but we cannot guarantee a response to each issue. It is the documentation, especially the sections concerning the license, the install process, etc. For bug reporting, there is http://windowsce.microsoft.com/buglog.asp, which can also be found from http://www.microsoft.com/windowsce/emb.

Windows CE Platform Builder, white papers and other tools.

Included in this version:

- HTTP/1.0 Support
- ISAPI Extensions
- ISAPI Filters
- Logging
- Extremely Configurable
- Basic Authentication (The final version will include NTLM Authentication as well.)
- ASP Support (for Jupiter devices only)

Here is a useful link that allows you to Administer the web server.

To see the complete description of features, see WebServe.doc.
### View and modify virtual paths

<table>
<thead>
<tr>
<th>Virtual Path</th>
<th>Physical Path</th>
<th>Authorization</th>
<th>Read Access</th>
<th>Execute Access</th>
<th>Script Access</th>
<th>Modify</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>/test</td>
<td>\</td>
<td>Public</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Modify</td>
<td>Delete</td>
</tr>
<tr>
<td>/Images</td>
<td>\Windows\www\wwwpub</td>
<td>Public</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Modify</td>
<td>Delete</td>
</tr>
<tr>
<td>/Dashboard</td>
<td>\Windows\MSOFFDD.c</td>
<td>Public</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Modify</td>
<td>Delete</td>
</tr>
<tr>
<td>/Admin</td>
<td>\windows\httpadm.dll</td>
<td>Public</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Modify</td>
<td>Delete</td>
</tr>
<tr>
<td>/</td>
<td>\windows\www\wwwpub</td>
<td>Public</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Modify</td>
<td>Delete</td>
</tr>
</tbody>
</table>

To save changes, click modify by the appropriate path. To make changes take effect, select Restart Web Server from the main page.

[Go to main page](http://www.zone-h.org).
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.2002</td>
<td>16:26</td>
<td>52736</td>
<td>Wireless Pack.exe</td>
</tr>
<tr>
<td>2.1.2002</td>
<td>16:26</td>
<td>38400</td>
<td>ProductInfo.dll</td>
</tr>
<tr>
<td>19.6.2003</td>
<td>17:58</td>
<td>306</td>
<td>WPPdata.dat</td>
</tr>
<tr>
<td>27.6.2002</td>
<td>12:17</td>
<td>0</td>
<td>CallHist.dat</td>
</tr>
<tr>
<td>27.6.2002</td>
<td>12:17</td>
<td>0</td>
<td>Outbox.dat</td>
</tr>
<tr>
<td>27.6.2002</td>
<td>12:17</td>
<td>0</td>
<td>Inbox.dat</td>
</tr>
</tbody>
</table>
Welcome to Pocket Internet Explorer
Tap below for useful sites and services!

PocketPC.com
HP
msn Mobile
AvantGo
Zone - H.org
Hello

This is a reminder that all materials for the DefCon 11 conference CD are due on July 15, 6PM, PST.

No exceptions. Materials that can be included on the CD are: presentations (.sxi versions must be accompanied by .ppt versions), white papers, tools, movies, demos, music, bibliographies, references, etc.

DON'T HOLD BACK. Also, please .zip or .sit all the content and send forth with dc-11-yourname Thanks in advance. -- The BlackBeetle "Playing with chopsticks will cause you splinters."

Zone-H.org
The default installation of Windows Beta Webserver allows an attacker to gain full remote access without authentication simply by logging to http://attacked_host/admin.
Privacy threat

- Cyber-stalking (GPS)
- Cyber-stalking (last node ID)
- Direct targeting. The wideband nature of the UTRA/FDD facilitates the high resolution in position location. The duration of one chip (3.84Mcps) correspond to approximately 78 meters in propagation distance. If the delay estimation operates on the accuracy of samples/chip then the achievable maximum accuracy is approximately 20 meters.
What a UMTS hacker should study: links

- [http://www.3gpp.org/specs/titles-numbers.htm](http://www.3gpp.org/specs/titles-numbers.htm) (all 3G specs and current releases)
Home automation

UMTS WORLD

H.A.S. WORLD (EIBA, X10)
The fridge’s built-in PC is a low-spec affair based on a 300MHz National Semiconductor Geode processor, 128MB of RAM and a 17GB hard disk.
The Internet refrigerator

The fridge’s built-in PC is a low-spec affair based on a 300MHz National Semiconductor Geode processor, 128MB of RAM and a 17GB hard disk.

It runs a modified version of Windows 98
The Internet refrigerator

The fridge’s built-in PC is a low-spec affair based on a 300MHz National Semiconductor Geode processor, 128MB of RAM and a 17GB hard disk.

It runs a modified version of Windows 98
The Internet oven

HONEY, OUR THANKSGIVING TURKEY HAS BEEN BURNED BY A PAKISTANI CYBERFIGHTER IN RETALIATION OF THE KASHMIR TERRITORY OCCUPATION ...
Are we now scared about the implementation of these new technologies?

What system will be invented to let us feel secure and keep our privacy safe?

Is there anyone who can help me to get rid of these techno-nightmares?

Zone-H.org