

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



Zone-H.org

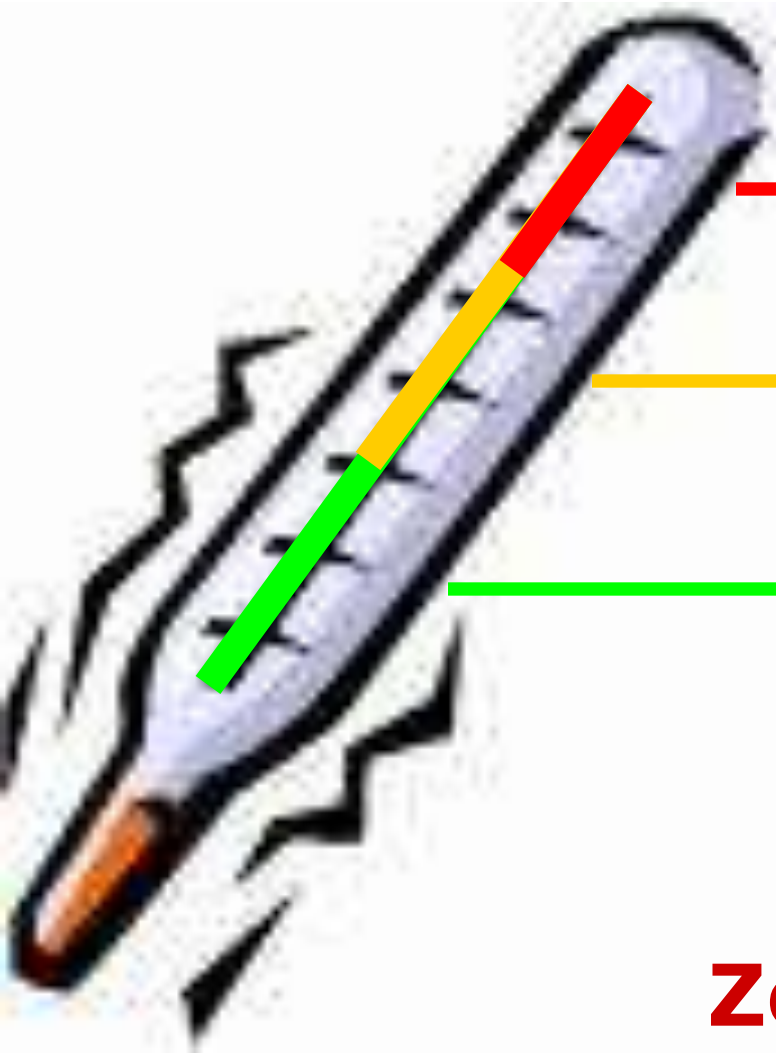


the fluffy bunny has owned you



this is to officially certify
that your
phone got 0wn3d !
ps: nothing was
deleted but everything
got stolen!
pps: I seeya through the
cam, so... smile!!!

Zone-H.org: the Internet thermometer?



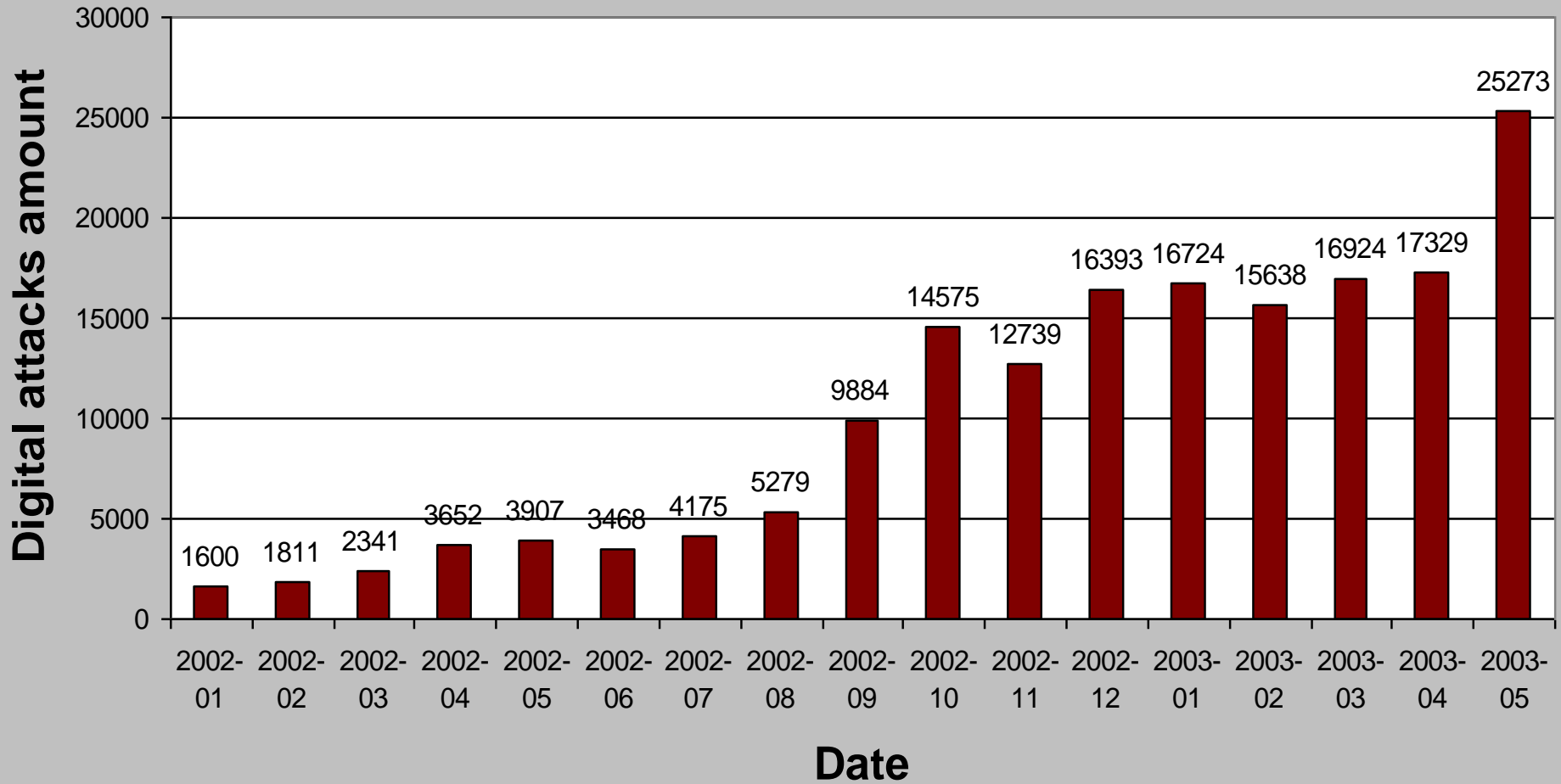
F#CKABLE

HACKABLE

SECURE

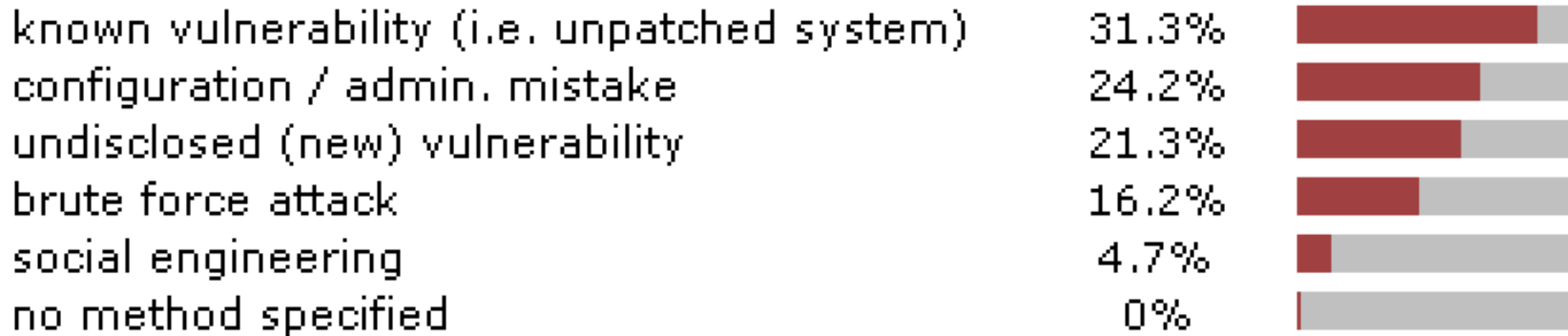
Zone-H.org

Digital attacks amount since 2002



attacks techniques and tools

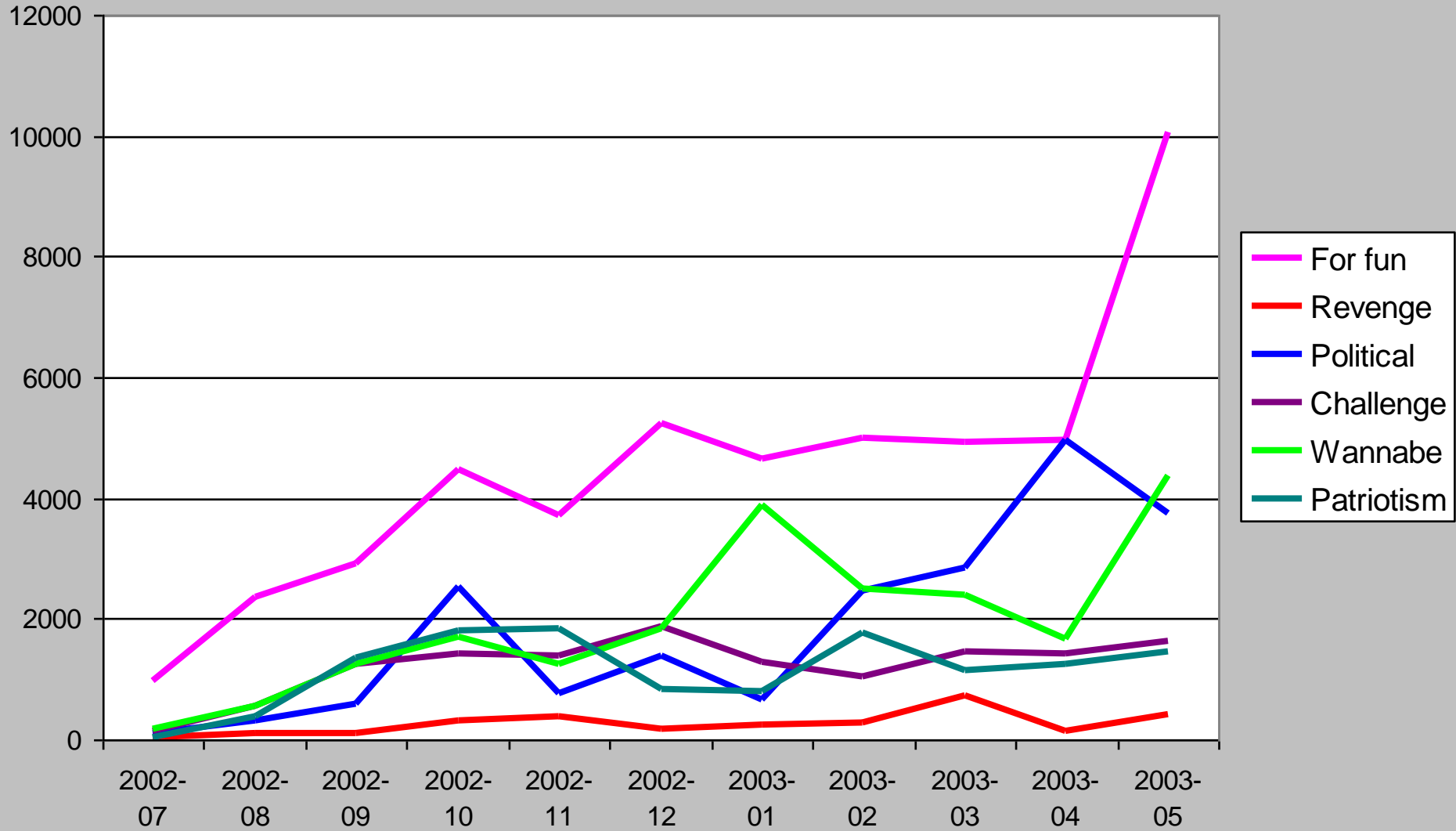
By attack method:



2003 top used vulnerabilities by attackers

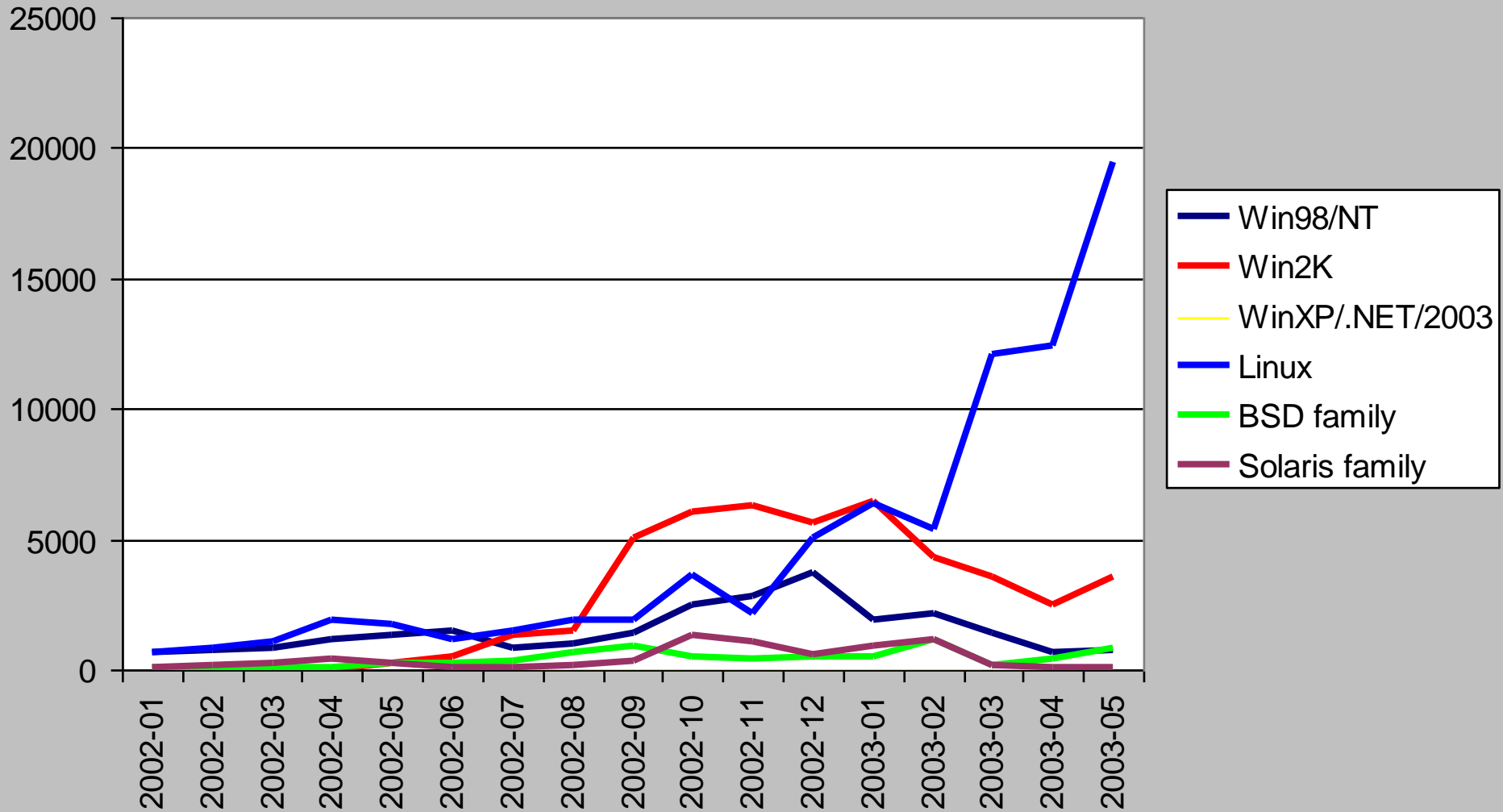
- Webdav
- Frontpage extensions
- Openssl
- Samba
- Php nuke

Defacement reasons

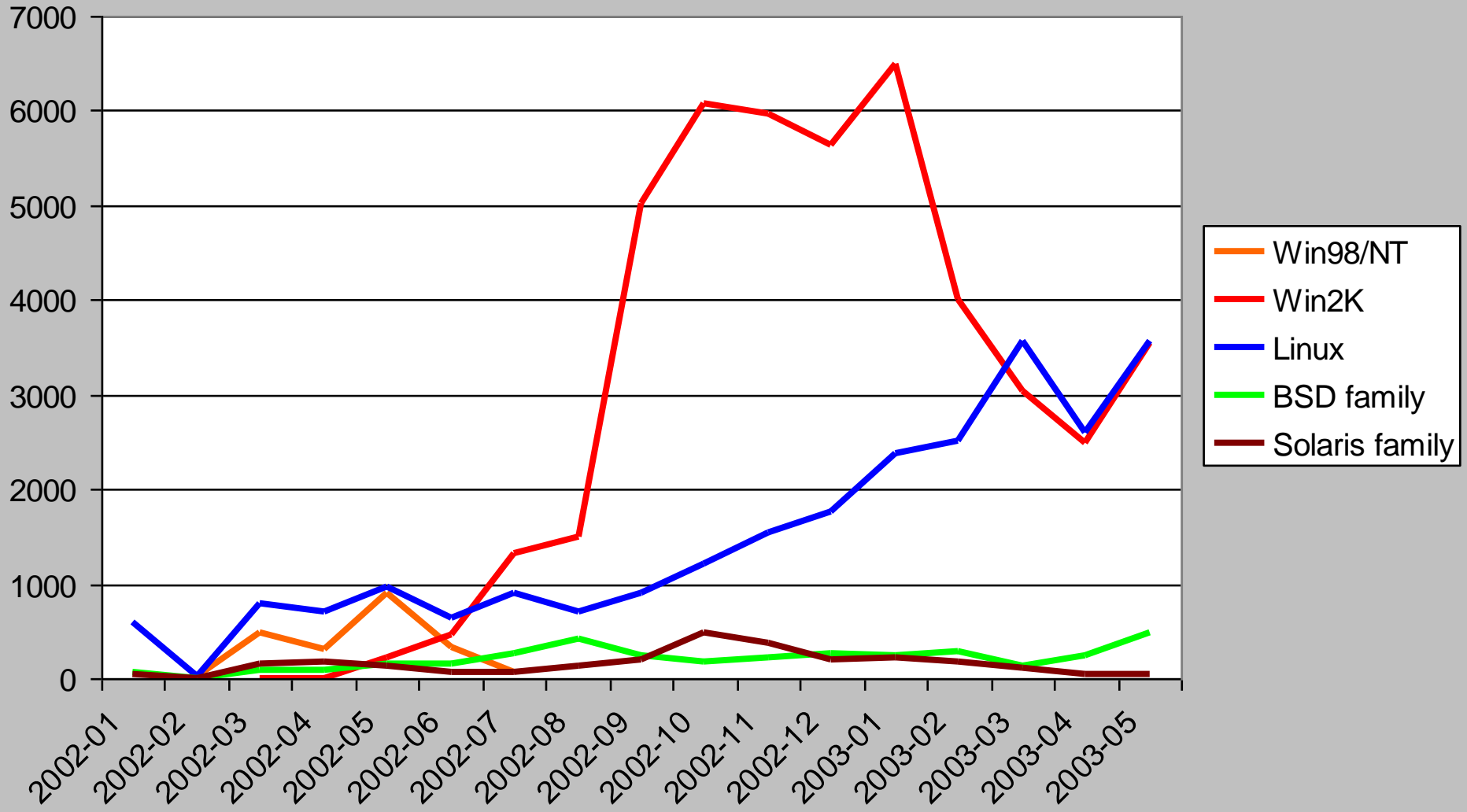


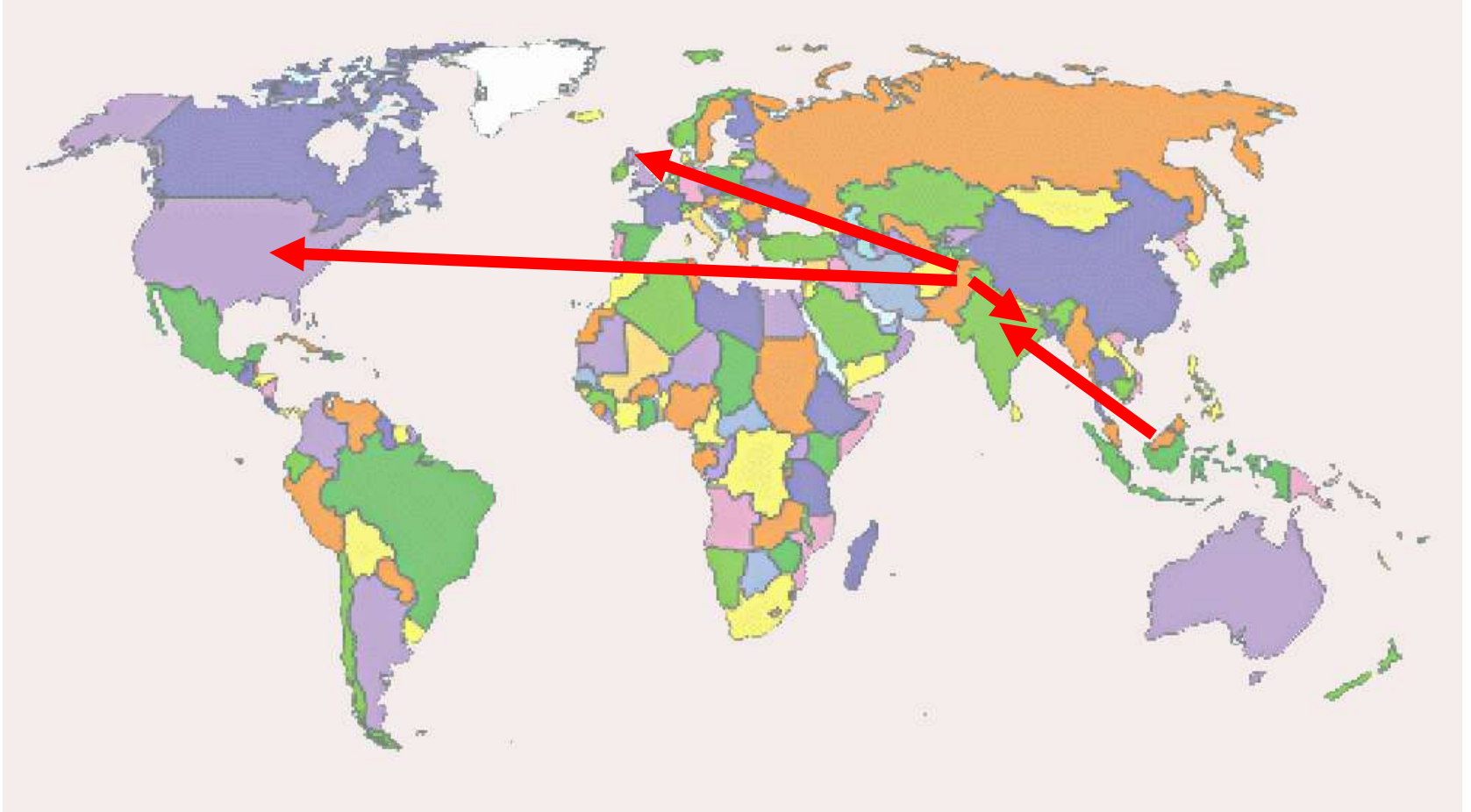
Zone-H.org

Defacements by OS



Defacements by OS (single IP)





CYBERFIGHTS

Kashmir related

Iraq war related

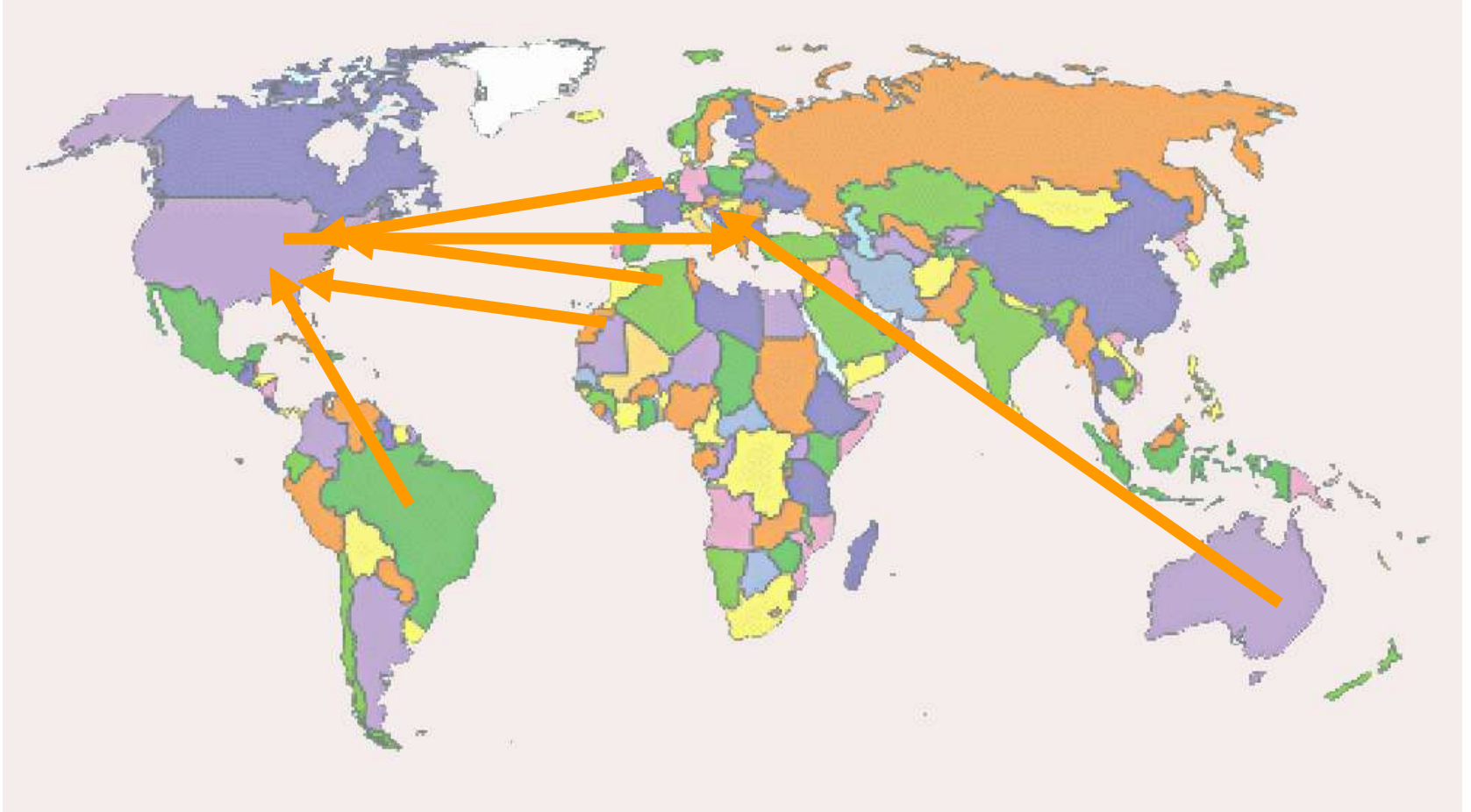
Code red release related

Palestine-Israel related

No-Global related



Zone-H.org



CYBERFIGHTS

Kashmir related

Iraq war related

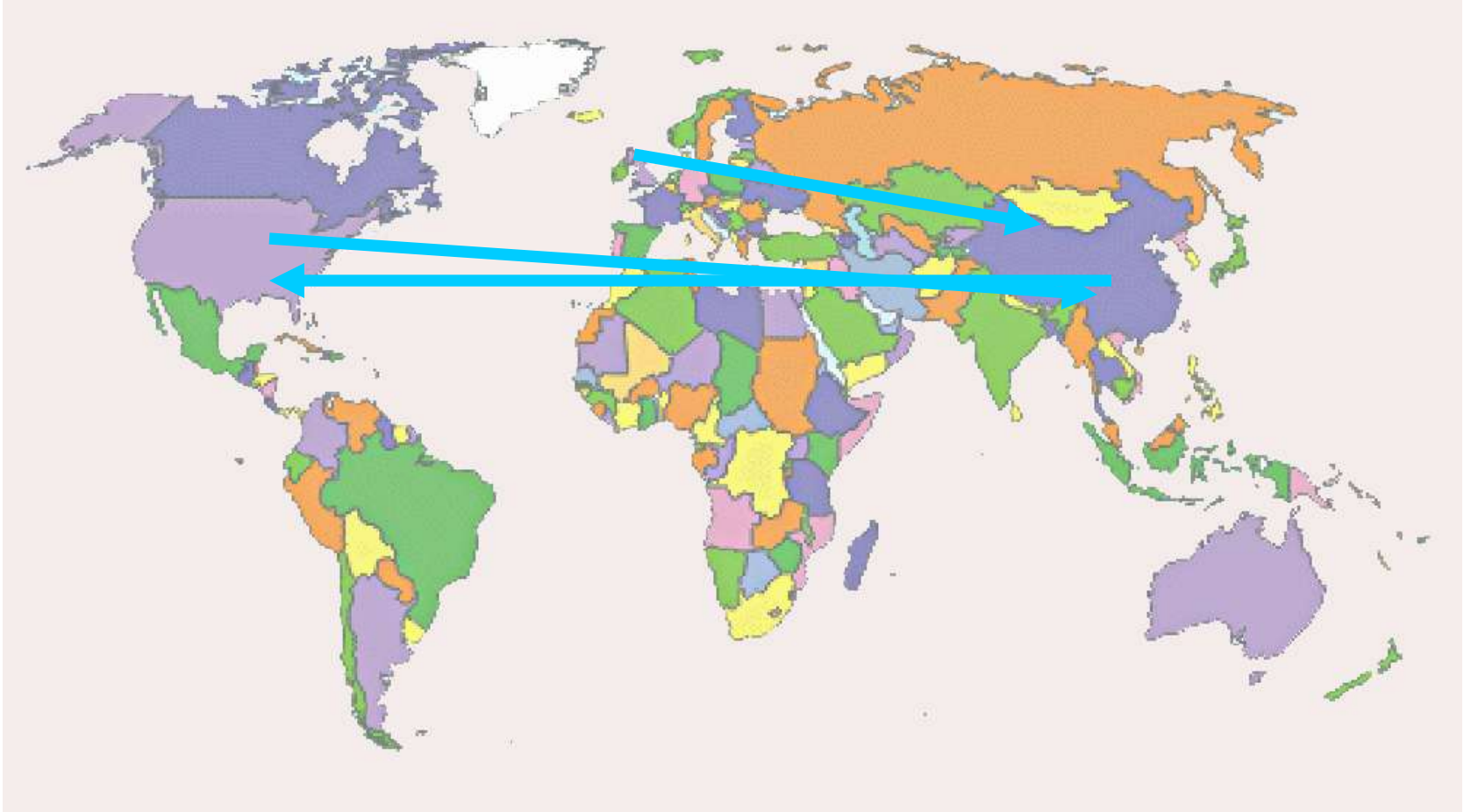
Code red release related

Palestine-Israel related

No-Global related



Zone-H.org



CYBERFIGHTS

Kashmir related

Iraq war related

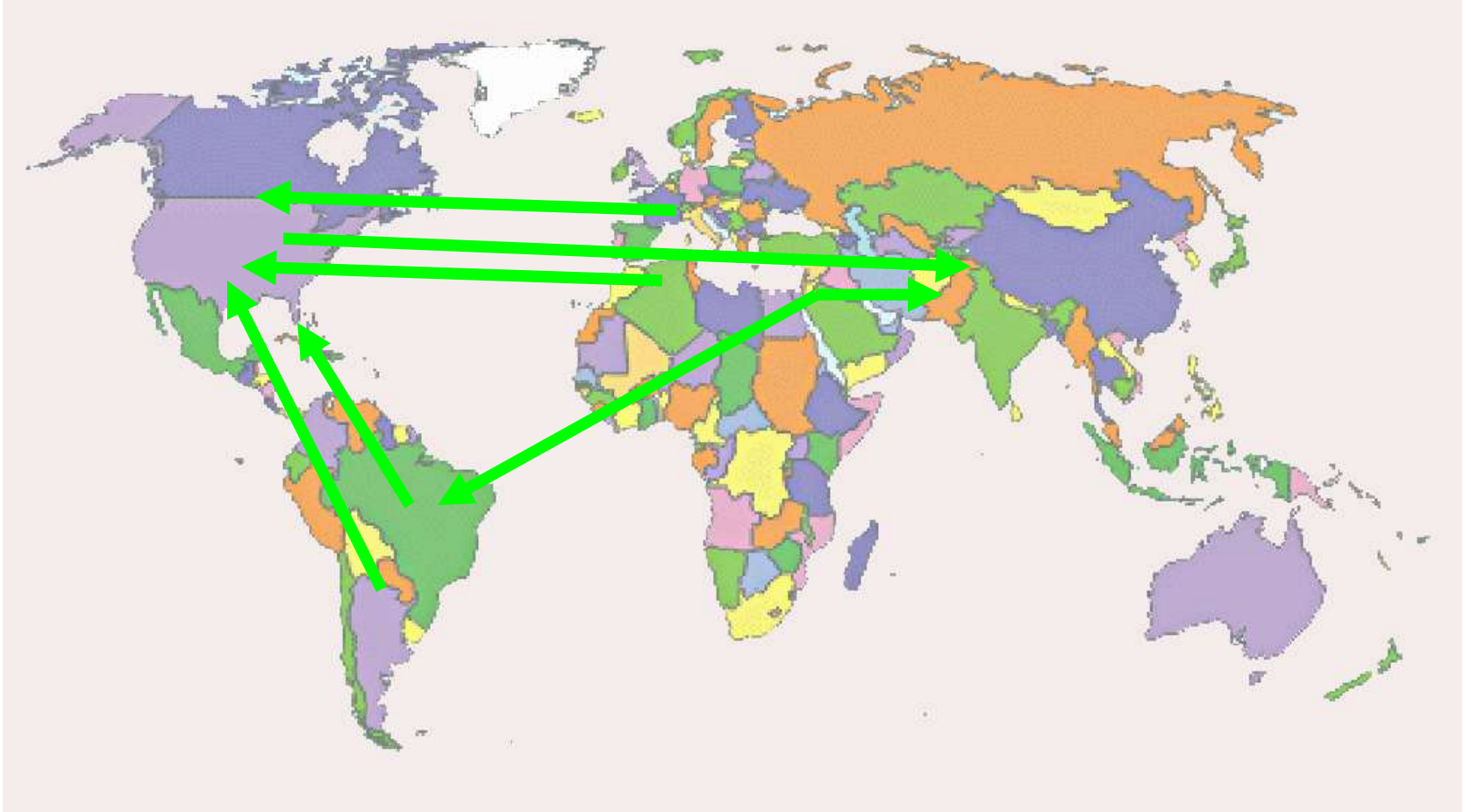
Code red release related

Palestine-Israel related

No-Global related



Zone-H.org



CYBERFIGHTS

Kashmir related

Iraq war related

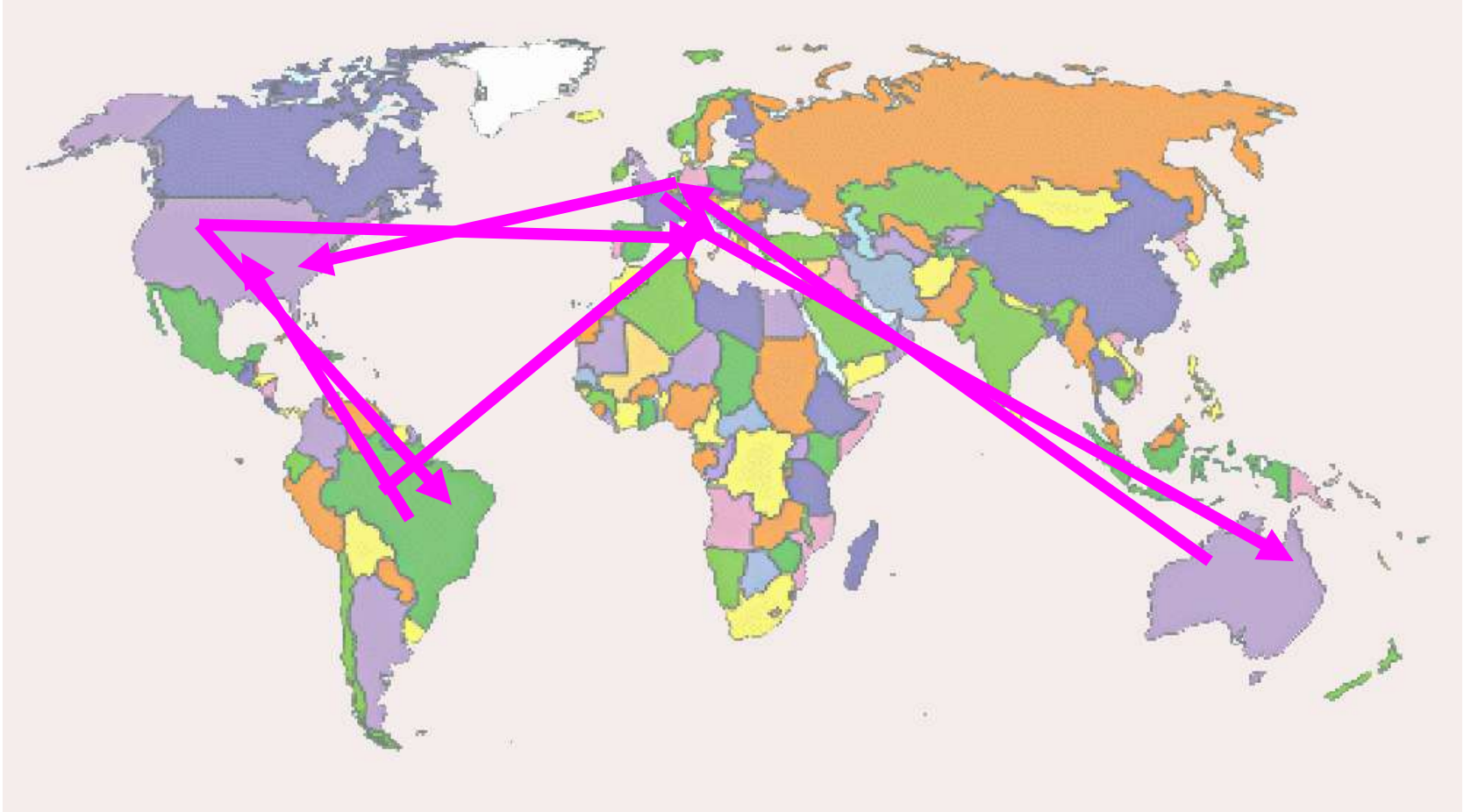
Code red release related

Palestine-Israel related

No-Global related



Zone-H.org



CYBERFIGHTS

Kashmir related

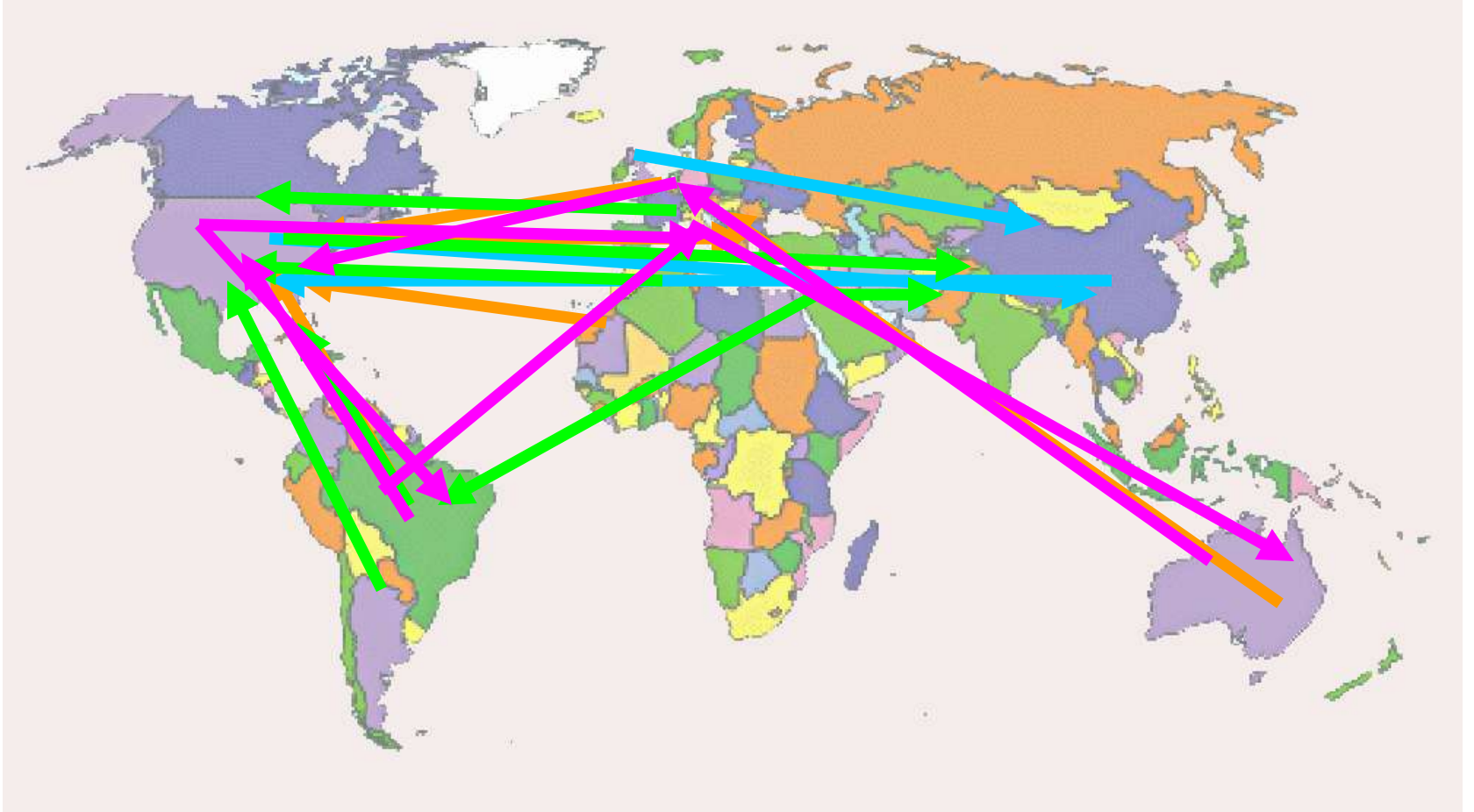
Iraq war related

Code red release related

Palestine-Israel related

No-Global related

Zone-H.org →



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.

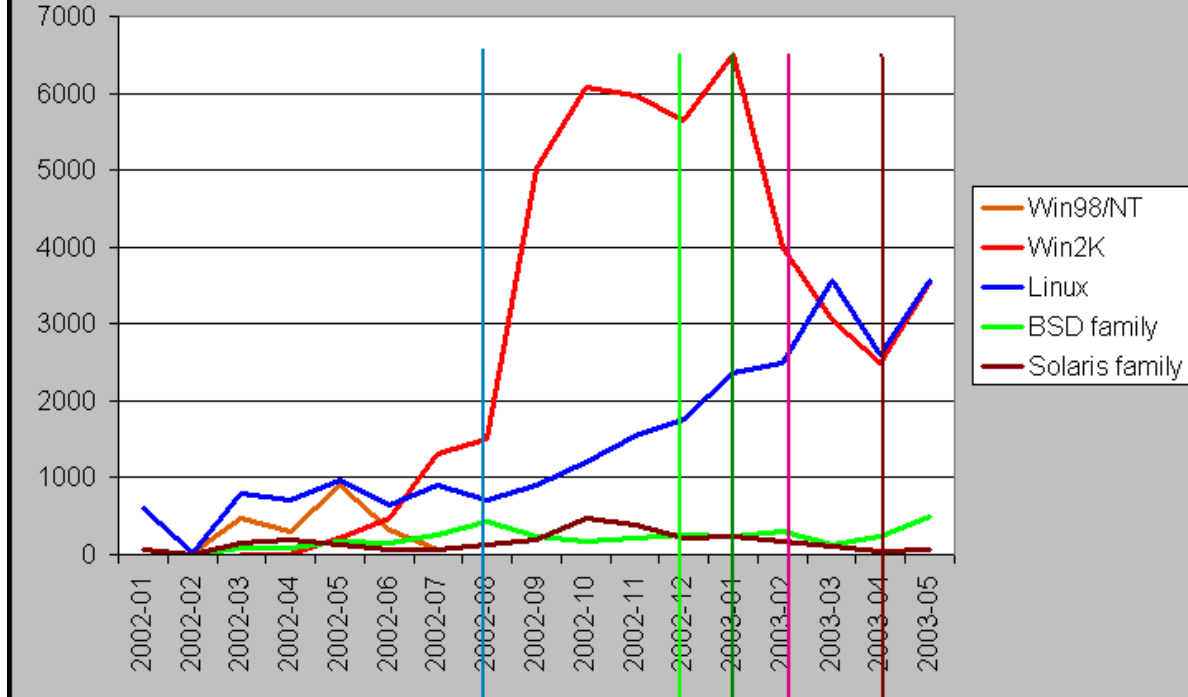


CYBER-CRIMES WILL NEVER STOP BECAUSE:

- Inherent slowness of the Institutions
- The Internet is getting more complicated
- Software producers are facing a market challenge

Defacements by OS (single IP)

copyright www.zone-h.org 2003



X-mas + Slammer worm

Slammer worm patching

Sept 11th anniversary

beginning of Iraq war

end of Iraq war

Zone-H.org

Traditional
hacker's
limited
world

UMTS

Our every day's
life activities

Universal

Mobile

Telecommunication

System



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

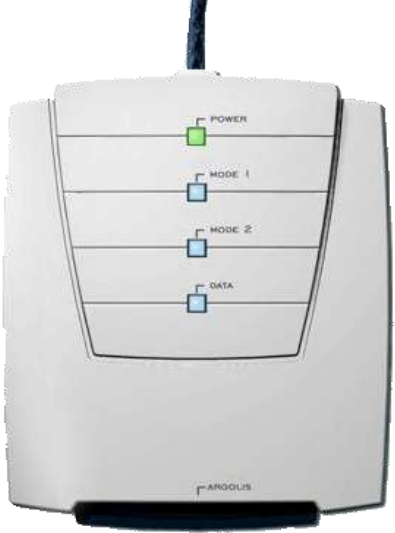
- Videoconference
- Full multi-media platform
- Data bank
- Office files
- Mobile computing
- Web browsing

NO LIMITS: they will do whatever a PC currently does as they will be powered by Windows, Linux and other commercial OSs





+



+



+



+



+



+



=

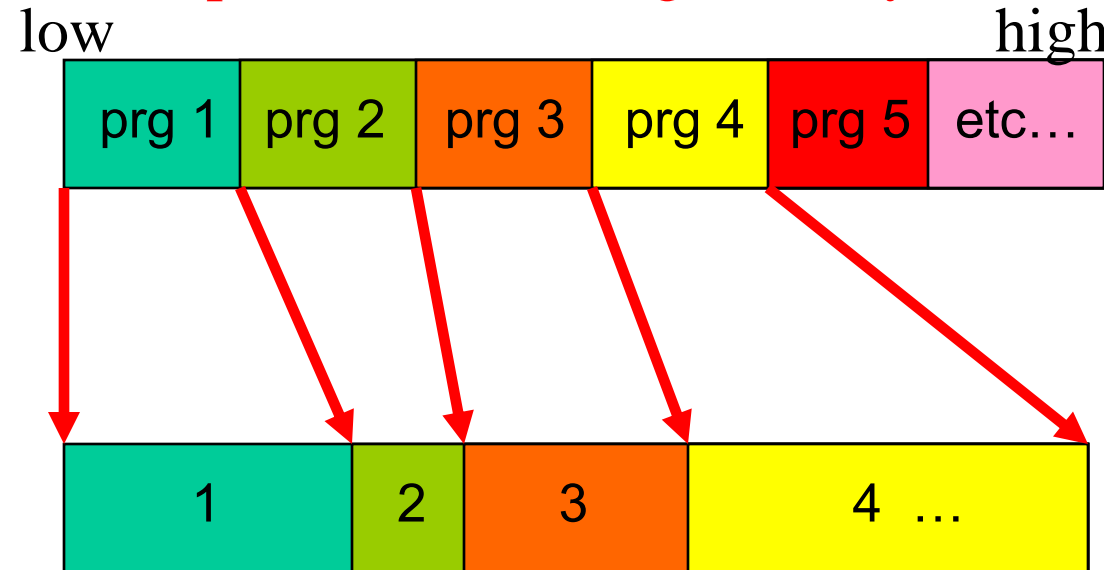


Zone-H.org

The conceptual weaknesses in UMTS

- Weakly built operative system
- Memory stacked application and data

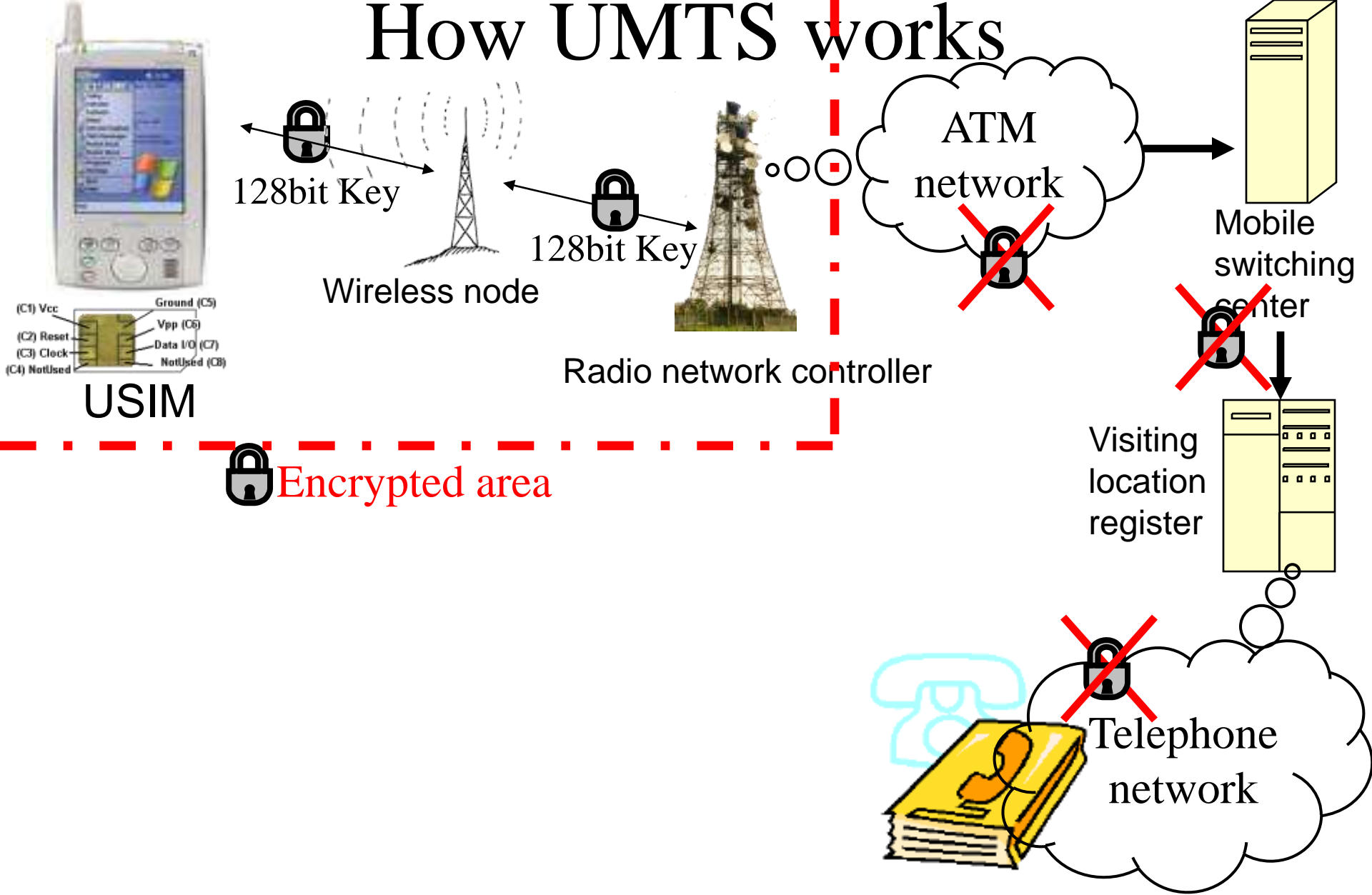
Win pocket PC running memory stack



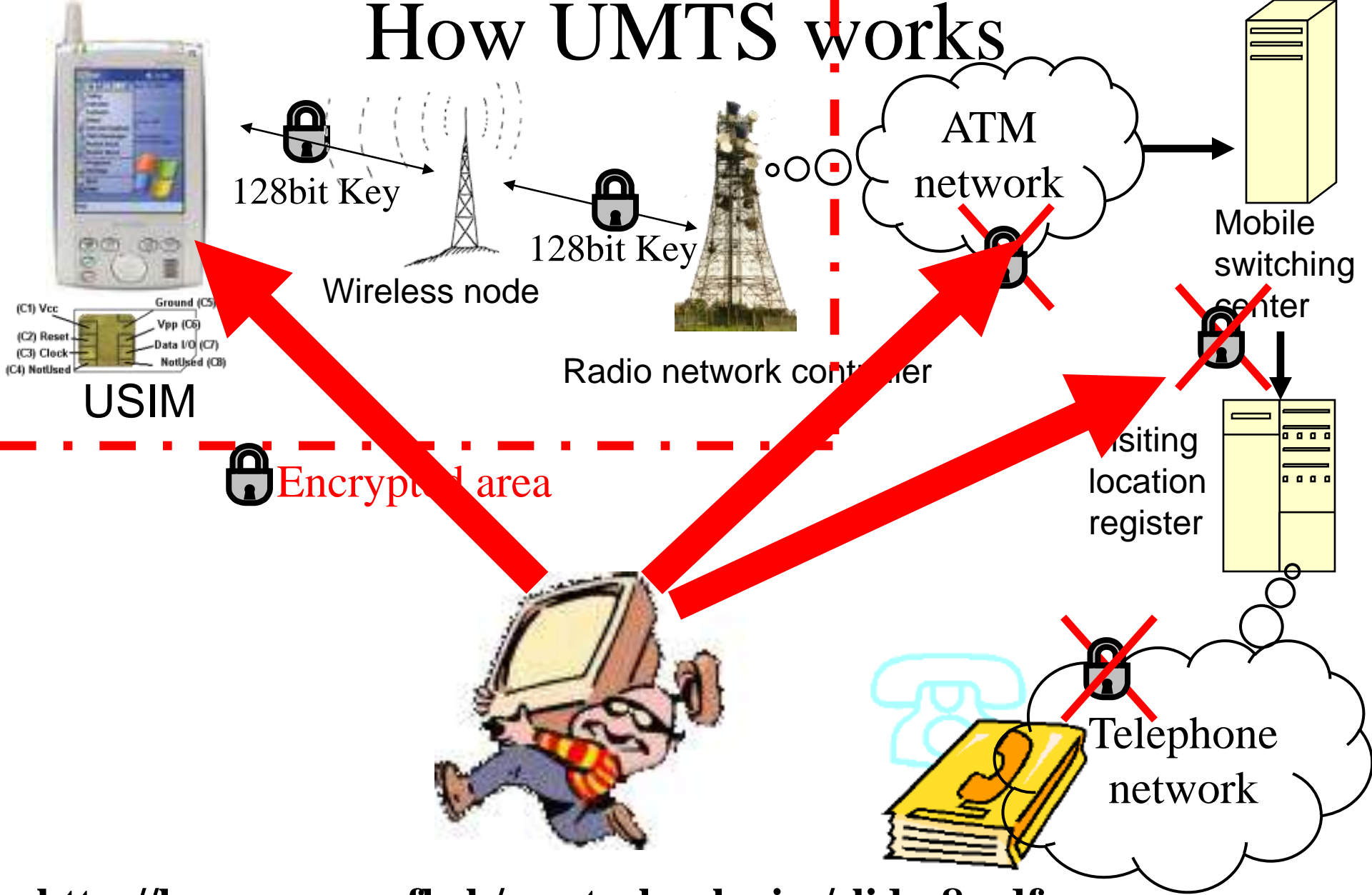
Win pocket PC storing memory stack

Region	Number	Currency	Time	Date

How UMTS works



How UMTS works



<http://lasecwww.epfl.ch/newtechnologies/slides8.pdf>

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

Zone-H.org


3 May 2003 Updated: 16:57 GMT **The Register**

Search The Register

Security flaw in Pocket PC Phone Edition

By Simon Rockman, What Mobile

Posted: 18/05/2002 at 08:50 GMT

 The page call

The page you are looking name changed, or is tem

WHAT MOBILE The June issue of What Mobile magazine reveals a security flaw in the supposedly integrated Phone Edition of the Pocket PC operating system.

Register Services Register ISP

Mobile phones offer protection against unauthorized use in the form

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



Microsoft SQL Server Digital Dashboard 3.0 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Address C:\sqldash\documents\install.htm

Microsoft

SQL Server Digital Dashboard 3.0

- Home
- Overview
- Release Notes
- System Requirements
- Install**
- Documentation

Installation

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

Zone-H.org

My Computer



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/embedded> 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.

Zone-H.org

View and modify virtual paths

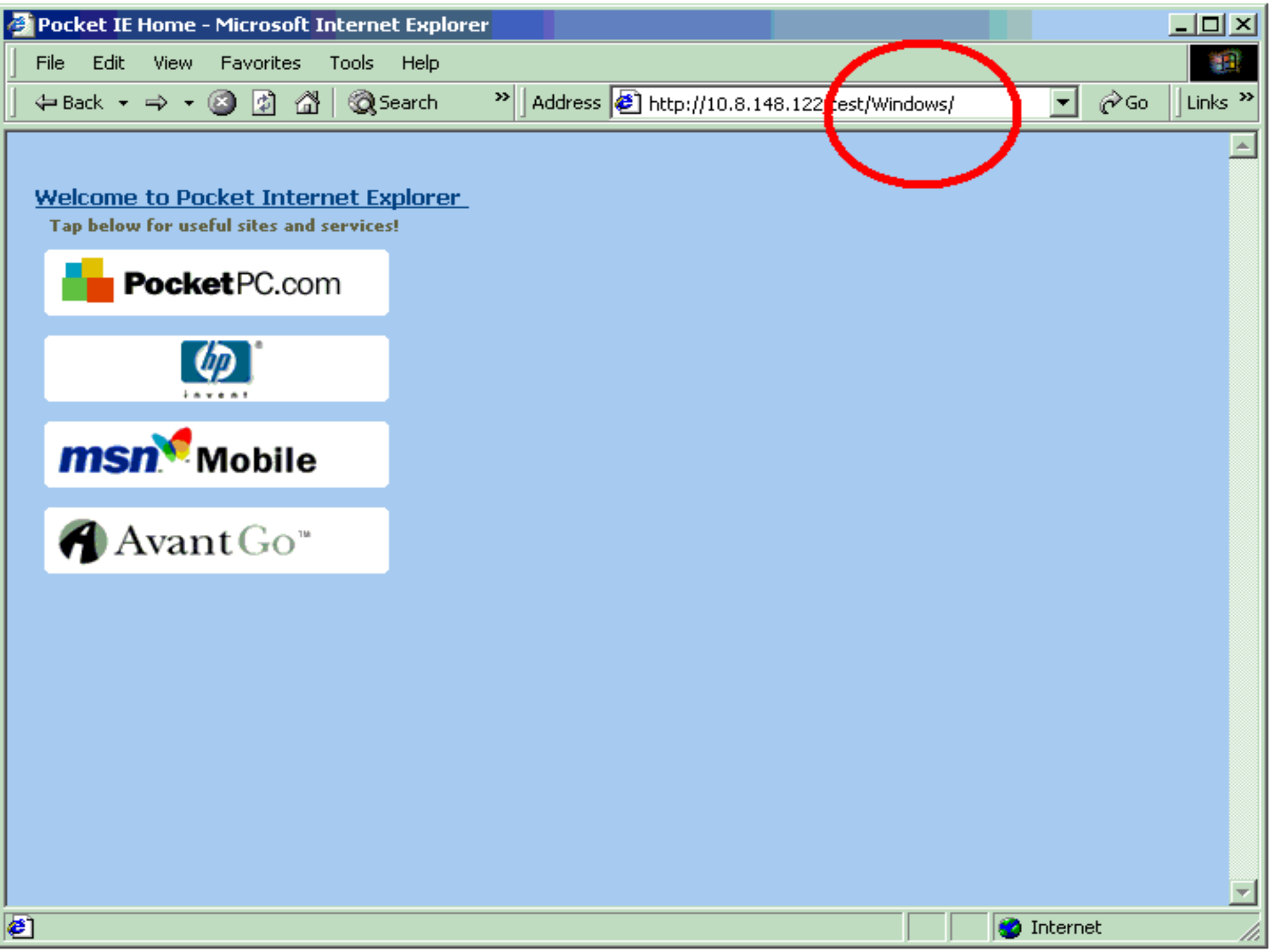
Virtual Path	Physical Path	Authorization	Read Access	Execute Access	Script Access	Modify	Delete
/test	\	Public	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Modify	Delete
/Images	\\Windows\www\wwwpul	Public	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Modify	Delete
/Dashboard	\\Windows\MSOFFDD.c	Public	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Modify	Delete
/Admin	\\windows\httpdadm.dll	Public	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Modify	Delete
/	\\windows\www\wwwpub	Public	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Modify	Delete
Add new virtual path	Add new physical path	Public	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Yes <input checked="" type="radio"/> No <input type="radio"/>	Add	

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.](#)

Pocketpc - /test/Program Files/Compaq/Phone/

[\[To Parent Directory\]](#)

2.1.2002	16:26	52736	Wireless Pack.exe
2.1.2002	16:26	38400	ProductInfo.dll
19.6.2003	17:58	306	WPPrs6.dat
27.6.2002	12:17	0	CallHist.dat
27.6.2002	12:17	0	Outbox.dat
27.6.2002	12:17	0	Inbox.dat




Welcome to Pocket Internet Explorer

Tap below for useful sites and services!

 **PocketPC.com**

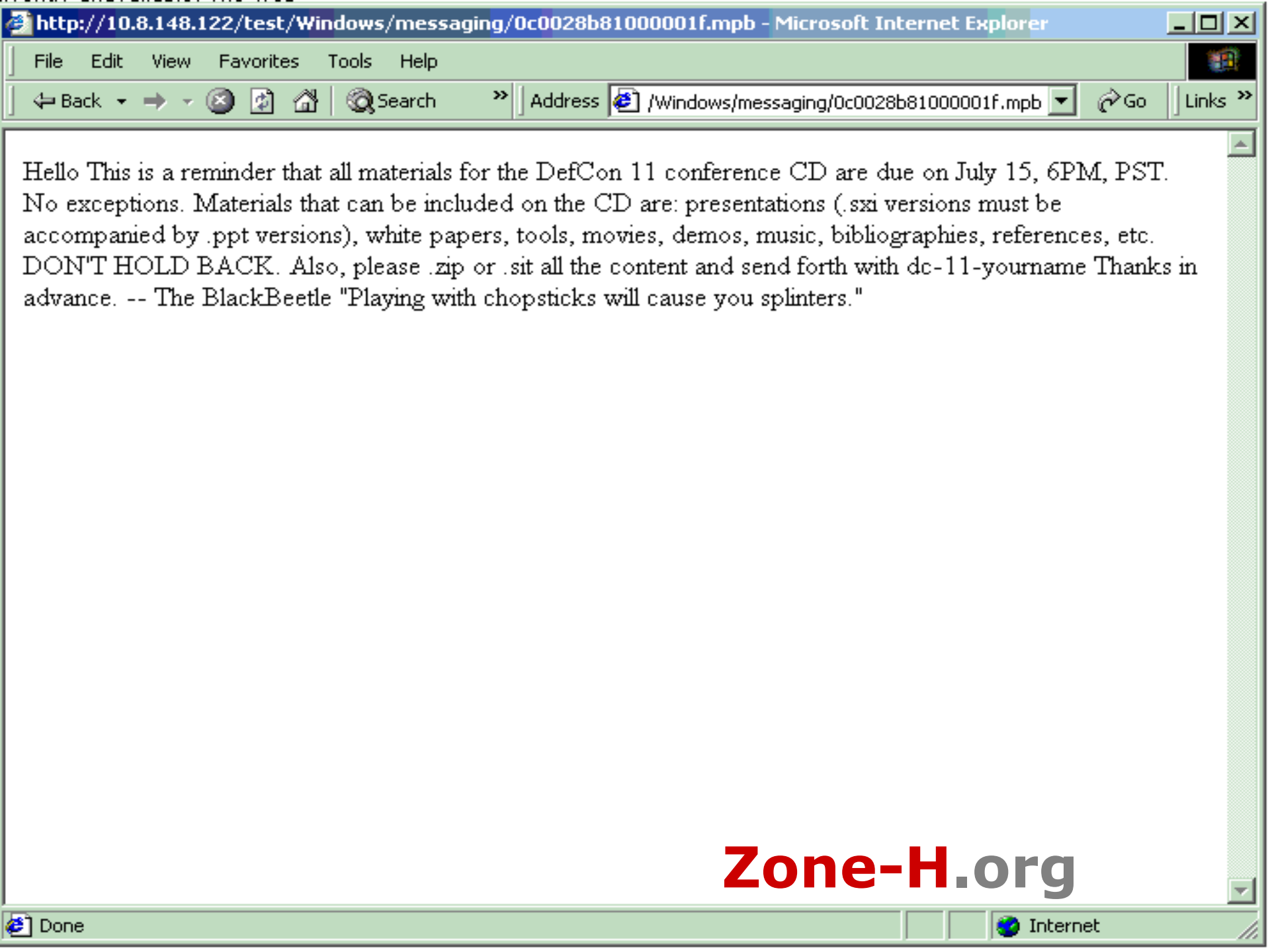


msn Mobile

 **AvantGo™**



½F€#-yk'Ü□!ª³dO' ÄKµδ%òòd, 3i~Ö% *ð□°Fm& 'ÅÚÖ□«~□TªW]b¶FP#á,□□ □□□□□□□□□□
 Zµδ%òòd, 3i~Ö% *ð□°Fm& 'ÅÚÖ□«~□TªW]b¶FP#á,□□ □□□□□□□□□□
 ð,□ÈÈBk î ñòÐ(e□M□M'□□ñ "□8††Ð+.³'□ÇeèEçV□ ÇJ□úÈ)
 □f'□A+H€Qh□8B□,°«à_æAh°Ž"^^□"□ÜKU□9#€s□□Í@);we-
 yD,°ÛæÛ¼'r□nÔŽ'r'8ÐkjÖ) —Ýç\$□£□#Î □Òfçýý□b□jÛP#□QÛÀt'U±□l□□
 FPÅ1Ø î□nç□'ÔXÌ'ò-¥Á...šÅ<æ,"AêŠÆØ□ŽDðf□#ª, ágLÅw]ýZh&PÒ=W'%
 Ä~@□+i. ¶ÛeâµX"/Fžy#¼Èç□/□22ã□dT^Ê^&, □çyglæÐÄ5ÇÑ°«'ý[□M,+ð□ □8□Ö?
 WyD>'x'ñü'.□=-ðsç□?£l5m□ñ□øûÒð¹øó□Ô0"...s.,+/a)□U□,□òýß\$□@/□vÐÑÉÍ□-T"Û□□-
 ànce□VâP)Ár(E).yG|5- y0W(æÝ~ð×□-ólø□øRQK□çy—□Ê□áÎ=í@WÖ□æ%∖Fì□□
 Nx□7èèfýCq]□îjy□zF|%o]ÍŠD"Û•cÁriÄ□%oÇ□ó=Vxüš¼?5žŽè3ù+f."cMK□<ÖÅPç
 =PÚ³i□² □d—†'□[□Êá]P|IM'Ó>ÎVpi.3è?èd~Q□kz½?
 (<~□øùk□Ûu22ý",b;lU^i2i&□³Ä□□áíð6"£□□G"Ýêð¾□vÇEK□^HgDêòì™m...
 IŽÛ/@XjÁ±R {\$"□€7-i'kè~CiÁ¼¶çæH□□ □Ä□□"öp\□Ž'Ñ'FÉ1kdl,†µ°òd%o
 ¼ÉZgo□çG½ðŽMø»□\$A^D\sf è%□3Ou çì□□Ô,ÜL¾4□> X†B□çŽN□□□Xdøøjójmwùðç
 \W□†Á'!pá\□ÆÒ□1§†4ÐìHøQ§t4³x&.,%o□éúé¼IÖìSWM\Çç□ÖJýÉfìbÖ1...K^Ö%o
 é ±4ûÖú0×±□...¾4d-ÊµÐv^T&h□'ý□xâýi«dÒPÐr²yÄ†ü□@i°-EO□¾—
 >Ud"§;□@jšñ□Ä×æ&Æ©×□F¹,IðJq¼ýF...)□□çy²x, Ð~jæ□(Ä)□HžO□-iC...sá@=□'□p d°
 Èa3-□.jÅxJ™tTÚÉ, 8†<ð«™gÉ□~Z±]~7ý4Í□½Ö□5«Ïý□,ð÷□0kóÇEU^"□□□'□éw
 úç□±(Í.0yÏGr_t(GZ-úŠÑ"ú□@;¼-¼úÐ:S°J3E(ÇepÓ(ª'Ž□ □Iã(Xi-€èü¶æ:r!8?èð,)
 °²H,-□d<□fáf d□'Š),A4Ò□p2Ç□Äç*?□ü¶□ü□□"@½□W_G'šj@□GA"□†;□xÐiMû□È Ì-
 iOZ'ý²□òk µî= vp□iC□Dhm□WZ'è□¾47>Béû¼Z7á+@... □sÖ ?~YçÛ□anâZQÉÔó, □NP%
 lç©Á□¾4çlæ2%o ý8□□—¶áíÈ.æKç9 *vOARžl



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

ZH2003-5SA

windows beta

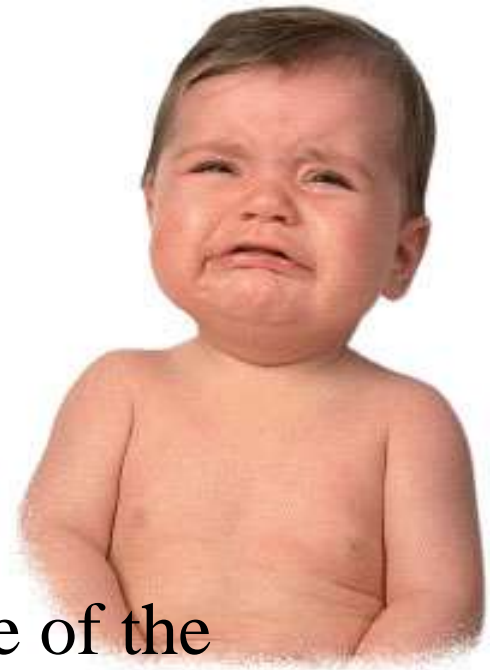
webserver for pocket
pc: full remote access

*The default installation of
windows beta webserver allows
an attacker to gain full remote
access without authentication
simply logging to
http://attacked_host/admin*



ASHAMED,
EMBARRASSED,
DISGRACED

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.tutorgig.com/searchtgig.jsp?query=umts> (several tutorials)
- http://www.ericsson.de/downloads/pressenews/presentation_cornelius_boylan.pdf
- <http://lasecwww.epfl.ch/newtechnologies/slides8.pdf> (excellent paper)
- <http://www.sans.org/rr/paper.php?id=253>
- <http://www.pocketpcdn.com/>
- <http://www.itsx.com/pocketpc/BH-AMS-2003-itsx.ppt>
- <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 Internet refrigerator



LG InternetFamily

Internet Refrigerator Demonstration

Digital Features

General

- Tilting, pull-out 15.1" touch-screen for accessing all services
- Built-in stereo speakers, CCD camera and microphone for entertainment, interactive and messaging services
- Electronic calendar for keeping important dates
- Electronic nutritional fact file for tips and information on food products purchased
- Track foods and their storage time in your fridge freezer
- Electronic user features and maintenance manuals
- Self diagnostic system for highlighting faults
- Phone Number Management
- External Management
- Cooking Recipes
- Weather Information
- Handwriting Recognition

Communication

- Full internet access
- E-mail, video mail, voice-only and on-screen text messaging services

[back](#)

© 2002 LG Electronics

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



LG InternetFamily

Internet Refrigerator Demonstration

Digital Features

General

- Tilting, pull-out 15.1" touch-screen for accessing all services
- Built-in stereo speakers, CCD camera and microphone for entertainment, interactive and messaging services
- Electronic calendar for keeping important dates
- Electronic nutritional fact file for tips and information on food products purchased
- Track foods and their storage time in your fridge freezer
- Electronic user features and maintenance manuals
- Self diagnostic system for highlighting faults
- Phone Number Management
- External Management
- Cooking Recipes
- Weather Information
- Handwriting Recognition

Communication

- Full internet access
- E-mail, video mail, voice-only and on-screen text messaging services

[back](#)

© 2002 LG Electronics

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



A screenshot of the LG Internet Family website. The top part shows a blue header with the LG logo and the text "LG InternetFamily". Below this, there is a section titled "Digital Features" with a sub-section "General". Under "General", there are two bullet points: "- Tilting, pull-out 15.1" touch-screen for accessing all services" and "- Built-in stereo speakers, CCD camera and microphone for". To the right of these bullet points, there is a red arrow pointing from the skull in the refrigerator image to the text "Ping -l 65535 xxx.xxx.xxx.xxx". Below this, there is another section titled "Communication" with two bullet points: "- Full internet access" and "- E-mail, video mail, voice-only and on-screen text messaging services". At the bottom of the screenshot, there is a "back" link and a copyright notice "© 2002 LG Electronics".

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



Call 1-800-AMISH !!!

sys64738 Zone-H.org admin@zone-h.org