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

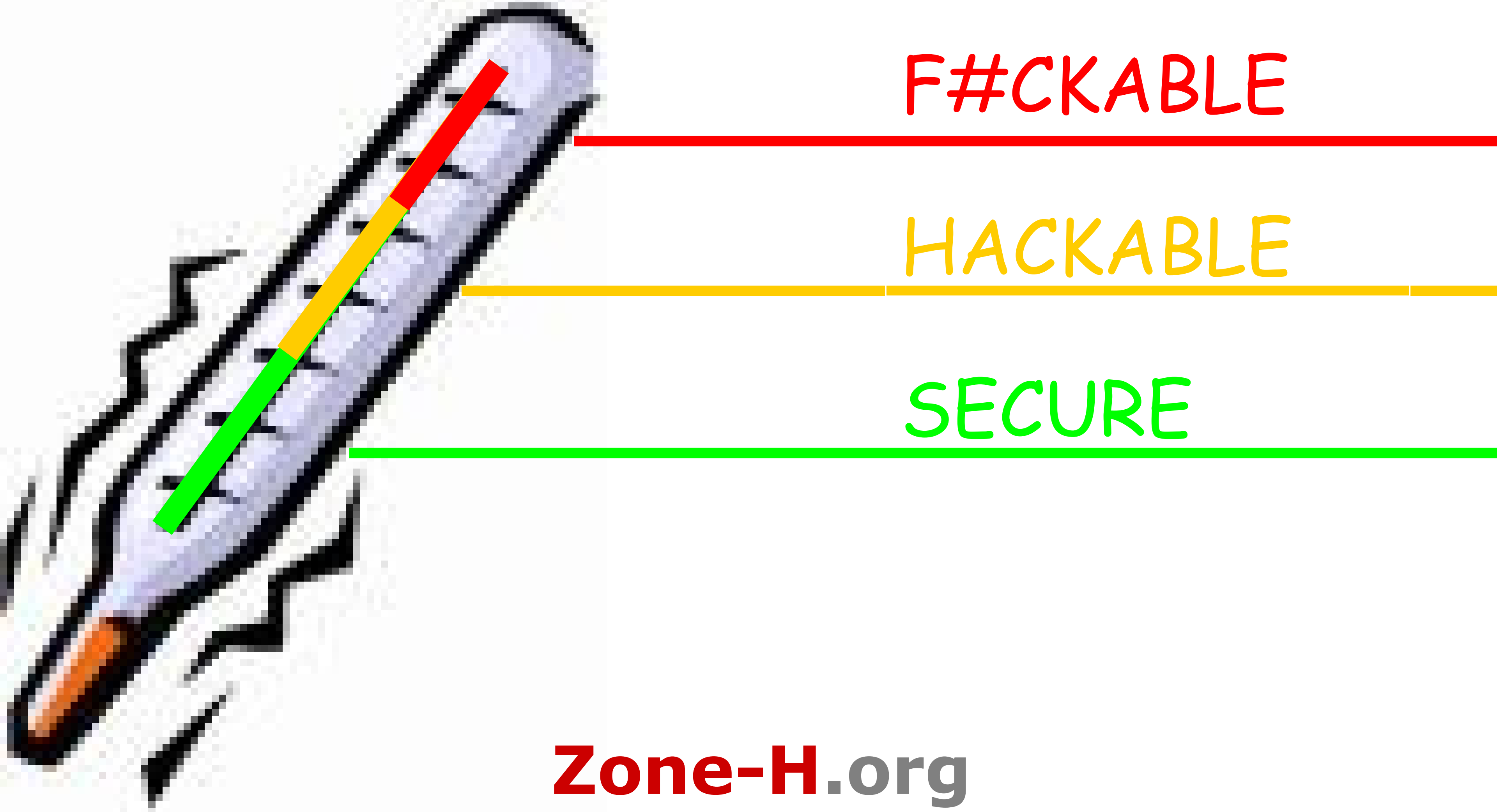
Speaker: SyS64738 www.zone-h.org

Zone-H.org

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

Zone-H.org: the Internet thermometer?

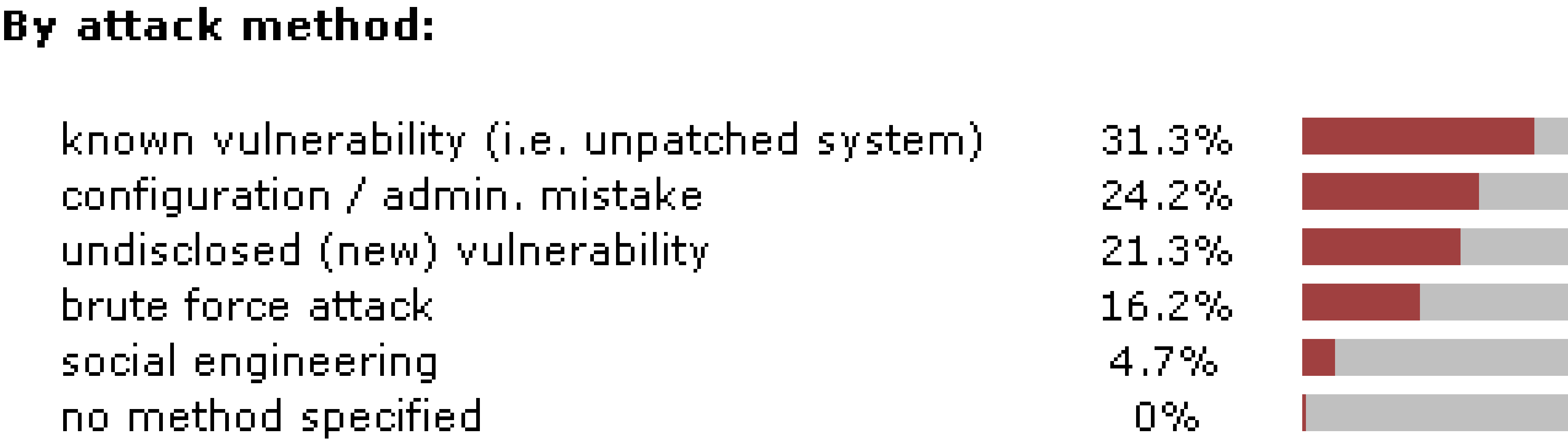


F#CKABLE

HACKABLE

SECURE

attacks techniques and tools



By attack method:

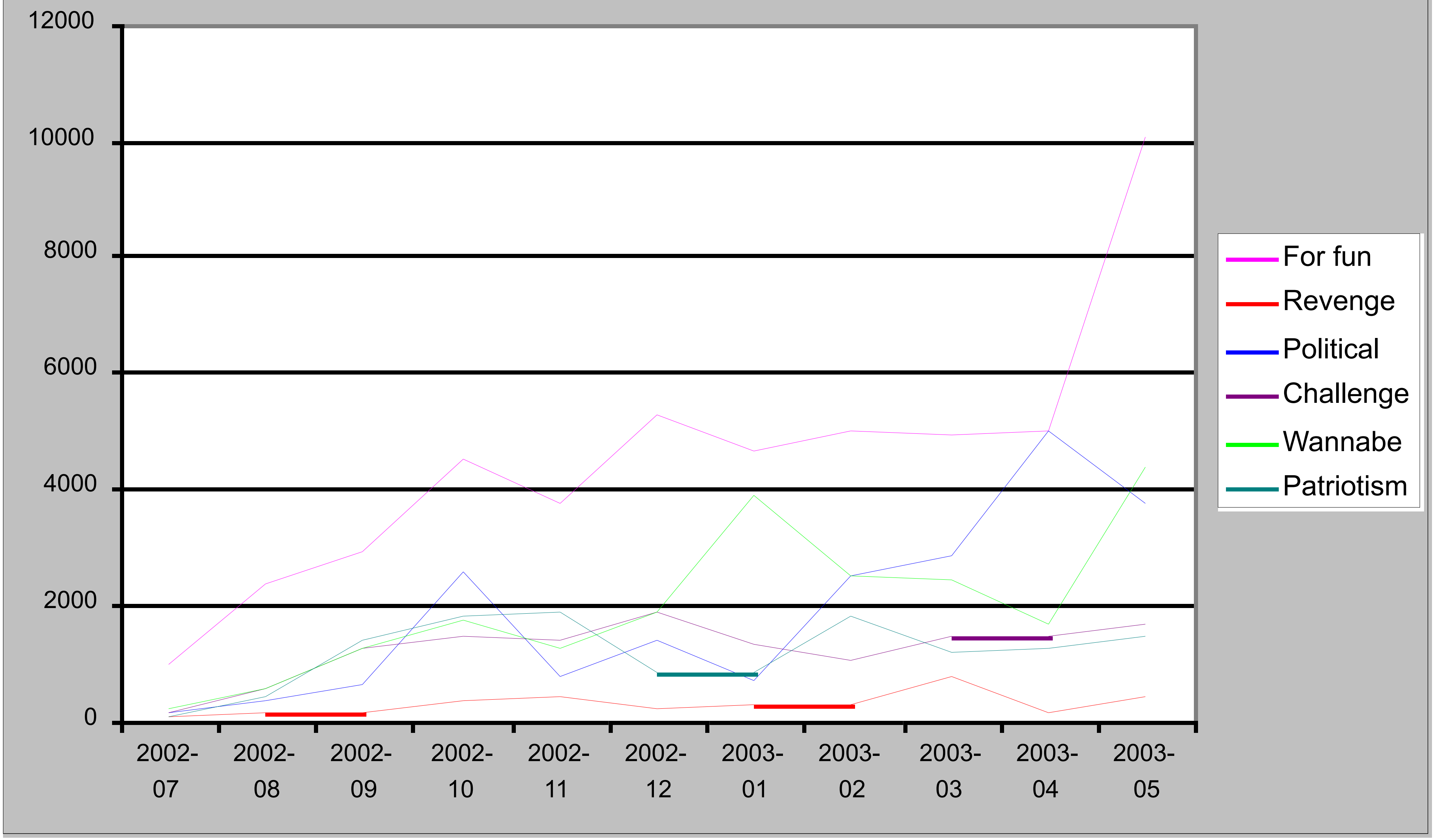
known vulnerability (i.e. unpatched system)	31.3%
configuration / admin. mistake	24.2%
undisclosed (new) vulnerability	21.3%
brute force attack	16.2%
social engineering	4.7%
no method specified	0%

2003 top used vulnerabilities by attackers

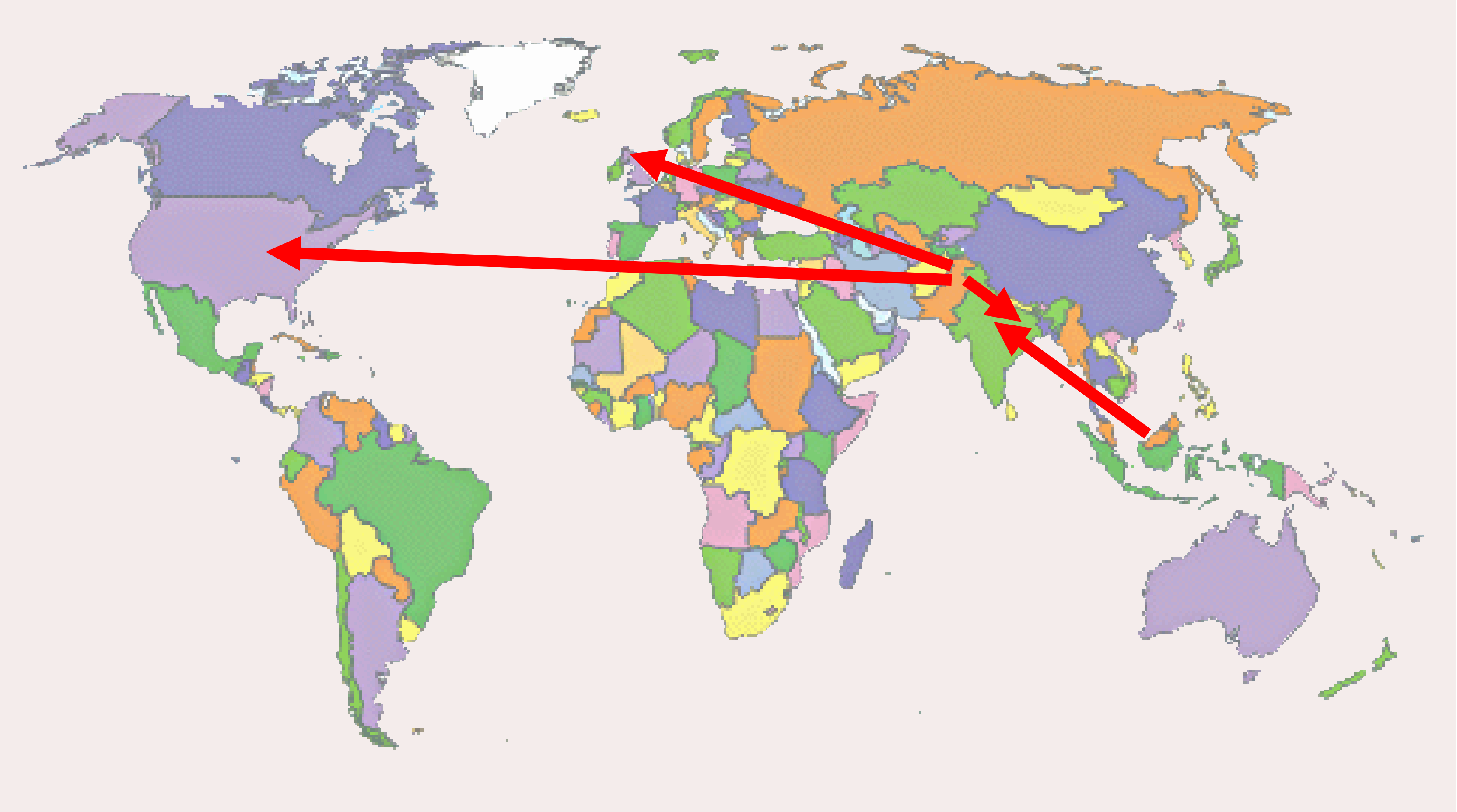
- **-Webdav**
- **-Frontpage extensions**
- **-Openssl**
- **- Samba**
- **- Php nuke**

Zone-H.org

Defacement reasons



Zone-H.org



CYBERFIGHTS

Kashmir related →

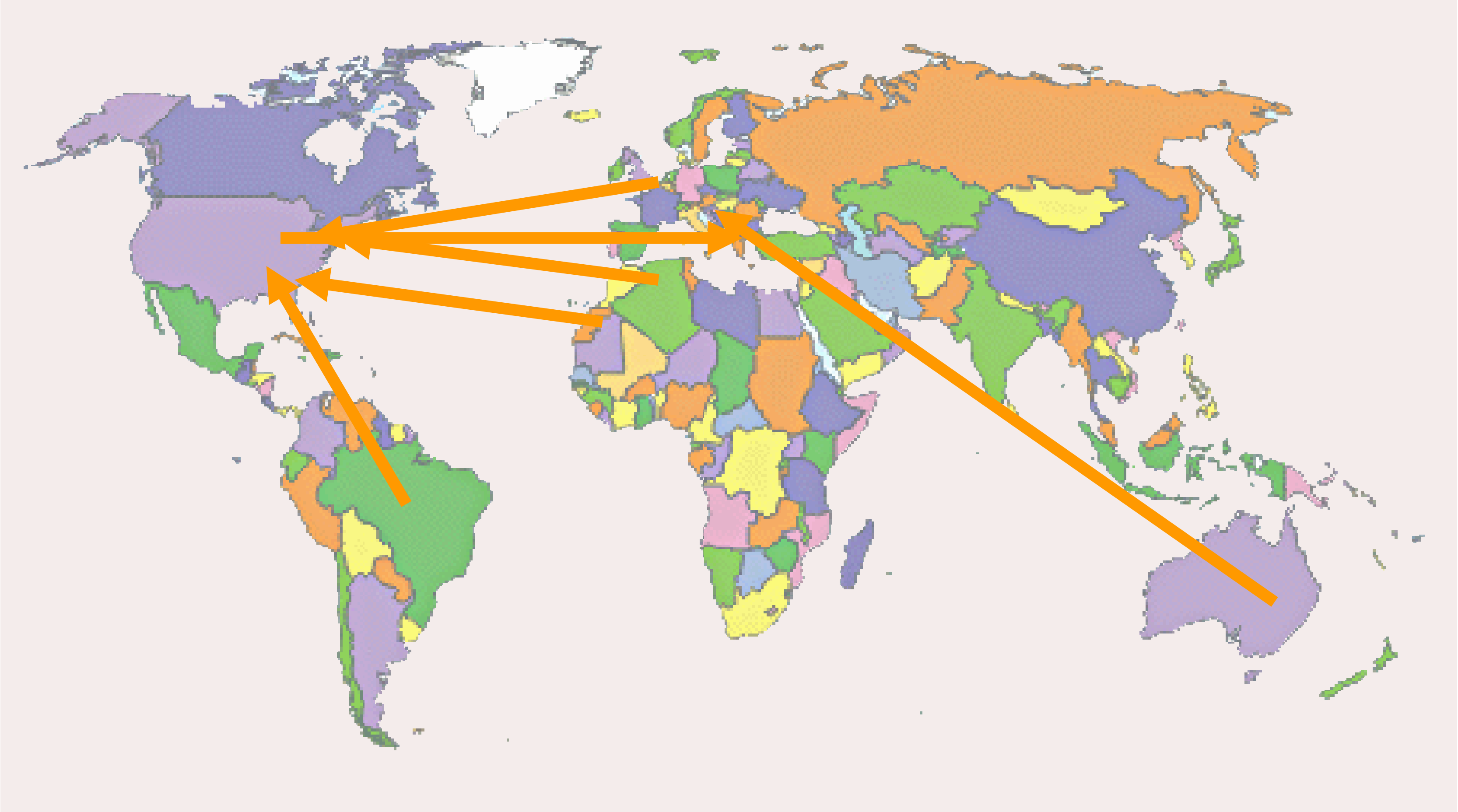
Iraq war related

Code red release related

Palestine-Israel related

No-Global related

Zone-H.org



CYBERFIGHTS

Kashmir related

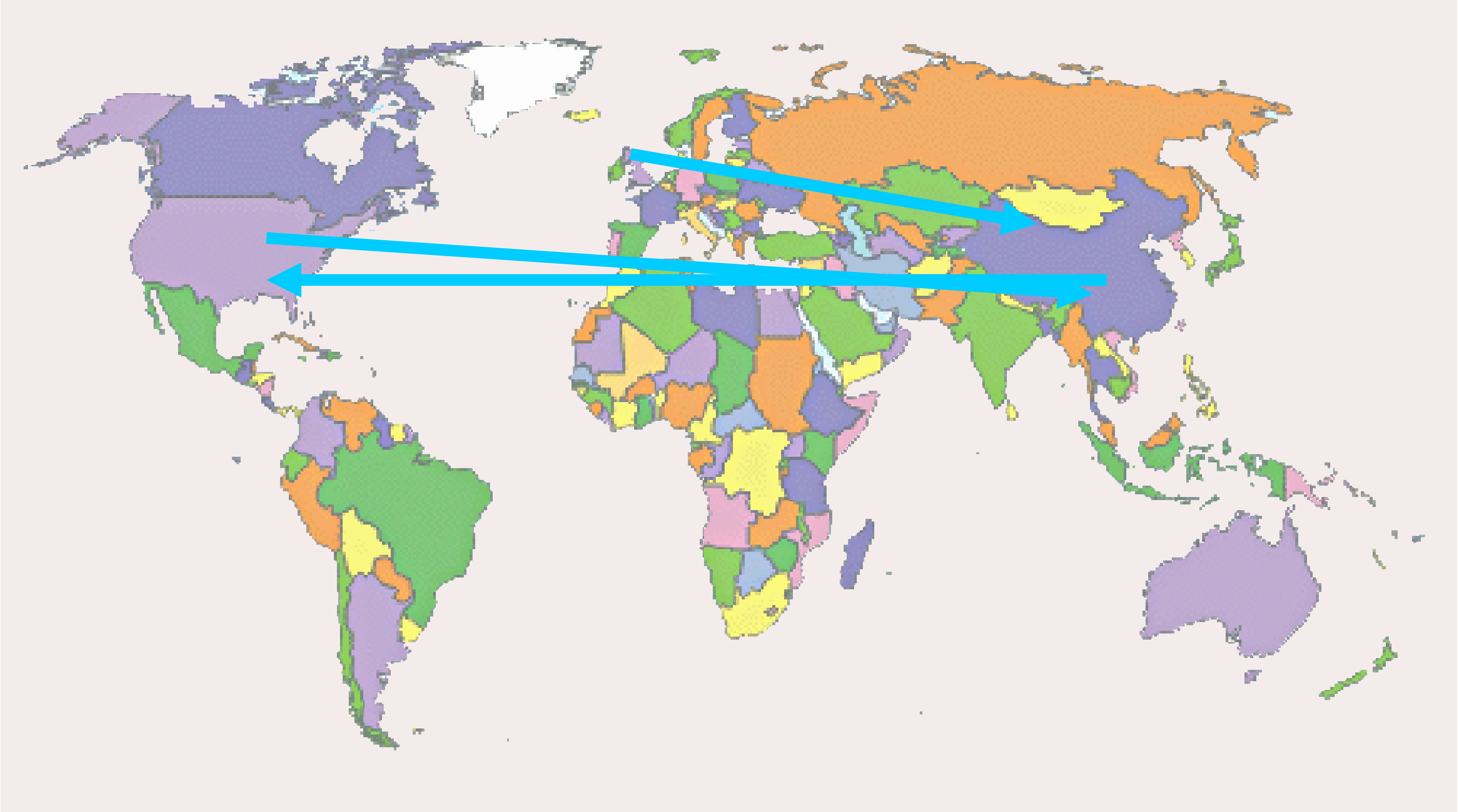
Iraq war related

Code red release related

Palestine-Israel related

No-Global related

Zone-H.org



CYBERFIGHTS

Kashmir related

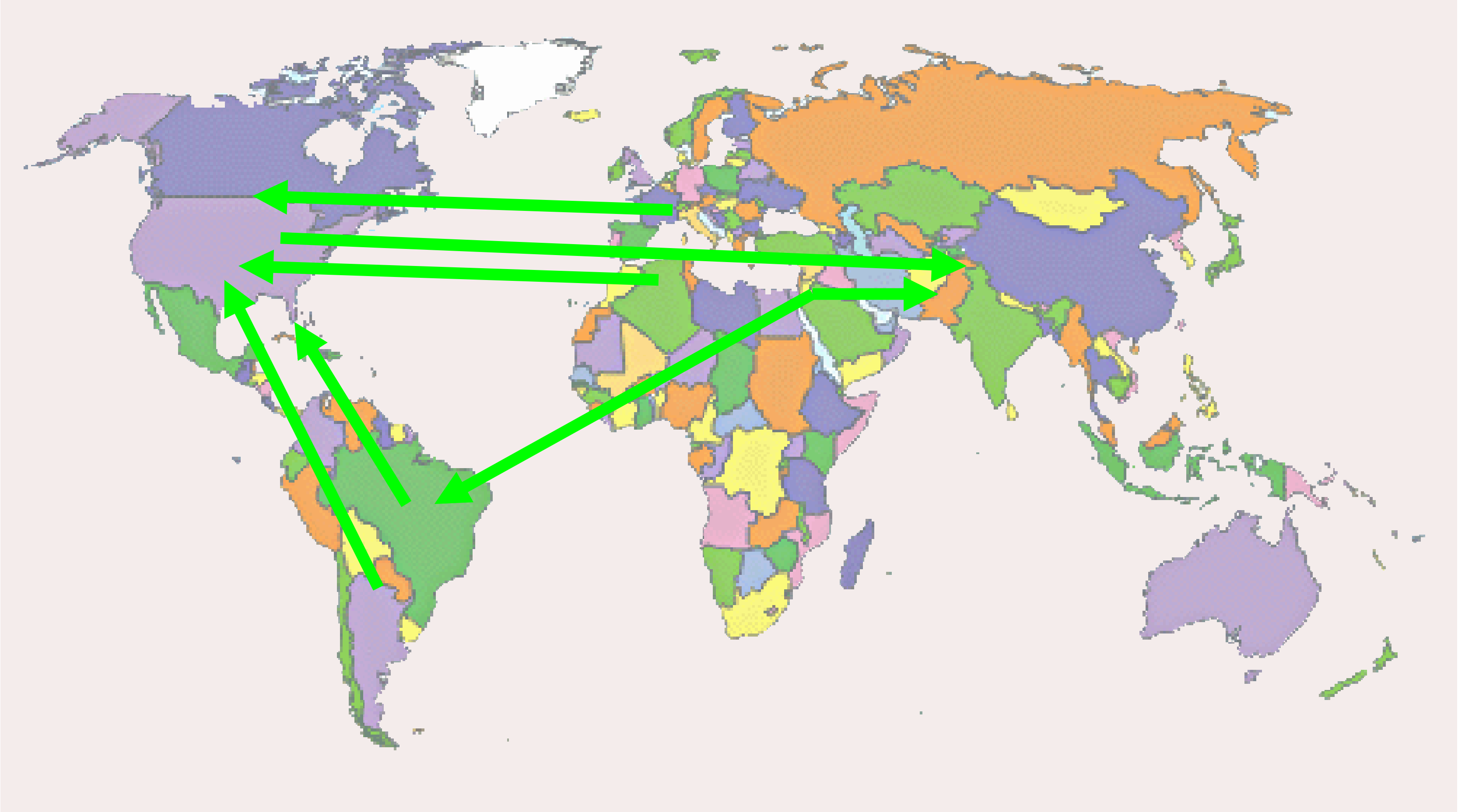
Iraq war related

Code red release related →

Palestine-Israel related

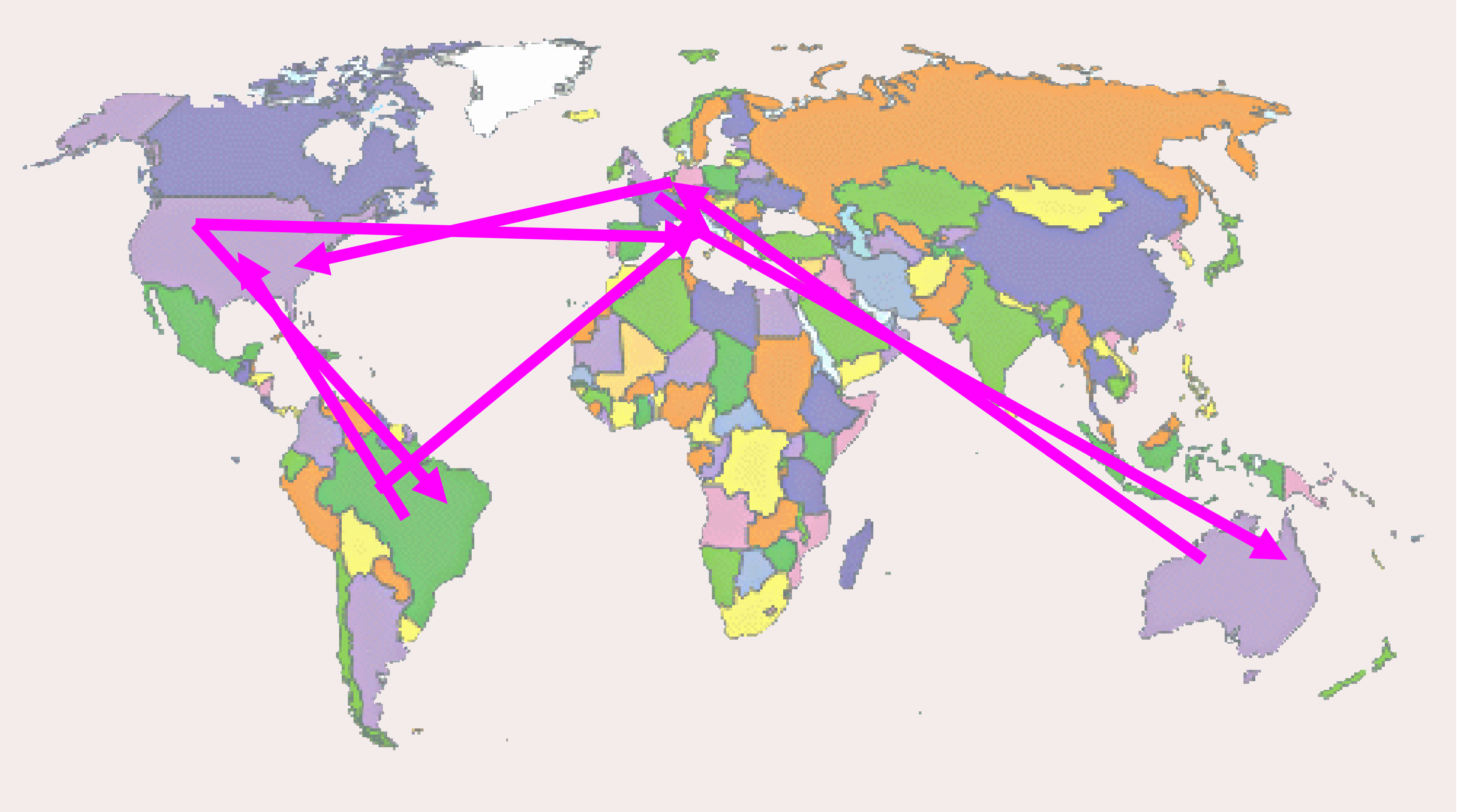
No-Global related

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

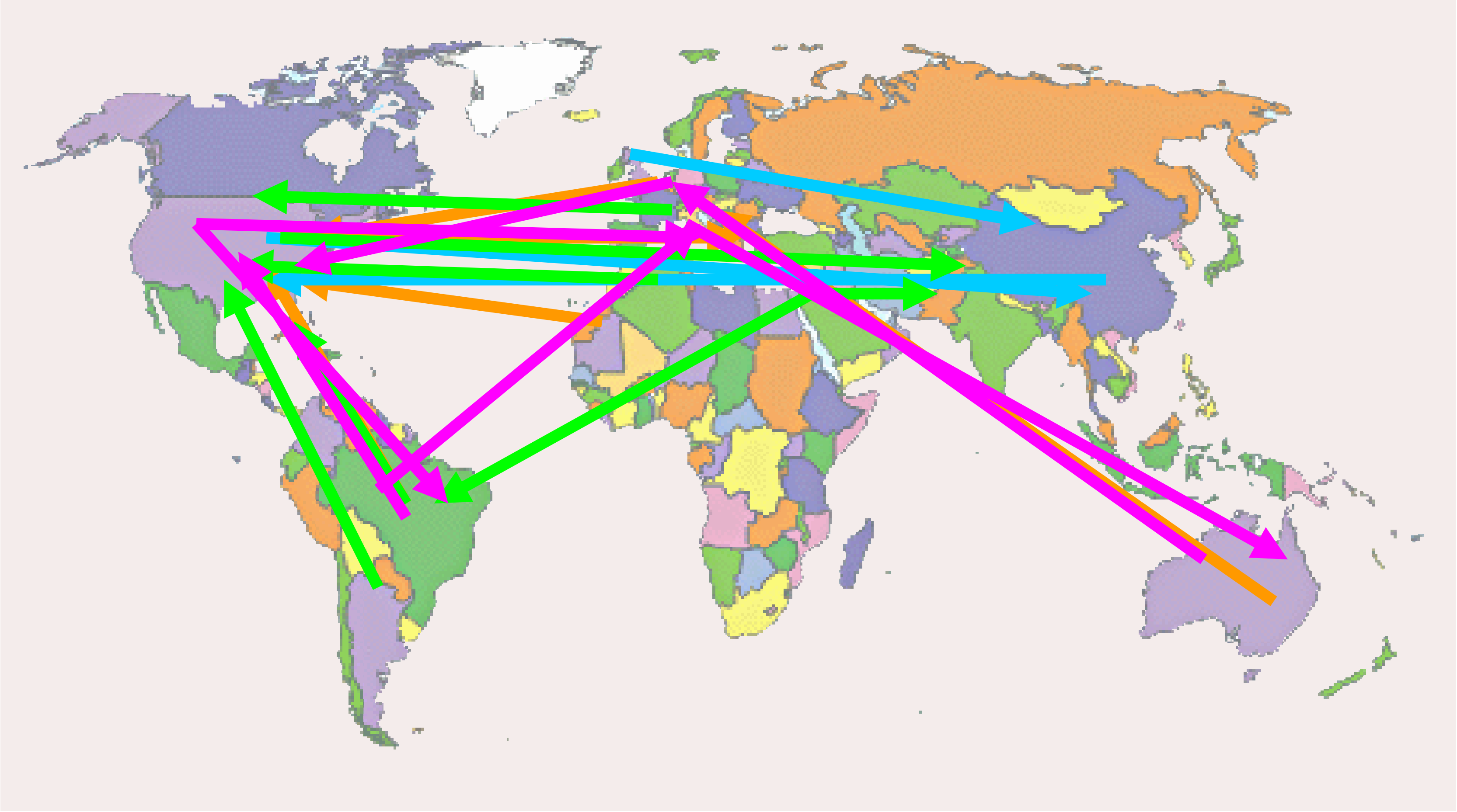
Iraq war related

Code red release related

Palestine-Israel related

No-Global related

Zone-H.org



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

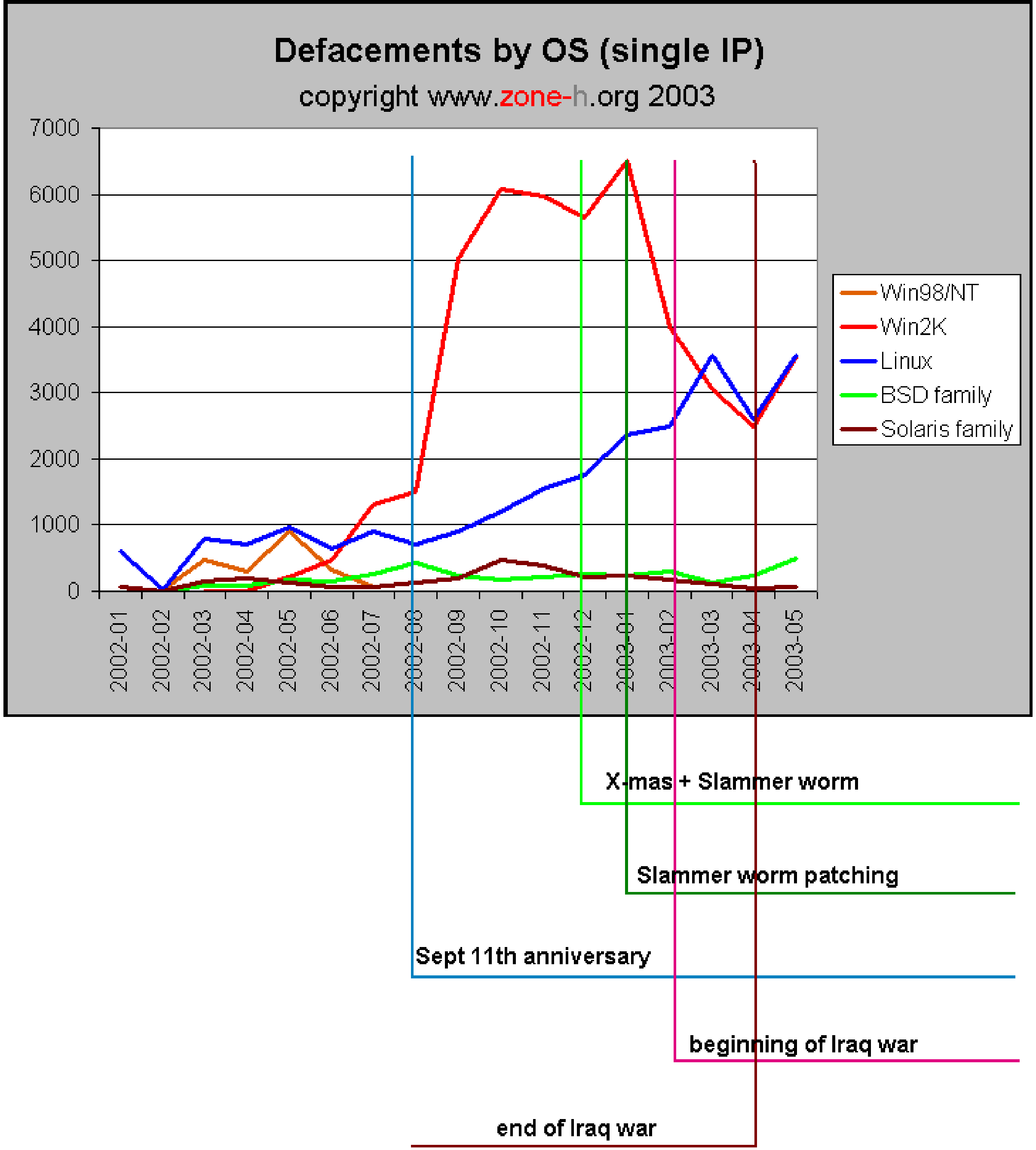
CYBER-PROTESTS ARE CONVENIENT BECAUSE:

- 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

Zone-H.org



X-mas + Slammer worm

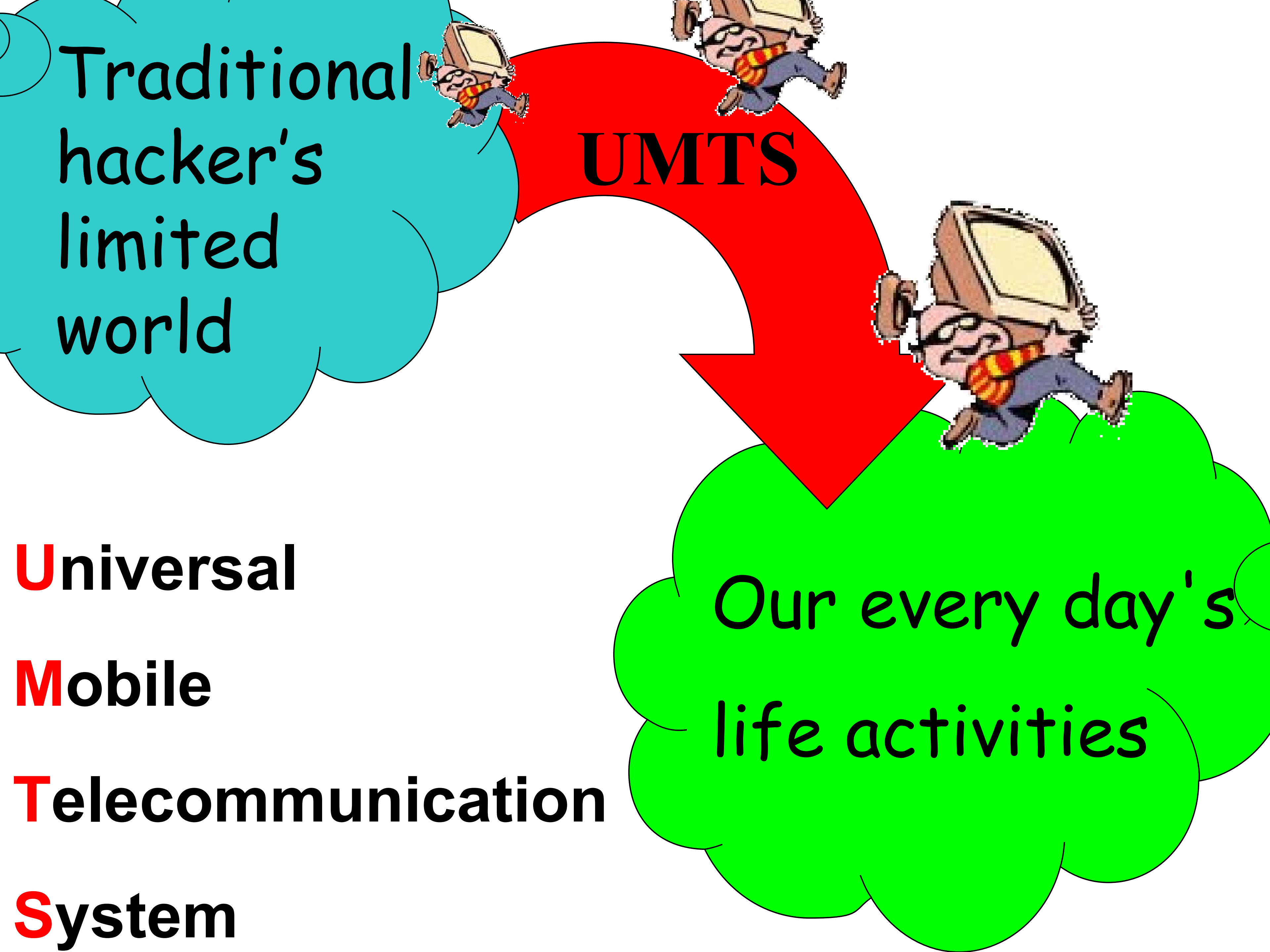
Slammer worm patching

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

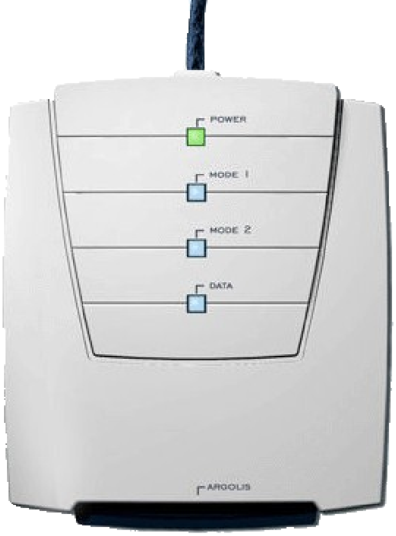
- Videoconference
- Full multi-media platform
- Data bank
- Office files
- Mobile computing
- Web browsing

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

smartCARD
7158 2084 4503 9283
SANDY TAYLOR 12/99

+


POWER
MODE 1
MODE 2
DATA
ARGOLIS

+

DELL

+

Microsoft®
Windows®
Powered

+

INTERNET

+

ZyAIR B-100
ZyXEL

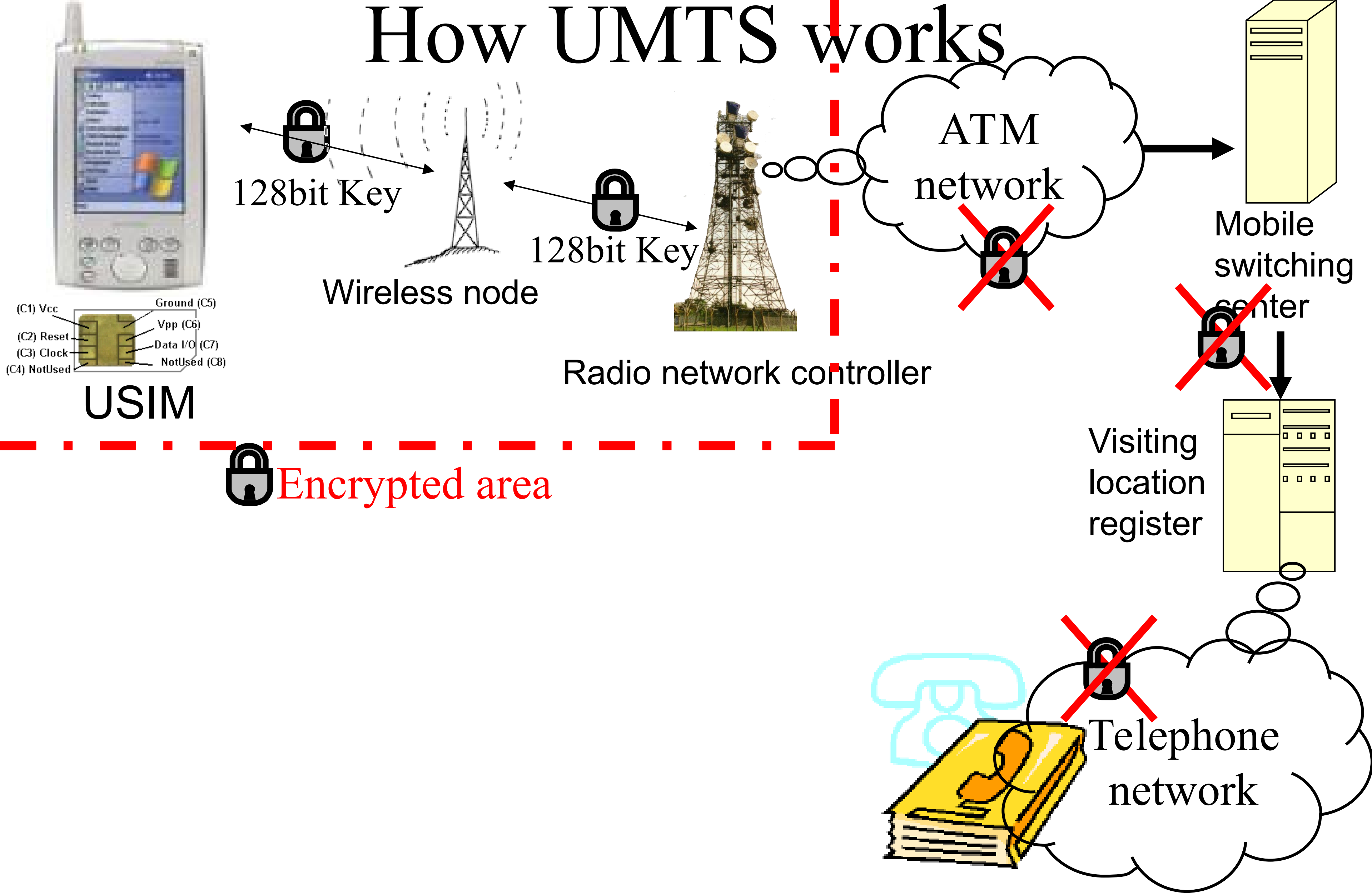
+

=

SAMSUNG
Start
Friday, October 18, 2002
Owner: George Jiang
Eva's Birthday
Team Meeting
Lunch w/Sam & Griffin
Quarterly Business Review
ActiveSync: 18 Unread messages
1 Active Task
www.cellular.it

Zone-H.org

How UMTS works



128bit Key

Wireless node

128bit Key

Radio network controller

ATM network

Mobile switching center

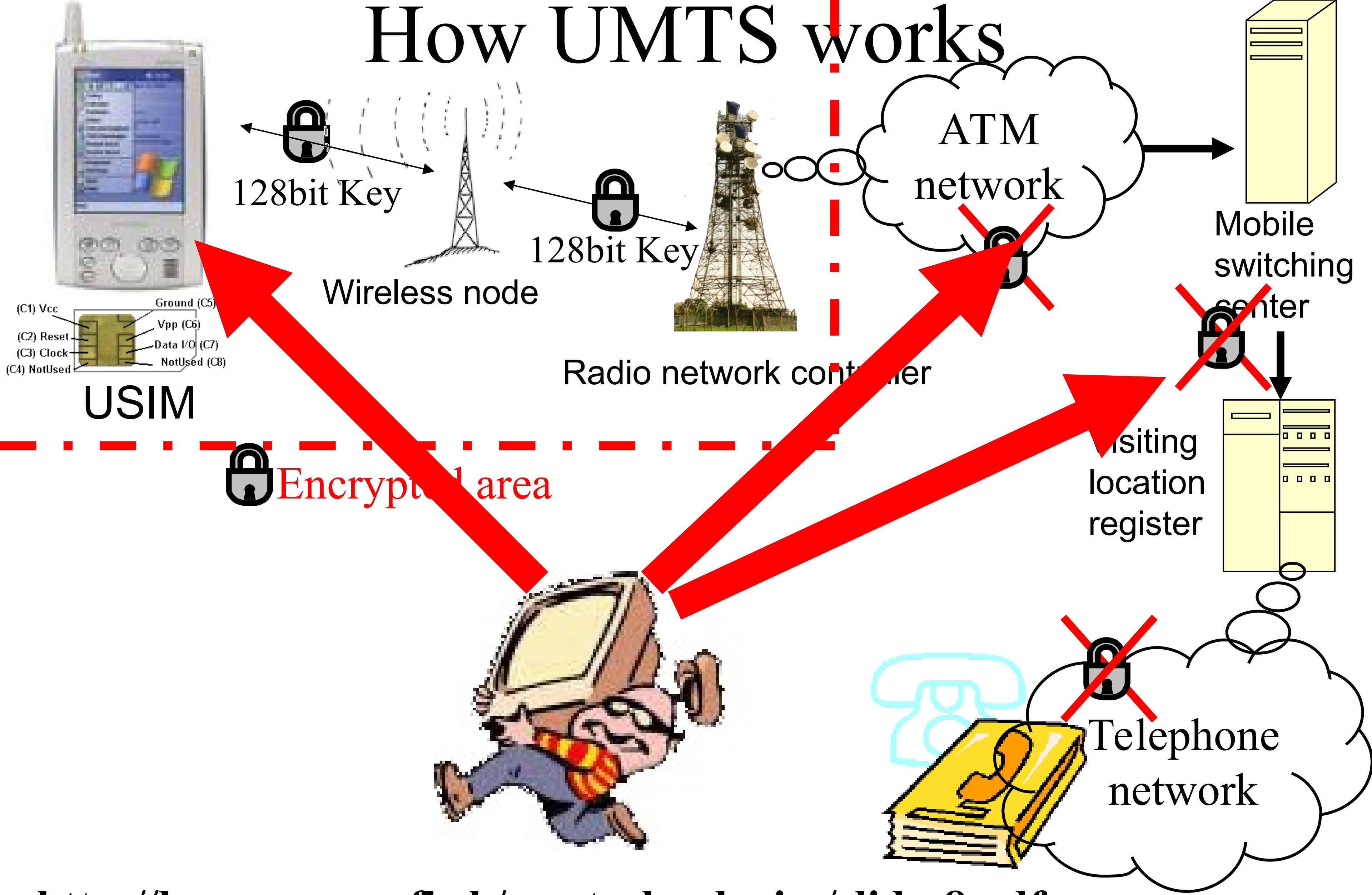
Visiting location register

Telephone network

USIM

Encrypted area

How UMTS works



USIM

128bit Key

Wireless node

128bit Key

Radio network controller

ATM network

Mobile switching center

Visiting location register

Telephone network

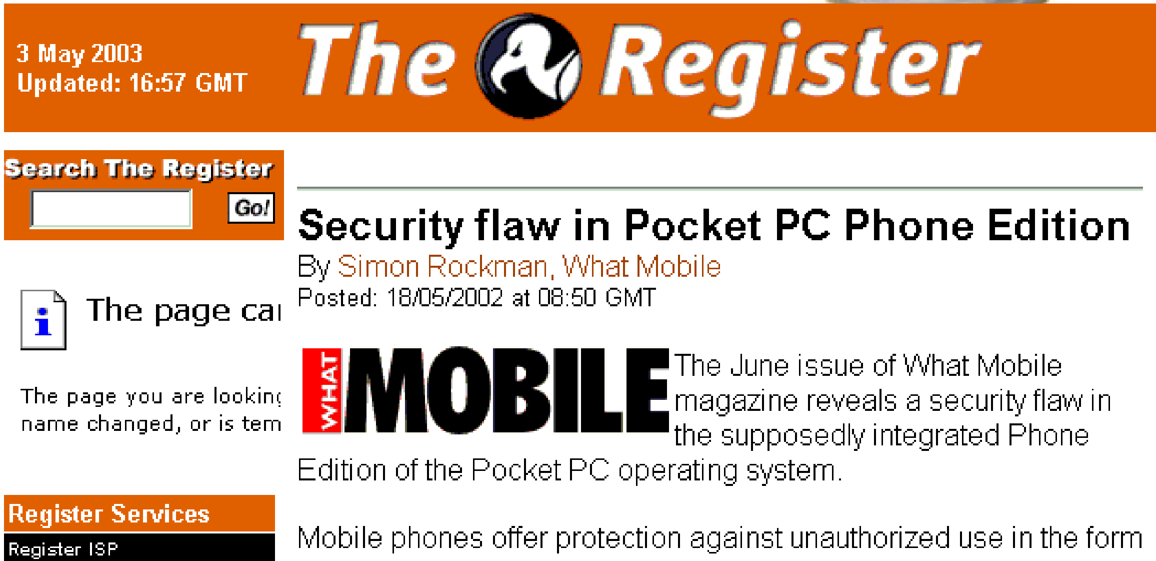
Encrypted area

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

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



3 May 2003
Updated: 16:57 GMT

The Register

Search The Register

Go!

The page ca

The page you are lookin
name changed, or is tem

Register Services

Register ISP

Security flaw in Pocket PC Phone Edition

By Simon Rockman, What Mobile
Posted: 18/05/2002 at 08:50 GMT

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.

Mobile phones offer protection against unauthorized use in the form

Zone-H.org

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

Zone-H.org

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

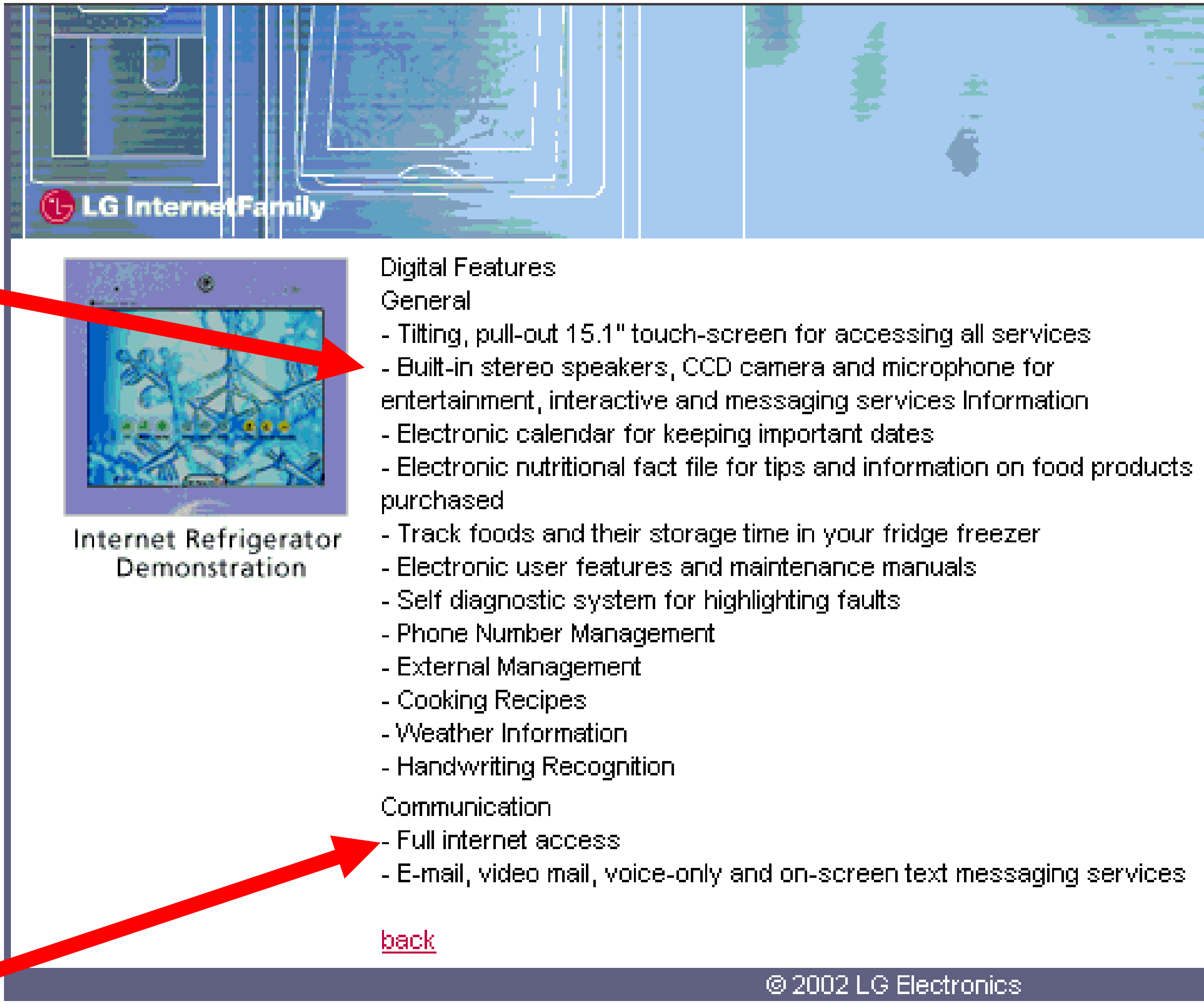
- http://www.tutorgig.com/searchtgig.jsp?query=umts (several tutorials)
- http://www.ericsson.de/downloads/pressenews/praesentation_cornelius_boylan.pdf
- http://lasecwww.epfl.ch/newtechnologies/slides8.pdf (excellent paper)
- http://www.sans.org/rr/paper.php?id=253
- http://www.pocketpcdn.com/
- http://www.itsx.com/pocketpc/BH-AMS-2003-itsx.ppt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

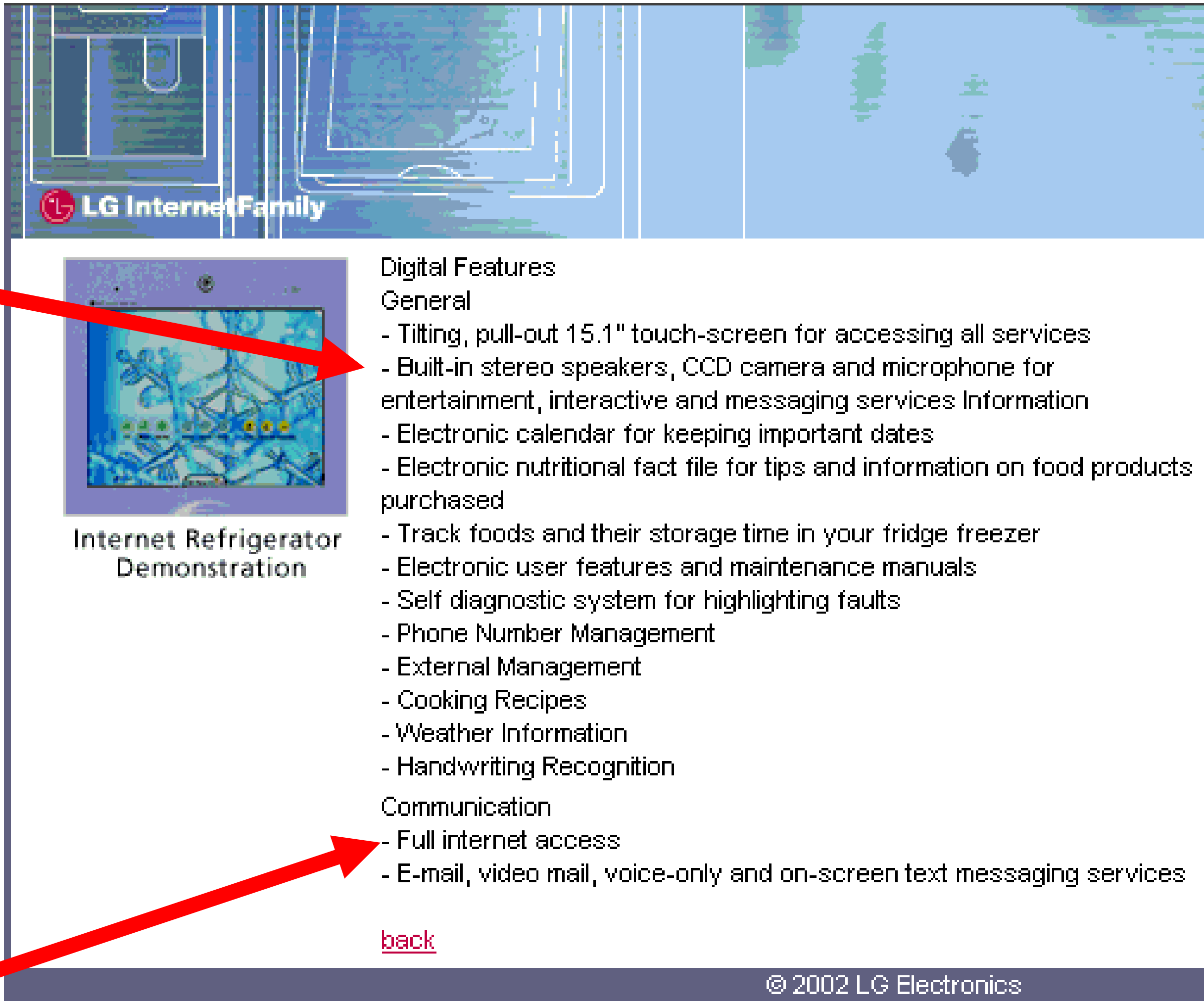
- Full internet access
- E-mail, video mail, voice-only and on-screen text messaging services

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



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 Information
- 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

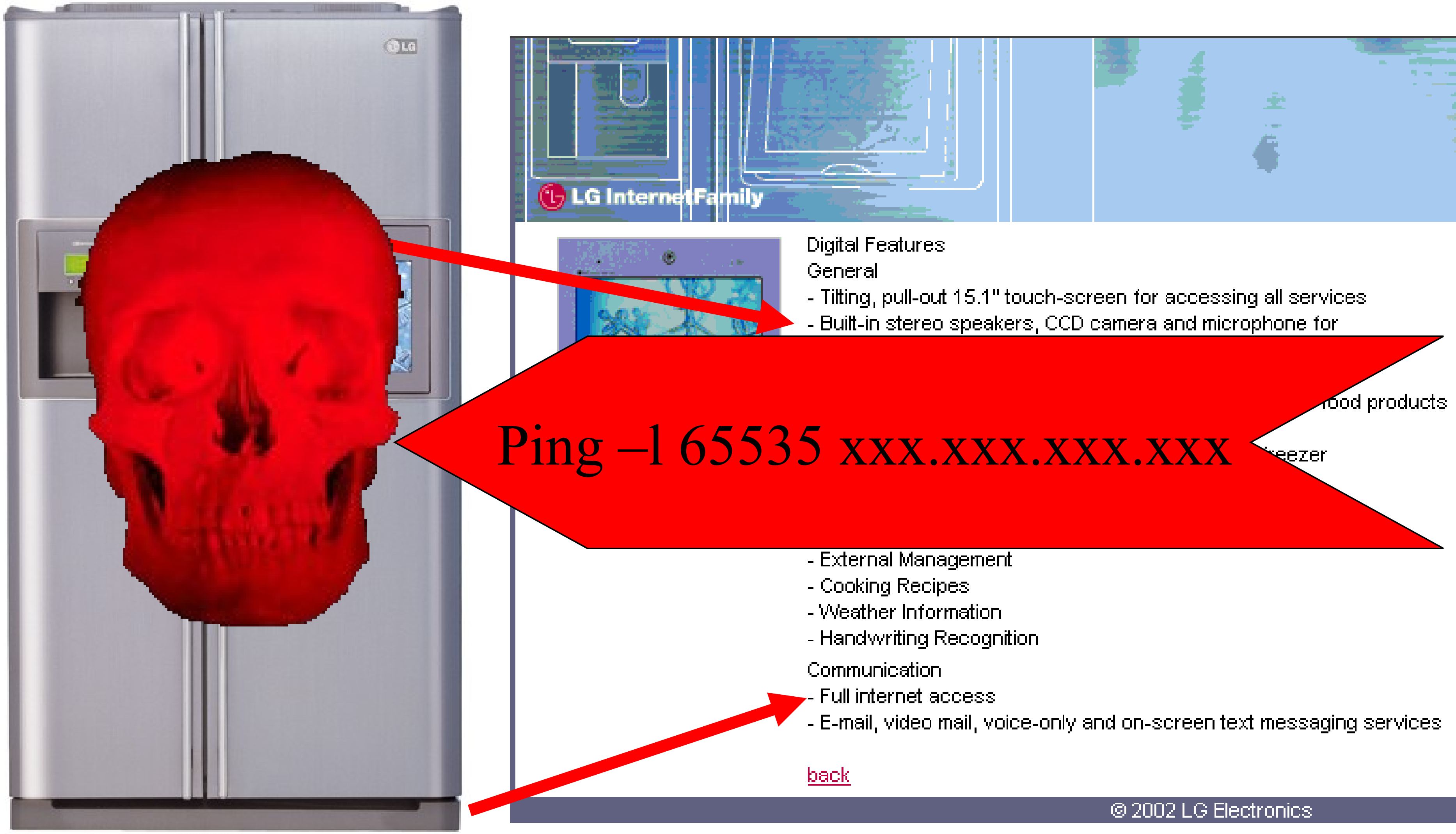
back

© 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



Digital Features

General

- Tilting, pull-out 15.1" touch-screen for accessing all services
- Built-in stereo speakers, CCD camera and microphone for

ood products

eezer

- 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

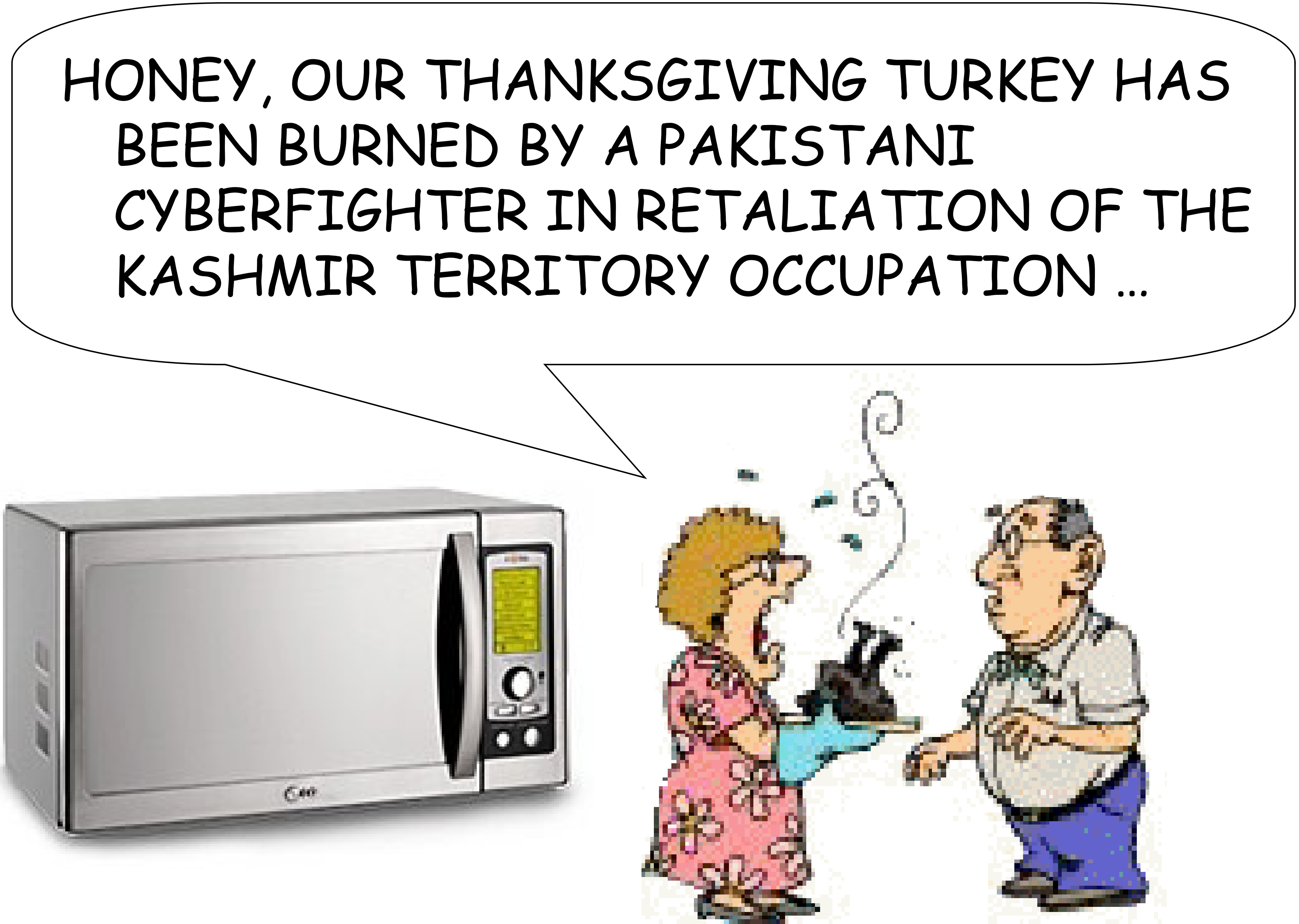
© 2002 LG Electronics

Ping –l 65535 xxx.xxx.xxx.xxx

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 !!!