






RedIRIS's Works in progress

francisco.monserrat@rediris.es
FIRST TC, Buenos Aires, 5 Oct 2005



- ☐ PGP related stuff
- ☐ Malware recollecting

<http://www.rediris.es/app/pgplist>

❑ Small script to setup GPG Mailing from /etc/aliases

- Sender verification is done from the PGP key instead of the mail address, posting is could be only done from members
- Incoming mail must be encrypted & signed to the mailing list address
- Outgoing mail is encrypted in separate mails to each of the list members

❑ All the configuration is handled from a separate file so, it's quite easy to have separate mailing list in the same server

❑ Current uses:

➢ Password and sensible information distribution

❑ Future work: Integrate with crypto-card to store private key **red.es**

<http://www.rediris.es/pgp/firmaweb>

❑ Why sign a web page ?

❑ Allow to publish information that could be checked against modification after browsing

❑ User can download the pages and check if the text, (HTML) has not been modified. Wget -O - <http://www.rediris.es/cert> | gpg

❑ The idea was to build a page, and use the remarks feature of HTML to store the signature.

❑ Most of IRIS-CERT, <http://www.rediris.es/cert> are PGP signed, you can browse the code to see how it was done

❑ Currently integrated in our web publishing system

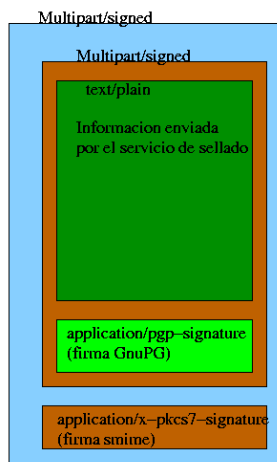
❑ Future Work: Automatic verification (FireFox plugin ?)

Problem: How to employ S/MIME and PGP signed messages at the same time.

❑ Needed for a document registering system , mail notary placed at RedIRIS , <http://www.rediris.es/app/sellado>

❑ Solution, Use Multipart/MIME messages, with both kind of signatures:

- SMIME enabled clients would process the signature and show it
- PGP/MIME messages are processed only in PGP enabled clients
- You can use old common PGP plain signed messages instead of PGP/MIME



Verification was tested and works:

- ❑ Netscape (SMIME)
- ❑ Netscape + Old plug-in (PGP)
- ❑ EXMH (PGP)

..

And other Unix programs for PGP

New generation honepots ?:

- ❑ <http://www.mwcollect.org> (Unix/ cygwin)
- ❑ Multipot, <http://labs.iddefense.com> (Windows)

Simulate vulnerabilities in common windows services (445, etc)

- Simulate a common exploit
- Got the shellcode and compare with a database of them
- Parse the information and download the binary

Very good to obtain bots and worms trying to attack your network

Problem: recollect attacks directed only to the IP address of the sensor

• We have most of the NetBIOS traffic blocked at the backbone , so no worm is attacking the collector

• Why not redirect all the traffic (AS766) to this collector ?

This could be useful to know the different bots and also detect new shellcodes and exploits

Now::

Redirecting traffic from one of connections (Spanish Exchange Traffic) to our office network only (3 C classes)

Result

- More than 1000 worms /bots downloaded every day
- Most of the files are the same MD5 checksum

Evolution

☐ Redirect the traffic:

- From all our external links
- To all the IP addresses in AS766 network (~ 20 different B class)

☐ Set up a automatic (new binaries) notification

☐ coordination with binaries analyzing project