Minutes of the Second Meeting of QUESTNet Security Emergency Response Team

Date: 17 November, 1992, 14:30

Duration: 2 hours

Present: Alan Coulter (UQ)
Geoff Dengate (GU)
Sid Duffy (QUT)
Marek Krawus (GU)
Rob McMillan (UQ)
John Noad (QUT)
Graham Rees (UQ)
Narelle Stone (GU)
Wilber Williams (UQ)

Apologies: George Michaelson (UQ)
Paul Riethmuller (Sun)
Greg Watson (GU)

1.0 Events Since the Last Meeting

1.1 Safe Machine

RM has been building a safe machine. This machine uses VMS 5.5-2 as it's operating system, and will be used for policy development and event logging.

1.2 Patch Application

Each site has received patches from Sun. The patches arrived on tape, with further patches mailed. It appears that the supplied patches were not the latest patches available. Furthermore, the supplied documentation was confusing and inadequate. All three institutions have spent varying amounts of time attempting to correctly interpret the documentation, and build fully patched operating systems. During this process a machine which QUT was using was cracked.

Problems also existed in matching patches against each other and interpreting the documentation. Other problems encountered were multiple patches for single images or command files, which is not neat, as well as different patch configurations for different hardware. Furthermore, the conventions for patch documentation and installation vary from patch to patch. This increases the difficulty in interpreting the documentation and applying the patch.

1.3 Mailing Lists

sert@cc.uq.oz.au has been enrolled in Sun's Customer Warning List.

1.4 Cracking Activity.

QUT has experienced further cracking activity. They have used bridges to segment labs from the world.

1.5 Tools

Phil Grimshaw from Sun had forwarded to each institution a report on similar incidents at the University of Texas. Because of these incidents, tools had been developed at this site for repelling crackers, and analysing attacks on machines.

QUT have down loaded these tools and found them to be quite useful. They are written for SunOS 4.1.1 and 4.1.2, but can be adapted for 4.1.3 with some modifications. They can possibly be ported to Ultrix also. SD will continue this work.

1.6 Mailing Lists

Mailing lists amongst the three institutions have been established. sert@cc.uq.oz.au explodes to gu-sert@gu.edu.au, qut-sert@qut.edu.au and uq-sert@cc.uq.oz.au. These lists have been used regularly since establishment. SD has developed a proposed expansion of these lists (incorporating new lists). After he has refined it, he, NS and RM will implement his proposal. This will allow for information dissemination via "private" and "public" channels.

These channels will be used for discussion of incidents and business, as well as distribution of warnings and patches.

WW will prepare some information on possible encryption strategies for information transmitted along "private" channels.

2.0 Dialup

GU has disabled anonymous dialup, and is in the process of implementing a dialback modem scheme. This scheme will improve security, but at a significant cost.

UQ has used Kerberos to implement a password protection scheme on dialup. There are internal modems on UQNet not under control of the Prentice Centre that are not password protected. This issue will be dealt with some time in the future.

QUT has a large number of modems (as do the other institutions), and is considering Kerberos for protecting dialup.

The issue of undergraduate access to AARNet was raised. QUT only allows such access if it is specifically requested by an academic on behalf of the student. Such access is available only via the VAX Cluster. UQ has more liberal rules, where access is available via individual departments.

Policy on this issue will be dealt with in future meeetings.

3.0 Mechanism C Grant

Grants for collaborative projects have not yet been announced. The application for an AARNSERT body has not yet been rejected, so there is some cause for cautious optimism. It is expected that the result of this application should be known by the next meeting.

4.0 Further Action.

4.1 Vendor Supplied Patches

The three directors will canvass opinions from other computer centre directors around the country, and then meet with Sun representatives with a view to alleviating the patch problems outlined in Section 1.2. They will require that Sun supply a patch list to take each SunOS version 4.1.1 through 4.1.3 to a known level of conformance. If this is unsuccessful, a boycott of Sun products is a possibility.

It is proposed to meet with Noel Pettit of Sun on Monday November 23.

In the meantime, each institution will continue work on compiling patch lists - one SunOS version per institution. This information, once compiled by an individual institution, will be shared with the others. Each package will have all patched files required, plus documentation describing what patches were applied, and which files were affected.

4.2 Machine Lists

No site has had a chance to generate local machine lists as yet. This will be done, but can possibly wait until the patch problem is cleared up.

4.3 Mailing Lists

SD to refine his proposal. SD, NS and RM to implement when possible. WW to prepare information on possible encryption strategies.

4.4 Next Meeting

The next meeting will be held on November 30, 1992 at 10:00 am. This immediately preceeds the AARNet NetworkShop for 1992.