From: [redacted]
Sent: 19 November 2009 17:15
To: [redacted]
Cc: [redacted]
Subject: Preliminary report on CRU/UEA hacking incident

Attachments: CRU stolen files - preliminary investigation

[redacted]

Below is a preliminary report on investigations so far and actions taken. I'll leave it to you to forward as you feel appropriate.

<u>CRU/UEA hacking incident - preliminary investigation and actions taken</u>

Summary of what has occurred
From the information presented so far and the preliminary investigation already carried out by [redacted] (see attached) , it appears that the 'stolen' files are of 3 types:

- Programs and datasets from CRU NFS mounted storage disks
- Documents from desktop PCs obtained either via the CRU PC Backup Service (most likely route), or directly from the PCs
- Emails, again either obtained from folders on the key individuals PCs or from the CRU Backup Service

A list of all files has been received from the RealClimate website administrator, but the contents of the emails involved is still awaited (this could aid further investigation).

The most likely routes for the hacking/theft appear to be via

- Compromise of [redacted] UEA account password and hacking of the cruweb1 web service, allowing access to the CRU PC Backup Service. Evidence in [redacted] report indicates that his account ([redacted]) was used without his knowledge to hack into the backup service and download files backed up from [redacted] PC.
- Possible hacking into the PCs of key UEA individuals e.g. [redacted] [redacted] [redacted]

The most likely route by which [redacted] password was compromised is by an individual using a UEA IT account to obtain a copy of the encrypted NIS password (NIS hash) for his account and then using cracking tools/techniques to derive the actual password from this. [redacted] password followed strong password security advice, but readily available cracking tools and powerful computers mean that even strong passwords can be cracked in relatively short periods of time. The individual concerned may have been a member of UEA, have given their account details to an external party, or their password obtained via a phishing attempt, although the specific nature of this hacking incident makes the latter seem unlikely.

This access route to UEA NIS passwords has been known for some time and plans are in hand to close it down, but this cannot be done until all UEA workstations cease to authenticate via this route and are migrated to Active Directory/ VAS authentication services. It is now only SCI faculty systems that are using NIS for authentication and it had already been agreed that CRU/ENV and MTH systems will move away from this by Xmas 09. Once all SCI systems are migrated off of NIS, the route to obtaining NIS hash passwords and being able to apply cracking tools to them will be closed.

Actions agreed

- [redacted] will temporarily close down the CRU PC Backup Service whilst further investigation takes place (already done). Note, [redacted] had already taken action to close a security loophole by disabling the administrator rights that had been assigned to his [redacted] account and by setting a new secure password on the account, but is still not fully satisfied that all is secure.

- [redacted] and [redacted] will use the administrator account to inspect the event logs stored on the PCs of the key individuals referred to earlier, to see if there is any evidence of hacking (this has now been done and nothing of interest has been found).
- [redacted] will organise a password change for all ENV staff and postgraduate accounts ***[Exempted pursuant to s.31(1), FOIA]*** this to be advertised to those affected by [redacted]. This has been arranged to happen on Friday 20/11/09.
- [redacted] will check whether spare disks are available to enable cruweb1 to be rebuilt securely from scratch, the old disks being kept in ENV's fire safe pending a decision on whether or not forensic investigation is required of these.

Decision/approval required on further actions

There is evidence of a possible sophisticated hacking of cruweb1, but investigation as to how this has been achieved would required a detailed forensic investigation of the system which is outside the skill range of both CRU IT support and ITCS staff. It is possible that a detailed forensic investigation of cruweb1 undertaken by a suitably qualified external agency might uncover more information and identify the exact route that was taken to hack into this, thus aiding prevention of such in future. This requires a decision by senior management as to whether this incident is serious enough to warrant such further investigation and cost.

Apart from the actions already listed above, there are no further specific actions that are recommended at this point in time. However whilst investigation is ongoing we think it advisable that as few individuals as possible are involved in the investigation and that ad-hoc investigation and conjecture is kept to a minimum.

[redacted]

[redacted]
IT and Computing Service
University of East Anglia
Norwich
NR4 7TJ
Tel: [redacted]
Fax: [redacted]
Email: [redacted]

Working days: Monday to Thursday
[redacted]

Information Services

CRU stolen files - preliminary...

Preliminary investigation of stolen CRU files

The files stolen from CRU fall into three categories:

1) Programs and datasets from the CRU NFS disks
2) Documents from desktop PCs
3) Emails

We have yet to determine the details of the email files. There are about 1000 files with numerical filenames in a directory called “mail”. [redacted] [redacted]where the files were posted, has viewed them to confirm they are CRU emails and will be sending them to us.

It is clear that items in category 1 could have be collected by anyone with access to a UEA account, as the CRU disks are mounted on a variety of machines including uealogin1 and, while we do need to allow access to non-CRU people for certain files, far too many have had general read-permission. Our immediate action will be to change all directory permissions on all CRU NFS disks to limit access to CRU staff only, then relax individual items later as needed. I will also devise an automated system to regularly check which directories are accessible.

Category 2 is more worrying, as it implies direct access to staff PCs. Although CRU PCs do not use the UEA Staff Desktop, we run the recommended McAfee virus scanner and updates are promptly applied. Additionally, we regularly run Malwarebytes Anti-Malware as a “belt & braces”. There could of course be a direct attack that goes undetected but that would be fairly sophisticated.

There is one additional place where all CRU desktop PC files are located. We run a backup server cruback3 using the BackupPC package. A small server program runs on each PC, to which cruback3 connects daily to back up the disk. Users can connect to cruback3 using a web-server interface (available only within UEA) using their NIS username and password, which then allows them to retrieve files that they may have accidentally deleted.

Because it is clearly a security pinch-point, cruback3 does not allow logins based on NIS or VAS but only with local accounts. NIS data for CRU accounts (plus a few others who use the Backup Service) is manually extracted from the NIS database on an occasional basis and transferred to cruback3 for use with Apache's authentication mechanisms.

I inspected cruback3's webserver error logs and found some suspicious entries:

```
[Mon Oct 05 01:20:33 2009] [error] [client 139.222.104.250] user backuppc not found: /backuppc/
[Mon Oct 05 01:21:28 2009] [error] [client 139.222.104.250] user backuppc not found: /backuppc/
[Mon Oct 05 01:26:40 2009] [error] [client 139.222.104.250] user [redacted] not found: /backuppc/
[Mon Oct 05 01:27:15 2009] [error] [client 139.222.104.250] user [redacted]: authentication failure for "/backuppc/":
Password Mismatch
[Wed Oct 07 05:48:34 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 05:48:34 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 05:58:14 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 05:58:14 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 05:58:14 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 05:58:14 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 05:58:14 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 05:58:14 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 06:37:58 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Wed Oct 07 06:37:58 2009] [error] [client 139.222.104.250] Premature end of script headers: index.cgi
[Tue Sep 29 04:41:56 2009] [error] [client 139.222.104.250] File does not exist: /var/www/BackupPC
[Tue Sep 29 09:03:21 2009] [error] [client 139.222.104.250] File does not exist: /var/www/[redacted]
```

Inspecting the access log for those times revealed further oddities, all of which had in common that they were from cruweb1 using the Lynx text web-browser. Connections were made using username backuppc (which would have failed) then [redacted] ([redacted] whose PC is not on the Backup Service, so they would not have found any information) then finally [redacted] which is my username.

Although access to PC backups is limited to the PC's owner, the one exception to this is me as I need to be able to initiate and cancel backups and do other housekeeping. In retrospect I should have realised that this left the whole thing open if my password got hacked, and should have used another local account instead. I have changed the [redacted] AD password, and the local password on cruback3. I have also removed [redacted] from the Admin users in BackupPC.

Using [redacted] they attempted a number of obscure actions clearly intended to break BackupPC, and they downloaded one filetree:

```
139.222.104.250 - [redacted] [05/Oct/2009:03:25:32 +0100]
"GET /backuppc/?num=390&host=angara.cru.uea.ac.uk&share=Cdrive&fcbMax=2&action=Restore&fcb1=/Documents%20and
%20Settings&type=2&compressLevel=9 HTTP/1.0" 200 16384 "-" "Lynx/2.8.5rel.1  libwww-FM/2.14"
```

“Angara” is [redacted] PC. Backup number 390 is dated 29/7/2009 and would have been the most recent backup of his PC at that time ([redacted] so his PC was switched off and daily backups did not take place).

If the emails from RealClimate turn out to all be no later than 29/7 we can conjecture that they came from [redacted] PC backup. If they are later than that, we still need to find the vector.

This does not account for files from [redacted] PC, the most recent of which was dated 11/11. There are no log entries showing attempts to access his files (indeed, no machines other than angara).

The password for [redacted] was most recently changed in July along with everyone else's. It is not a particularly weak password (eight characters, mix of digits+lowercase+uppercase with no words in any language). I suppose if it were targeted and the hash had been obtained from NIS then it would not take forever to break : (10+26+26)^8 = 218 trillion combinations.

I assume that cruback3 itself was not hacked, as the logfiles have been left unaltered.

I assume that cruweb1 has been hacked, as there are no unexpected login entries around the 5/10. I have booted it to a LiveCD and run chkrootkit with no results, but as the rest of the attack seems to have been quite sophisticated I'm inclined to believe that it has been subverted. I intend to reinstall Linux from scratch once any further forensic examination has taken place.