

Remanence: The difficulty of deletion

4/5/2010

Administrative Announcements

- All discussion sections are cancelled tomorrow (4/6)



Oliver North may go down in history as the first government official snared because of incriminating information exchanged through e-mail.

Back in 1985, North was a Reagan administration official and a key figure in the Iran-Contra scandal, which involved secretly selling weapons to Iran to fund Nicaraguan rebels. The actions were illegal and North was convicted of three felony counts--which were eventually overturned on the theory that Congress had granted him limited immunity in exchange for his testimony.

What makes North a candidate for this gallery of rogues is that when the scandal broke in November 1986, he and John Poindexter began deleting more than 5,000 e-mail messages from White House computers. What they didn't seem to know is that backup tapes were kept, and investigators were able to reconstruct the correspondence.

Remanence on hard disk

- Deleting a file does not delete the file
 - ... even if you empty the Trash
 - Contents of file remain on disk; only the link from its containing directory is deleted
- A usability flaw: users might reasonably expect “delete” to mean “delete”, but it doesn’t
- Solution? Use a secure file delete program

Remanence on hard disk

- Formatting a drive does not delete the data on it
 - It just deletes the filesystem metadata
 - 2002 study bought & imaged 129 second-hand hard drives: 12 (9%) had been properly sanitized. 81 (63%) had deleted-but-recoverable files. 42 (32%) had credit card numbers. One was from an ATM; another had 3,722 credit cards.
- Solution? Use disk-wipe software (e.g., DBAN) that securely overwrites all sectors of the disk
 - Warning: on a modern disk, this can take days (!)

Remanence on disk

- If hard disk detects a failing sector, it automatically copies the data to another sector and remaps the sector (transparently)
 - This might cause sensitive data to remain on your hard disk long after you thought you deleted it
- Secrets stored in memory might get copied to disk during paging, or during suspend-to-disk
 - You think you deleted the secret from memory, but it still remains on your hard disk longer than expected

Remanence in memory

- What's wrong with this code?

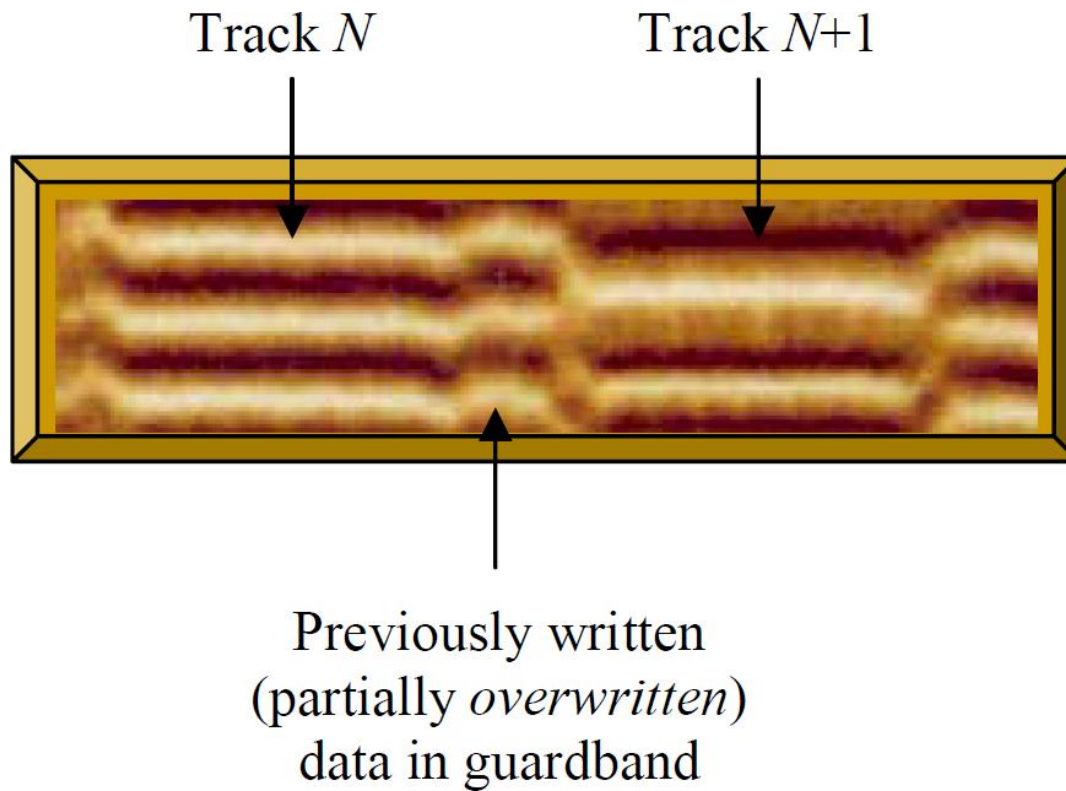
```
void f() {  
    char passwd[64];  
    if (getpass(passwd) == 0)  
        dostuff(passwd);  
    memset(passwd, 0, sizeof(passwd));  
}
```

- Answer: The compiler might optimize the memset() away!

Remanence in hardware

Recovering data from hard disks

- When overwriting a track, the head may not be perfectly aligned both times, leaving remnants of the “deleted” data



DRAM memory

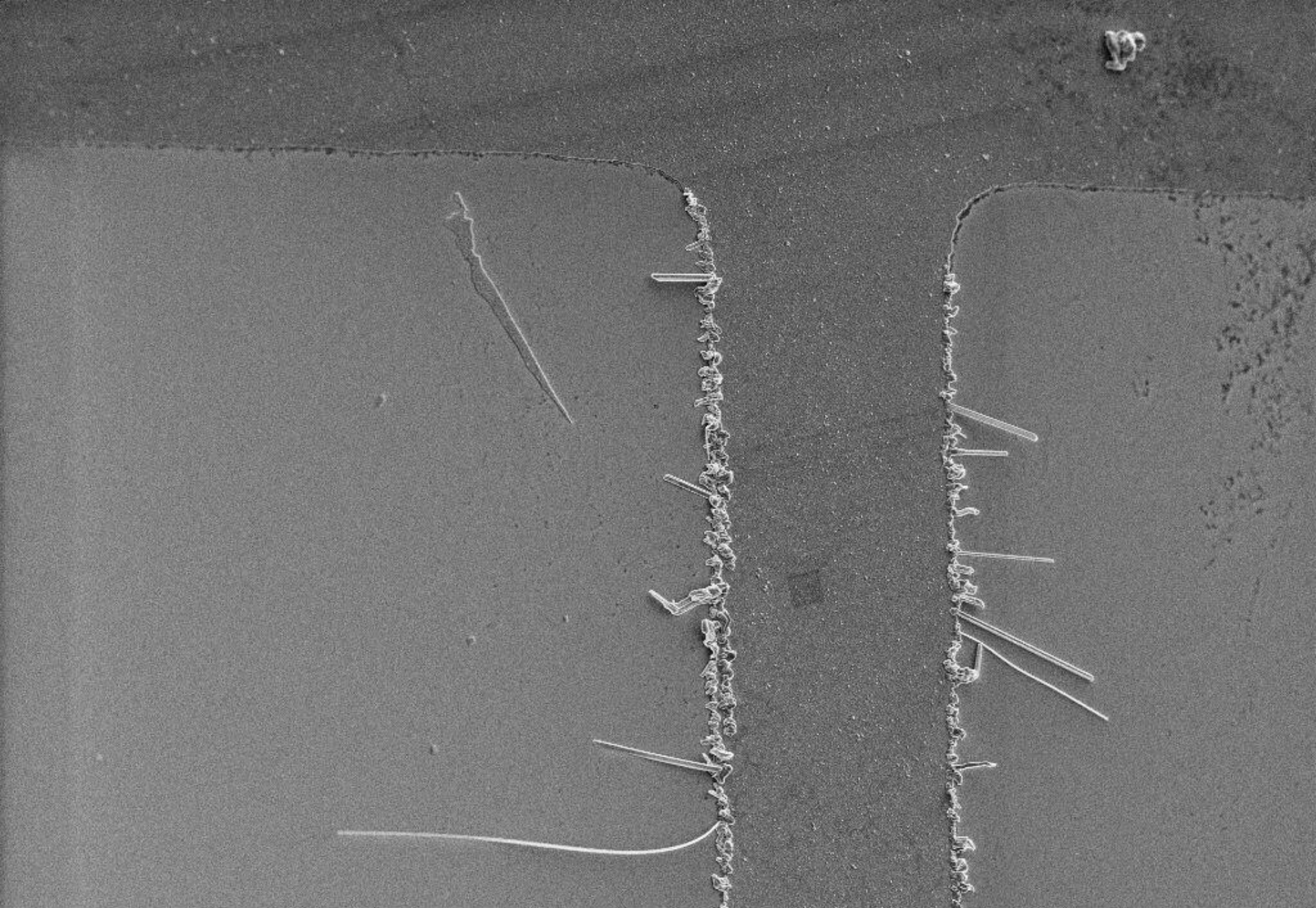
- DRAM cells need to be refreshed, or else they lose their memory of what was stored
 - System automatically refreshes them, e.g. every 90 ns
- What if DRAM cell isn't refreshed?
 - Turns out data can remain for 2-35 seconds
 - At lower temperatures, data lasts longer






Implications

- Attacker with physical access to your laptop can recover any secrets stored in memory
- Example: You use disk encryption software, which stores crypto key in memory. You set a strong password and rely upon OS to prevent access to this memory. You engage a screenlock, or suspend-to-RAM, and walk through security checkpoint.
 - Attacker who steals your computer can freeze your RAM chip, then reboot via USB (or: freeze chips, remove them, place them in his own laptop), and learn your crypto key, even though he doesn't know your login password.



EHT= 5.38 kV
10μm 

WD= 8 mm
Photo No.=1095

Mag= 1.00 K X
Detector= SE1

Defenses?

- When crypto keys are stored in memory, periodically flip all their bits

Flash memory

- Each bit of flash storage can only be written a limited number of times (e.g., 10,000x); after that, it breaks down and no longer works.
- To address this, many flash subsystems use “wear levelling”.
- But wear levelling creates its own risks – it means that “overwriting” a file may not overwrite the data stored in flash, but may just overwrite a copy of the data.

The difficulty of redaction

NY Times publishes redacted document

June 18, 2000

Editor's Note:

The C.I.A.'s history of the 1953 coup in Iran is made up of the following documents: a historian's note, a summary introduction, a lengthy narrative account written by Dr. Donald N. Wilber, and, as appendices, five planning documents he attached. On April 16, 2000, The New York Times on the Web published the introduction and several of the appendices.

The Times has now decided to publish the main body of the text after removing certain names and identifying descriptions. The editing was done after consultations with historians who believed there might be serious risk that the families of some of those named as foreign agents would face retribution in Iran.

S E C R E T

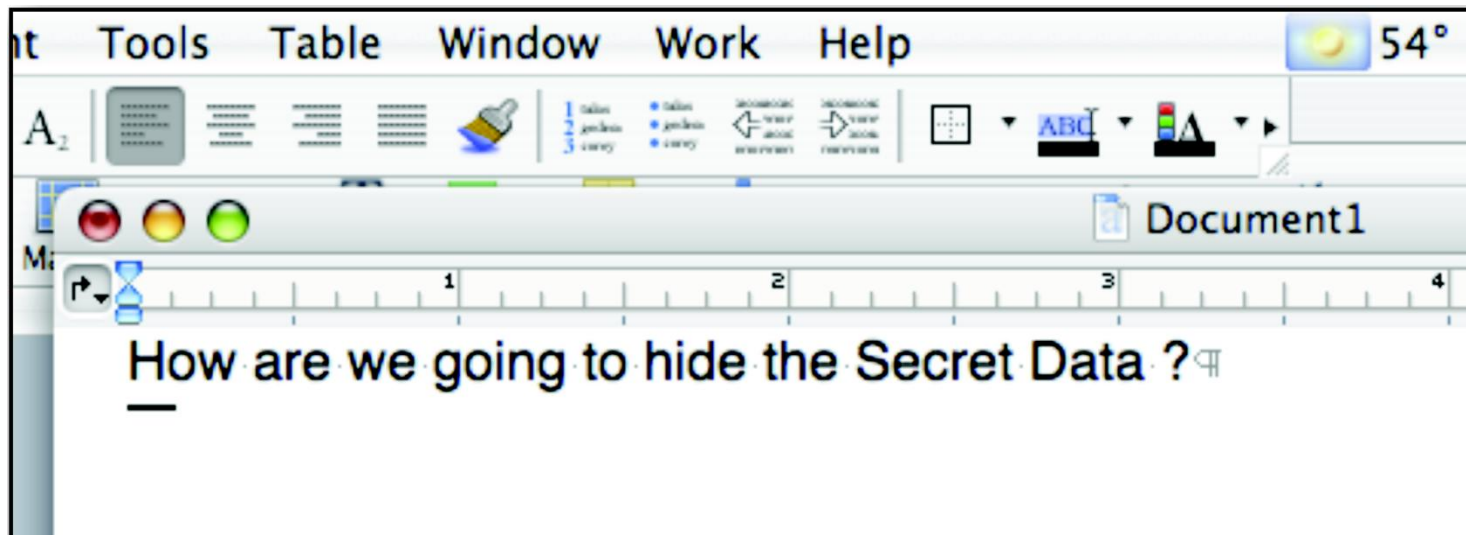
Ambassador Henderson and General McClure were out in the garden in front of the residency, and Roosevelt wore a path back and forth to reassure them that no Persians were hidden out in the compound, so that they could in all honesty so inform Mossadeq if the question were asked. The council of war went on for about four hours, and in the end it was decided that some action would be taken on Wednesday the 19th. As preparation for this effort, several specific activities were to be undertaken. In the field of political action, it was planned to send the Tehran cleric [REDACTED] to Qum to try to persuade the supreme cleric, Ayatollah Borujerdi, to issue a fatwa (religious decree) calling for a holy war against Communism, and also to build up a great demonstration on Wednesday on the theme that it was time for loyal army officers and soldiers and the people to rally to the support of religion and the throne. In the field of military action, support from outside of Tehran seemed essential. Colonel [REDACTED] was sent off in a car driven by a station agent (US national Gerald Towne) to [REDACTED] to persuade Colonel [REDACTED] commanding officer of the [REDACTED] garrison, to declare for the Shah. Zahedi, with Carroll, was sent to Brigadier General [REDACTED] at [REDACTED] with a similar request. Through station facilities these

Ambassador Henderson and General McClure were out in the garden in front of the residency, and Roosevelt wore a path back and forth to reassure them that no Persians were hidden out in the compound, so that they could in all honesty so inform Mossadeq if the question were asked. The council of war went on for about four hours, and in the end it was decided that some action would be taken on Wednesday the 19th. As preparation for this effort, several specific activities were to be undertaken. In the field of political action, it was planned to send the Tehran cleric [REDACTED] to Qum to try to persuade the supreme cleric, Ayatollah Borujerdi, to issue a fatwa (religious decree) calling for a holy war against Communism, and also to build up a great demonstration on Wednesday on the theme that it was time for loyal army officers and soldiers and the people to rally to the support of religion and the throne. In the field of military action, support from outside of Tehran seemed essential. Colonel [REDACTED] was sent off in a car driven by a station agent (US national Gerald Towne) to [REDACTED] to persuade Colonel [REDACTED] commanding officer of the [REDACTED] garrison, to declare for the Shah. Zahedi, with Carroll, was sent to Brigadier General [REDACTED] at [REDACTED] with a similar request. Through station facilities these

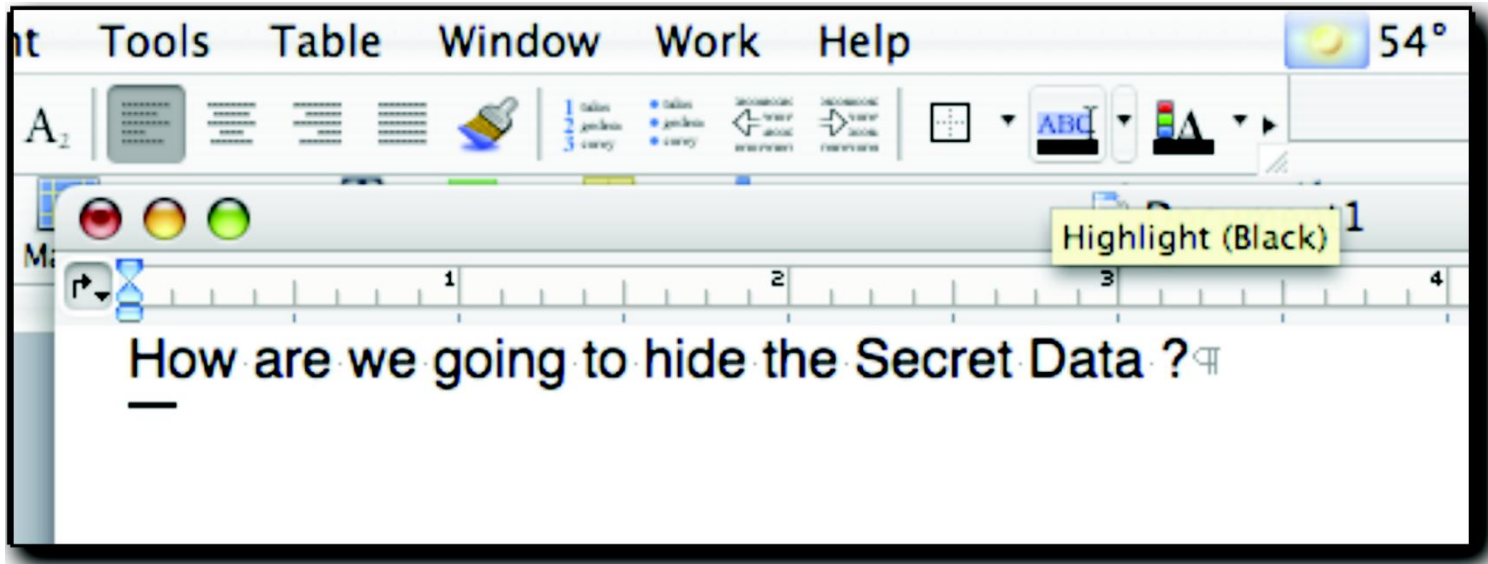
Ayatollah
Behbehani

Farzanegan

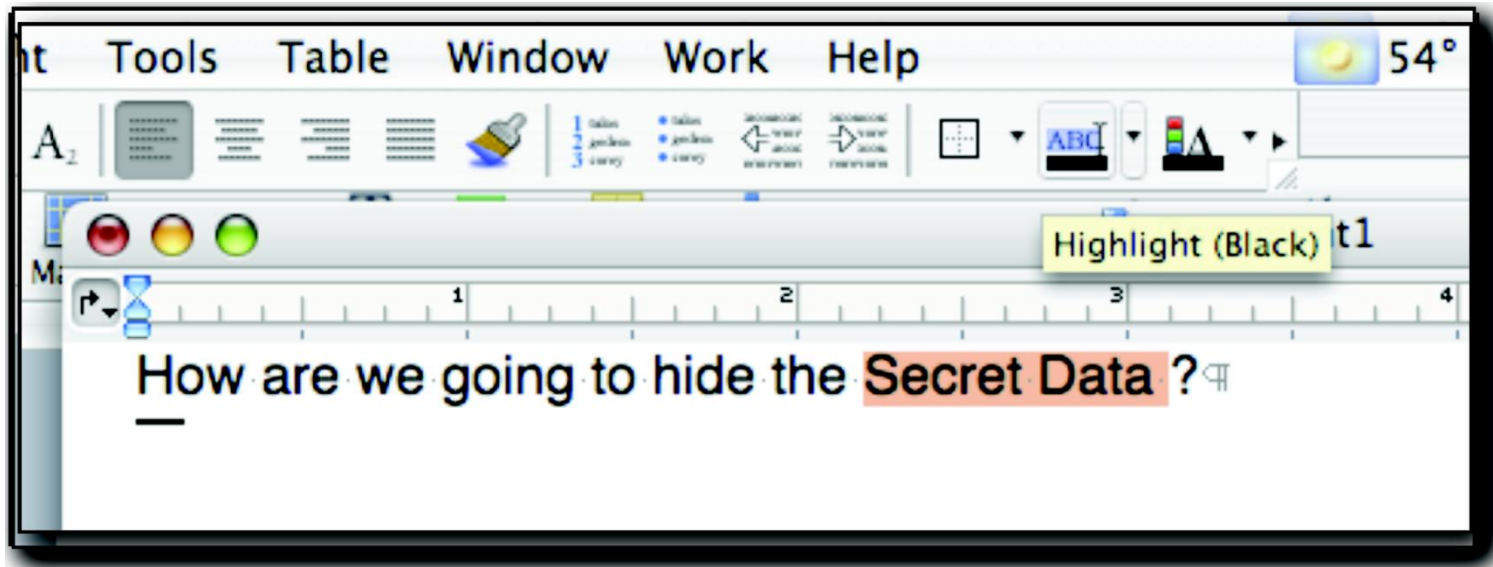
Redacting in Microsoft Word



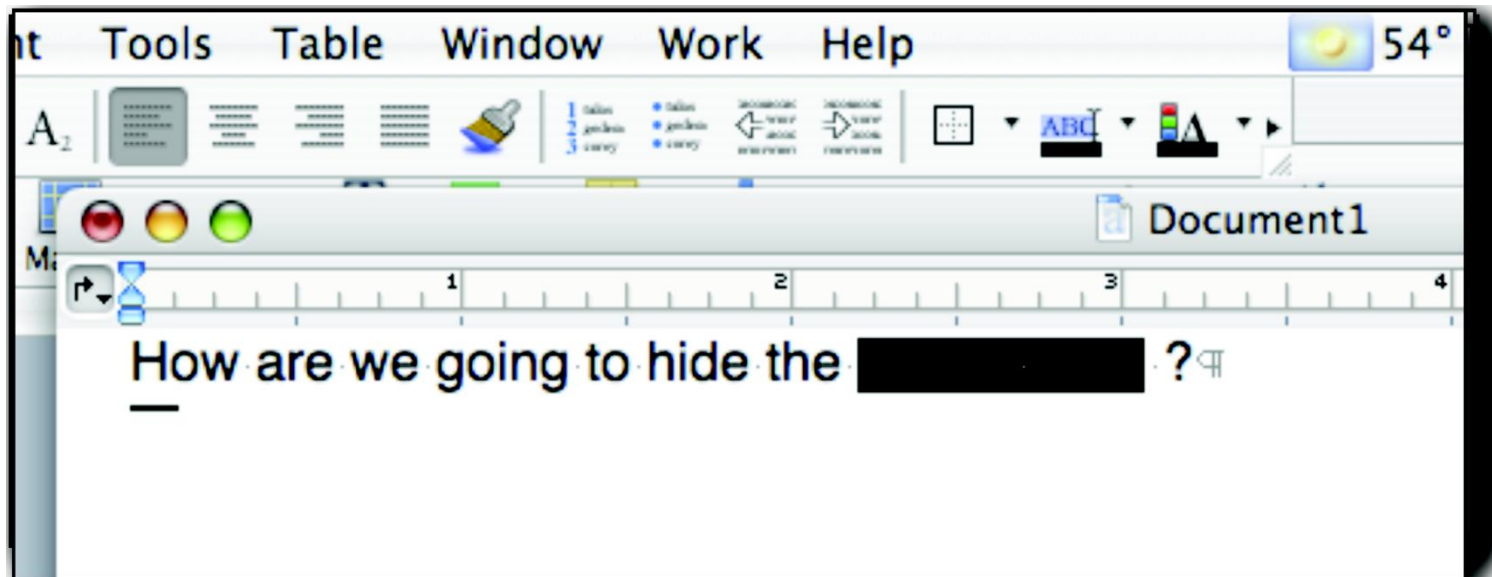
Redacting in Microsoft Word



Redacting in Microsoft Word



Redacting in Microsoft Word



This doesn't work!

When the Word document is exported to PDF:



This is a usability flaw in Microsoft Word (and in some PDF editors, too).

IRAQ – ITS INFRASTRUCTURE OF CONCEALMENT, DECEPTION AND INTIMIDATION

This report draws upon a number of sources, including intelligence material, and shows how the Iraqi regime is constructed to have, and to keep, WMD, and is now engaged in a campaign of obstruction of the United Nations Weapons Inspectors.

Part One focusses on how Iraq's security organisations operate to conceal Weapons of Mass Destruction from UN Inspectors. It reveals that the inspectors are outnumbered by Iraqi intelligence by a ratio of 200 to 1.

Part Two gives up to date details of Iraq's network of intelligence and security organisations whose job it is to keep Saddam and his regime in power, and to prevent the international community from disarming Iraq.

Part Three goes on to show the effects of the security apparatus on the ordinary people of Iraq.

While the reach of this network outside Iraq may be less apparent since the Gulf War of 1990/1991, inside Iraq, its grip is formidable over all levels of society. Saddam and his inner circle control the State infrastructure of fear.

Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"

Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"

Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"

Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"

Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"

Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"

Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"

Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"

Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"

Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"

Paul Hamill - Foreign Office official

John Pratt - Downing Street official

Alison Blackshaw - The personal assistant of the Prime Minister's press secretary

Murtaza Khan - Junior press officer for the Prime Minister

Risks with Microsoft Word

- Document may contain previous revisions
 - ... which in some cases may reveal unrelated docs
 - or may reveal, e.g., which embarrassing details were deleted before publication, or what terms in the contract were changed
- May reveal local filenames, usernames, author names, and other metadata

"Xbox is on track for an awesome [European](#) launch in ~~fall 2001~~[early 2002](#)," said ~~Robbie Bach, senior vice president and chief Xbox officer~~[Sandy Duncan, Vice President, Xbox Europe](#). "With more than 200 game companies around the world creating Xbox games for launch and beyond, the unveiling of the Xbox design is just the start of great things to come."

Defenses?

- Print, then mark with ink, then scan