

# Secure Data Deletion

January 2009 Super Users Group

John Lupton

ISC Information Security

# Sanitization Types

- **Clearing:** protects data from robust keyboard attack, forensic or other data recovery software (e.g. overwriting with random data)
- **Purging:** protects data from a laboratory attack with signal processing equipment (e.g. degaussing a tape, overwriting an ATA drive)
- **Destroying:** protects data from all known and theoretical recovery methods (e.g. melting)

# Recommended Sanitation

Device	Hard reset	Overwrite	Degauss	Destroy*
ATA drive		X		
SCSI drive		X	(to purge) <sup>†</sup>	
USB drive		X		
CD/DVD				X
Tape		impractical	X	
Zip disk		X	(to purge)	
Cell phone	(delete 1st)			
PDA	(delete 1st)			
Printer	X			

<sup>†</sup> Makes drive unusable

\* Incinerate, melt, or shred to  $\leq 25\text{mm}^2$  pieces

# Overwrite Options

Windows	PGP Desktop: “shred” function Heidi Eraser (already-deleted files, whole disk) Secure Erase ( <a href="http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml">cmrr.ucsd.edu/people/Hughes/SecureErase.shtml</a> )
Mac	PGP Desktop: “shred” function Finder → Secure Empty Trash Disk Utility (already-deleted files, whole disk)
UNIX	Wipe ( <a href="http://wipe.sourceforge.net">wipe.sourceforge.net</a> )

Comprehensive List: [www.upenn.edu/computing/provider/recycle.html#prepare](http://www.upenn.edu/computing/provider/recycle.html#prepare)