



# Secure Erase Options for Solid State Drives (SSDs)

Jack Winters, CTO



[www.foremay.net](http://www.foremay.net)



# Why Secure Erase Is Important

## Computer loss and theft:

- Statistics show that 1 of every 14 laptops is stolen, and over 2,000 computers are stolen every day in this country. ((Information Week)
- A computer is stolen every 43 seconds
- Over 98% of stolen laptops are never recovered. (FBI)
- A survey of 769 corporate IT managers revealed that 64% had experienced laptop theft. (Tech Republic)



# Legal Penalties for Failure to Sanitize Data

The following table summarizes the fines and jail penalties for violation of the data security laws.

	Gramm-Leach-Bliley	Sarbanes-Oxley	FACTA	HIPAA
	Financial Services Modernization Act	Public Company Accounting Reform & Investor Protection Act	Fair and Accurate Credit Transaction Act	Health Insurance Portability & Accountability Act
<b>Directors and Officers</b>	\$10,000	\$1,000,000		\$50,000 to \$250,000
<b>Institution</b>	\$100,000			
<b>Years in Prison</b>	5 to 12 years	20 years		1 to 10 years
<b>FDIC Insurance</b>	Terminated			
<b>Impact on Operations</b>	Cease and Desist			
<b>Individual</b>	\$1,000,000		Civil Action	\$25,000
<b>Institution</b>	1% of assets			

Source: CMRR



# Where Secure Erase is Needed

## Application Examples

1. Mission Critical Applications
2. Military, Defense
3. Government Systems
4. Public health agency
5. Financial and insurance institutions
6. Banking systems
7. High Reliable Enterprise
8. High Reliable Stock / Security Exchange
9. Public Security
10. Medical Equipment

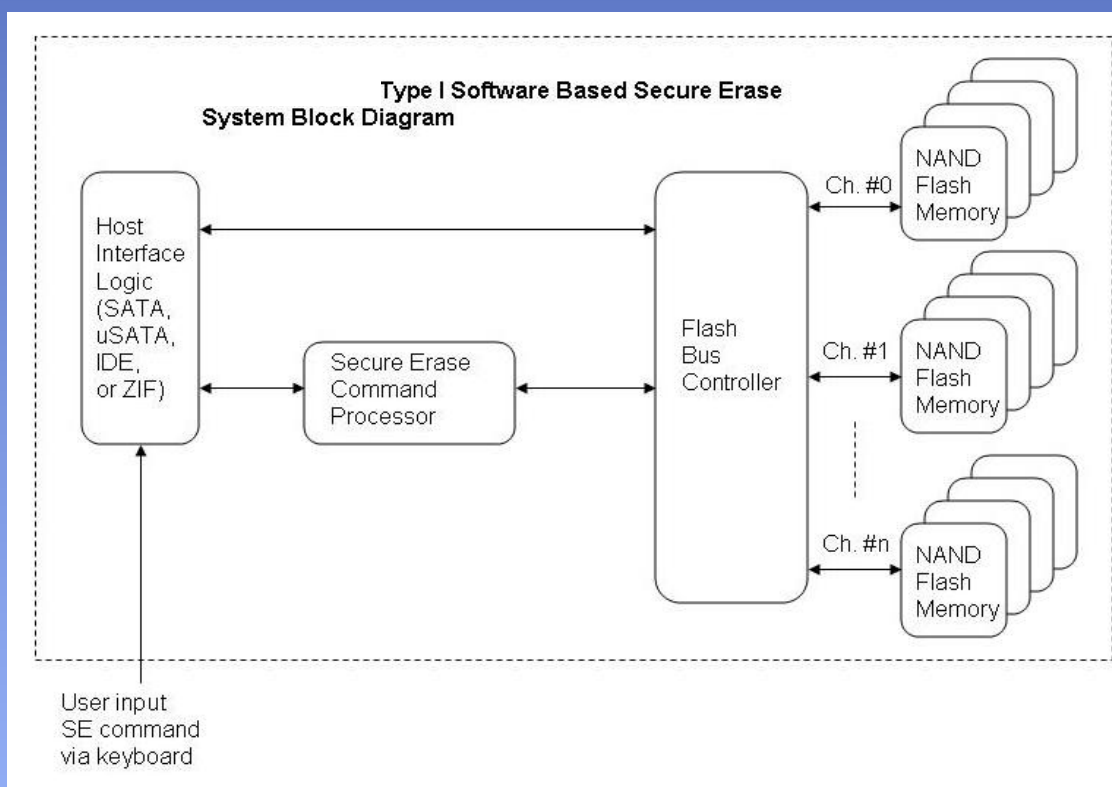


## Why Deleting a File is not Adequate

- In a regular SSD, deleting a file only removes its name from the directory or file table
  - User data remains until overwritten by new data
  - Reformatting the SSD also leaves data intact
- Need to overwrite all user data in allocated blocks, file tables, and data in reallocated defective blocks

# Secure Erase Types – Type I

Type I – Software-based SE through ATA command.

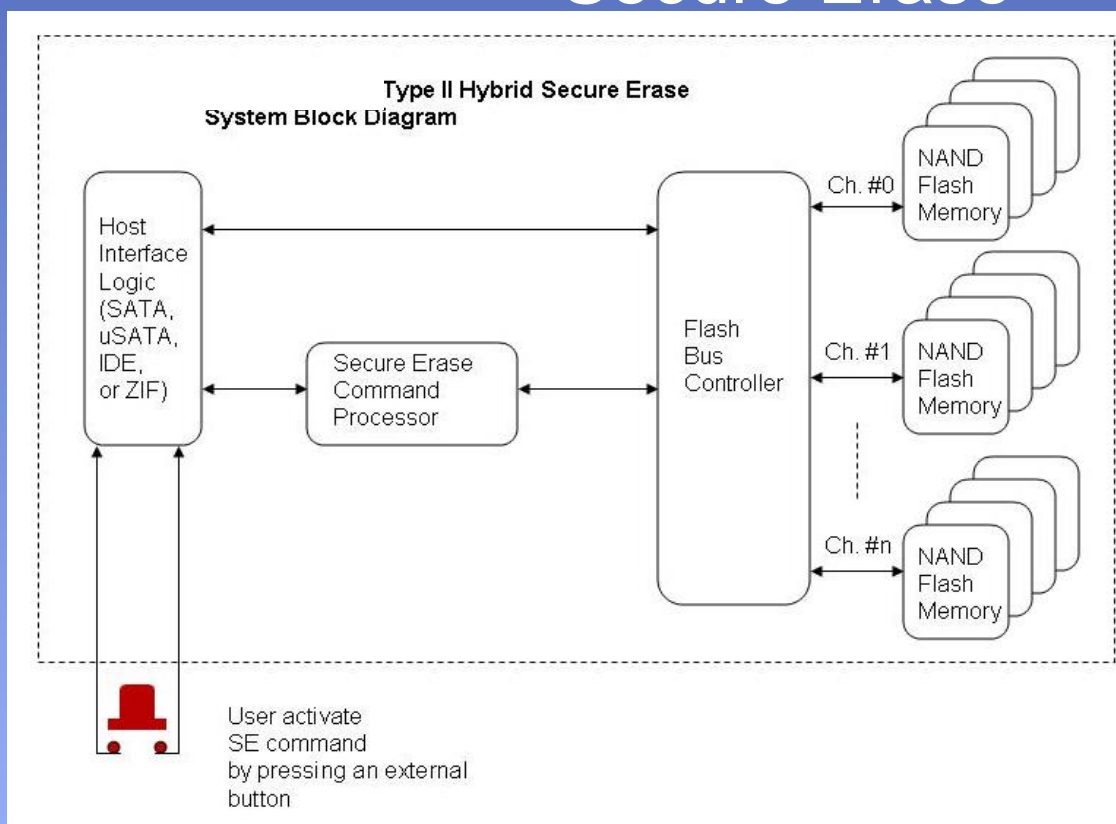


Features:

- Uses sanitize command
- Drive not suitable for reuse as bad block table also erased (but option for reuse)

# Secure Erase Types – Type II

## Type II – Hybrid software and hardware combined Secure Erase

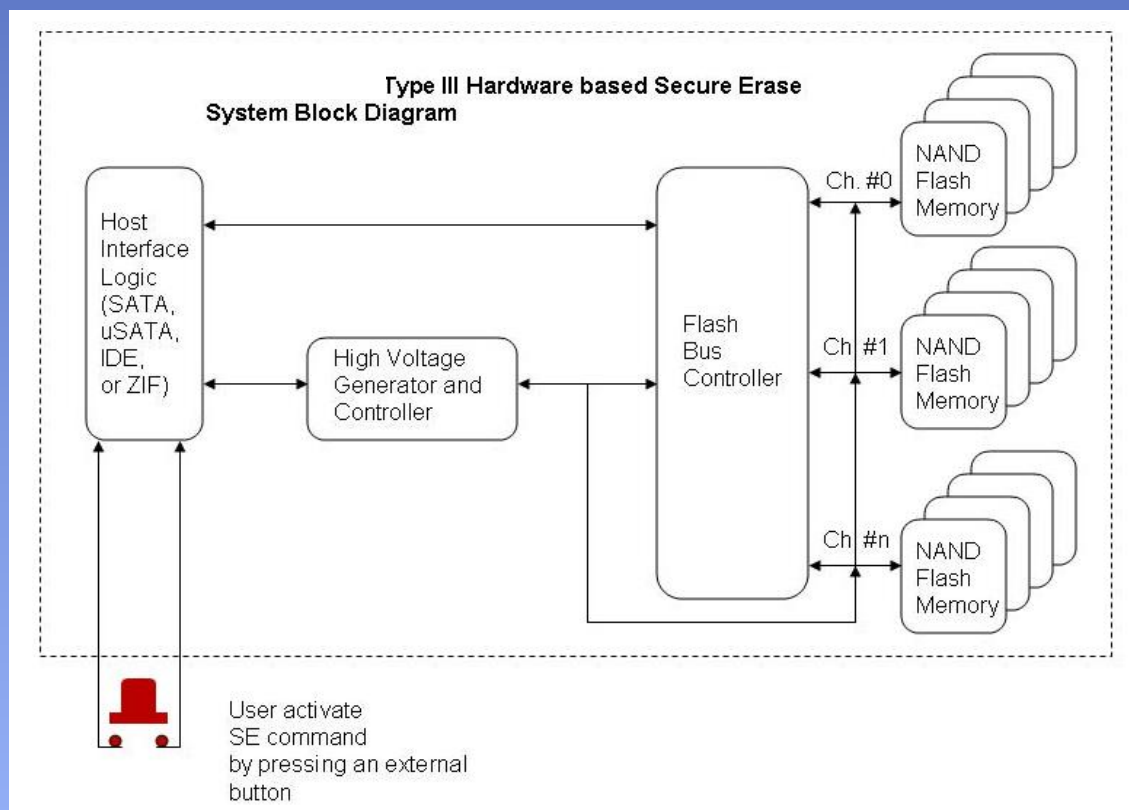


### Features:

- Uses external button and internal firmware
- Drive suitable for reuse after reformatting

## Secure Erase Types – Type III

### Type III – Hardware based one-key self-destroy disk purge



#### Features:

- Uses external button
- High voltage destroys NAND flash in 3 sec.
- Drive not usable after purge



# Secure Erase Method Summary

SE Type	Mechanism	SE Speed (approx.)	Reusable after SE
Type I	Software based SE through ATA command	5 seconds for every 32GB	Yes or No per request
Type II	Hybrid software and hardware combined SE	5 seconds for every 32GB	Yes
Type III	Hardware based one-key self-destroy	3 seconds for entire SSD	No



## Secure Erase Standards

Secure Erase technologies typically need to support the following Secure Erase methods (Ex: Foremay's Avalanche®):

1. DoD 5220.22-M
2. IREC (IRIG) 106
3. Air Force AFSSI 5020
4. Navy NAVSO P-5239-26
5. Army 380-19
6. NSA Manual 130-2
7. NISPOMSUP Chap 8, Sect. 8-501
8. Filled with all "0"
9. Filled with all "1"
10. Random fill
11. Gutmann method
12. Customized fill



## Secure Erase SSD Interfaces

Secure Erase technologies typically need to support the following SSD interfaces  
(Ex: Foremay's Avalanche®):

1. SATA
2. micro SATA
3. IDE/PATA
4. PCIe / PCI Express
5. SAS
6. SCSI
7. ZIF
8. LIF
9. mini PCIe
10. CF card
11. Industrial USB



# Summary

Secure erase needs to be done with different:

- Types
- Standards
- Interfaces



## Questions?



**Corporate Headquarters:**  
225 S. Lake Ave., Ste.300  
Pasadena, CA 91101, USA  
Tel: +1 408 228 3468  
Fax: +1 408 521 3468  
[www.foremay.net](http://www.foremay.net)