

# Secure Erase for Embedded SSDs

Jack Winters, CTO

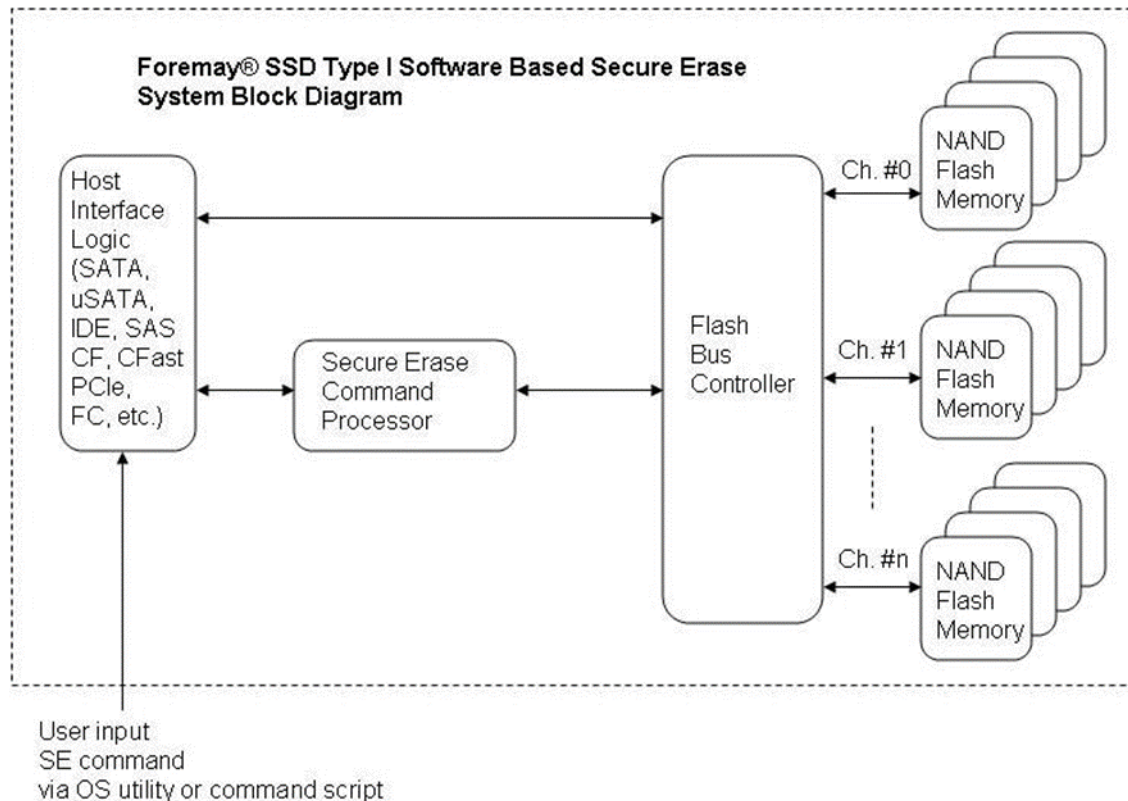


# SSD Secure Erase Technologies

- At Flash Summit 2010, I gave a presentation on why secure erase is important.
- Four years later, that is no longer in question.
- Instead, now the focus is on technology options for Secure Erase (SE).
- There are three categories of secure erase techniques:
  - Type-I software based secure erase
  - Type-II hardware based secure erase
  - Type-III self-destroy secure erase

# Type-I Software Based SE

There are three sub-categories of Type-I SE  
- SSD is re-useable after Type-I SE



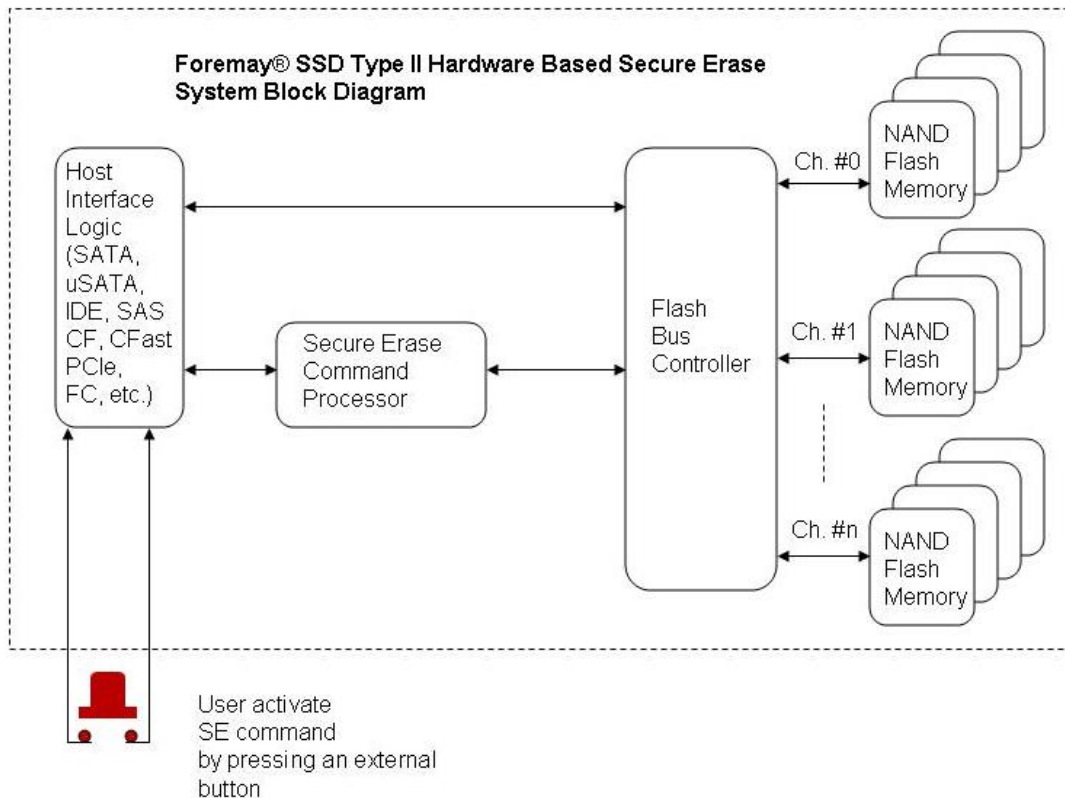
1. To execute SE via DOS based or other OS based utility tools
2. To execute SE via standard ATA command
3. To execute SE via vendor specific ATA commands

# Type-I Software Based SE

	Difficulty to Use	Erase Time	Erase Result	Sanitation Level
via DOS based or other OS based utility tools	Low	Medium to Long depending on SE method chosen	All "0" or preset by specific SE method	High, with military secure erase methods
via standard ATA command	Medium	Fast	All "0"	Medium
via vendor specific ATA commands	High	Medium to Long depending on SE method chosen	Preset by specific SE method	High, with military secure erase methods

# Type-II Hardware Based SE

There are two sub-categories of Type-II SE  
- SSD is re-useable after Type-II SE



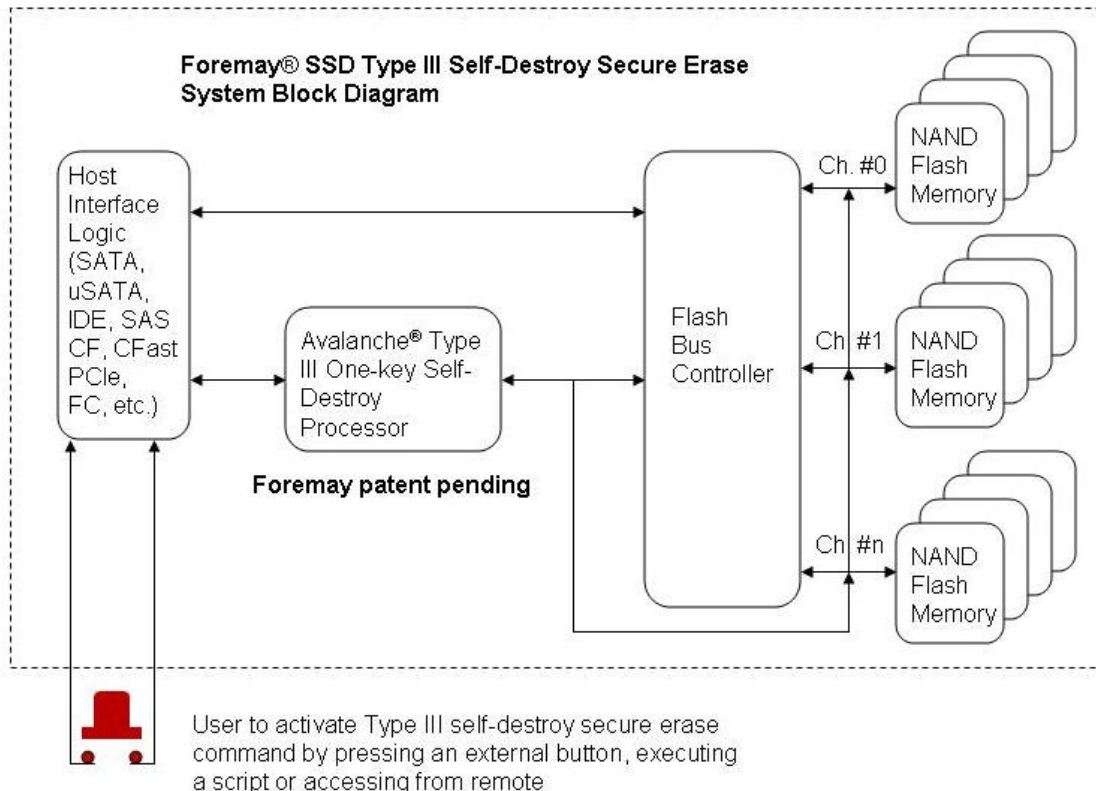
1. To erase and overwrite with "0" in a single pass
2. To erase and overwrite with preset patterns in multiple passes based on military secure erase methods

# Type-II Hardware Based SE

	Difficulty to Use	Erase Time	Erase Result	Sanitation Level
To erase and overwrite with "0" in a single pass	Low	Fast	All "0"	Medium
Military secure erase methods with multiple passes	Low	Medium to Long depending on SE method chosen	Preset by specific SE method	High, with military secure erase methods

# Type-III Self-Destroy SE

There are three sub-categories of Type-III SE  
- SSD is NOT useable after Type-III SE



1. To destroy NAND flash
2. To destroy firmware
3. To destroy encryption key

# Type-III Self-Destroy SE

	Difficulty to Use	Erase Time	Erase Result	Sanitation Level
Destroy NAND flashes	Low	Fast	NAND flash is destroyed physically	High
Destroy firmware	Low to medium	Fast	Firmware and index mapping table are destroyed to leave useless scattered bits	High
Destroy encryption key	Low to medium	Fast	Encryption key is destroyed to leave useless scrambled bits	High



# SSD Secure Erase Outlook

- Combined Type-I, II and III SE for enhanced sanitation level
- The execution of SE can be done not only locally but also remotely
  - GPS and cellular triggered
  - iPhone and Android app triggered
- Faster erase speeds for multi-pass SE via
  - Block erase
  - Bank erase
  - CE and/or channel erase
- Additional NAND flash physical destruction methods:
  - Chemical melting
  - Laser dicing
  - Mechanical shredding
  - Vanishing Programmable Resources program (DARPA) - crumble into small, sand-like particles in a fraction of a second when an electrical trigger is applied. <http://www.militaryaerospace.com/articles/2014/02/parc-ibm-vapr.html>



# Multi-Pass SE Standards - Military and Non-Military

- NSA/CSS 9-12
- NSA/CSS 130-2
- DoD 5220 22-M NISPOM
- DoD 5220 22-M NISPOM, Sup 1
- NISPOMSUP Chap 8, Sect. 8-501
- Air Force AFSSI 5020
- Navy NAVSO P-5239-26
- Army AR 380-19
- RCC-TG IRIG 106-07
- CSEC ITSG-06
- HMG IS5
- AG-ISM 2012
- BSI/VSITR
- Gutmann method
- Customized method
- Avalanche (TM): erase all blocks and then overwrite all blocks with a known fixed ASCII character X ("0x58").

Avalanche is registered trade mark of Foremay and Avalanche secure erase method is an intellectual property of Foremay, Inc.

# Where Secure Erase Is Needed

- Secure erase application examples
  - Mission critical applications
  - Military, defense and national security
  - Aerospace
  - Government systems
  - Public health agencies
  - Social security
  - Financial and insurance institutions
  - Banking systems
  - High-Tech enterprises
  - Stock / security exchanges
  - Public security
  - Medical equipment

# Questions?

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



Corporate Headquarters:  
225 S. Lake Ave., Ste. 108  
Pasadena, CA 92821, USA  
Tel: +1 408 228 3468  
Fax: +1 408 521 3468  
E-mail: [info@foremay.net](mailto:info@foremay.net)