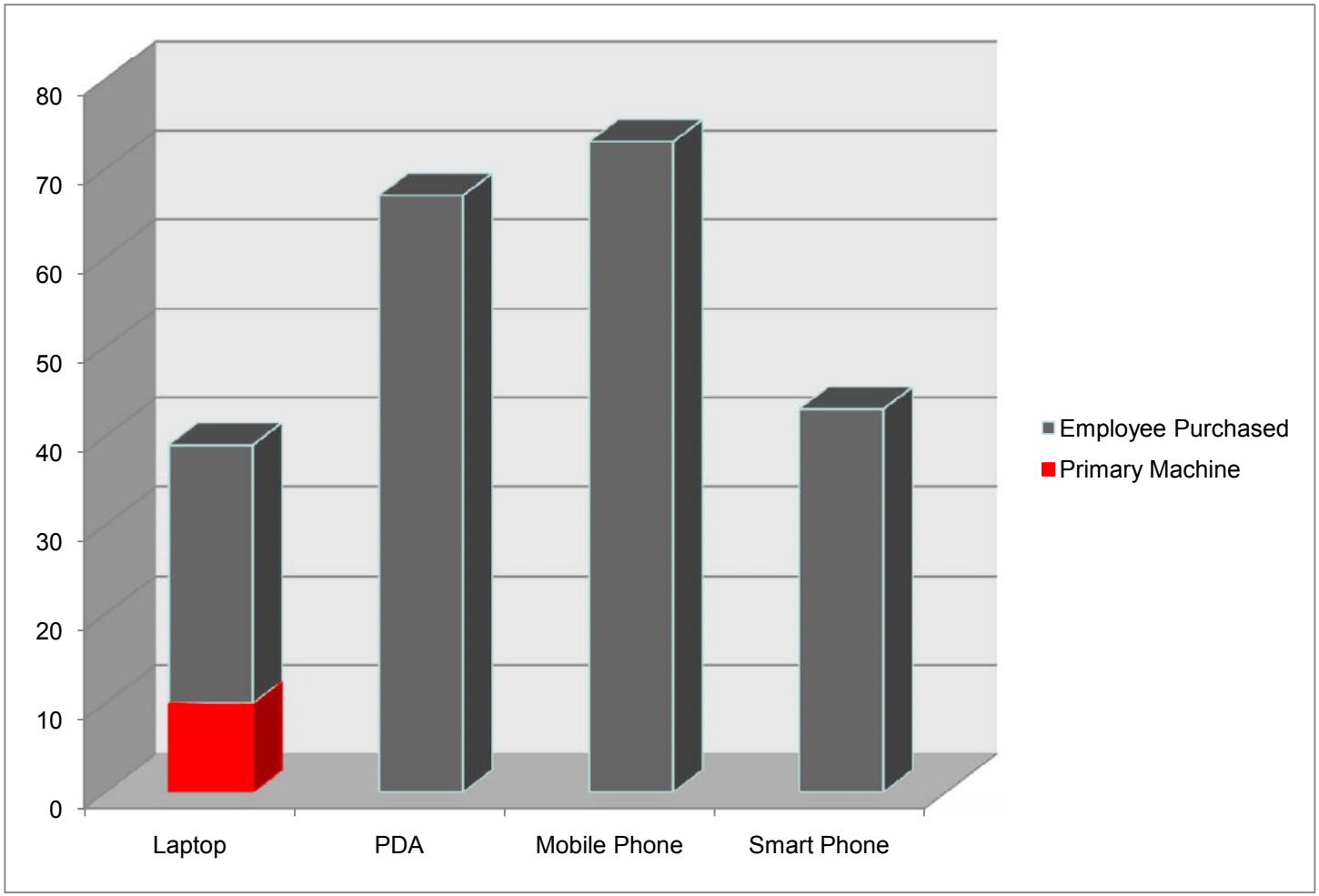
A PC In Every Pocket

Ron LaPedis
SPYRUS, Inc.

Agenda

- The consumerization of IT
- Flash controller optimization
- Windows Embedded Standard OS
- NT File System (NTFS)
- Secure Pocket Drive

How Widespread Is Consumerization?



Source:In-Stat

How It Happens

How It Happens

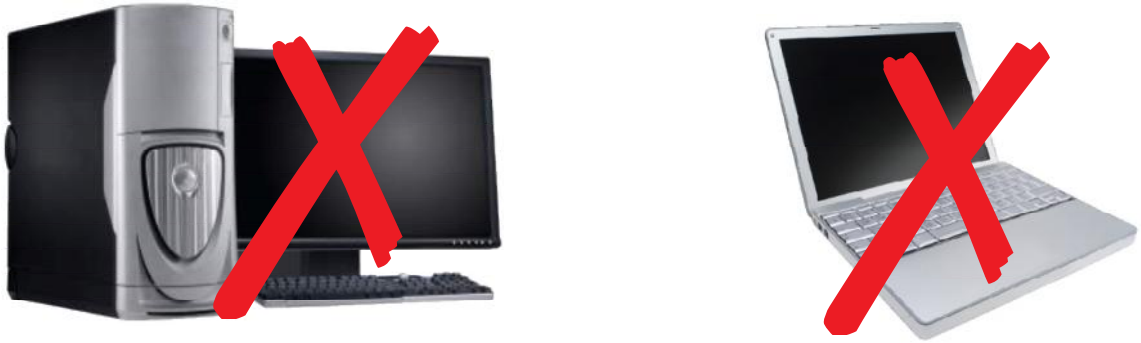
- Don’t want to use your Pentium III with 256mb RAM & 60gb HD
- Don’t want to use your OS
- Don’t want to use IE6
- Don’t want to use your software tools
- Don’t want to be locked down

What To Do About It

- Separate personal and work environments

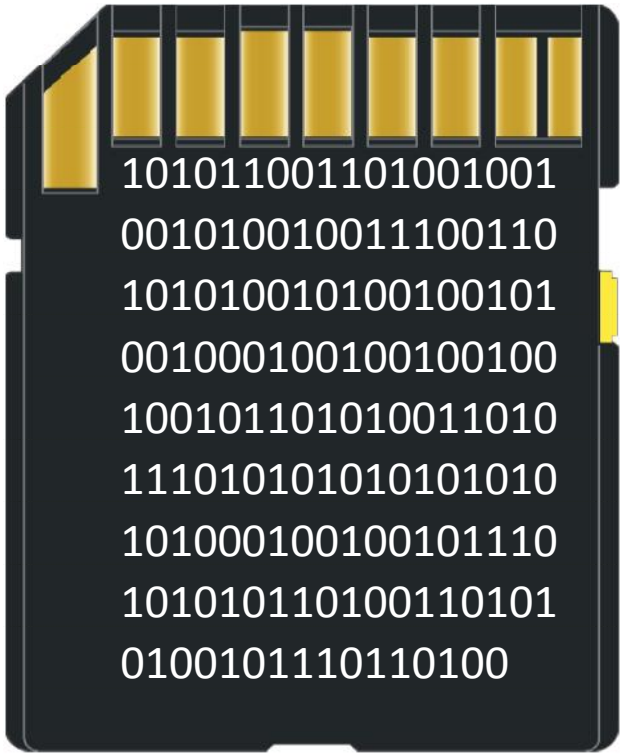
Secure Pocket Drive

PC in a Pocket



Smaller than a desktop, smaller than a laptop.
Carry an encrypted PC in your pocket and boot it most anywhere!

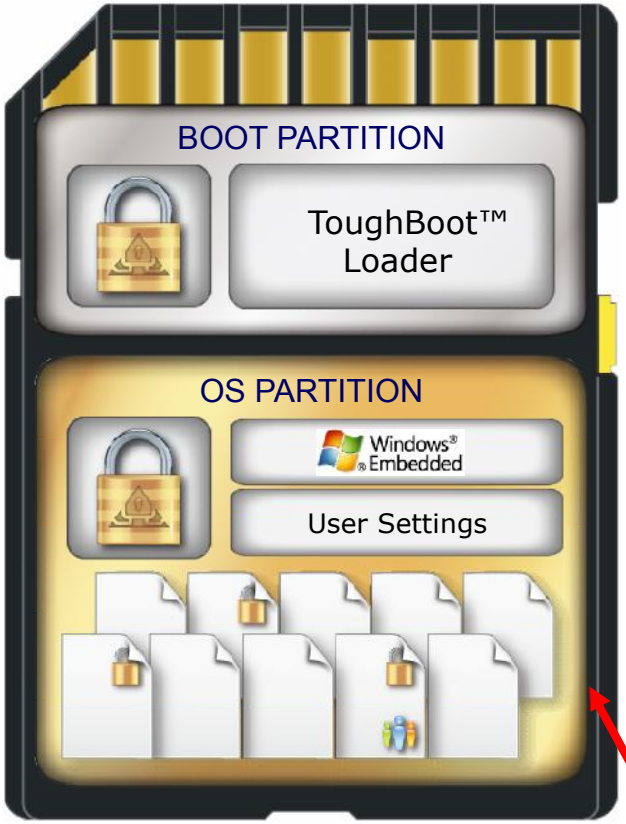
No Password, No Contents



- Unpowered drive is protected by NIST SP800-38E, XTS-AES 256 hardware encryption using unique internally-generated keys, providing data at rest protection.
- The entire memory is encrypted prior to formatting so that even the file system structure is protected from an attacker.
- Power on cryptographic validation of:
  - Hardware
  - Firmware
  - Bootloader

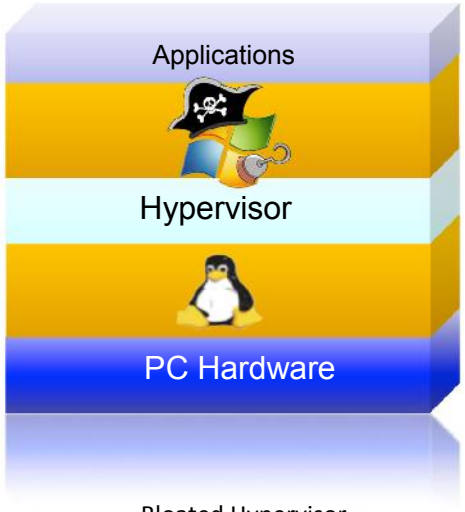
- During the manufacturing process the encrypted partition is cryptographically signed using SHA-384 and ECDSA P-384 using the device's unique private key. This signature was stored on and is validated by the hardware of the SPD.
- If any tampering is detected the boot process will not continue.

Flash Layout

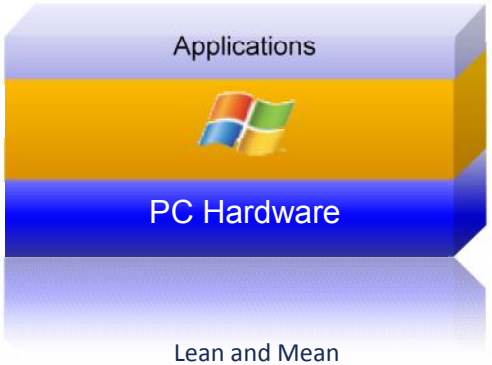


- Boot Partition
  - SPYRUS Secure ToughBoot™ Loader
  - Read only, obfuscated compartment
- OS Partition
  - XTS-AES 256 Encryption
  - Operating System
  - Applications (including all temp files)
  - User profiles, dictionaries, etc.

Secure Pocket Drive Versus Virtualization



Bloated Hypervisor
The Competition



Lean and Mean
Secure Pocket Drive

Flash memory

Windows Embedded Standard

Windows Embedded Standard 7

- Modular design for embedded systems
- Uses NTFS
- Write Filtering directs writes to RAM cache
  - File-Based Write Filter, which operates at the file level (Selective persistence)
  - Enhanced Write Filter, which operates at the sector level
- Cache can be trashed or flushed at shutdown

NT File System (NTFS)

NTFS

- Journaled file system
- Based around a number of structures stored in hidden files
- Journaling cannot be disabled
- Even reads are journaled
- Journal bypasses filtering

Takeaways

Takeaways

- Flash designed for high read-to-write ratio
- Controllers optimized for large serial access
- NTFS writes even when reading
- Flash + NTFS is not the best combination
- Backup / restore to new memory required

For more information

rlapedis@spyrus.com
(415) 939-8887

http://www.spyrus.com/products/secure_pocket_drive.asp