Security Considerations for USB 3.0 Windows on a Stick

A briefing to Flash Summit

by

Duane J. Linsenbardt

Executive Director Systems Engineering
SPYRUS, Inc

Security Like You Mean It

- Many diverse requirements depending on the market segment
  - Government
  - Enterprises
  - Consumers
- SPYRUS is a security company bringing our expertise to the memory & storage drive market
  - Trust must be anchored in hardware for high assurance
  - Legacy of hardware based secure memory devices
    - 1996 – Secure Compact Flash
    - 2007 – Secure Bootable Windows XP
    - 2009 – Secure Bootable Embedded Windows XP & Windows 7
    - 2012 – Secure Microsoft Certified WTG (Windows 8)

Windows on a Stick
Enterprise Requirements

- To provide a portable, high assurance processing environment so that users have a high degree of confidence they are working in a trusted environment
- To allow enterprise organizations to support a wide variety of operational scenarios, such as telecommuting and traveling users, without seriously compromising their security policies
- Performance must be as good as or better than rotating hard drives
- To protect against the multitude of security attacks being mounted today

Users of Flash Memory Are Facing Real Security Threats

- Confidentiality and Nonrepudiation
  - Data at Rest, Data in Transit, Data in Use.
- Infiltration of Malware
  - Infected devices and files, spreading malware into the enterprise environment.
- Exfiltration of Data
  - Accidental loss; deliberate theft or disclosure by disaffected or dishonest employees.
- IT Policy Enforcement and Auditing
  - Who knows who is doing what and when, and how the rules are being followed and by whom?

Windows on a Stick Confidentiality and Nonrepudiation

- Simple encryption with long keys is NOT enough
  - High entropy key generation is required
  - Strong protection of all critical security parameters is a must
  - Modes of encryption should vary with application
- Data at rest protection (FDE) is only a partial solution
  - Once authenticated, data in use protection becomes critical
  - To be useful data must be shared making data in transit protection an essential security element – secure file sharing
- Defense in Depth with complementary software solutions provides protection against the accidental failure or compromise of one defensive solution
- Validating source and authenticity of data and applications is important element of any solution

Windows on a Stick
Infiltration of Malware

- Malware and the techniques for getting it on your machines and in your networks have become more and more sophisticated
  - USB devices are notorious for delivering malware
- Need to maintain a clean operational environment
  - Comprehensive integrity validation is important each time a device is booted
    - This allows a user to trust their operational environment
  - Strong mechanisms to block malware intrusion needed
    - White List / Black List
    - Read Only – most effective approach
      [The most trusted end point solution for cloud computing]
  - Standard anti-malware detection and cleanup applications are still needed

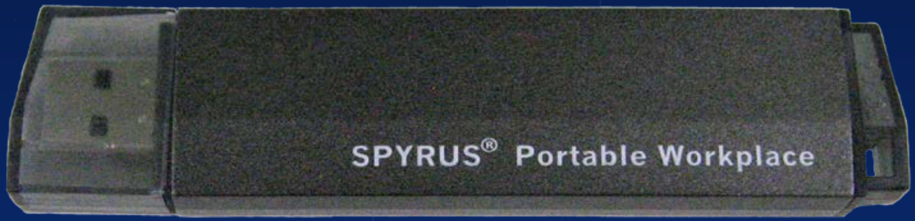
Windows on a Stick
Exfiltration of Data

- Prime suspects are those who have legitimate access to sensitive data
- Controlling who accesses data is necessary but NOT sufficient
  - Strong user authentication is a must
    - Password complexity and mandatory change enforcement
    - Exhaustive password search protection
  - Need to control where data can be accessed
    - Limit device use to specific machines, domains, & networks
    - Control who can communicate with whom
  - Need to control conditions under which data can be accessed
    - Multi-party access controls
  - Need centralized/remote disable, enable, & destruction

Windows on a Stick
Policy Enforcement and Auditing

- Having a strong security policy without enforcement is ineffective – history speaks
  - Most data loss is from unintentional policy violation
- Flexible policy control of individual devices is required in our modern processing environments
  - Windows policies must be effective on portable devices
  - Device control policies must work in pre-boot environment
  - Requirements change and so must policies
  - Centralized management and control is most effective
  - Even (especially) administrators need policy enforcement
- Auditing is essential element in policy enforcement
  - Maintain who accesses devices and data and where they go
  - Centralized auditing necessary for positive control

Windows on a Stick
Comprehensive Security Solution

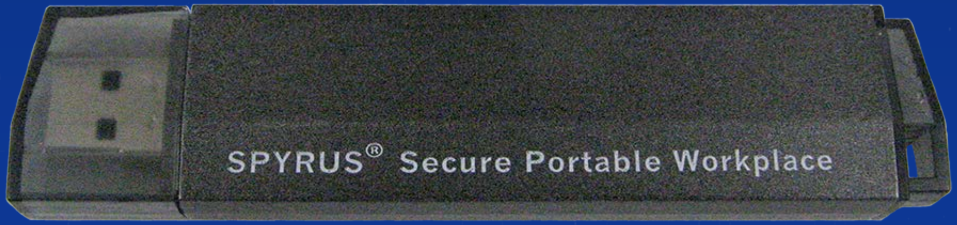


Microsoft Certified
WTG Drive

H/W Based XTS AES-256 Full Disk Encryption
Strong Key Generation & Management
Strong Multi-User Authentication
Remote Device Management
Policy Enforcement
Integrity Validation
Read Only Mode
Enclave Mgmt.
Auditing

Supplemental Security Apps
- Software FDE
- Anti-virus
- Firewall
- App Management
- VPN

Hardened Operating System
- Local Machine Policies
- Group Policies
- User Access Controls
- Application Settings



Microsoft Certified
Secure WTG Drive

More Information?

www.spyrus.com

www.spyruswtg.com

Duane Linsenbardt

dlinsenbardt@spyrus.com