



Secure Mobile Computing ON USB Drives

**Jack Sebbag, MXI Security - VP Sales &
Marketing North America**

2321 Cohen, Montreal, QC

Tel: 1-888-422-6726 E: jsebbag@mxisecurity.com



Agenda

- **What are secure mobile computing solutions on USB?**
- **The different types of mobile USB solutions**
- **Mobile Computing on USB**
- **Challenges**
- **Security features of Boot from USB solution**
- **Usability**
- **Use cases**



What are Secure Mobile Computing Solutions on USB?

- Portable operating environments allow employees to access their business applications and information with increased mobility.
- Secure USB flash drives are becoming new alternatives to the traditional mobile environment



Different Types: Portable Applications

▪ Portable Applications

Not an OS per-se but rather applications installed on USB

Pro's

- No installation on host machine
- Wide range of business applications

Con's

- No support for widely used apps such as MS Office



Different Types: Virtual Machines

■ Virtual Machines

Full OS virtualized on USB device

Pro's

- Full OS and range of OS Support
- All business applications supported within the virtual OS

Con's

- Requires a player on the host machine to be available.
- Limits true portability often due to lack of administration rights



History: Boot from USB

▪ Boot From USB

Pre-boot environment requires authentication and full OS launched after user authenticates.

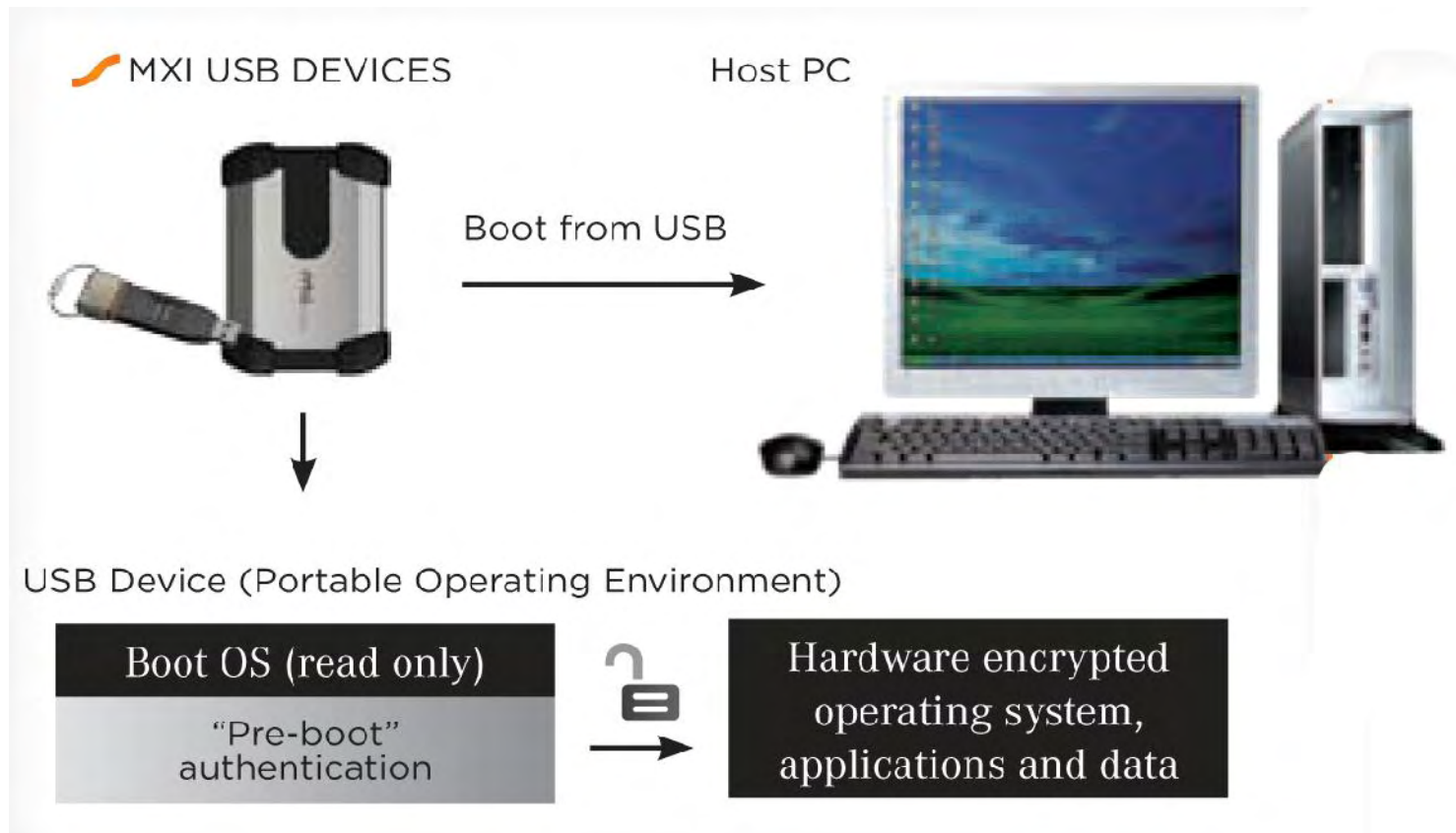
Pro's

- Secure working environment
- Doesn't use host HDD

Con

- Requires host to be configured to boot from USB

BOOT FROM USB: Flow Diagram





Mobile Computing on USB

- Offers the most security for protecting enterprise data while also maintaining the best overall mobility and functionality.
- It is a solution that can instantly turn an unmanaged, non-trusted machine into a trustworthy environment and consequently enables a number of significant cost effective solutions for the enterprise.
- Cost savings are realized through a reduction in laptops and management of machines.



Mobile Computing on USB : Challenges

- **Portability**
 - Making a desktop usable on different machines
- **Security**
 - Protecting the desktop if lost
 - Securing the desktop from the user themselves
- **Placement on USB drives**
 - Multi-gigabyte size and raw time-to-copy
 - Secure transport
- **Management**
 - Ability to securely define and update devices as needed



Mobile Computing on USB : Security Features

- **Disables persistent Malware on host PC**
 - Isolates host machines HDD from use, preventing host HDD from ever being used.

- **Data leakage prevention when in use**
 - Disabling the local HDD prevents any data being stored on it. Including temp files.

- **Data leakage prevention at rest**
 - Boot from USB solutions should prevent the user tampering with the OS environment on the flash drive.



Mobile Computing on USB : Security Features

- **Protection of data**
 - The USB drive should be secured using strong hardware encryption
 - The USB drive should require strong authentication to access the pre-boot environment (passwords, Biometric, Digital identity)

- **No trace of user session**
 - Disabling the host disk drive prevents temporary files being written.



Usability

- **Any boot from USB solution must be usable**
 - **Provisioning of the environment**
 - Scalable and secure provisioning a must
 - Vendor should provide solutions to drastically increase scalability whilst maintaining a secure environment
 - **User experience**
 - As close to the users normal work environment



Usability

▪ User Training

- BIOS issues, ensuring PC's are configured to work
 - Users encouraged to work with IT teams to ensure home pcs can be supported
- Sudden removal of flash drive can result in data loss or corruption
 - Every one pulls out USB drives
 - Education needed to avoid this scenario



Example Use Cases

- **Isolation of multiple environments for compliance or security**
 - Regional desktop data must not leak to global desktop environment; reboot from USB for regional mode
 - Machines normally locked down with reduced functionality; reboot from USB to access Internet, etc.



Example Use Cases

Thin Client

- Reuse old machines
- Boot from USB can be used to mimic thin clients
- Configured to mimic thin client environments

Teleworking

- Allow employees to use home computers instead of issuing laptops
- Boot home (non-trusted) PC from USB into secure, managed environment.
- Ideal for soldiers in-theater, remote field workers and road warriors
- Ideal solution in response to the Teleworkers Act.



Example Use Cases

- **Emergency Management**

- When a disaster such as an earthquake or hurricane strikes, a bootable USB is easily transported to the site.
- Eliminates needs to ship expensive and bulky laptops and computers.
- Workers have the ability to log on to a secure environment anywhere, at any time.

- **Secure Transactions and Online Banking**

- Combine a portable web browser with a full-featured PKI token for anywhere, anytime certificate-based authentication.

- **Forensics**

- Boot from USB : analyze or image hard disk without leaving a trail



About MXI Security

MXI Security is a division of Memory Experts International which was founded in 1994. It is privately held with 180 employees.

MXI Security was established in 2001.

International Locations

- Montreal (Headquarters)
- Santa Ana, CA (Manufacturing)
- Ottawa, ON
- London, UK
- Hong Kong, China



Who We Are

- MXI Security is the industry-leading provider of managed portable security solutions.
- Our focus is not on portable storage, rather we focus on **secure portable enterprise computing**.
- Our products and solutions provide our clients with the highest security and privacy technology, protecting their data and providing peace-of-mind.
- Our focus on innovation is key: MXI's first-to-market technologies continue to exceed our clients' expectations and anticipate their future needs.



Speaker Biography

Jack Sebbag - Vice President of Sales, North America, MXI Security

Jack Sebbag has over 22 years of sales and executive management experience in the Information Technology market and is responsible for driving all sales and marketing efforts in North America for MXI Security. Prior to joining MXI Security, Jack held such positions as Regional Director of Technology sales at Oracle and Vice President and General Manager at McAfee, where he was instrumental in building and developing a best-of-class sales organization and driving record sales growth. Jack holds a BA in Economics and Industrial Relations from McGill University.

jsebbag@mxisecurity.com / T (888) 422.6726



Questions