Flash Memory Summit

A Moving Target Defense for Data Storage Devices

Presenter: Don Matthews
President and CEO
NexiTech, Inc.

Protecting Critical Data

- **What** we do
  - Layers and fit
  - Foundational work
- **How** we do it
  - Technical attributes
  - Reference architecture
- **Why** does it matter to you?
  - This solution provides ransomware protection
  - Cyber attacks can result in real-world physical damage

Moving Target Defense

- ✓Reduces the attacker's window of opportunity
- ✓Increases the cost of the attacker's probing efforts

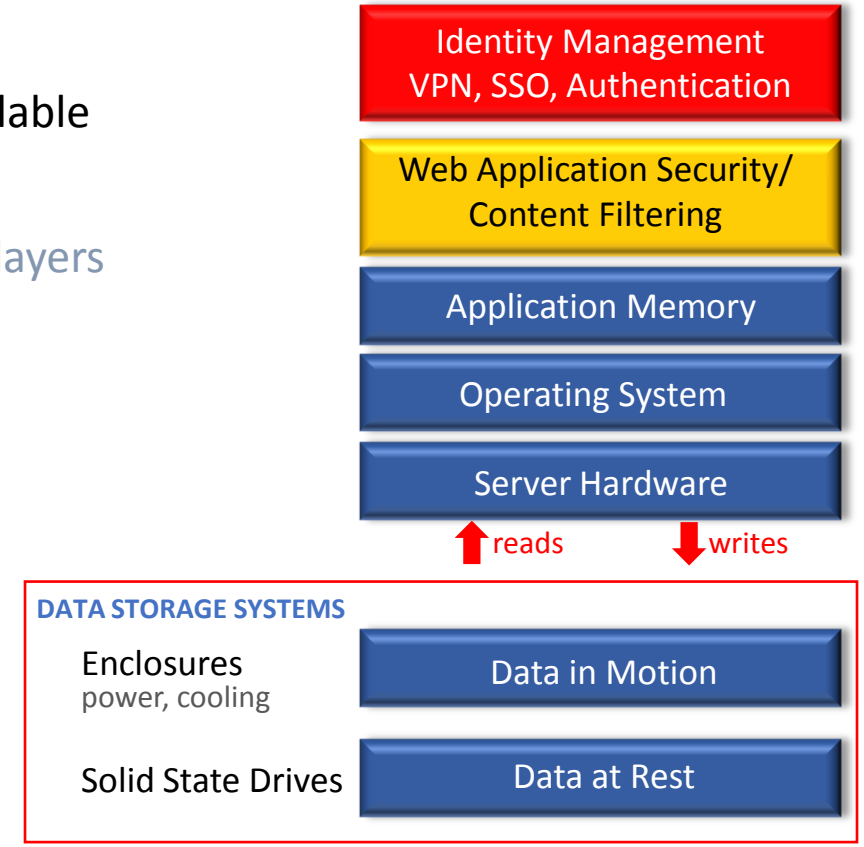
Changing Multiple Dimensions

Storage Threat Layering

Multiple attack vectors are available

Multiple vendors protect most layers

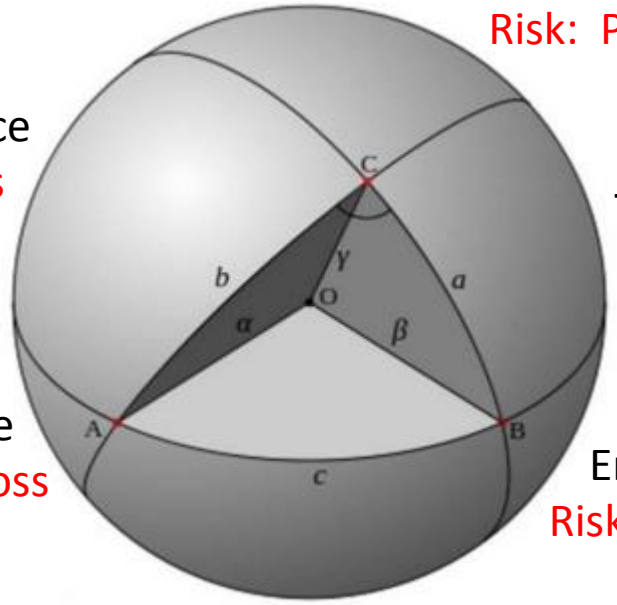
NexiTech stands alone with comprehensive **Moving Target Defense** at the Data Storage Layer



Storage Attack Surfaces

Enclosure CONTROL Surface
Risk: Physical Damage

Disk CONTROL Surface
Risk: Online Data QoS Loss



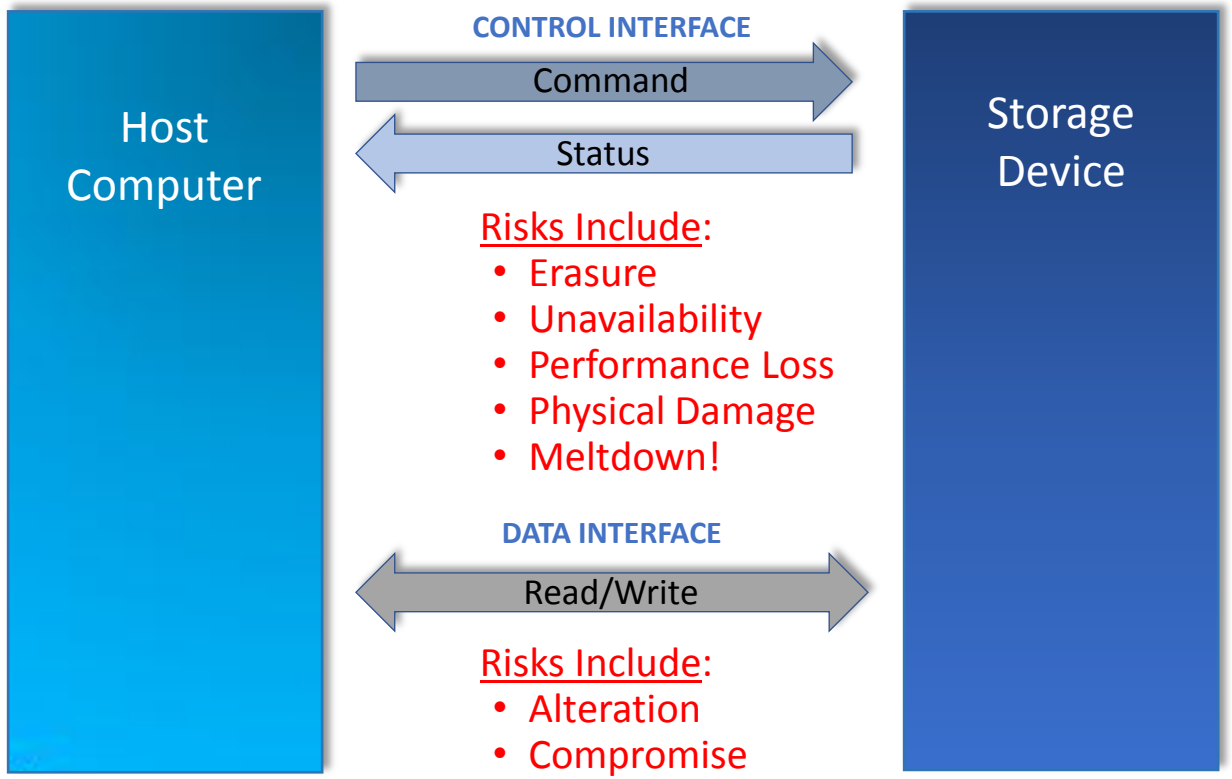
Tape DATA Surface
Risk: Backup Data Compromise

Tape CONTROL Surface
Risk: Backup Data Loss

Enclosure DATA Surface
Risk: Physical Damage

Disk DATA Surface
Risk: Online Data Loss or Compromise

Storage Attack Surfaces



Our Place In The World

Cyber Security Domain

Data Storage Domain

Federal Customer Engagements

Flash Memory Summit

Mission Planning Environments

Silicon Valley Innovation Program

2012 → 2017

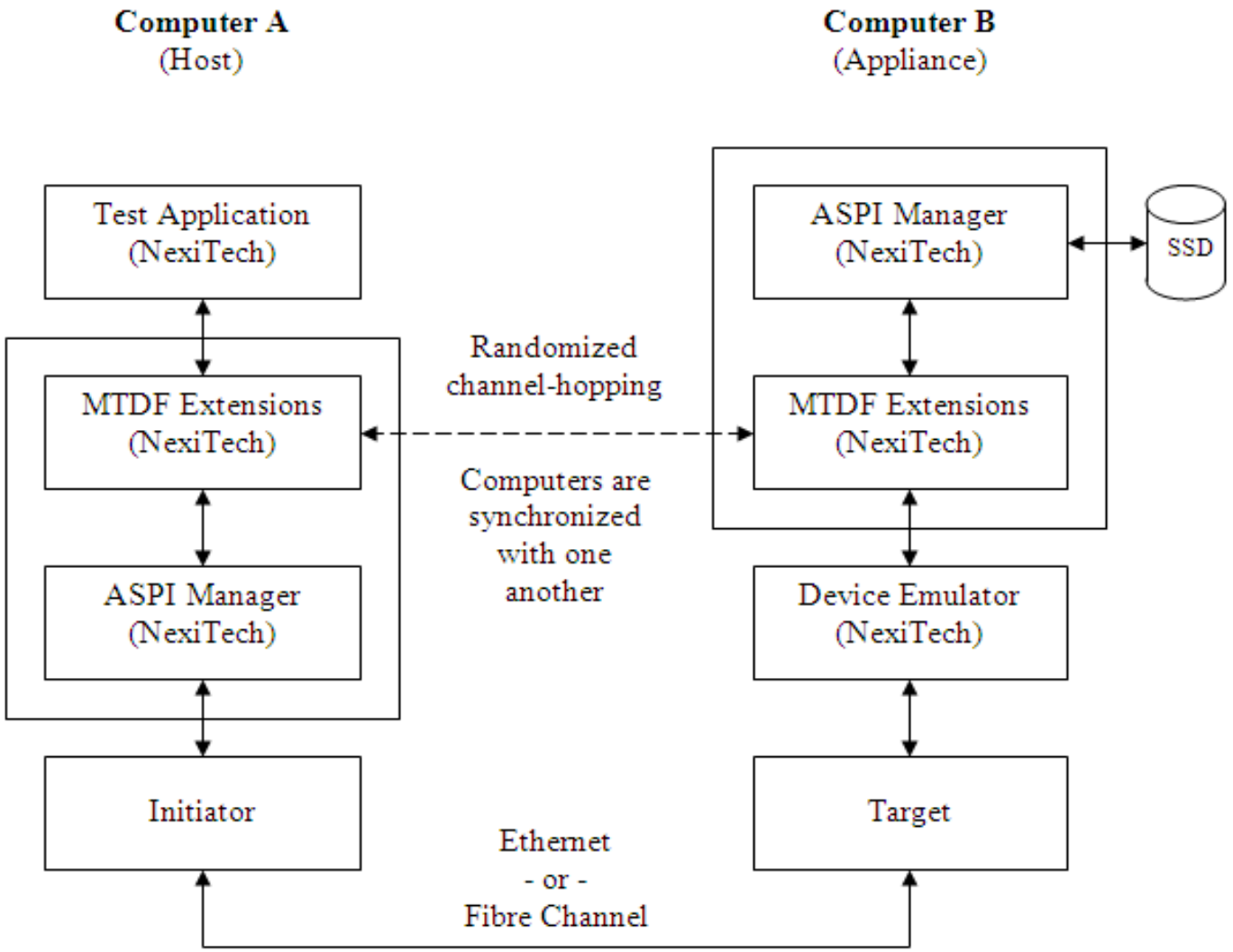
Our Technical Solution

- Isolate the device
  - Change the device type from "disk" to “unknown" inside a storage appliance.
  - Create multiple abstractions of the device using storage virtualization.
- Obfuscate the command set
  - Change the command set for the device inside the appliance.
  - Makes it more difficult for an attacker to access the device, but not impossible.
- Now introduce a Moving Target Defense (MTD)
  - Change the communications channel from one command to the next.
  - Change the command set itself from one command to the next.
- Statically link the interface library
  - Only specific applications can access the device.

How It Works

An autonomous system that randomly changes multiple dimensions of the attack surface, making it unpredictable to adversaries.

MTD Reference Architecture



Technical Attributes

- Autonomous
- Multi-dimensional
- Uses randomization
- Unpredictable by adversaries
- Dynamic network configuration
- Gathers metrics and reports breaches
- Optionally may use a Honeypot (i.e. Decoy)
- Address Space Layout Randomization (ASLR) for DATA STORAGE

Anti-Ransomware Vault (ARV)

- Ransomware cannot encrypt files it cannot see!
- Application accesses “dark space” beyond partition boundaries
- Presently optimized for use as an archival / backup solution
- Implements a proprietary file system
- Innovative IP that learns about the workload
- Adapts its metadata requirements accordingly

Why Should You Work With Us?

Flash Memory Summit

- Evolving the technology
- Expanding market opportunities
- Forming a network of partnerships
- Exploring a number of additional use cases
- Subject Matter Expertise in NVMe
- Subject Matter Expertise in Kernel Drivers

Summary

- The core technology is adaptable
- It uniquely protects data-in-flight for the storage

  DATA surface and also the storage CONTROL surface
- Can exist in an appliance …
- … or can be embedded in the device itself
- This is one more tool in the toolkit when it comes to fighting ransomware and stopping cyber attacks!

MTD – The Last Line Of Defense

Let’s Start a Conversation!

Flash Memory Summit

Questions?

NexiTech, Inc.
Don Matthews
Founder & CEO
970-702-2388
matthews@nexitech.com
www.nexitech.com