SNIA India

Mitigating Ransomware Threat - a Backup Solution perspective

Arindam Panna (Senior Principal Software Engineer, Veritas Technologies)

Narayan Subramanian (Senior Principal Software Engineer, Veritas Technologies)

Today’s Presenters

Arindam Panna

Senior Principal Software Engineer

Veritas Technologies

Narayan Subramanian

Senior Principal Software Engineer

Veritas Technologies

SNIA Legal Notice

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

- Introduction
- Real-world Examples
- Solution
- Code Injection Prevention
- Key Aspects
- Additional Protection Mechanisms
- Future Directions
- Key Takeaways

Introduction

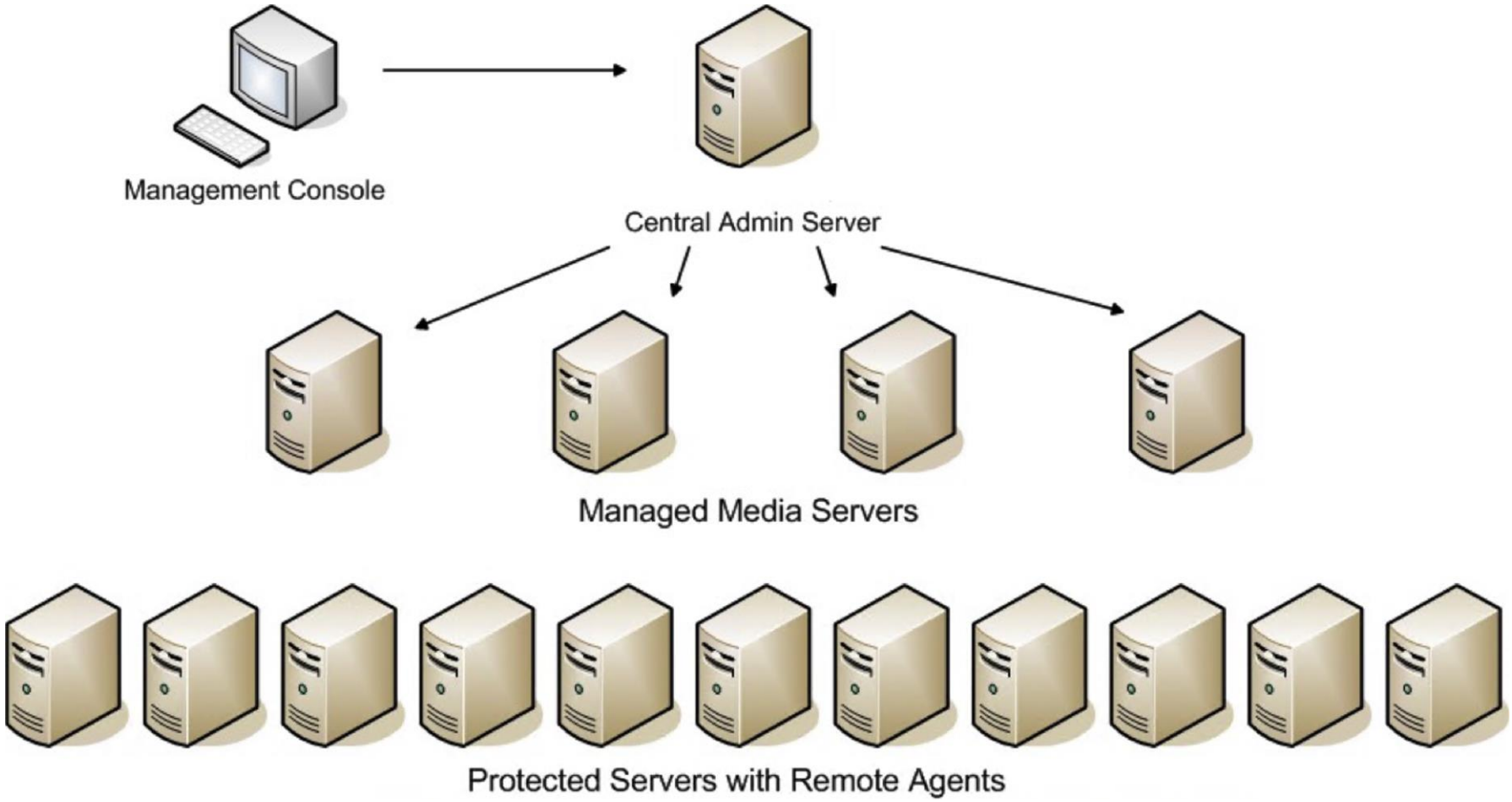
What is ransomware

- Malware that encrypts victim's valuable data and asks for money in return for decryption key.
  - LockBit, Conti, WannaCry, Petya, Clop to name a few
- Uses phishing and code exploits to escalate privilege and propagate
- Some ransomware employ advanced techniques
  - Deletes VSS snapshots, system restore points
  - Injects code into running processes
- **Having backup copy of data is a critical component to defending against ransomware**

Typical Backup Solution

- Data protection solution
- Example workloads: File Server, Email server, DB server etc.
- One or more media servers and agents on workload servers
- Supported Target Storage: disk, cloud, dedupe (disk/cloud based), tape
- The ransomware resilience technology that we will be doing a deep-dive of today protects **disk-based** backup images accessed locally or over network from malware

Typical Backup Solution Architecture



Ransomware Defense - Pillars

Detect

- Anomaly detection
- Malware scan
- I/O pattern monitoring
- Access pattern monitoring
- Audit logging

Protect

- Immutable file system
- Immutable point-in-time image
- Immutable disaster recovery copies
- Compliance clock
  - To protect against system clock tampering

Recover

- Identify latest good backup image to restore from
- Rapid recovery

Defense against Ransomware – Backup Perspective

- Use of immutable storage (WORM)
- Hardening of backup infrastructure
- Use the 3-2-1 rule
  - 3 copies of data on 2 different storage media types and 1 copy kept offsite
- Whatever happens keep backup images safe
- **This deep-dive is about protecting backup images from untrusted processes**

Ransomware Resiliency - Protection Mechanisms

- Allow only trusted backup software processes to make changes to backup images
- Trusted processes need to be protected from **code injection**
- The protection must be in both **kernel mode** and user mode
- The communication of control information to the driver needs to be trusted/secure.
- Have a **centralized trusted** user mode component to handle all communication to the driver
  - In order to supply control information (like which file system location to protect) to the driver other components talk to this user mode component.

Shared Disk Scenario

- An environment can have a federation of backup servers
- One backup server can expose a disk storage so that others can write via SMB/CIFS
- Need to protect the folder containing backup images in this case

Self-Protection of the Lockdown Driver

- **Must be able to protect backup images in absence of the user mode component**
- Start in early boot phase
  - Least possible window where protection is unavailable
- Do not allow driver unload
  - Prevent malware from disabling protection mechanisms
- Do not allow deletion, rename of the driver
- Protection of configuration information
  - If stored in registry / file, those keys/files need to be protected
- Handling uninstallation
  - Allow genuine uninstall, block malware

Real-world Examples

Real-World Examples

- We have had exposure to real-world scenarios involving ransomware attacks and backup technology
- Seen this technology thwart ransomware attacks on the backup images while the entire environment got attacked
- Had cases where the entire environment could be successfully restored from backups when it seemed that all was lost

Solution

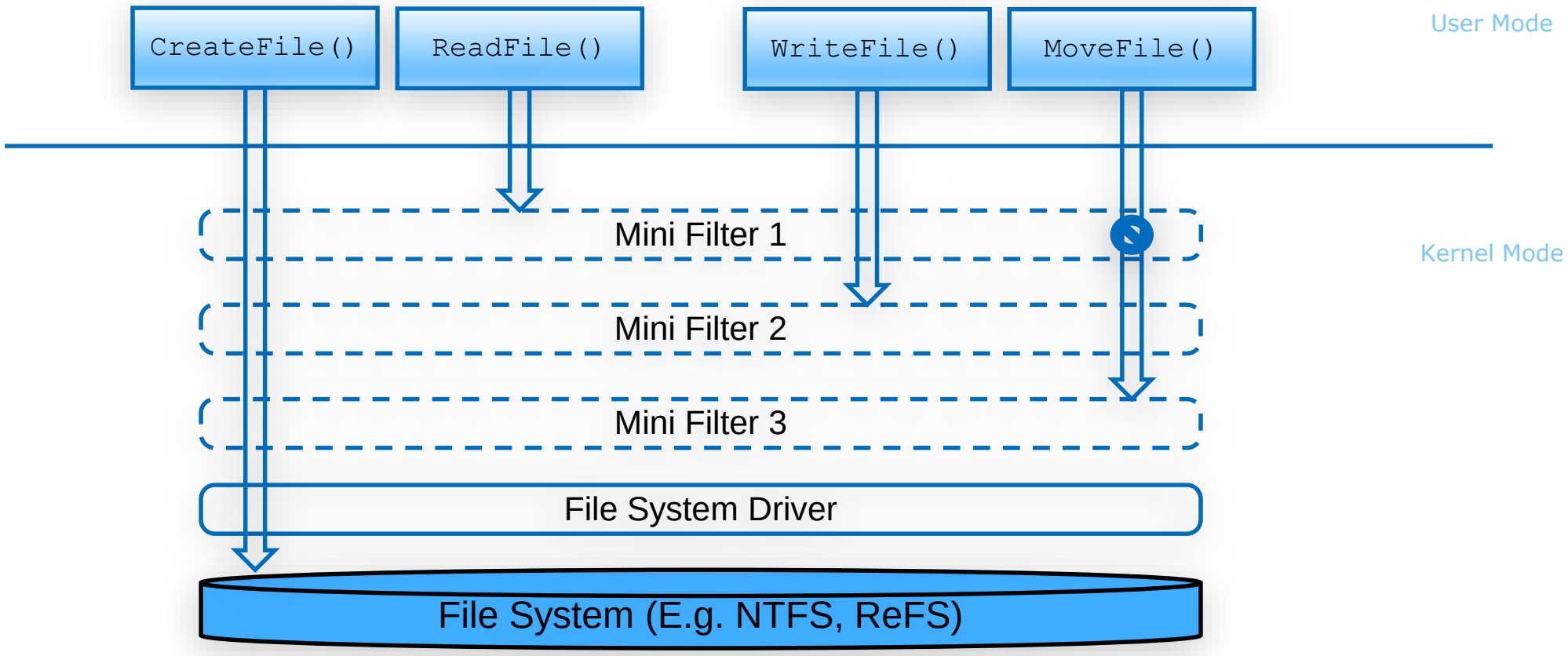
Solution - How

- File System Mini-Filter Driver to prevent unauthorized access
- A “Lockdown Service” (LDS) that operates in conjunction with the driver
  - User Mode Service
  - Implements logic to determine which processes / servers are authorized

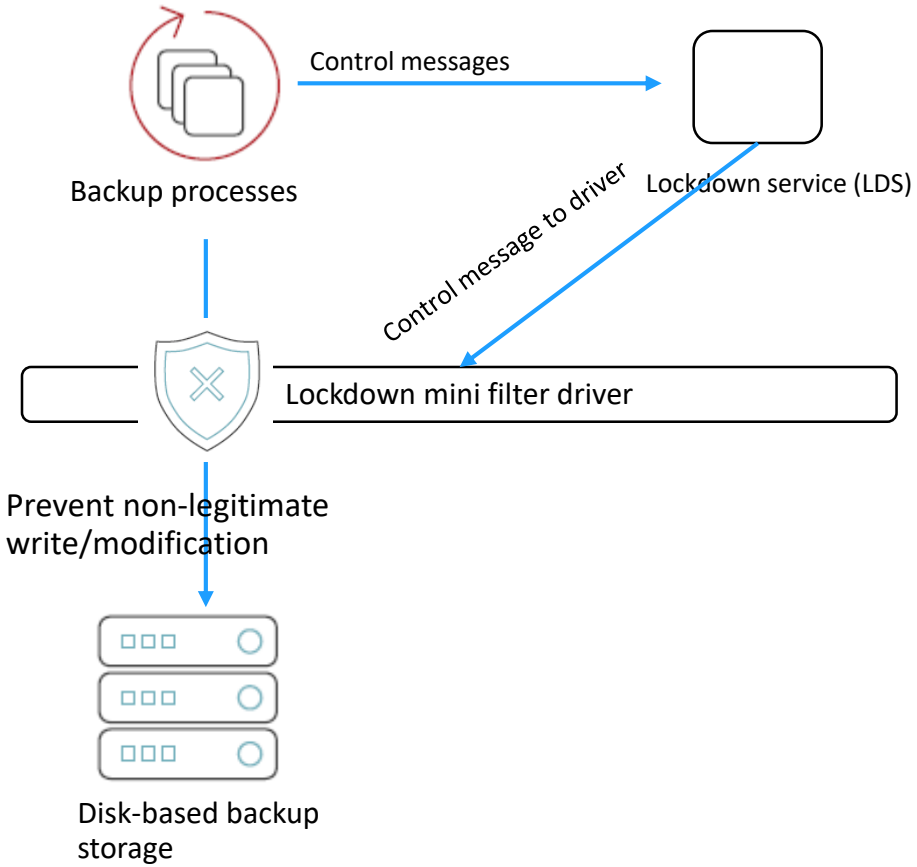
Why File System Mini-Filter Driver?

- Typical solution to prevent unauthorized access is to employ ACLs (Access Control List)
- However, Ransomware running with administrative privileges can workaround ACLs
- File System Mini-filter can see all IOs on a volume
- Has the ability to prevent a particular IO operation

What is a FS Mini-Filter Driver?



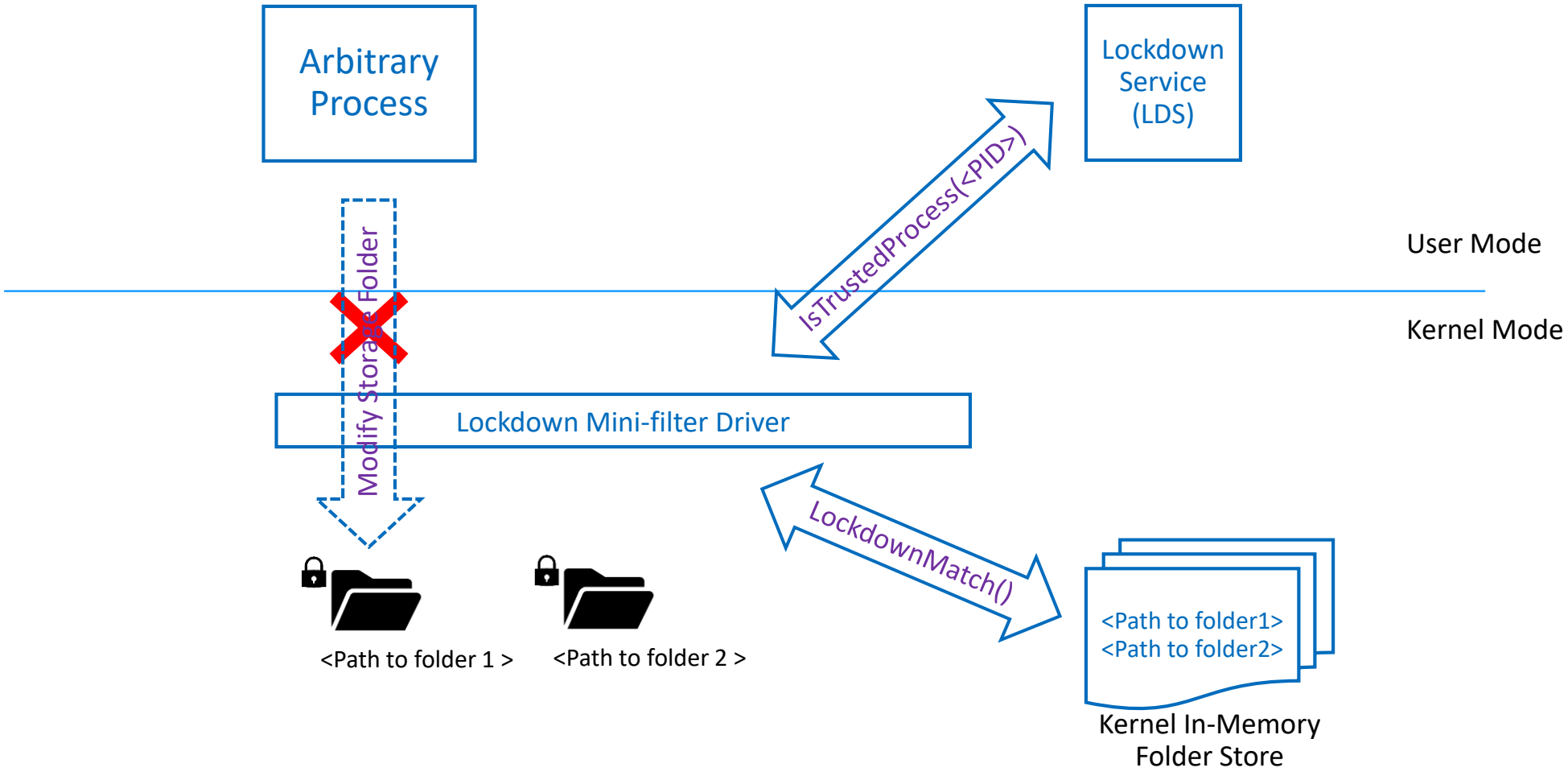
LDS – Simple Centralized Architecture



Lockdown Mechanics

- LDS may receive PID of process attempting to modify protected folder
- LDS should use a secure mechanism to validate the process
  - E.g., check the Authenticode Certificate of Process binary using Certificate APIs
  - WinVerifyTrust() API only verifies trust chain terminates in a trusted certificate
    - Use **custom checks** to validate other parameters such as Subject / Public Key of known Intermediate Provider

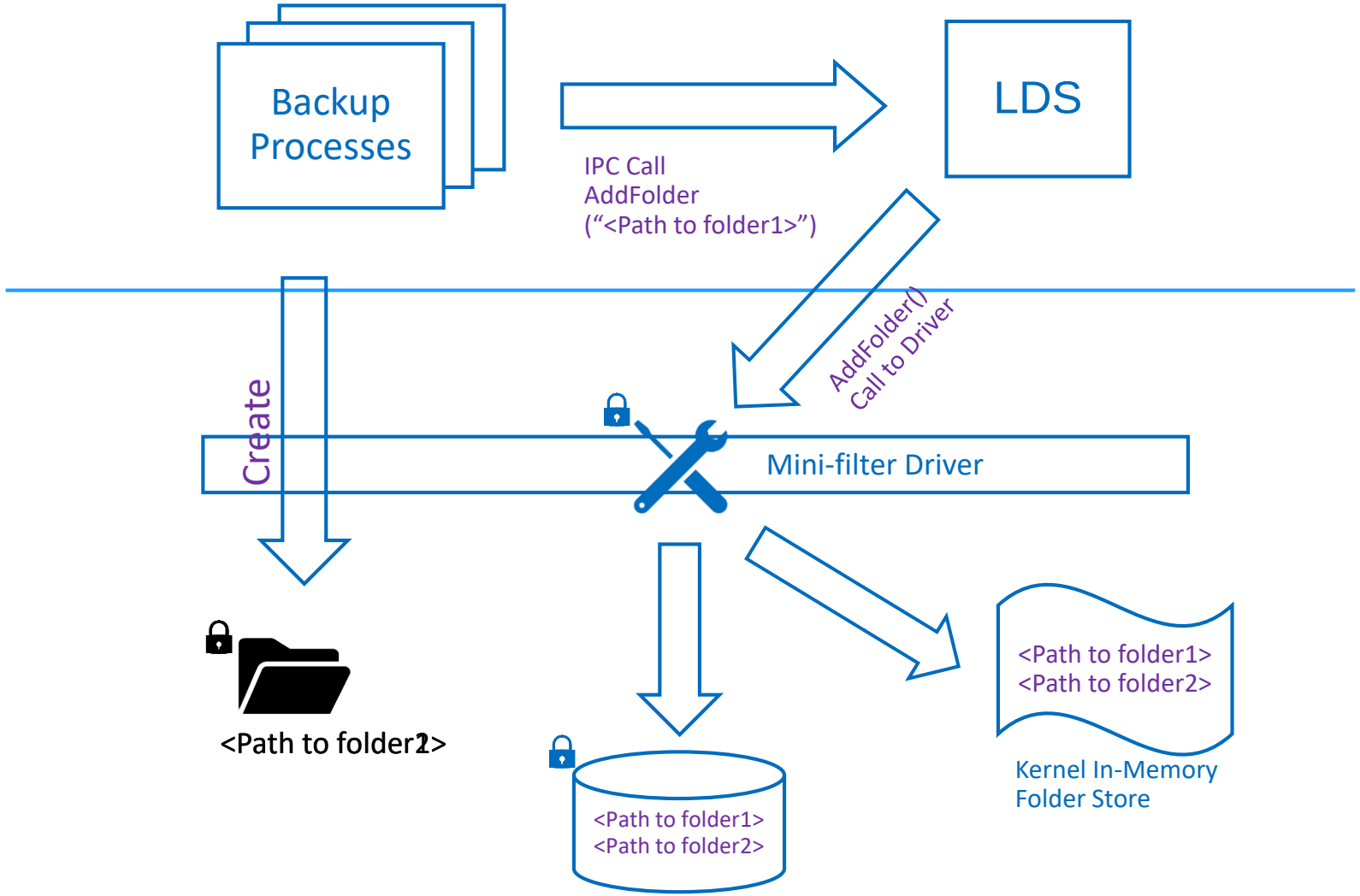
Lockdown Mechanics



LDS Control plane architecture

- Control plane operations
  - Adding/removing backup storage folders for lockdown
  - Enable/disable lockdown
  - ...
- It is critical to identify the authenticity of the LDS clients
- Need an IPC mechanism that allows verifying the authenticity of the connecting client
- Usage of RPC allows LDS to
  - Query RPC client PID via RPC runtime APIs
  - Use client PID to validate various process parameters such as name / path etc.
  - Perform Authenticode Certificate Validation

LDS Control plane architecture



Trusting the trusted

- Need to ensure that the driver can indeed trust the user-mode LDS
- Use mechanisms involving cryptographic hash of binaries and a secure handshake mechanism
  - Even the cryptographic hash needs to be secured in a configuration store
  - If the configuration store is maintained in the registry, use the Lockdown Driver itself to protect this store via kernel mode registry callback APIs

Network Storage Protection

- Necessary where network folders are used as storage destination
  - Also in multi-server deployments
- Challenges
  - Network path can be accessed in a variety of ways:
    - \\MachineName\Share\Folder
    - \\MachineName\c$\<PathToFolder>
    - \\FQDNName\Share\Folder
    - \\IPvAddress<v4/v6>\Share\Folder

- This can be solved using marker file etc.

Code Injection Prevention

Why

- We have made sure that only the trusted processes can modify backup storage
- What if the trusted processes are compromised?
- Code injection allows attacker to run in the context of trusted processes and evade any kind of checks

Code Injection Prevention Mechanism

- Code Injection attack
  - Open Process Handle
  - Allocate Memory in process context and write a stub of executable code
  - Create a remote thread to execute that stub and load a malicious Dll to do the actual damage
- Use kernel-mode mechanisms like Windows **object manager callbacks** to monitor any attempts to gain write access to process memory
  - Disallow and log attempts to gain such access

Code Injection Prevention – Special Considerations

- To those technically inclined, a few more points...
- Parent process needs to have complete access to child process / thread handles / memory space
  - Places restrictions on who can launch Backup processes / services
- Windows Privileged Processes also need to have access to every process
- Need to separate ‘Services’ from user launchable executables / tools

Key Aspects

Key Aspects

- Consider protection against indirect ways for file modification
  - Memory mapped, file handle duplication, open using file id
- Balance between usability and security
  - Require password / captcha for un-install?
- Supportability
  - Non-Killable LDS?
- Where to monitor
  - File system, volume level, disk level
- Provision to disable protection
  - For supportability, debugging
- Provision to exclude other specific application
  - E.g. AMSI client

Additional Protection Mechanisms

Additional Protection Mechanisms

- Immutable Devices
- Use of cloud storage
- Ransomware Resilient Storage System
  - Can be physical / virtual

Future Directions

Future Directions

- Many possibilities along each of the 3 pillars -- Detect, Protect, Recover
- Protection of configuration / Backup Catalogs in addition to storage
  - No recovery of backup server necessary
- Orchestrate recovery from ransomware attacks factoring cross-system and cross-application dependencies
  - E.g., Recovery path: Active Directory → Domain Controller → Exchange Server
- Research mechanisms for detect – use of AI / ML based approaches
  - Visibility into entire environment being a Backup Solution

Key Takeaways

Key Takeaways

- Ransomware attack is a major threat
- Backup is critical component of defense against ransomware
- Remember the three pillars
  - Detect, Protect, Recover
- Protecting from ransomware demands deep technical capabilities
  - Often requires kernel mode presence

Q&A

After This Webcast

- Please rate this webcast and provide us with feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- Follow us on Twitter @SNIA_India

Thank You

