SNIA | NETWORKING
NSF | STORAGE

Storage Technologies & Practices Ripe for Refresh

Live Webcast

February 3, 2021

10:00 am PT

Today's Presenters

Tom Friend
Moderator
Illuminosi

Alex McDonald
Independent Consultant
Vice Chair SNIA NSF

Eric Hibbard
CISSP, CIPT, CISA
Chair, SNIA Security Technical Working Group

John Kim
Chair, SNIA NSF
NVIDIA

SNIA-At-A-Glance

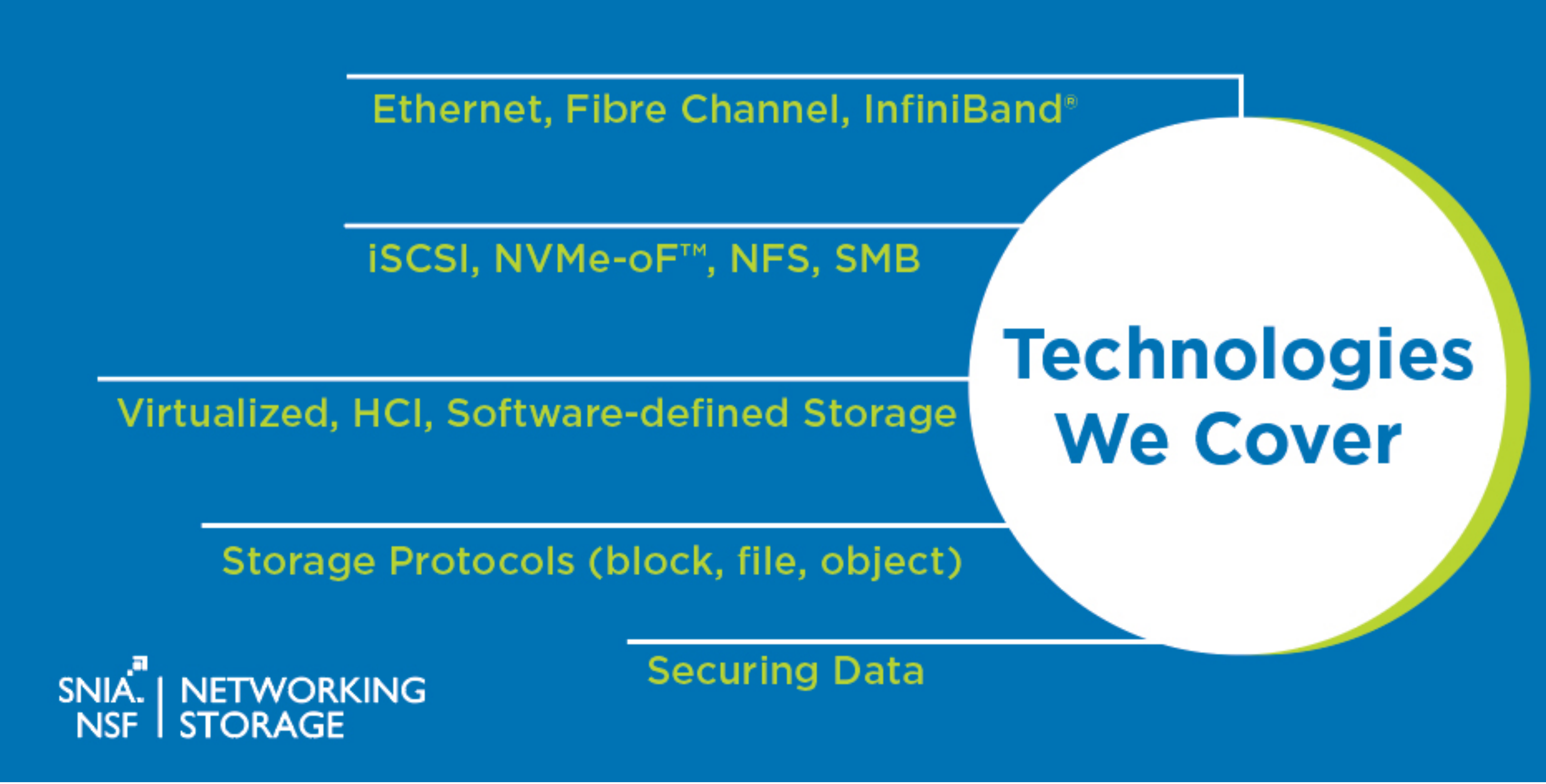
SNIA-at-a-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

Learn more: **snia.org/technical** **@SNIA**



Technologies We Cover

- Ethernet, Fibre Channel, InfiniBand®
- iSCSI, NVMe-oF™, NFS, SMB
- Virtualized, HCI, Software-defined Storage
- Storage Protocols (block, file, object)
- Securing Data

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

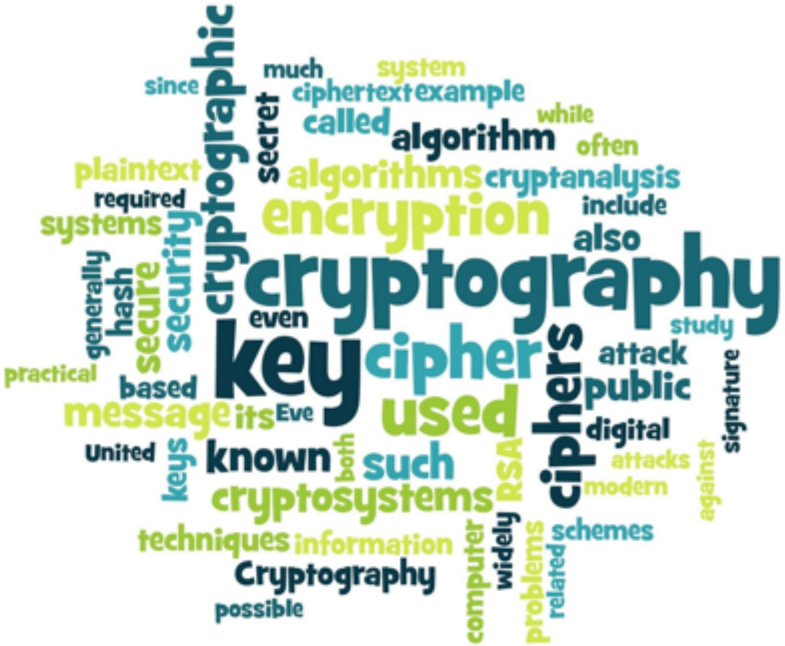
- Security problems
- Not quite retired network protocols
- NAS protocols

Security Problems

Eric Hibbard

Compromised Cryptography

- Weak Encryption Algorithms
  - Ciphers Considered Broken: RCx, DES
  - Inadequate Key Sizes – Provides Less Than 128 bits of Security Strength
- Hash Algorithms
  - Unacceptable Collision Rates
  - MD5, SHA-1
- Key Negotiations
- Inadequate Entropy



SSL & TLS

- Secure Socket Layer (SSL)
  - All versions are vulnerable and easily exploited; banned in most environments
- Transport Layer Security (TLS)
  - Protocol Versions Prior to TLS 1.2 Considered Vulnerable
  - Cipher Suites
    - Weak cryptographic algorithms
    - Inadequate key sizes
- Invocation Mechanism
  - StartTLS Versus Dedicated Port

Poor Security Options

- WiFi
- SNMP Prior to Version 3
- SSH Prior to Version 2
- DNS and NTP Without Security

Not Quite Retired Network Protocols

Networking You Should Consider Upgrading

John Kim

Aging Network Protocols

- RoCE v1 vs. RoCE v2
- NTP vs. PTP
- HTTP vs. HTTPS
- DNS vs. DoH
- VLAN vs. VXLAN

Rocky Road for RoCEv1

- RDMA over Converged Ethernet
- Most popular RDMA transport for Ethernet
- RoCEv1 runs InfiniBand transport (Layer 4) over IP
  - Use on one Layer-3 subnet only–not routable
- RoCEv2 runs UDP on top of IP
  - Routable, works with overlay networks
- RoCEv2 is default usage today
  - RoCEv1 still used in a few legacy implementations at rack scale

NTP vs. PTP—A Timely Topic

- NTP = Network Time Protocol
  - Precision to a few milliseconds based on software time stamps
  - V0 in 1985; V1 in 1988; V2 in 1989; V3 in 1992; V4 RFC in 2010
- PTP = Precision Time Protocol
  - Precision to 1 microsecond or better w/hardware time stamps
  - IEEE 1588: “V1” in 2002; “V2” in 2008; V2.1 in 2019
- Both popular, PTP used when high precision required
  - NTP V0/V1/V2 obsolete, V3 has vulnerabilities
  - PTP “V1” (IEEE 1588-2002) is obsolete

HTTP vs. HTTPS

- HyperText Transfer Protocol runs the web
  - Application layer, unsecured, port 80
  - Connections can be hacked fairly easily
- HTTPS is more secure
  - Uses SSL and/or TLS to encrypt traffic, port 443
  - (SSL is obsolete, as noted earlier)
  - Not just for e-commerce
- Secure web sites get better search rankings

DNS vs. DoH

- DNS = Distributed Name Service
  - How servers find other servers
  - Translates domain names into IP addresses
- DoH = DNS over HTTPS
  - Encrypts DNS requests and responses
  - Improves privacy, reduces tracking, but disables DNS controls
- Regular DNS still far more popular
  - DoH is still very new, not all ISPs/networks support it
  - Other DNS proposals are DNS over TLS and Oblivious DoH

VLAN vs. VXLAN

- VLAN = Virtual LAN
  - Subdivides network, up to 4096 virtual networks
  - Manages broadcast traffic, improves security
- VXLAN, NVGRE, GENEVE (and others)
  - Support network virtualization/tunneling, up to 16M segments
  - More extensible, lets L2 networks span L3 domains
  - Ideal managing virtual machines and containers
- VLAN ready to retire from Large Clouds
  - VXLAN is the most popular replacement today

NAS Protocols

Alex McDonald

NAS Protocols: SMB and NFS

- SMB and NFS: File system protocols
  - File System has a long history; term in use in the 1960s
  - NFS from Sun in mid/late 1980s
  - SMB (aka CIFS) from IBM in mid 1990s
- Why change?
  - **Security**: Software that is over 30+ years old probably has vulnerabilities
    - (Not always, but …)
  - **Performance**: is much improved
    - Modern protocol stacks are generally lower latency & better suited to WAN
  - **Scalability**: supporting more
    - Parallelism, large files support
  - **Features**: to support modern technologies
    - Databases, space efficiencies

SMB1 – Just Say No

- SMB1 can & has been exploited for ransomware
  - Wannacry and Petya
- No longer installed by default (hoorah!)
  - Stop using SMB1: https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858
- SMB2 and SMB3
  - SMB2 (2006), SMB3 (2012)
  - Current version is 3.1.1
- Features in SMB3
  - Transparent Failover, Scale Out, Multichannel, Direct
  - Encryption, VSS for file shares, Directory Leasing
- Backward compatibility
  - Older clients using SMB2 can be supported by SMB3 server
- SNIA SMB3 presentation
  - https://www.snia.org/educational-library/rockin-and-rollin-smb3%C2%A0-2017

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

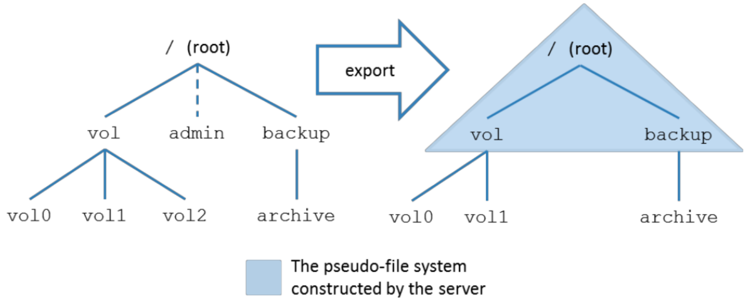
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

NFSv3 vs NFSv4

- Major differences don’t make migration that smooth, but…
- Several advantages of V4
  - Security (always a winner)
  - Modern network relevance
    - Works better over WAN due to (for instance) compound RPC operations
  - Internationalization; supports UTF-8
  - Pseudo file system; supports different hierarchical views
  - Thin provisioning, hole punching save space
- Paper & presentation on NFSv4
  - https://www.snia.org/sites/default/files/ESF/FINAL_SNIA_An_Overview_of_NFSv4-4_20Oct2015.pdf
  - https://www.snia.org/educational-library/what%E2%80%99s-new-nfs-42-2015

Pseudo File system



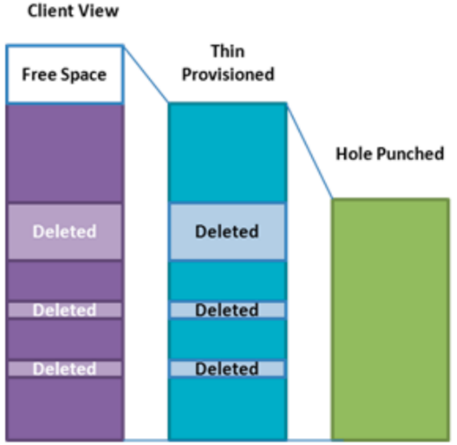


Figure 6; Reservations & Hole Punching

“Ripe for Refresh” Summary

- Review cryptography settings
  - MD5, SHA-1, DES…
- Replace SSL, TLS1.0/1.1
- Review SSH, SNMP, WiFi use
- HTTP→HTTPS everywhere
- Replace SMB1
- Consider ROCEv1→ROCEv2, NFSv3→NFSv4
  - Ask your suppliers for assistance/advice

Questions

After this Webcast

- Please rate this webcast and provide us with your feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast, including answers to questions we couldn’t get to today, will be posted on our blog at https://sniansfblog.org/
- Follow us on Twitter @SNIANSF

Thank You