SNIA NSF | NETWORKING STORAGE

Storage Networking Security Series: Protecting “Data at Rest”

Live Webcast

May 27, 2020

10:00 am PT

Today's Presenters

Presenter:
Pierre Mouallem
Lenovo

Presenter:
Dr. Ahmad Atamli
Nvidia

Moderator:
Steve Vanderlinden
Lenovo

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
- iSCSI
- NVMe-oF
- InfiniBand
- Fibre Channel, FCoE
- Hyperconverged (HCI)
- Storage protocols (block, file, object)
- Virtualized storage
- Software-defined storage

SNIA NSF | NETWORKING STORAGE

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.

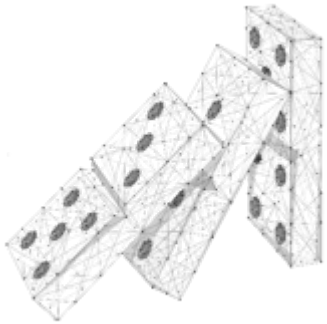
Agenda

- Security in a complex world
- Why security for Data-at-rest
- Data-at-rest vs. Data-in-flight
- Key Management
- Ransomware
- Importance of validating data backups
- Q&A

Security in a Complex World

What are the Basic Threats to Data at Rest?

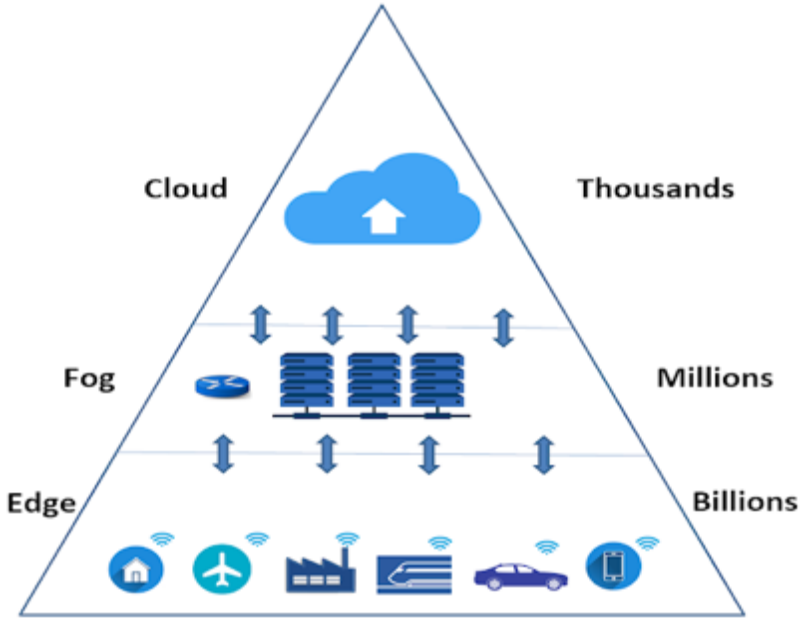
- Lost
  - Equipment failure, Human error
  - Natural disaster
- Compliance problems
  - Access, retention
  - Storage method/location
- Stolen
- Held for ransom



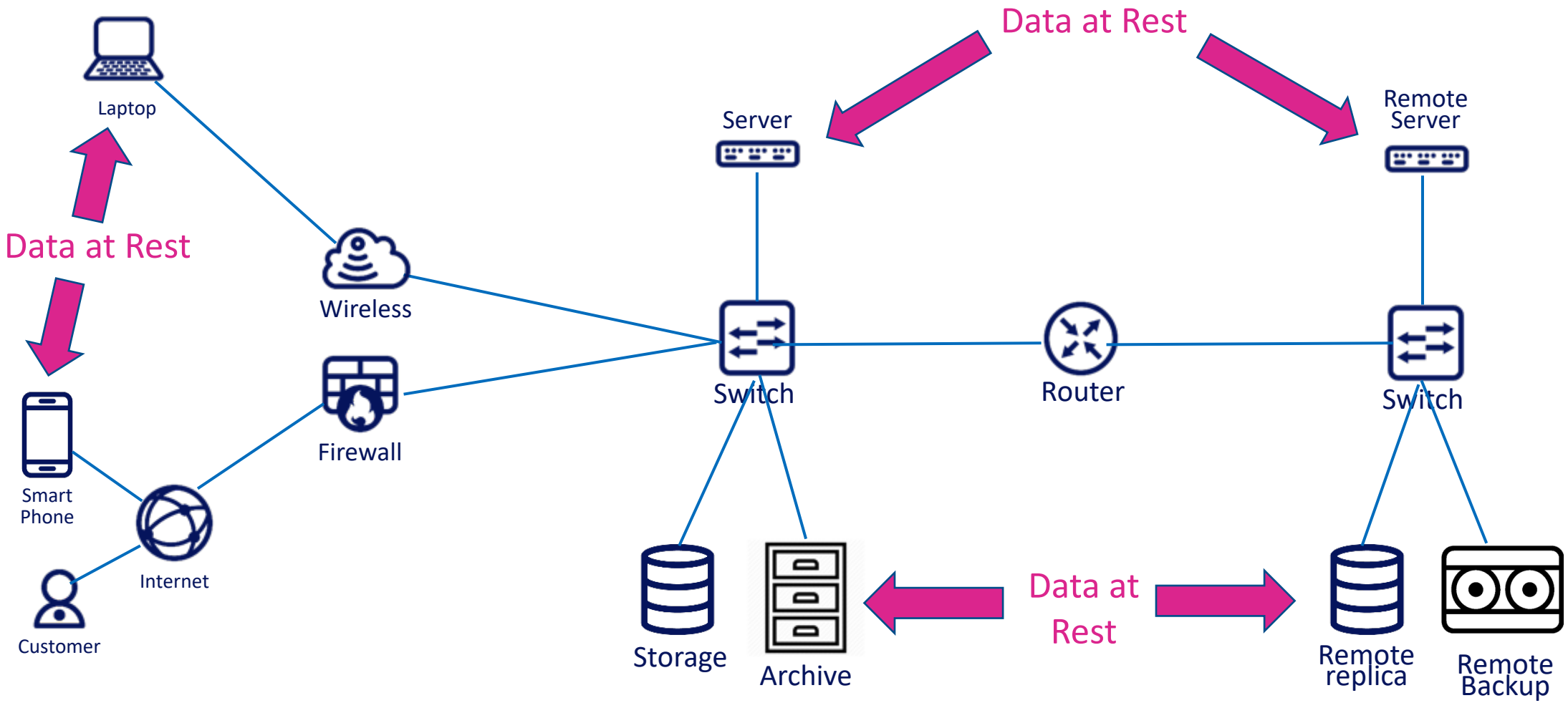
Data in a Complex World

- It's common to miscalculate the threats
  - Where is the data stored?
- Data stored in personal computer limit the threats calculated to one device
- Data stored in the cloud move between thousands of devices

PC

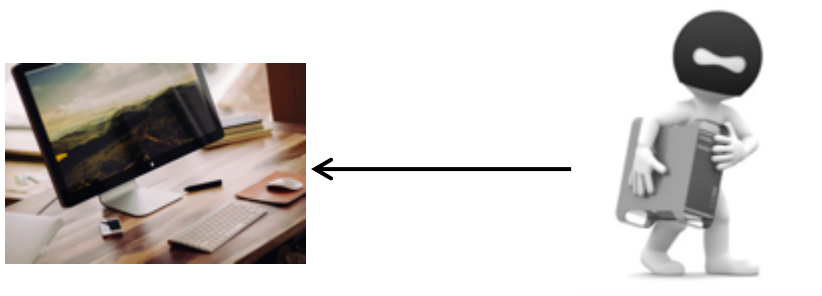


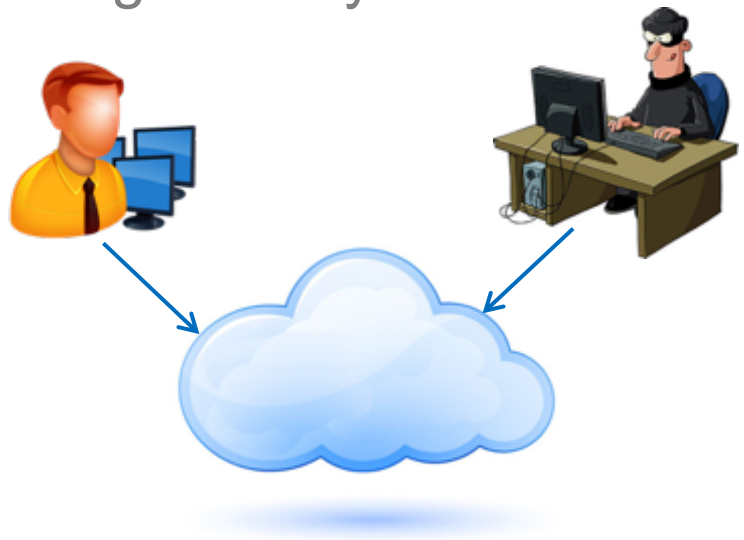
Typical Data-at-Rest Locations



Protecting Data-At-Rest, why?

- It's easy to remember the data accessed daily
  - Anti-virus, firewalls are the typical security controls involved in protecting data
    - How is the data protected when the anti-virus license expire in 3 years?
- it's easy to forget about data we do not use
  - What about data and archives stored that haven't thought of in years?
  - Who has access to your data ?





Compliance

Data-at-rest vs. Data-in-flight

- Cryptography was initially created to protect data-in-motion
- Data-in-flight rely on session keys that are short lived while Data-at-rest rely on storage keys that live for a long time
  - Which type of keys has a higher risk of exposure?
- Storing storage keys is as important as the data being stored
  - The golden solution is to store a key in someone's brain and make her immune to physical and emotional attacks
  - What is the lifetime of a storage key?

Data-at-rest vs. Data-in-flight

- Limiting the use of storage keys to reduce the risk of leakage is not practical or sufficient
  - Protecting access control is as important as protecting the keys
    - Does the key length matter for an attacker?
- It's sufficient for an attacker to hack into the system to get hold of a key once
  - We cannot rely on communication security to solve our system security problems

Key Management

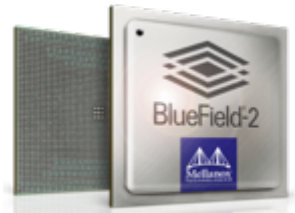
- "Key Management is one of the hardest subjects in security" - Applied Cryptography, Bruce Schneider
- Cryptographic keys are the pillars for secure communication, secure storage, and authentication
  - Break it once, break-it-all
- Cryptographic keys protects data from exposure and modification
- Protecting cryptographic keys is not easy
  - Where do we store a key?
  - What is the lifecycle of a key?
  - When is it most at risk of exposure?

Key Management - Protecting Keys

- Frequency of using the key may produce enough information to decipher the data without knowing the key
  - It's enough to get matching plaintext/ciphertext pair of every word in the English dictionary to decrypt one sentence in English
- Key Managers implemented in software leak data to other applications
  - Side-channels are exploited to leak keys from key mangers
- Single mistake in the implementation of a cryptographic function may result in weak and easy to break cryptography
  - Cryptography fails miserably when deviating from standard guidelines

Key Management

- To reduce the likelihood of exposure, we need to limit who has access to keys and how keys are accessed
  - How is this achieved?
  - Who can we trust to use the keys?
    - Neighbor? Admin? Operating System? System Firmware?
- Guidelines for key management design
  - Apply Trusted Computing principles
    - Trusted hardware
  - Apply privilege separation
  - Apply protection measures against software and hardware attacks
    - E.g. side-channel attacks, software and firmware attacks



Ransomware

- Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.
- There are a number of vectors ransomware can take to access a computer:
  - phishing spam - most common
  - Exploiting security vulnerabilities
- Everyone is a potential target for a Ransomware attack, from individuals to the largest corporations

Cost of Ransomware

- One of the fastest-growing malware hazards of the 21st century
- Example of Ransomware Attacks:
  - WannaCry in 2017, impacting UK's National Health Service
    - 200,000 computers in over 150 countries
    - Brought hundreds of NHS facilities to a standstill for several days
  - Erie County Medical Center in NY
    - Lost access to 6000 computers, requiring six weeks of manual operations
    - Recovery process that cost US$10M
  - Tech vendor Nuance
    - Attack cost 68M in refunds to customers for service disruptions and another $24M in cleanup costs.
- Total ransoms surged from $325M in 2015 to $5B in 2017, and are projected to reach $11.5B by 2020

Safeguarding against Ransomware

- Ensure that system(s) are kept up-to-date
- Perform frequent backups and verify backups regularly
- Store backups separately. Ideally on devices that aren't network accessible
- Train your organization.
  - Provide regular, mandatory cybersecurity awareness training
  - Implement phishing assessments that simulate real-world phishing emails

Importance of Validating Data Backups

- Data backups can be accidently erased, become corrupted or become invalid for a number of reasons
- Data Backups must to be validated on a regular basis to ensure data integrity and availability
- Data Backup validation provides an extra layer of protection against Ransomware, and ensures that your organization can handle Disaster Recovery

Conclusions

- Cyber-Criminals capabilities are on the rise and attacks are getting stealthier
- Data-at-rest can be easily forgotten and easily accessed when data is not encrypted
- Cryptographic keys are the pillars for protecting data at rest, protecting the keys is a challenge
- Compromised data at rest can be detrimental to organizations as seem in the ransomware examples
- Validating data at rest is a critical component of protecting that data

The Storage Networking Security Webcast Series

On-demand at the SNIA Educational Library: snia.org/educational-library

- Understanding Storage Security and Threats
- Protecting Data at Rest
- Encryption 101
- Key Management 101 – June 10, 2020
- Follow us on Twitter @SNIANSF for dates and times of others planned:
  - Applied Cryptography
  - Protecting Data in Transit
  - Securing the Protocol
  - Security Regulations
  - Securing the System: Hardening Methods

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

