SNIA NSF | NETWORKING STORAGE

Understanding Storage Security and Threats

Live Webcast
October 8, 2019
10:00 am PT

Today's Presenters

Steve Vanderlinden
Lenovo

Pierre Mouallem
Lenovo

J Metz
Cisco

John Kim
Mellanox

SNIA-at-a-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

Learn more: **www.snia.org/nsf**

@SNIANSF

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.

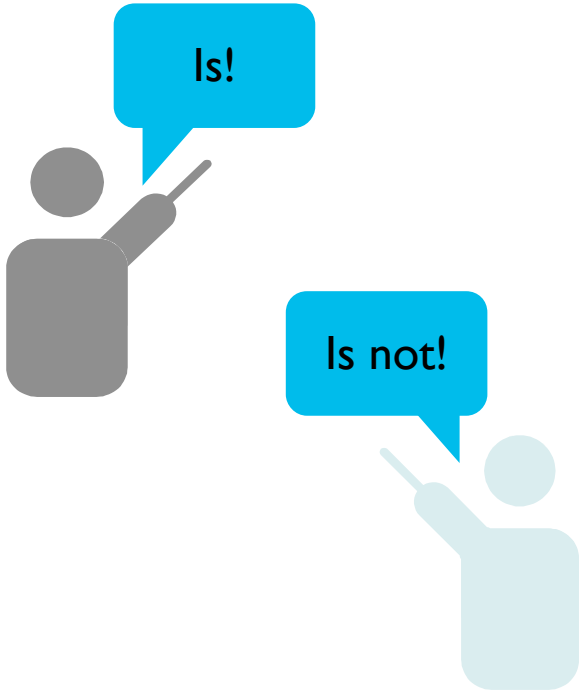
NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

About The Storage Security Series

What this Series is/is Not

- This series *is*…
  - A holistic view on aspects of securing storage, from devices to networks, from encryption to regulation, from the technical to the human
  - Storage-oriented and focused
- This series *is not*…
  - Proscriptive
  - A guarantee for success
  - Comprehensive

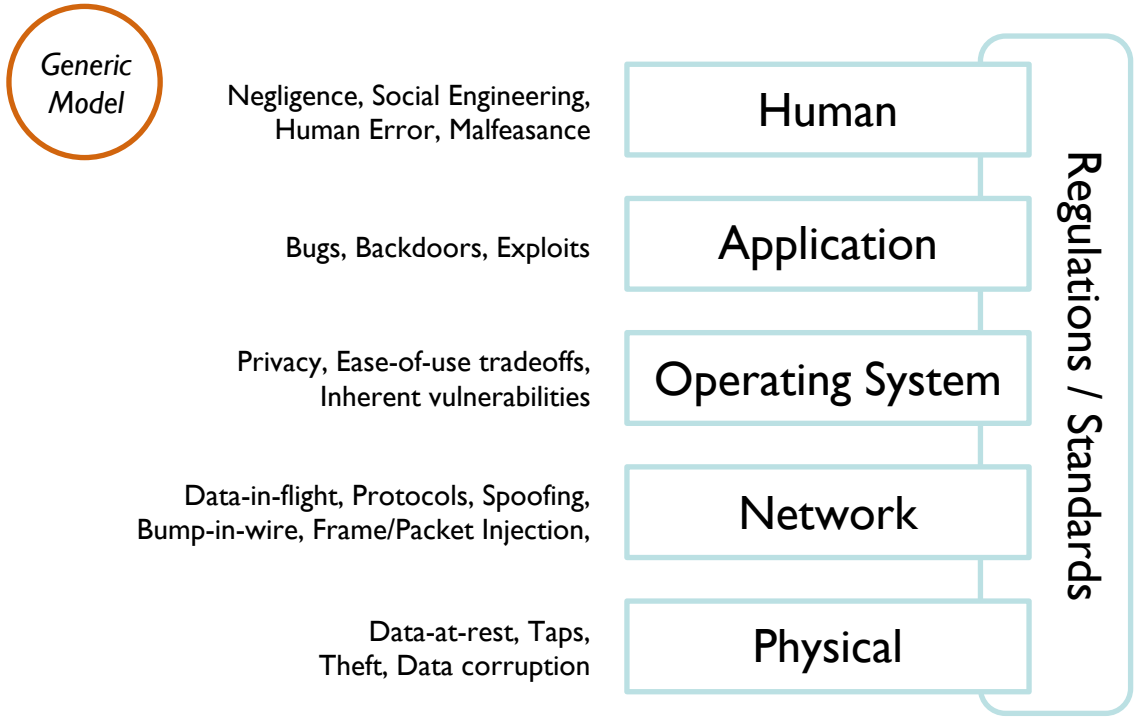


Storage Security Series

After this introductory session, the other units can be viewed in any order

- Overview and Security Principles
- Securing Data Processing
- Storage Encryption
- Securing Data in Transit
- Securing Data at Rest
- Understanding Security Regulations

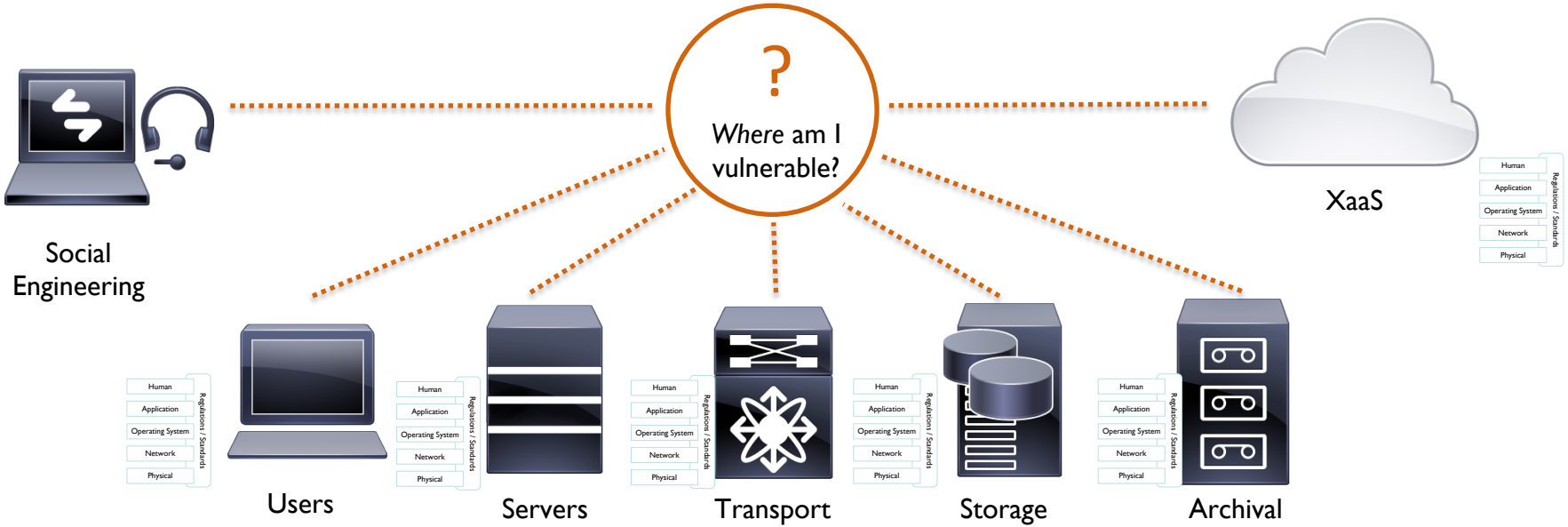
Working In Layers



- Holistic model is basically an extended OSI model
- Each layer has its own peculiar vulnerabilities

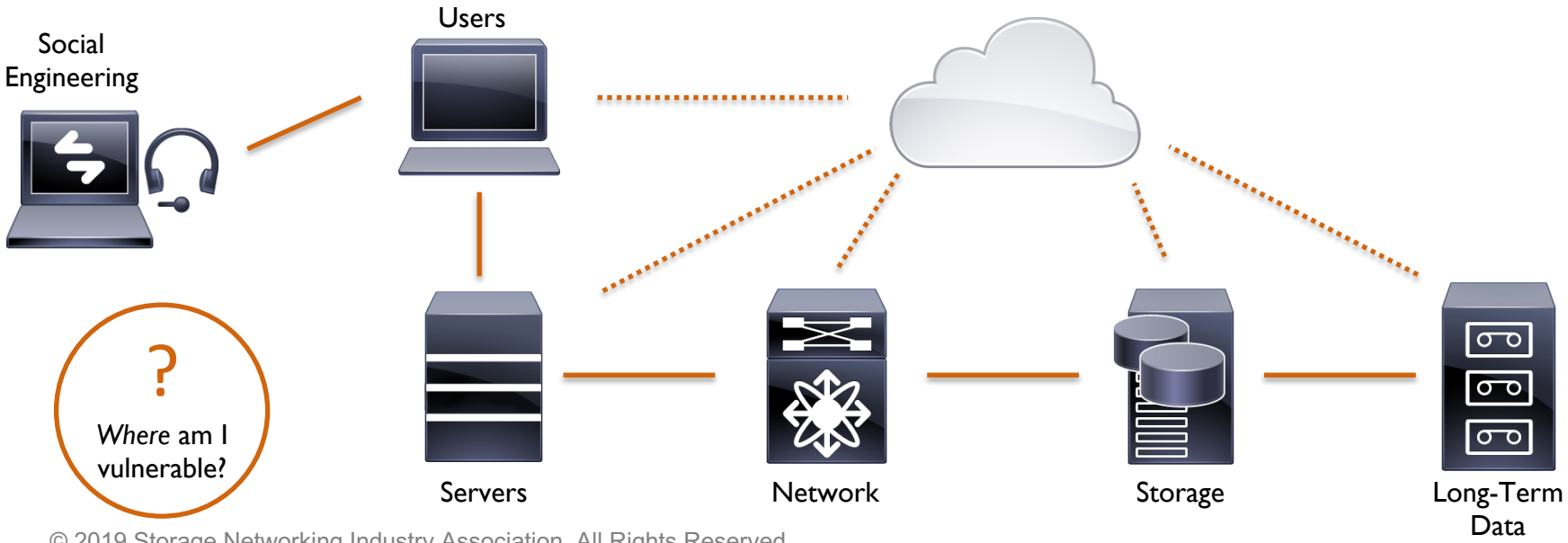
Big Picture

- You can secure components, and you can secure architecture
- Knowing *where* you are vulnerable is critical to being secure



Big Picture

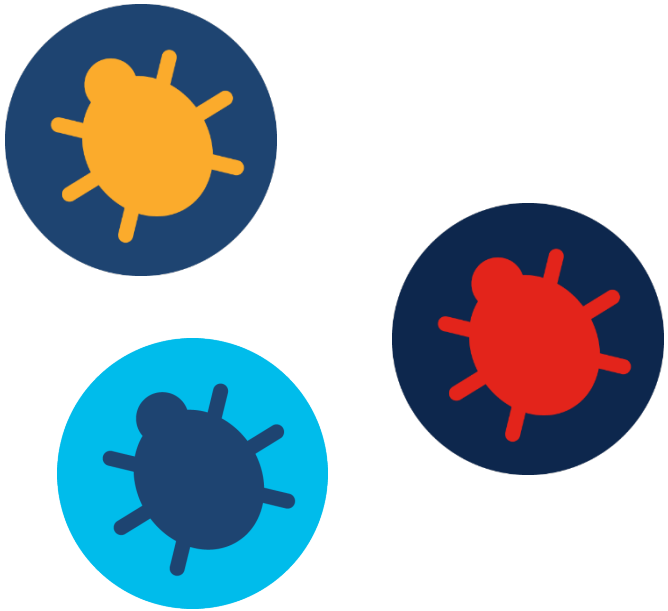
- You can secure components, and you can secure architecture
- Knowing *where* you are vulnerable is critical to being secure



Terminology

Security Terminology

- Threats, Vulnerabilities and Risk
- Attack Vector and Attack Surface
- Malware and Malicious Actor
- Regulations and Compliance



Security Threats and Vulnerabilities

SNIA NSF | NETWORKING STORAGE

Threat

- Potential attempt to compromise system or data
  - Steal/ransom data
  - Control your systems
  - Cause downtime
- External or internal
- Usually digital
- Threat carried out = *attack*

Vulnerability

- Design, gap, or flaw that increases susceptibility to a *threat*
  - Makes attack more likely to succeed
  - Often exists because specific *threat* or *attack vector* was unknown or not anticipated
- Software, HW, or physical

Security Risks

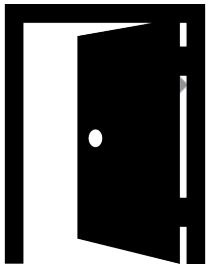
- **Risk**
  - Chance of something bad happening to your systems or data
    - Varying probabilities
    - Non-security risks: fire/flood/cut fiber/blackout

In security terms:

***Threat* + *vulnerability* = risk**

Attack Vector and Surface

Attack Vector



- Route for *threat* to reach a potential *vulnerability*
- Different levels / categories
  - Social / human
  - Application / software / OS
  - Network / media / physical
- Vector existence doesn't guarantee attack success

Attack Surface

- Sum of *attack* vectors

Keeping the attack surface as small as possible is a security best practice

Malware and Malicious Actor

SNIA NSF | NETWORKING STORAGE

Malware

- Short for Malicious Software
- Software that purposely designed to cause damage to a server or application
- Sent by a *malicious actor*
- Types of Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, and adware

Malicious Actors

- Person or organization that attacks data or systems
- 4 types: Cyber Criminals, Hacktivists, State-sponsored attackers, Insider Threats

Regulations and Compliance

SNIA NSF | NETWORKING STORAGE

Regulations

- Rules that affect how, where and/or how long you must store and protect data
- Might regulate access, use, privacy, hardware, systems
- Proscriptive or prohibitive

Compliance

- Practice, agency, or people that ensures regulations are followed
  - Internal employees and/or external agency
  - Under penalty threat

Regulations – Examples

- Current and proposed regulations
  - General Data Protection Regulation (GDPR)
  - Service Organization Control (SOC1, SOC2, SOC3)
  - Federal Information Security Management Act (FISMA)
  - Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)
  - Federal Risk and Authorization Management Program
  - DoD Cloud Computing Security Requirements Guide (SRG)
  - Criminal Justice Information Services
  - National Institute of Standards and Technology (NIST)
  - Payment Card Industry (PCI) Data Security Standard DSS Level 1
  - Federal Information Processing Standard (FIPS)
- Privacy Laws
  - Health Insurance Portability/Accountability Act (HIPAA)

Attack Objectives

Attack Objectives

- Denial of Service
- Data Infiltration, Modification or Exfiltration
- Impersonation

Denial of Service

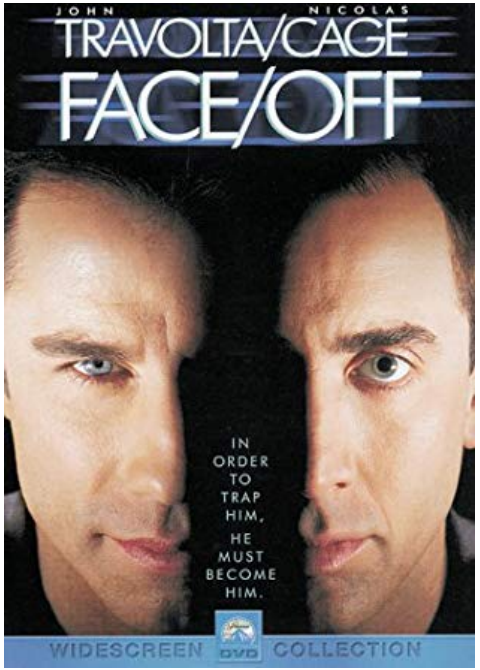
- **Denial-of-service** (**DoS**) **attacks** are attacks in which perpetrators seek to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host.
- Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled
- **Distributed denial-of-service (DDoS) attacks** is a variant of DoS where the incoming traffic flooding the victim originates from many different sources, making it harder to stop the attack by simply blocking a single source

Data Infiltration, Modification or Exfiltration

- **Data Infiltration** is the unauthorized injection of data on a target system
- **Data Modification** is the unauthorized data modification on a target system
- **Data Exfiltration** is the unauthorized data transfer from a target system. It is also commonly called data extrusion or data exportation

Impersonation

- An **impersonation attack** is an **attack** in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol



Safeguards Overview

Core Security Concepts - CIA Triad

- Confidentiality
  - Ensures that only “only” authorized users can be permitted to access the required information
- Integrity
  - Ensures that “no one can alter” the data without proper Authorization throughout the entire lifecycle
- Availability
  - Ensures that data and resources are available for legitimate users

Core Security Concepts - Authentication, Authorization, Accounting (AAA)

SNIA NSF | NETWORKING STORAGE

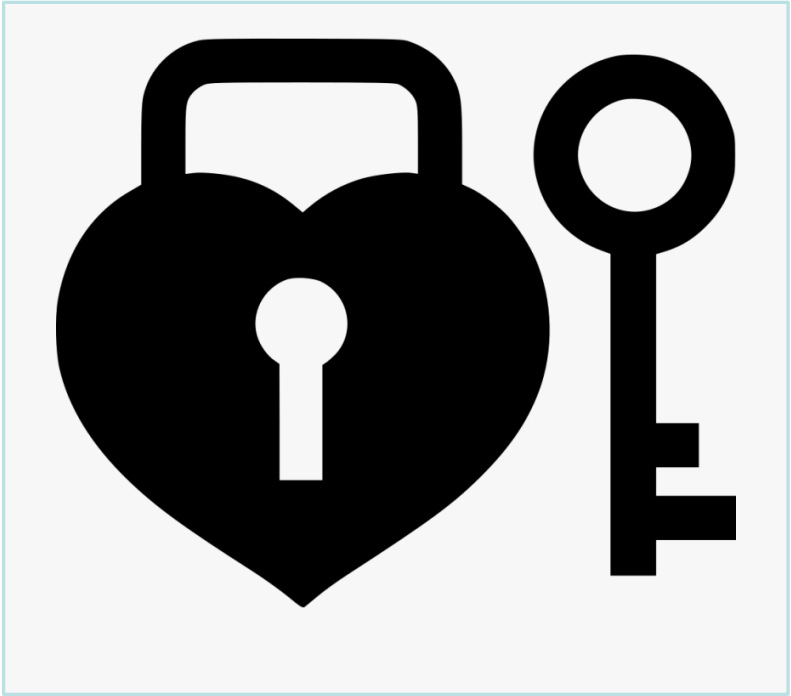
- Authentication
  - Verifying you are truly who you say you are
- Authorization
  - Checking and controlling what you are or are not allowed to see, do, change, and delete
- Accounting
  - Recording who did what, when (and sometimes how and from where)
  - Might also identify improper behavior or imposters

Remediation Strategies

- Adopt the following Principles
  - Least Privilege
  - Separation of Duties
  - Defense-in-Depth
  - Fail-Secure
  - Simplicity
  - Trust Nobody
  - Least Common
  - Secure Weakest Link
  - Leverage Existing Functionality

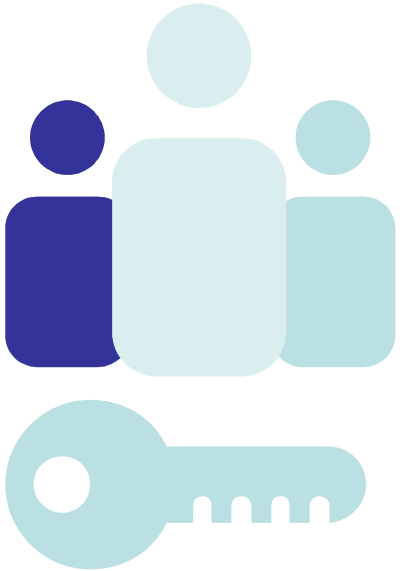
Protections

- Safeguarding the People
- Safeguarding the Data
- Safeguarding the Components
- Safeguarding the System



Safeguarding the People

- Multi-way street
  - Protect the producers of the data
  - Protect the consumers of the data
  - Protect the gatekeepers to the data
- Eliminating Default Credentials
- Ease-of-Use versus Security
  - What's the Trade-off?
- Ethical responsibility
- "Social" Hacking
  - Phishing
  - Blackmail
  - Malicious (ex?) Employees
  - Unintentional infection
    - (e.g., bring swap USB drives with a home/school laptop that has been infected at the school)



Future of this Series

Where To Go Next?

These webinars will be released over time…

- Overview and Security Principles
- Securing Data Processing
- Storage Encryption
- Securing Data in Transit
- Securing Data at Rest
- Understanding Security Regulations

Conclusion

Summary

- The most important step is the first one
  - This is the first step in understanding storage security – knowing what we mean when we talk the terms
- Storage security isn't just about locking down a device, or a server, or a drive
  - Nor is it about how strong your encryption is
- Storage security is a holistic process that works both up and down the stack, as well as across devices

After This Webcast

SNIA NSF | NETWORKING STORAGE

- Please rate this webcast and provide us with feedback
- This webcast and a PDF of the slides will be posted to the SNIA Networking Storage Forum (NSF) website and available on-demand at www.snia.org/forums/nsf/knowledge/webcasts
- A full Q&A from this webcast, including answers to questions we couldn't get to today, will be posted to the SNIA-NSF blog: sniansfblog.org
- Follow us on Twitter @SNIANSF

Thank You