THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

SERVICE RELIABILITY AND SECURITY STANDARDIZATION

Michael Tortorella, Ph.D.
Rutgers University
Piscataway, NJ 08854

OVERVIEW

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- Theme
- Current challenges
- Service reliability framework
- Service security framework
- Conclusion
- Acknowledgments

THEME

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- Reliability and security are major concerns of service users
- Technology in the service delivery infrastructure is constantly changing
- Some new services are enabled by these changes
- Legacy services thrive in new Service Delivery Infrastructures (SDIs)

THEME

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- Service Reliability and Security are technology-agnostic
- Users don't know or care what spiffy technologies you use to deliver their service(s)
  - It doesn't matter how clever or how proud of your achievements you may be, users want reliable, secure services no matter what

CURRENT CHALLENGES

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- SDN
- NFV
- Just some more in the long line of cost reductions and technology enhancements that the telecom industry has seen for many decades
- Concurrently, understanding of service reliability and security has evolved considerably in the past few years
  - POTS was simple
  - Even TCP/IP does not defy understanding
  - Usually the big problem was that networks were overbuilt, leaving $$ on the table
    - Was the 2 hours in 40 years TDM switch downtime objective really needed?

CURRENT CHALLENGES

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- SDN and NFV add centralized controls that can be a service reliability risk
- Reliability requirements are needed for networks that use SDN and NFV
- These have to be derived from
  - Service reliability requirements
  - Service delivery infrastructure (SDI) modeling that connects failures and outages in the SDI to service failures and outages

CURRENT CHALLENGES

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- Reliability requirements for SDI network elements cannot be specified independently of reliability requirements for services
- How to maintain network resiliency in an SDN/NFV world?
  - Formerly used multiple paths, TCP/IP, etc.
  - Modeling using “representative connections” is totally inadequate and obsolete
    - Networks are connectionless

CURRENT CHALLENGES

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- NFV is a consistent platform architecture hosting many network functions
  - Faults within the platform architecture could span many (or even all) functions
  - Chance of a catastrophic failure could be higher than with current networks
    - Physical infrastructure
    - UDP, TCP/IP, and other protocols

CURRENT CHALLENGES

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- Designing resiliency into SDN/NFV networks requires novel approaches
  - Internal service chain resiliency
  - Parallel service chains with load balancers
  - Real-time reconfiguration (e.g., FASTAR)
- All of these require new service reliability models before reliability requirements can be assigned to network elements and functions

A WAY FORWARD

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- Define standard reliability requirements for services
  - Accessibility
  - Continuity/Fulfillment
  - Release
- Commission modeling studies of SDIs using SDN/NFV focused on how SDI element/software/protocol failures lead to service failures

A WAY FORWARD

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- Develop reliability requirements for SDIs using SDN/NFV from
  - The service reliability requirements
  - The relationships uncovered n the modeling work
- Industry/university partnerships
  - SDI modeling
  - Networks with unreliable elements

SERVICE RELIABILITY ECOSYSTEM

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- User-centric requirements tailored to the service
- Modeling standards
  - Connect reliability of the service to reliability of the SDI and its elements
    - Hardware
    - Software
    - Protocols
- Data collection standards matched to service and SDI reliability needs

SERVICE SECURITY ECOSYSTEM

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- User-centric requirements
- Modeling standards
  - Now including attacks
- Data collection standards

CONCLUSION

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

- We propose a standardized framework for setting user-centric service reliability and security requirements
- With minimum requirements for modeling, data collection, and analysis

ACKNOWLEDGMENTS

- S. Makris (Palindrome Technologies)
- Participants in the IEEE 2014 CQR Roundtable
  - B. Levy
  - D. Lu
  - C. Qiao
  - M. Ulema
  - G. Xie
  - Y. C. Yeh