



Threats and Realities in Fibre Channel Security

A Rasputin-free Conversation about Fibre Channel

Landon Curt Noll & Dr. J

T11-14-114v0 - 2014 Apr 01

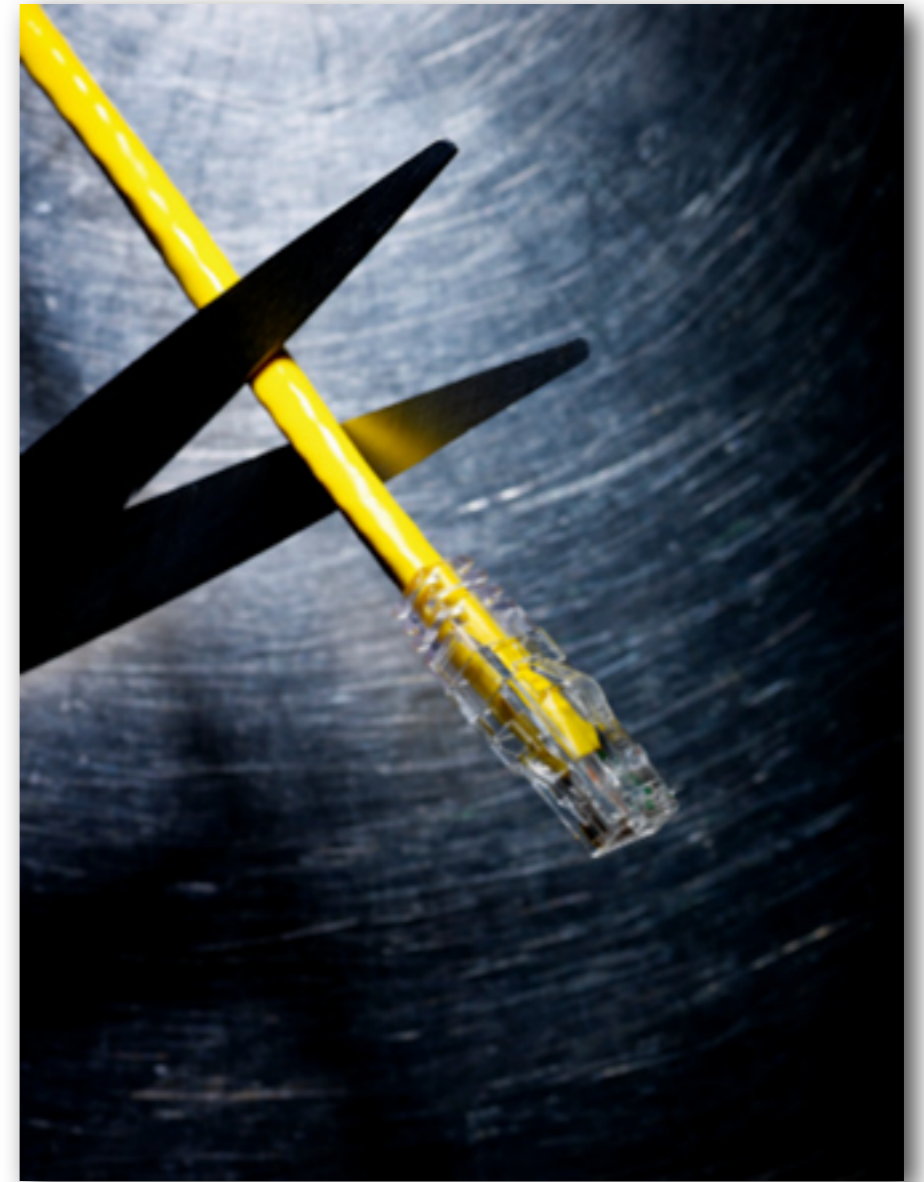
Administrivia

- Sponsorship of T11/FCIA events
 - Speaking slots available
- Call for Interest in future plug-fests



Topics

- What is the purpose of “Security”?
- Fibre Channel and Security
 - Is it secure?
 - *Isn't* it secure?
- Now that we have SP2, isn't FC secure *now*?
- What's missing?
- What does T11 (and/or FCIA) need to do?



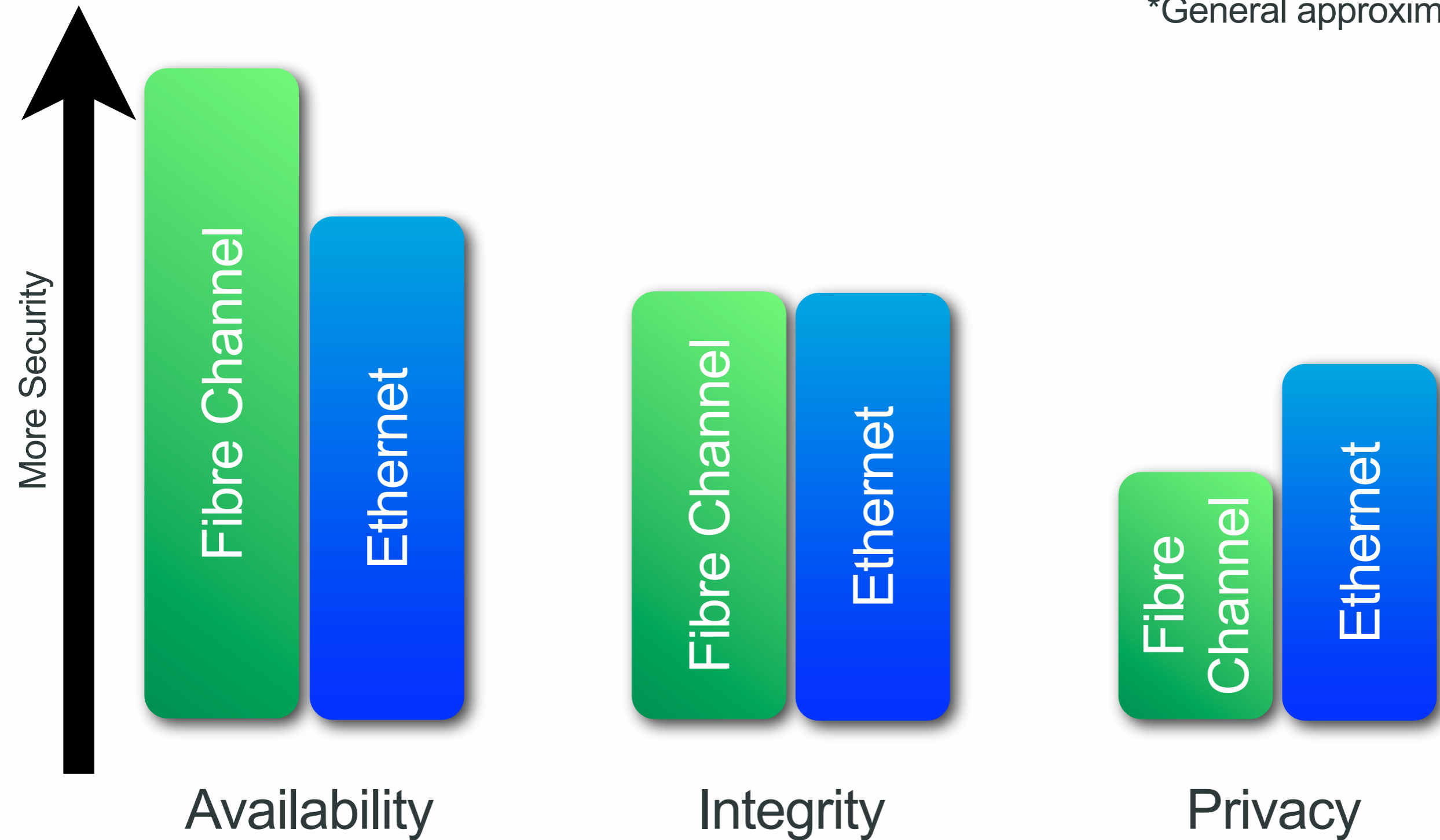
What is Security?



- For the services offered, the purpose of Security is to enable an appropriate level of
 - Availability
 - Integrity
 - Privacy
- Well designed and maintained security is a Positive
 - not simply something that denies certain actions
- Process, not a destination

Ethernet & FC - Which Is More Secure?*

*General approximations



Transitive Trust Problem

If A can screw B

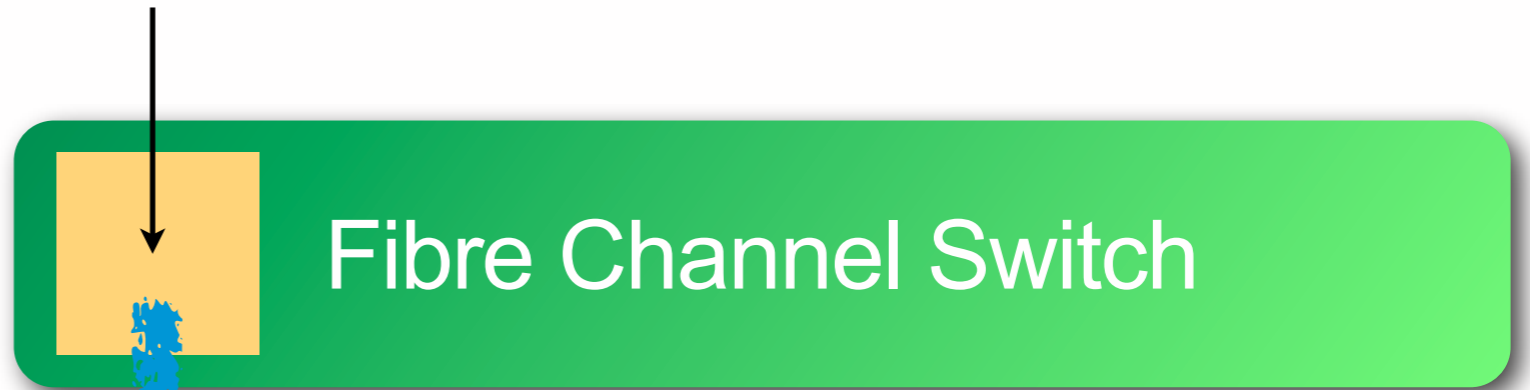
...and B influences FC...

...then A can screw FC

by way of B



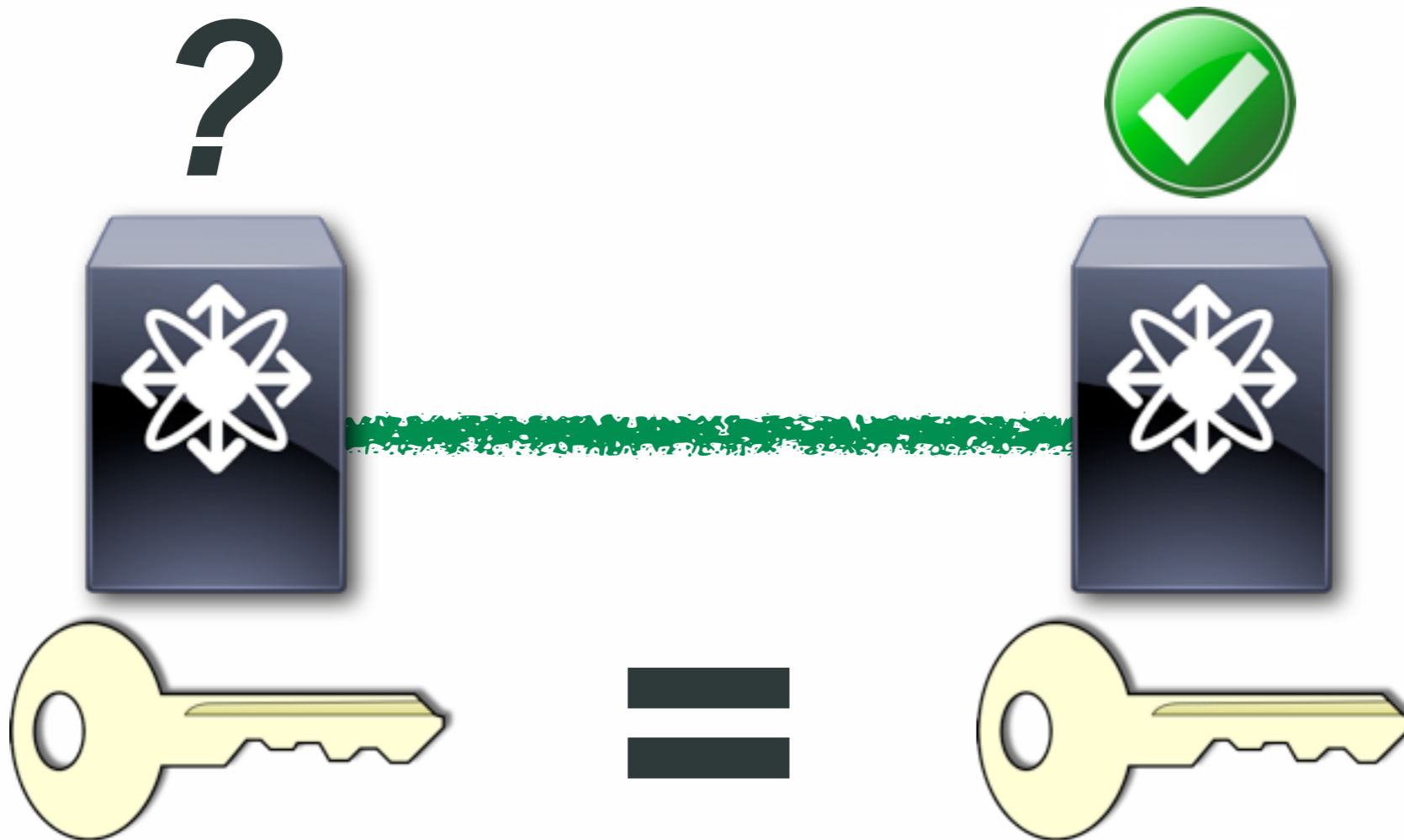
Management Interface



Mwuah-ha-ha-ha!!!

Okay, what is SP2?

- Two machines want to talk in a way that other people can't mimic, confuse, corrupt, snoop, etc.
 - These two things that come up with a key so that if you don't have a key, you can't participate
 - Can compute a key on the fly and say, "Let's use *this* key."



Agreement between the switches that says, "I know you are who you say you are."

Right Questions to Ask



- What tools are needed for customers to secure their FC-based storage?
- How can we improve the tool set used to secure FC-based storage?
- How does the security of FC-based storage fit into a larger context, e.g.,
 - Storage security in general
 - Data Center security
- How well does FC fit into requirements for security mandated by others?
 - Industry associations
 - Government requirements
 - Best practices

What's Missing?

- FC-SP-2 key management
- Guidance on one to select appropriate FC-SP-2 options
- FC security profiles
- Auditing of FC activity
- FC roles
- FC threat model

... just to name a few



T11's Next Steps



- Understand FC is not secure by default
- Create a comprehensive FC threat model
- Determine how emerging technologies impact the FC threat model
- Learn how to attack FC so we can understand how to defend it
- Examine issues of confidentiality of a fabric
- Develop FC security profile structure
- Establish security liaisons with relevant standards bodies

FCIA's Next Steps

- Identify important FC usage profiles
- Identify relevant industry, government & best practice profile requirements
- Prioritize on the more important FC profiles
- Request T11 to initially focus on those FC profiles



Bottom of talk.

Any Questions?

Thank you.



Landon Noll Touching the South Geographic Pole \pm 1cm
Antarctica Expedition 2013