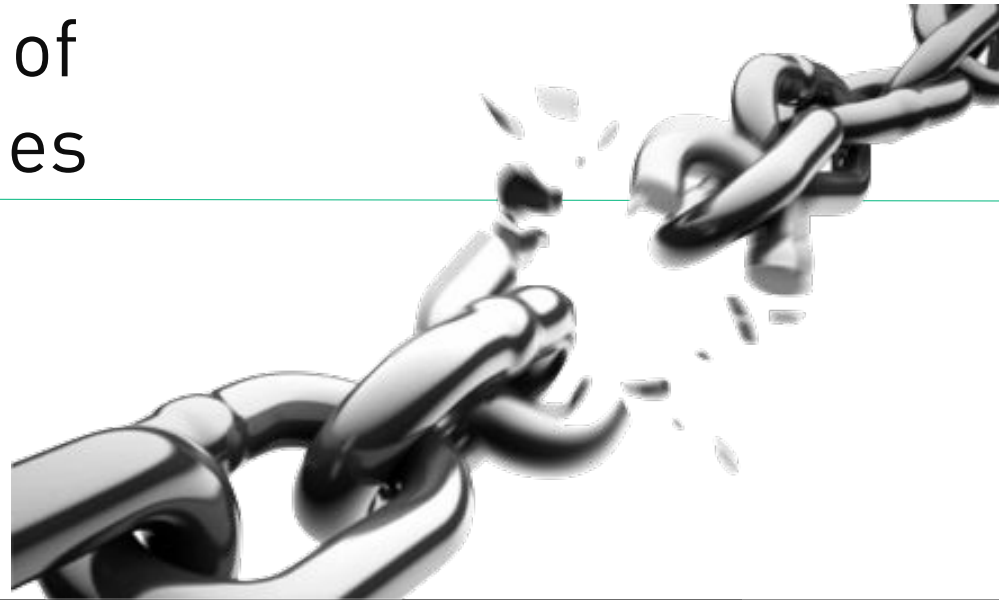


# Security Implications of Disruptive Technologies

Enno Rey, [erey@ernw.de](mailto:erey@ernw.de)  
[@Enno\\_Insinuator](https://twitter.com/Enno_Insinuator)



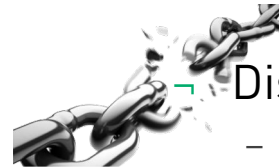
# Agenda



- News Kids in Network Town
  - Some future protocols & their conduct

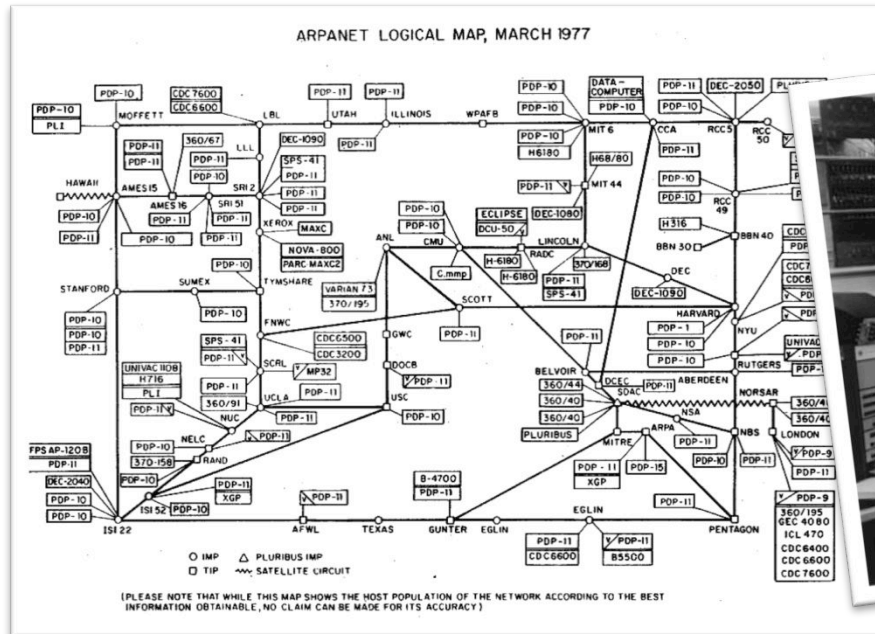


- The Internet & Its Inhabitants
  - Some history



- Disruption
  - What all this might mean

# In the Beginning



DARPA Internet Architecture

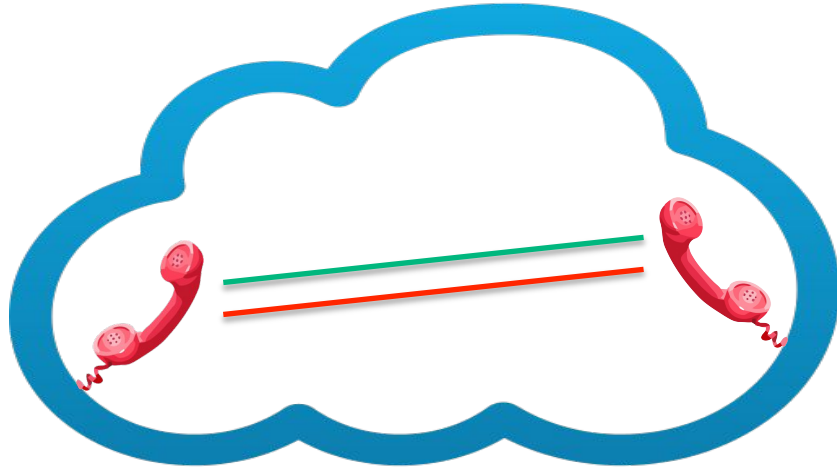
## Design Philosophy



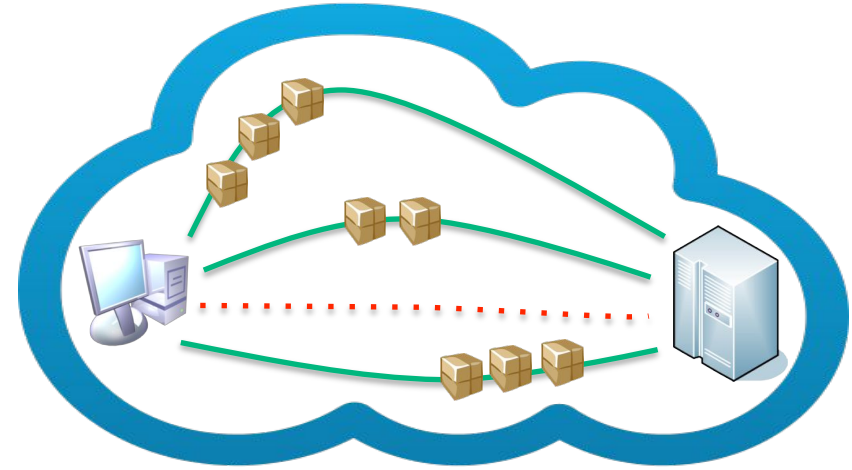
*“The top level goal for the DARPA Internet Architecture was to develop an effective technique for multiplexed utilization of existing interconnected networks.”*

[Clark88]

# Circuits vs. Datagrams/Packets



Circuit-based network



Packet-based network

# Fundamental Principles at the Time



*Survivability  
in the  
Face of Failure*

[Clark, 1988]



*End-to-end  
principle*

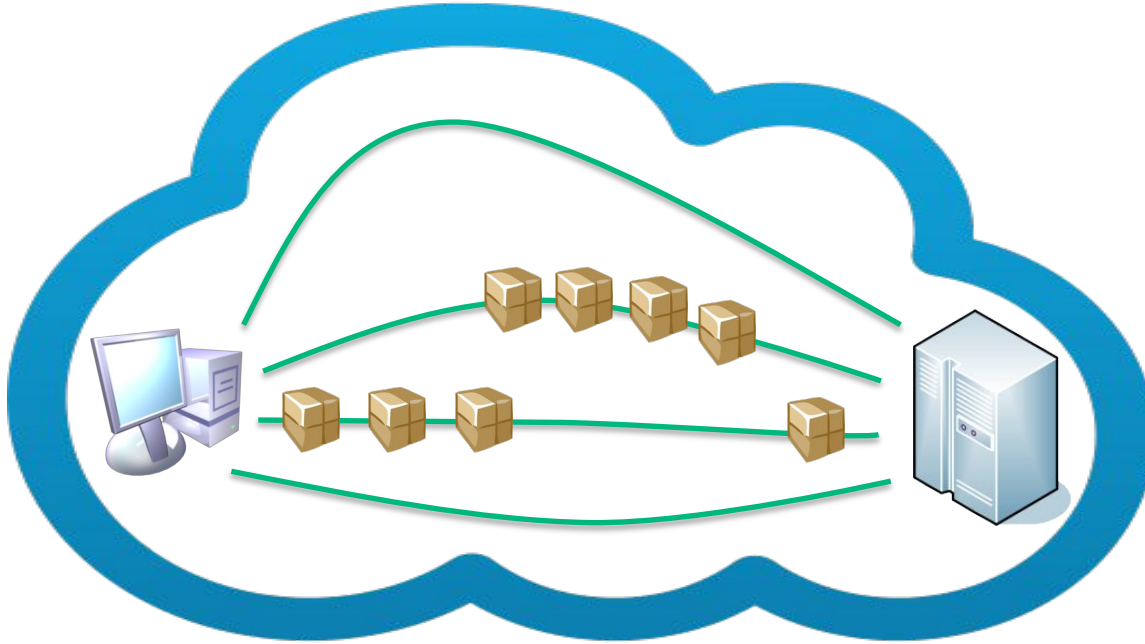
[Saltzer, 1981]



*Robustness  
Principle*

[RFC 761, 1980]

# Let's Have Closer Look at Some of Them:



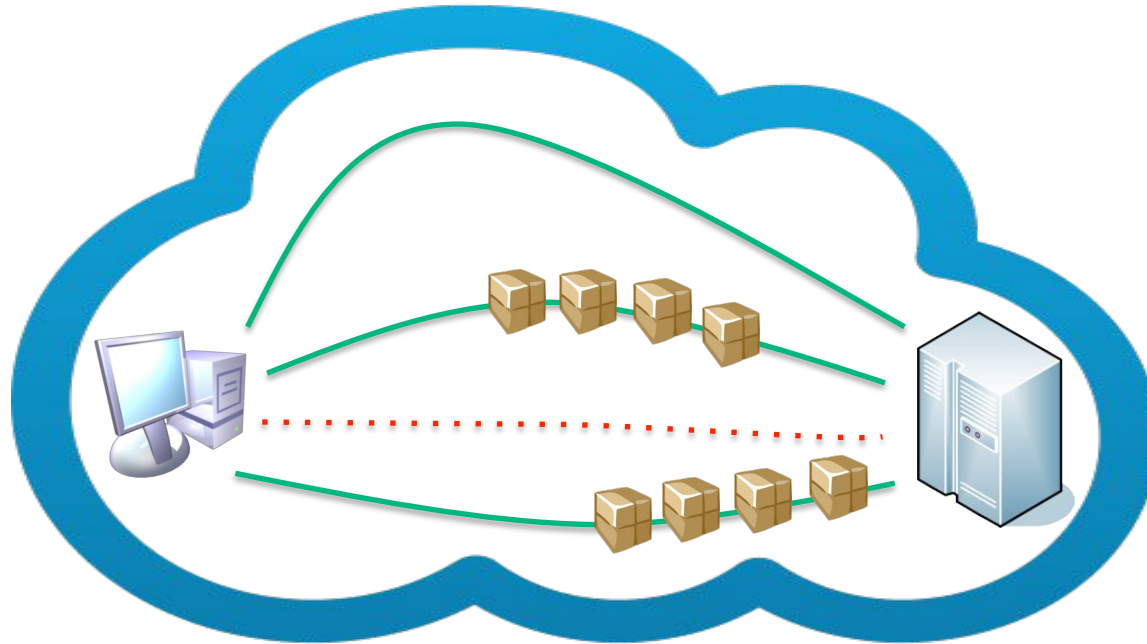
Packet-based NETWORK

## Survivability in the Face of Failure

(Clark 1988)



# Let's Have Closer Look at Some of Them:



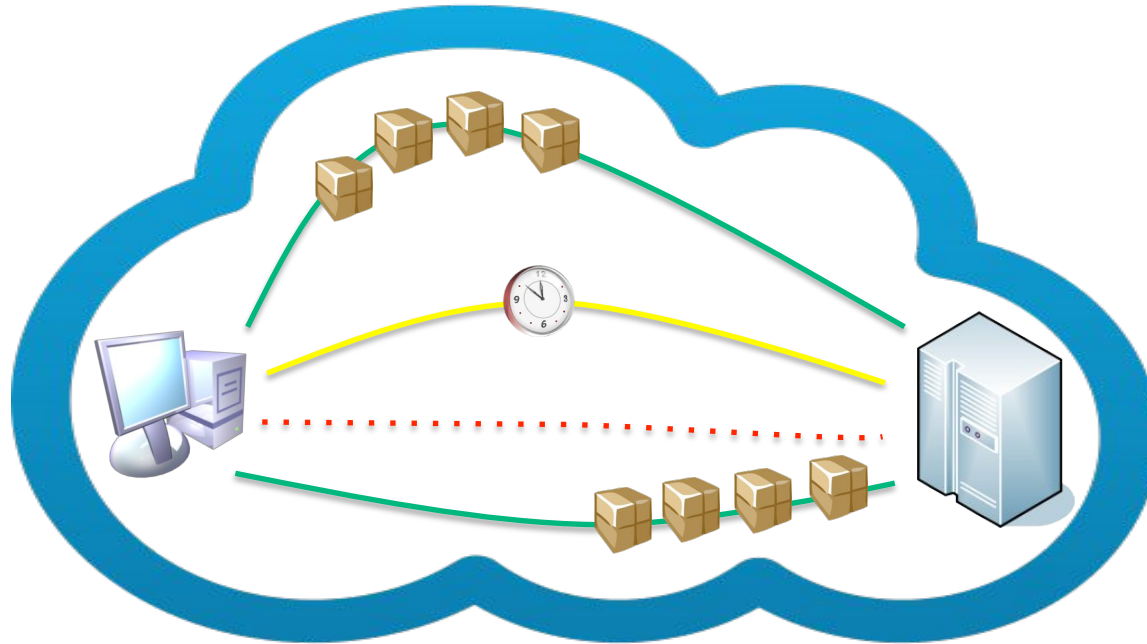
Packet-based NETWORK

## Survivability in the Face of Failure

(Clark 1988)



# Let's Have Closer Look at Some of Them:



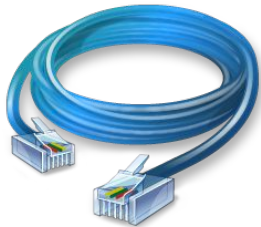
Packet-based NETWORK

## Survivability in the Face of Failure

(Clark 1988)



## End-to-end Principle



*“The principle, called the end-to-end argument, suggests that functions placed at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level.”*

Read:

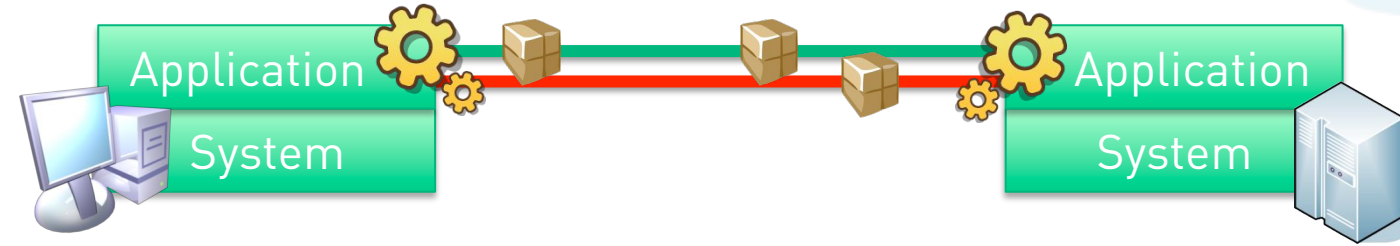
“the network” – which is an unreliable thing anyway – is not supposed to interfere with the communication acts of “end systems”



Packet-based NETWORK

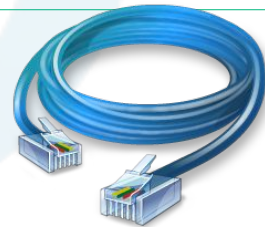
## End-to-end principle

(Saltzer, 1981)



End-to-end principle

(Saltzer, 1981)



Packet-based NETWORK

## “Fate-Sharing”

End-to-end principle (Saltzer, 1981)

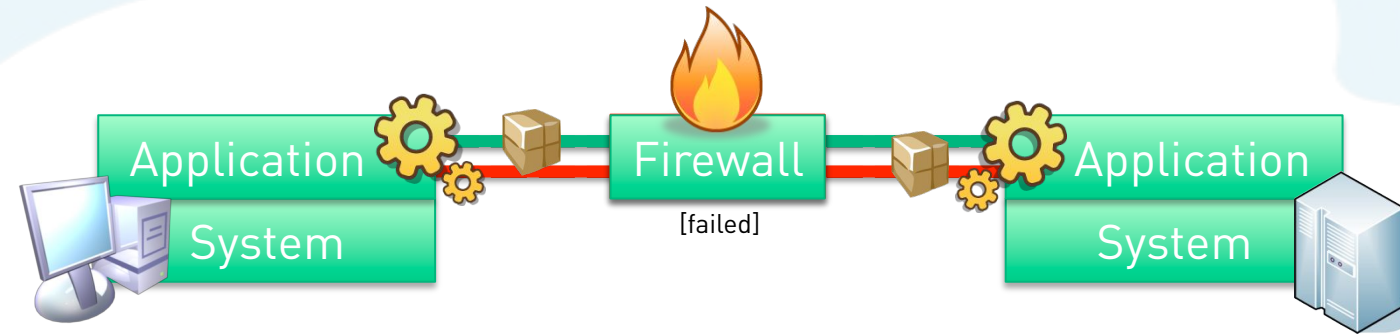


*“The fate-sharing model suggests that it is acceptable to lose the state information associated with an entity if, at the same time, the entity itself is lost.”*

Read:

not being able to communicate with another system is only ok if that system is dead (or I am dead myself).

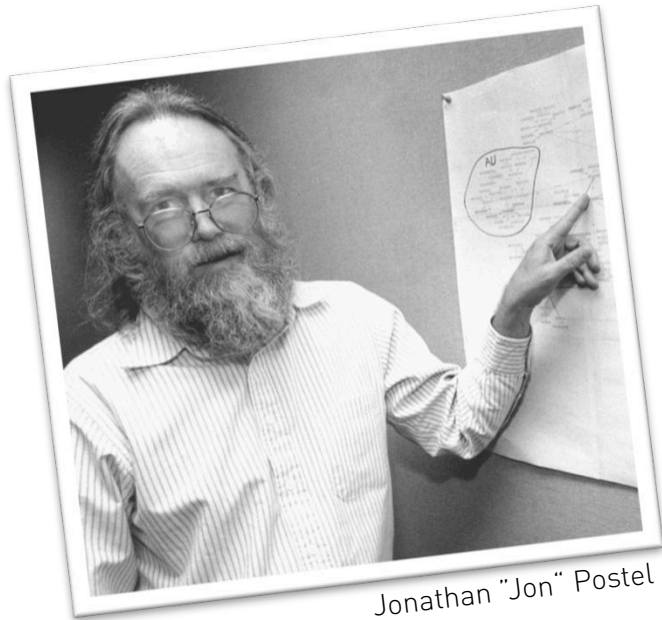
→ Don't keep *state* “in the network”!



“Fate-Sharing”

Negative Example –  
How it’s not supposed  
to be!

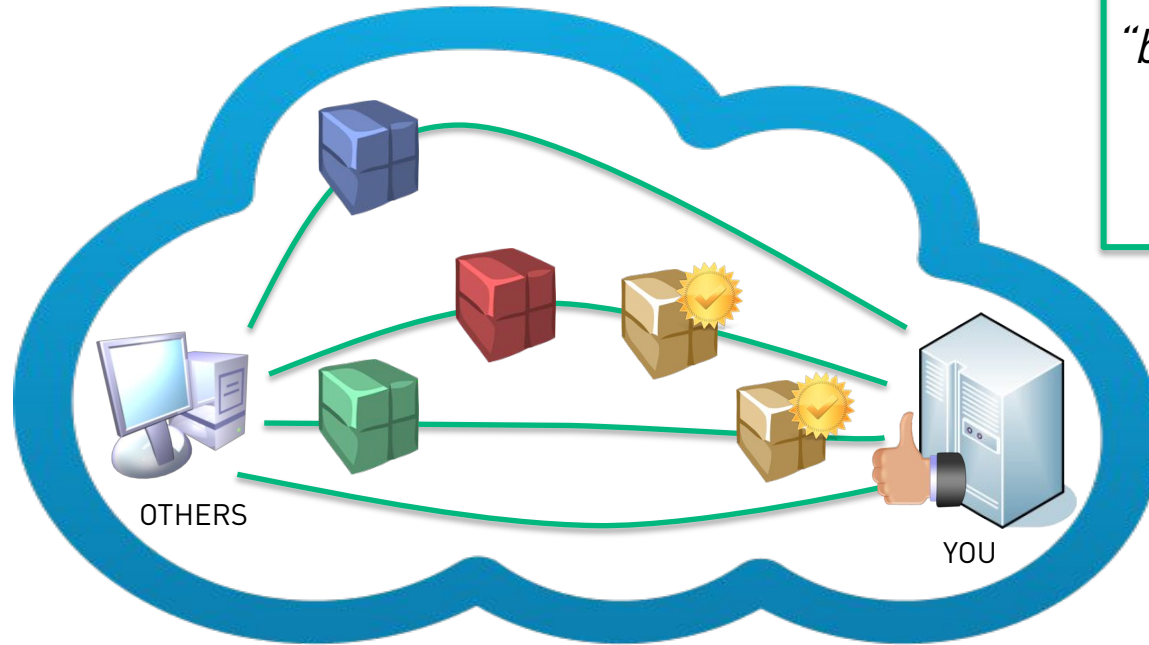
## Robustness Principle



Jonathan "Jon" Postel

*"be conservative in what you do, be liberal  
in what you accept from others"*

[RFC 761]



*"be conservative in what you do,  
be liberal in what you accept  
from others"*

[RFC 761]

## Robustness Principle

## Quick Recap



University of California, Berkeley  
– sometime in the 70s

*“the Internet originally developed among a community of like-minded technical professionals who trusted each other”*

[RFC 3724]

- Don't put anything of use for an end system on the network layer
  - Let alone “security functions”.
- Be ready to accept “inaccurate input” from a communication peer
  - Still trust her she's benevolent.

## But then Something Changed

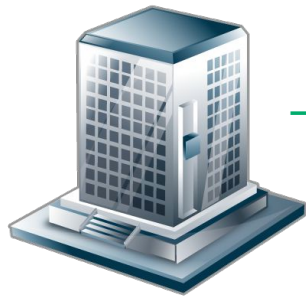


*“Today, the motivations of some individuals using the Internet are not always entirely ethical, and, even if they are, the assumption that end nodes will always co-operate to achieve some mutually beneficial action, as implied by the end-to-end principle, is not always accurate.”*

[RFC 3724]

## New Players in Town

In *The Internet of Cooperators* suddenly there were...



### Enterprises

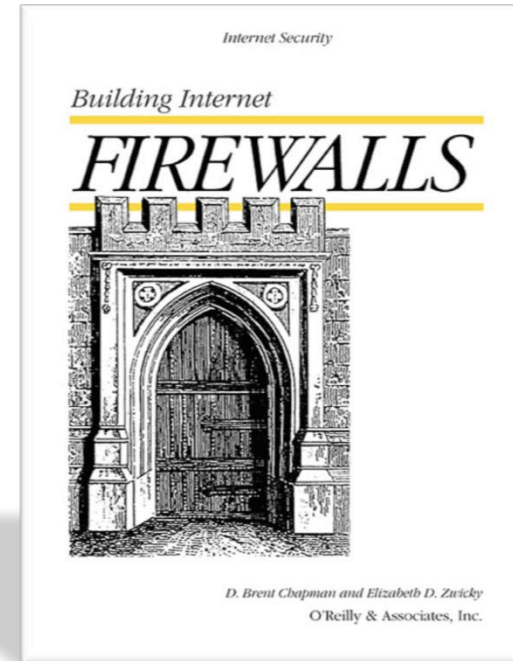
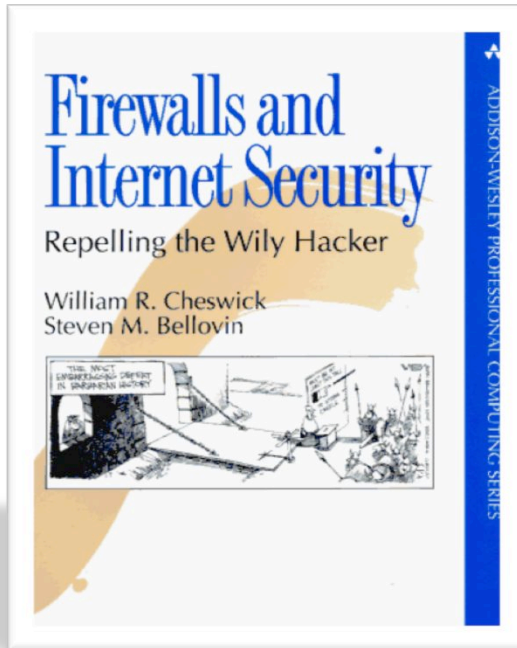
- Trying to protect their assets



### Hackers

- Trying to play with the assets ;-)

# These Are some Books from the 90s



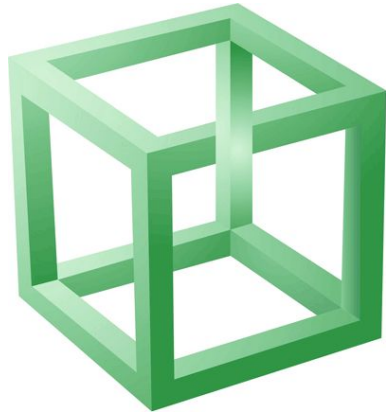
# The Rise of the Middleboxes

---



## Middleboxes

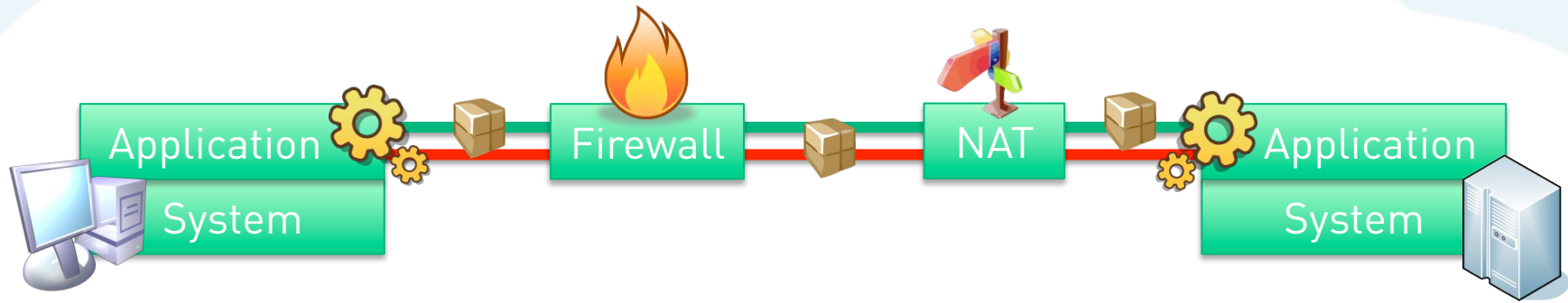
---



*“any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host”*

[RFC 3234]

# Middleboxes in the Field



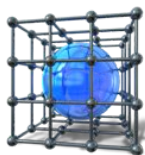
# Security-wise, Middle-boxes Can Do a Lot of Things



- ▢ Substitute reputation for trust
  - ▢ Mainly in context of email & web content



- ▢ Create circuits ;-) & filter on those
  - ▢ Stateful firewalls



- ▢ Isolate

- ▢ Filter packets



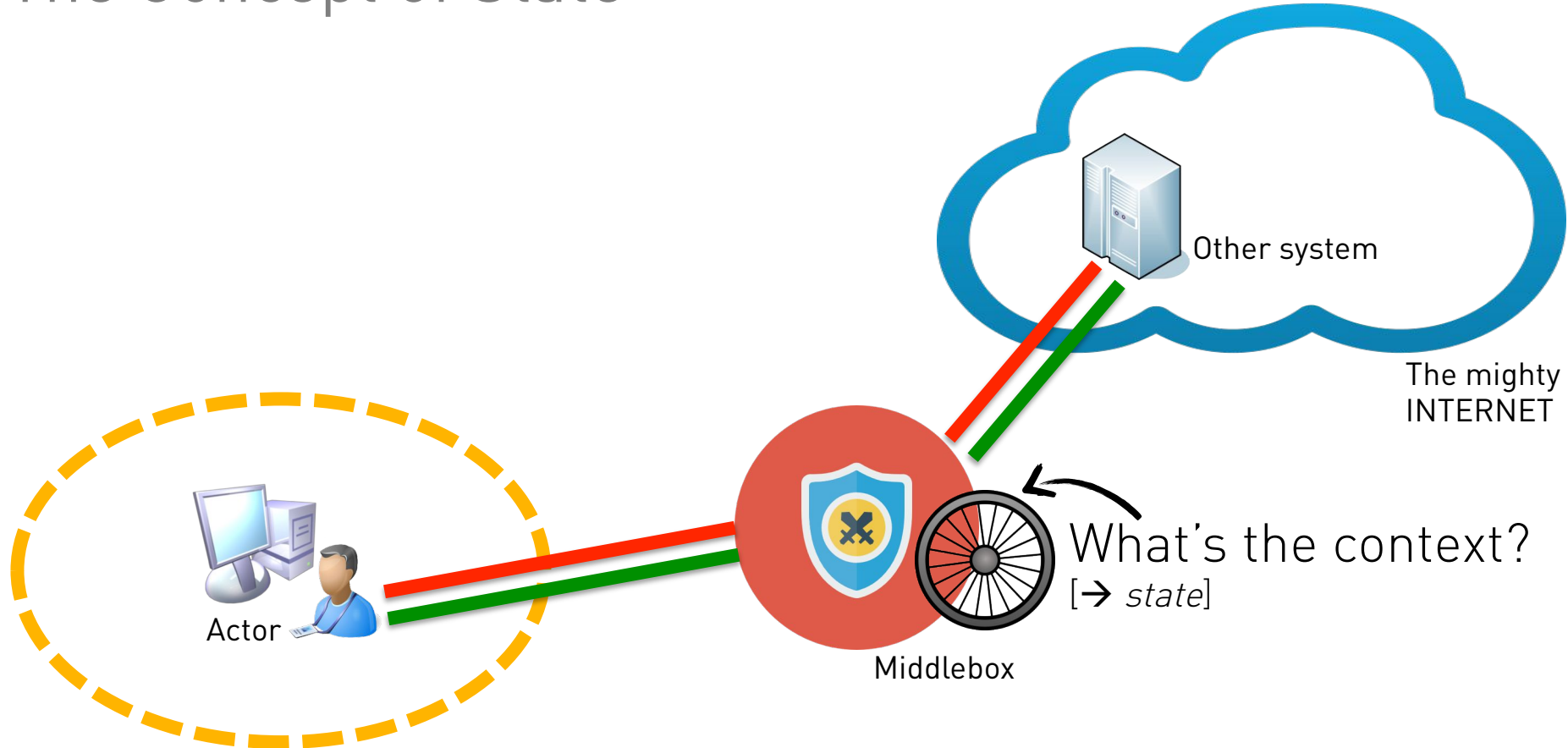
- ▢ Authenticate



- ▢ Inspect packets/circuits for bad stuff



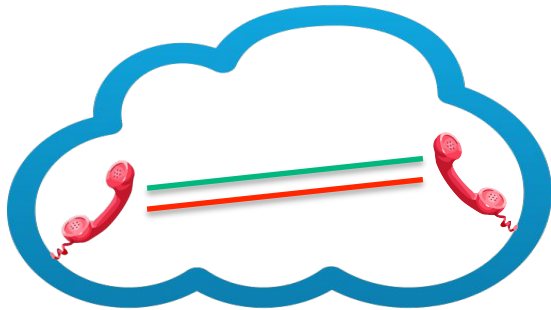
# The Concept of State



## To Do All This

There's Some Assumptions

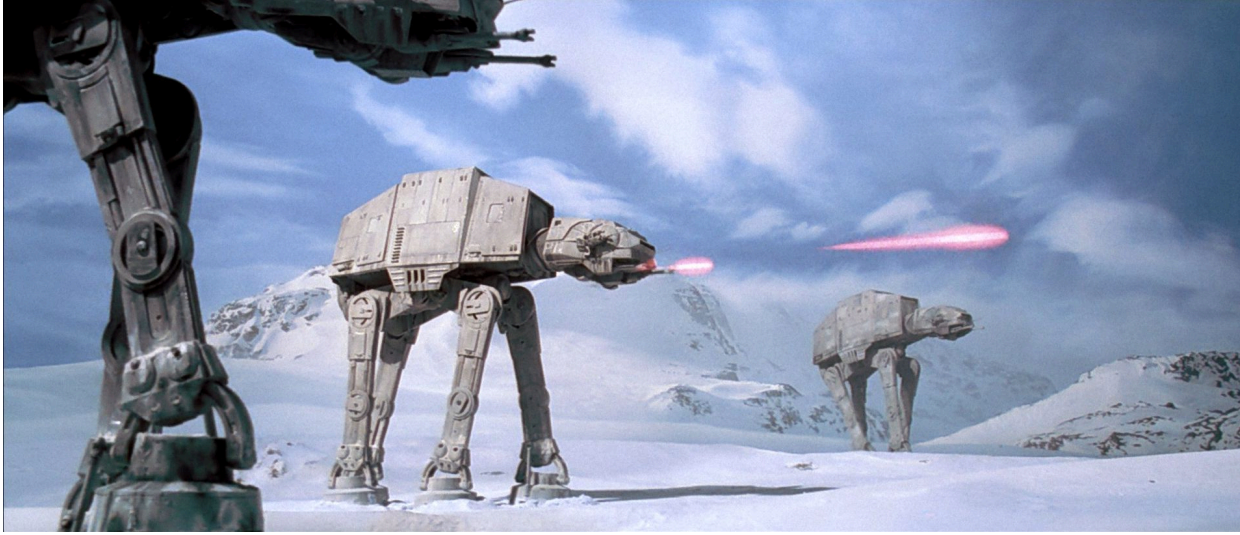
- All packets of a communication act must pass some *choke point*.
- A security enforcement module must be able to fully understand the communication act.



## You've Certainly Noticed

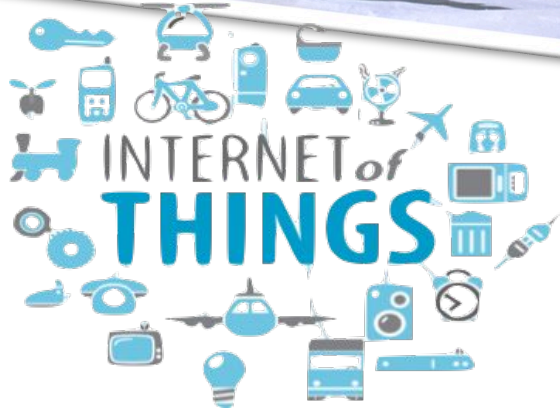


- These concepts (circuit & choke point) are diametrically opposed to the Internet's early goals
  - Datagrams which can be “routed around failures”
  - End-to-end
  - Robustness principle (?)
- Still, the choke-point & middlebox security model is quite prevalent in today's Internet.
- But...



# The Internet Strikes Back

---




- That picture was chosen with intent ;-)
- Tomorrow's Internet will be an *Internet of ~~Machines~~ Things*
- I have another buzzword for you:
  - *M2M communication*
  - You did notice it's not "M2FW2M communication", didn't you?


## The Internet Strikes Back



– Here's some protocols that might play a huge role in the not-too-distant future:

– IPv6 

– MPTCP 

– HTTP/2 

## IPv6



- A whole new 😊 universe in itself
- Some characteristics which are important for this talk
  - End-to-End principle was a prevalent design goal.
  - Some flexibility as for packet header.
  - Some changes in the space of addressing
    - /64 being the norm prefix for endpoints
    - Much larger “possible” networks.
    - Potentially many different addresses per system including short-lived ones.

# What an IPv6 Datagrams Looks Like...



# Problem

- Variable types
- Variable sizes
- Variable order
- Variable number of occurrences of each one.
- Variable fields



$\text{IPv6} = f(v, w, x, y, z,)$

## IPv6 Packet Header

A comparison



**vs.**

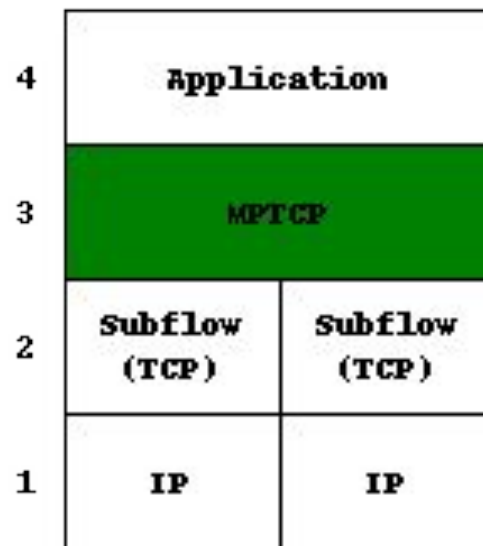


TROOPERS

**vs.**

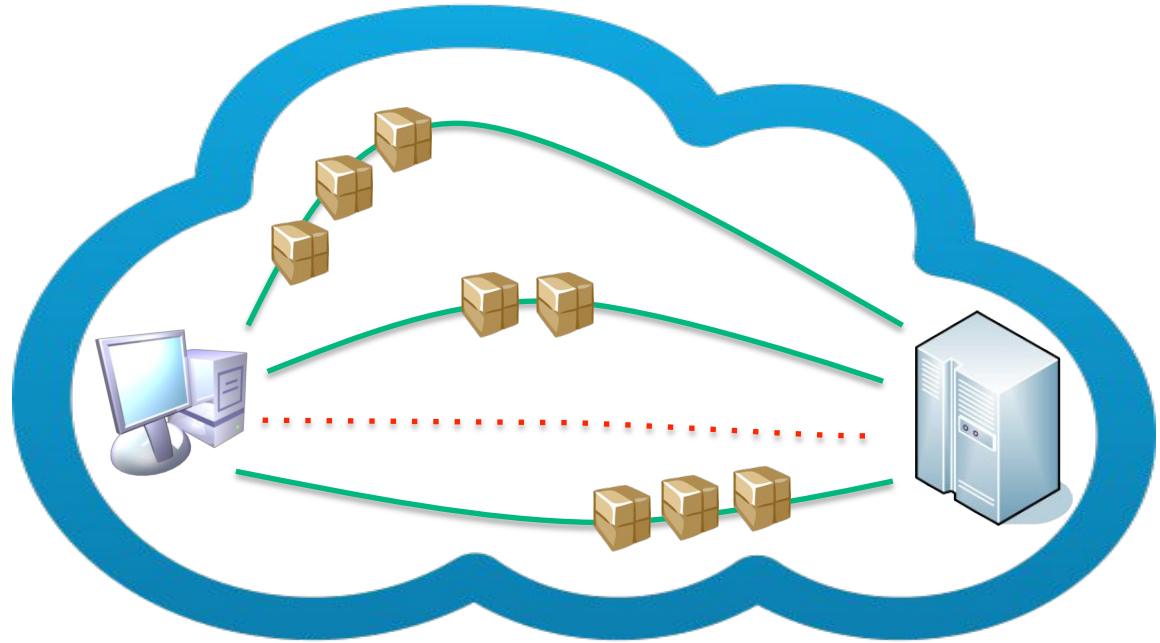


## MPTCP in a Nutshell



## Back to the Roots

It's all about packets again



# MPTCP

---

Some use you all know



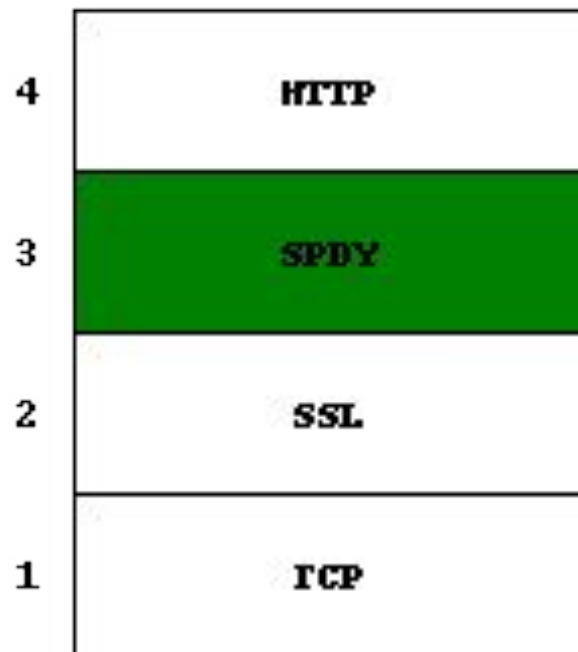
Siri

## SPDY in a Nutshell

HTTP/2



<https://tools.ietf.org/id/draft-ietf-httpbis-http2-14.txt>, now in *working group last call*



# SPDY

Main properties

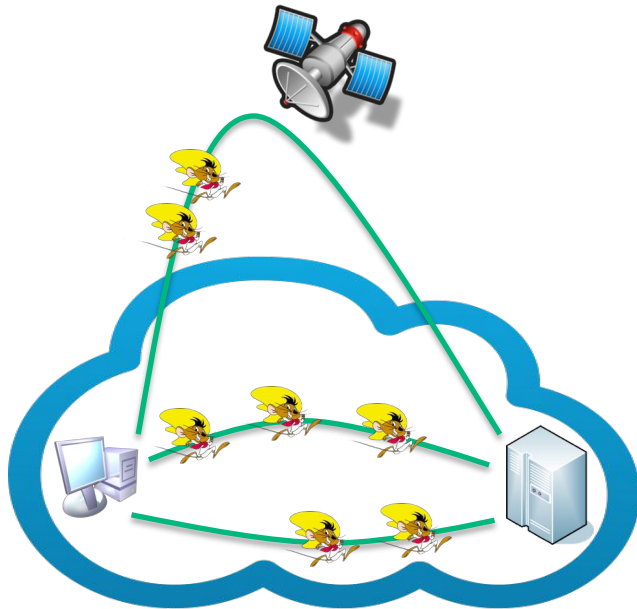


- Everything TLS encrypted by default
- Multiple concurrent streams over one TCP connection possible.
- “Server push”
  - Streams are bi-directional (both server and client can initiate connection).

<http://www.chromium.org/spdy/spdy-whitepaper>

## SPDY (+MPTCP)








Multiplexing illustrated



- Non-multiplexed environment:

Next TROOPERS conference is...

- Multiplexed:
 

Next		}	Mobile carrier connection
TROO			
PERS		}	(W)LAN route #1
conf			
eren		}	(W)LAN route #2
ce i			
s...			

- BTW:  
March 16<sup>th</sup> – 20<sup>th</sup> 2015, Heidelberg, [www.troopers.de](http://www.troopers.de)



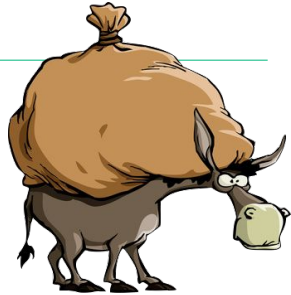
# Disruption

---

What does all this mean?



## What Does All this Mean?



- There's some elements that will have a hard time working properly.



- There's some elements of current sec architectures that won't work at all, anymore.



- Some paradigm shift might be needed.

## Elements Having a Hard Time

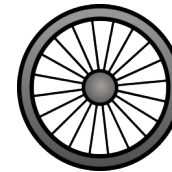
---



– Reputation based stuff



– Stateful stuff



## Reputation



**M<sup>3</sup>AAWG**  
MESSAGING MALWARE MOBILE

### Messaging, Malware and Mobile Anti-Abuse Working Group M<sup>3</sup>AAWG Policy Issues for Receiving Email in a World with IPv6 Hosts

September 2014

Internet mail anti-abuse efforts have often relied on the reputation associated with a sending host's IPv4 address. This reputation data provides an identifier for active agents in email handling. Although less stable and less reliable than would be preferred, IPv4 addresses have proved useful for rate limiting and reputation assessment, and most anti-abuse systems will be unable to function if the effectiveness of these mechanisms are degraded. Over the years, there has been a continuing effort to develop reputation assessment based on the more stable alternative of domain names, with or without associating an IP address. The advent of IPv6 addresses makes this essential, along with improved address-based mechanisms.

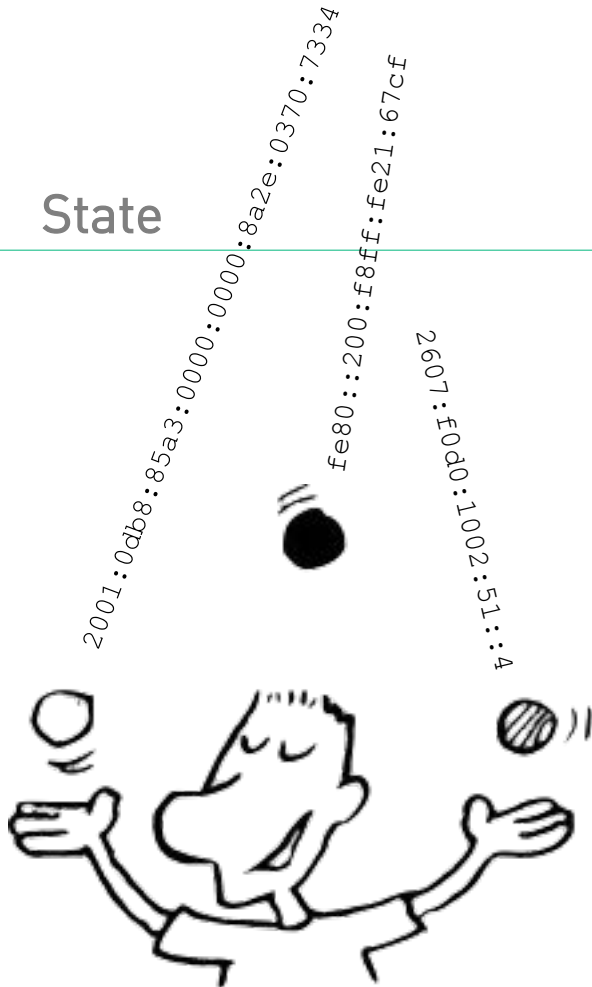
M<sup>3</sup>AAWG encourages the industry's development of technologies, policies and procedures to address this concern for relaying email across administrative domains by pursuing the targeted efforts described here. These efforts will provide a solid foundation for building and operating integrated Internet mail and anti-spam systems that include IPv6 in the operational mix. The goals are: to aggregate the massive address space into more easily trackable assignments, to require operators to identify hosts intended to act as outbound mail

- Right now most reputation based systems don't work well with IPv6.
- Not sure if this will change in the future
  - Internet of things & services

## See also:

- <https://moderncrypto.org/mail-archive/messaging/2014/000780.html>
- [http://www.m3aawg.org/sites/maawg/files/news/M3AAWG\\_Inbound\\_IPv6\\_Policy\\_Issues-2014-09.pdf](http://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Inbound_IPv6_Policy_Issues-2014-09.pdf)

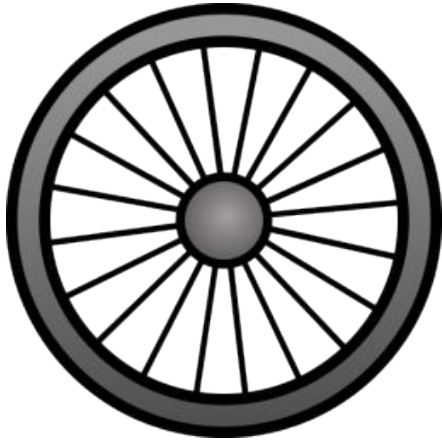
## State



- Simple rule: the higher the complexity of a communication act, the higher the cost of keeping state of it.
- IPv6 has a high degree of complexity...

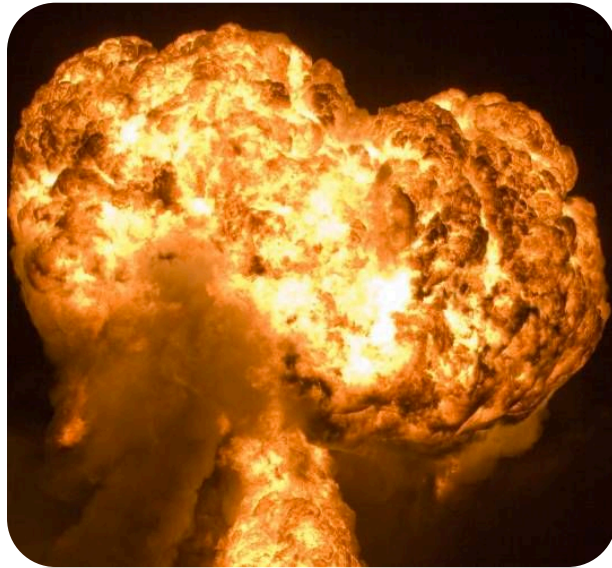
## A Well-known *State* Related Security Problem

Neighbor Cache Exhaustion (NCE)



- In the end of the day, *neighbor cache exhaustion (NCE)* is a *state* problem
  - ARP had an *incomplete* state as well.
  - You just rarely saw segments > 24 exposed to the Internet.
- Let's assume NCE is a mostly solved problem.
- Still, there's much more opportunities for a state oriented sec model to fail in the IPv6 age
  - I'm very interested to see how vendors of stateful firewalls will handle scenarios like "single infected machine sitting in a broadband /64 and establishing valid connections to web server from many many random source addresses". BCP 38 won't solve this.

## Need (Another) Real Life Example?



*“Our network switches have been observed using far more CPU than has historically been the case, we have had a variety of packet storms that appear to have been caused by forwarding loops despite the fact that we run a protocol designed to prevent such loops from taking place, and we have had a variety of unexplained switch crashes.”*



From: Network Meltdown due to MLD state

- <http://blog.bimajority.org/2014/09/05/the-network-nightmare-that-ate-my-week/>

# Ceterum Censeo

[RFC 3439] – Go read it. Again!

Network Working Group  
 Request for Comments: 3439  
 Updates: 1958  
 Category: Informational

R. Bush  
 D. Meyer  
 December 2002

## Some Internet Architectural Guidelines and Philosophy

### Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

### Abstract

This document extends RFC 1958 by outlining some of the philosophical guidelines to which architects and designers of Internet backbone networks should adhere. We describe the Simplicity Principle, which states that complexity is the primary mechanism that impedes efficient scaling, and discuss its implications on the architecture, design and engineering issues found in large scale Internet backbones.

### Table of Contents

1. Introduction . . . . .	2
2. Large Systems and The Simplicity Principle . . . . .	3
2.1. The End-to-End Argument and Simplicity . . . . .	3
2.2. Non-linearity and Network Complexity . . . . .	3
2.2.1. The Amplification Principle. . . . .	4
2.2.2. The Coupling Principle . . . . .	5
2.3. Complexity lesson from voice. . . . .	6
2.4. Upgrade cost of complexity. . . . .	7
3. Layering Considered Harmful. . . . .	7
3.1. Optimization Considered Harmful . . . . .	8
3.2. Feature Richness Considered Harmful . . . . .	9
3.3. Evolution of Transport Efficiency for IP. . . . .	9
3.4. Convergence Layering. . . . .	9
3.4.1. Note on Transport Protocol Layering. . . . .	11
3.5. Second Order Effects . . . . .	11
3.6. Instantiating the EOSL Model with IP . . . . .	12
4. Avoid the Universal Interworking Function. . . . .	12
4.1. Avoid Control Plane Interworking . . . . .	13

## Stuff not Working at All

- All/most content/signature based stuff once:



- Traffic is encrypted



- Traffic is not sanitized



- Link to slides, tool & whitepaper:  
<http://www.insinuator.net/2014/08/ernw-blackhat-us-2014/>

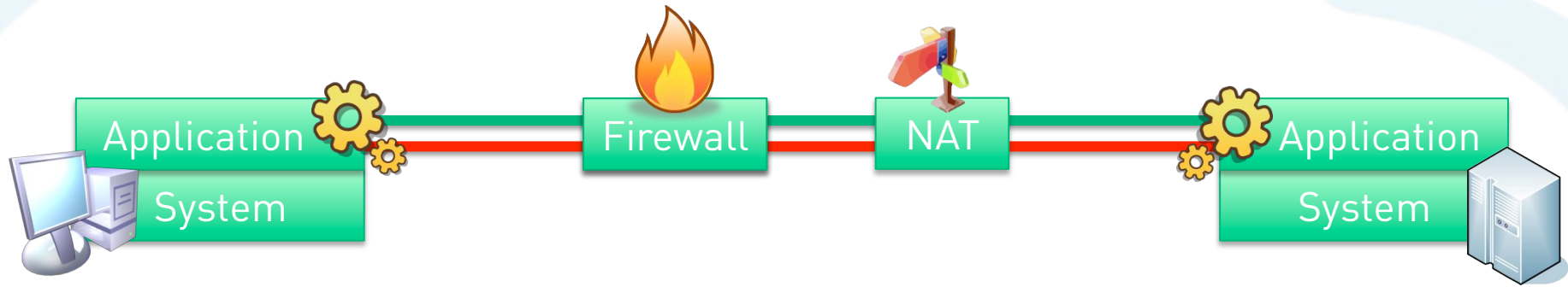


## What's the Cure, Man?



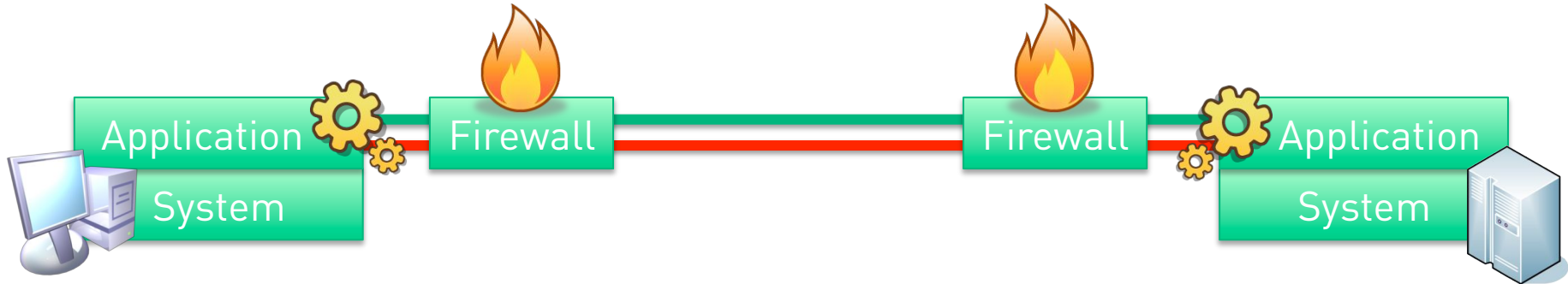
- Move security functions to end-points
- In case of choke-point sec model perform sanitizing before inspection
  - Some architecture change needed, maybe.
- Forget about state
  - Stateless ACLs might be your friend.

# Move Sec to End-points



# Move Sec to End-points

- This is happening anyway
  - Think: hypervisor-firewalls
- We understand you'll keep the centralized stuff for compliance reasons (and/or to save discussions with the PCI auditor)
  - As you do with anti-virus...



# In Case You Use an IDPS



- You MUST decrypt and (header-wise) scrub the traffic before entering the IDPS.

## Forget about State

```
permit tcp any host 2003:60:4010:10A0::11 eq smtp
permit tcp any host 2003:60:4010:1090::11 eq www
permit tcp any host 2003:60:4010:1090::11 eq 443
```



- Again, it's back to the roots:
  - On the network layer look at *packets*.
  - The concept of “connections & circuits” might be hard to maintain.
- Stateless ACLs will be good enough.
  - “Good enough” is just that.
- Again, you might keep the *stateful* stuff for compliance reasons...

## Last but not Least

It's not about feature parity



- IPv6 is very different from IPv4
  - So is IPv6 security.
- Don't rely on transforming v4 models 1:1 to v6. Do not!
- Think *feature suitability* instead.

## Summary



- The world is turning
  - Every day ;-)
  - This includes the Internet's protocol landscape (at a somewhat slower rate though).
- Upcoming technologies might require adapted security architectures.
- Think about it!

There's never enough time...

**THANK YOU...**



**...for yours!**

We would love to see you guys back in Heidelberg!

March, 16<sup>th</sup> – 20<sup>th</sup> 2015  
Heidelberg, Germany  
Make the world a safer place.



REGISTRATION OPEN: [www.troopers.de](http://www.troopers.de), seats are filling fast!

## References

---

- Eric Allmann: The Robustness Principle Reconsidered
  - <http://cacm.acm.org/magazines/2011/8/114933-the-robustness-principle-reconsidered>
  
- D. Clark: The design philosophy of the DARPA internet protocols
  - <http://delivery.acm.org/10.1145/60000/52336/p106-clark.pdf> [requires login]
  - <http://ccr.sigcomm.org/archive/1995/jan95/ccr-9501-clark.pdf>
  
- Saltzer: End-To-End Arguments in System Design
  - <http://dl.acm.org/citation.cfm?id=357402>



## References

---

- RFC 1958 Architectural Principles of the Internet
- RFC 3724 The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture

