Do we need a new Internet?
Part 1: Basic Issues

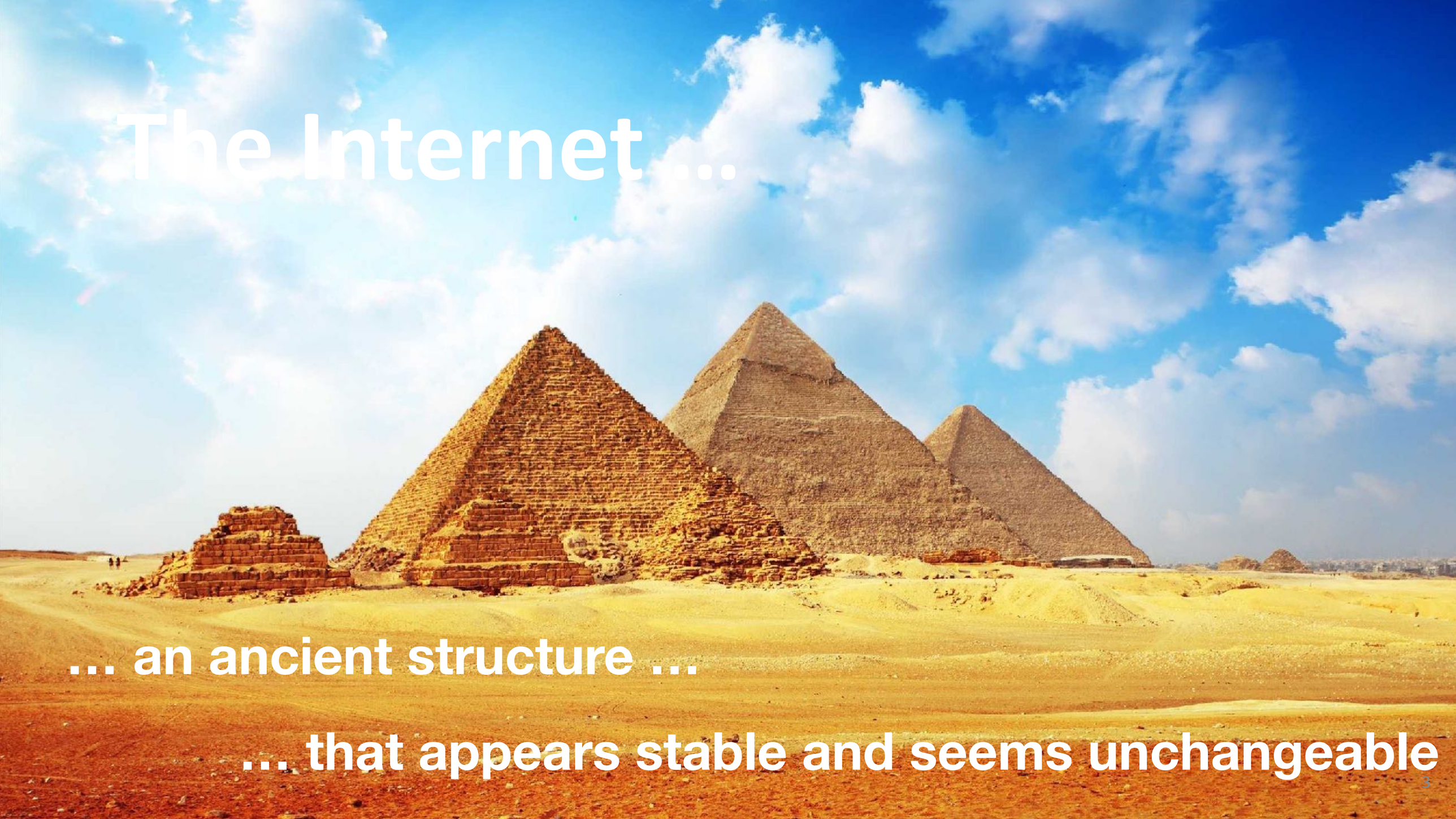
Adrian Perrig

Network Security Group, ETH Zürich

ETH zürich

SCION

Imagine a building or structure
that represents the Internet


The Internet …
… an ancient structure …
… that appears stable and seems unchangeable

More like today's Internet …

Problem 1: Availability

Poor Availability

- Well-connected entity: 99.9% availability (86 s/day unavailability) [Katz-Bassett et al., Sigcomm 2012]
  - Plug-into-the wall telephones: 99.999% availability (0.86 s/day unavailability)!
- Numerous short-lived **outages** due to Border Gateway Protocol (BGP) route changes and route convergence delays
- Outages due to **misconfigurations**
- Outages due to **attacks**
  - E.g., prefix hijacking, DDoS

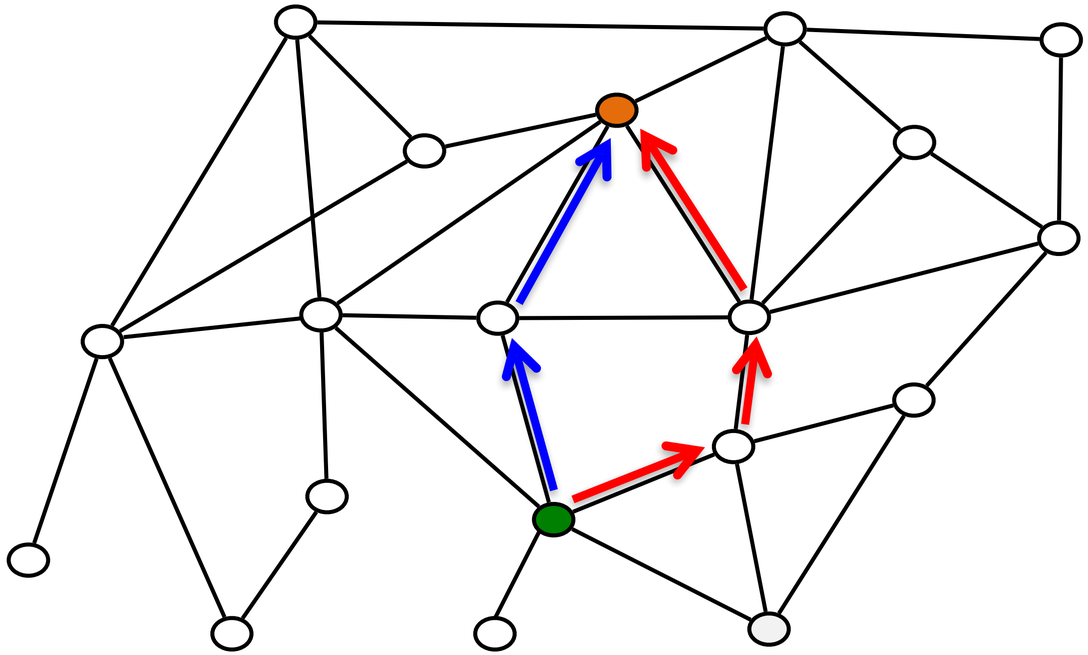
Problem 2: Control

Who controls Internet Paths?

- Current Internet offers limited control of paths
- Paths can be hijacked and redirected

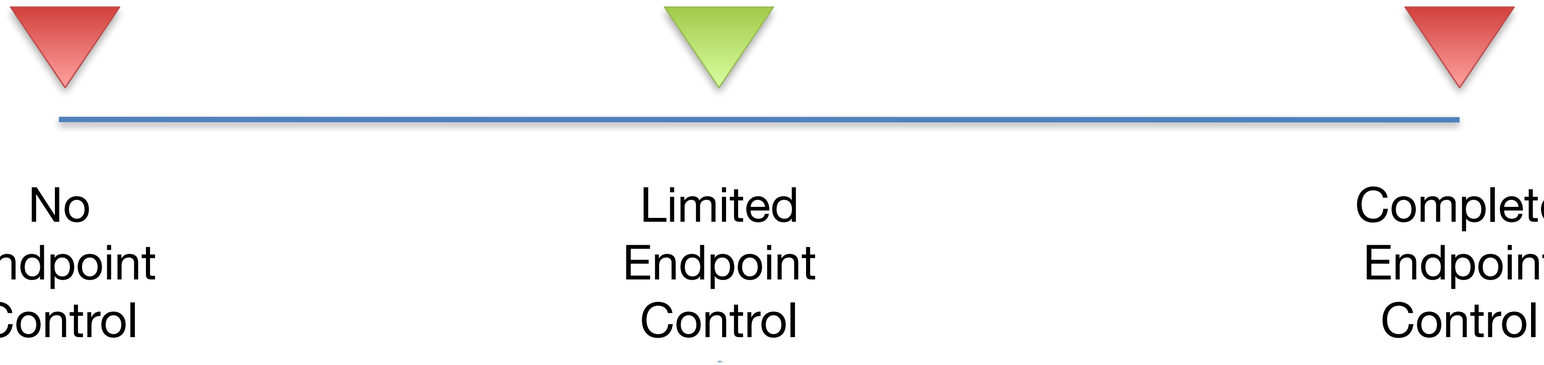
Limited Path Control in BGP

- Current Internet offers limited control of paths
  - Border Gateway Protocol (BGP) floods announcements for destinations
  - No inbound traffic control



Who should control Paths?

- Clearly, **ISPs** need some amount of path control to enact their policies
- How much path control should **end domains** and **end points** (sender and receiver) have?
  - Control is a tricky issue … how to empower end points without providing too much control?



Problems due to Lack of Path Control

- Limited traffic load balancing for sender and receiver
- No multi-path communication
- No optimization of networking paths for sender and receiver
- Poor availability
  - Outages cannot be circumvented
  - Connection can suddenly break
- Traffic redirection attacks become possible

Problem 3: Transparency

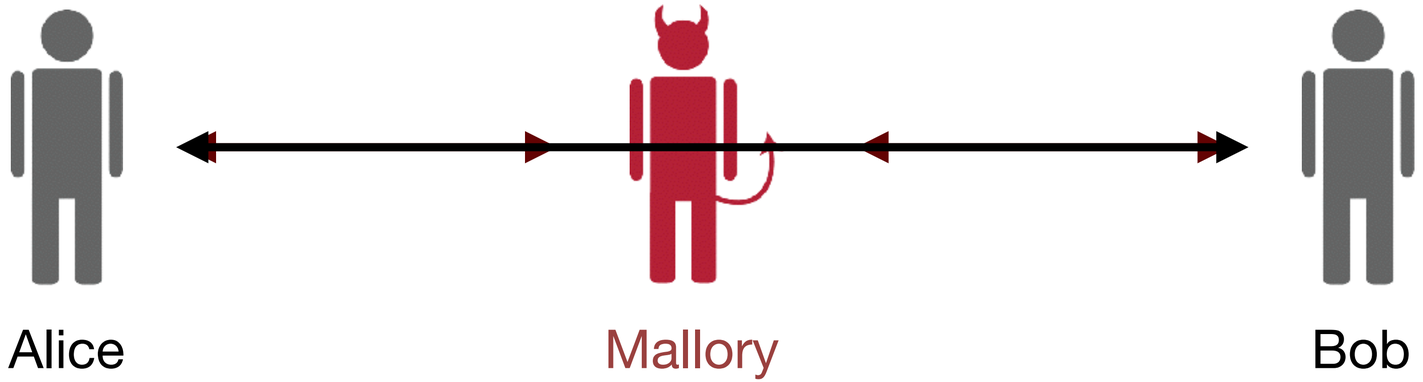
Transparency

- Path transparency
  - Today, sender cannot obtain guarantee that packet will travel along intended path
  - Impossible to gain assurance of packet path
    - Because router forwarding state can be different from routing messages received
- Trust transparency
  - Today, we cannot enumerate trust roots we rely upon

Problem 4: Secure E2E Communication

Fake Certificates lead to Attack

- Adversary misuses fake certificate to impersonate one party to the other (man-in-the-middle attack)



Problems with SSL / TLS Certificates

- Famous case: false Microsoft ActiveX certificate issued by Verisign in January 2001
- VeriSign Hacked, Successfully and Repeatedly, in 2010
  - VeriSign attacks were revealed in a quarterly U.S. Securities and Exchange Commission filing in October 2011
- March 2011: Attack on Commodo reseller, several fraudulent certificates were issued: mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org, login.live.com
  - Suggested that attack originated from Iranian IP address
  - http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html
- August 29, 2011: news broke that DigiNotar, a Dutch CA, improperly issued a certificate for all Google domains to an external party
  - Claim: 250 certificates for an unknown number of domains were released
  - Iranian government spied on Iranian citizens' communications with Google email during the month of August 2011
- Stuxnet used compromised certificates from 2 Taiwanese CAs

Non-Scalability of Trust

- As the Internet has grown to encompass a large part of the global population, trust relationships have become heterogeneous: **no single entity trusted by everyone**
  - Complicates construction of entity authentication infrastructures
- Current Internet authentication infrastructures have weak security properties
  - Single points of failure
  - Security of the weakest link

Summary: Which Problems Should we Address?

- High availability: enable end-to-end connectivity despite network disruptions
- Path control: ISP, sender, and receiver, jointly control end-to-end paths
- Transparency
  - Path transparency: sender should be aware of packet's path
  - Trust transparency: known roots of trust that need to be relied upon
- Resilience to compromised trust roots: limit global scope of certification authorities

For More Information …

- … please see our web page: www.scion-architecture.net
- Chapter 1 of our book “SCION: A secure Internet Architecture”
  - Available from Springer this Summer 2017
  - PDF available on our web site
- Part 2 of this presentation: “Motivations for Change”