Do we need a new Internet?
Part 2: Motivations for Change

Adrian Perrig

Network Security Group, ETH Zürich

ETH zürich

SCION

Worst Internet Security Problems?

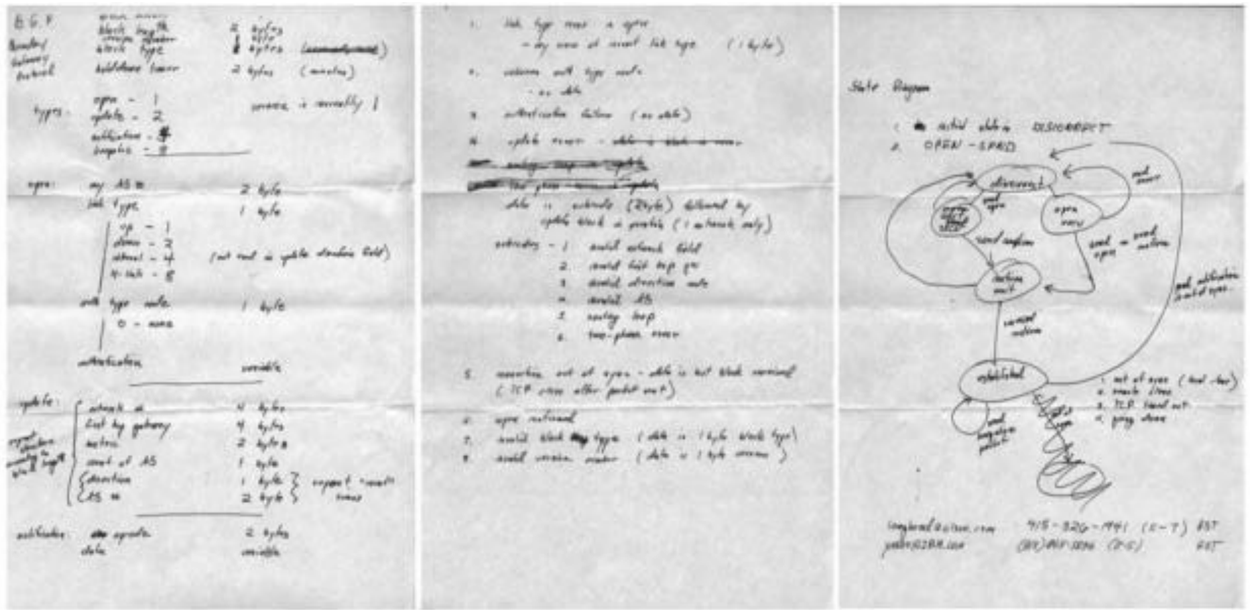
- Malware (worms, viruses, etc.)
- Spyware
- Ransomware
- APT
- HTTP-based attacks
- Spam, phishing
- Compromised IoT devices

Most Fundamental Internet Security Issue

- Basic Internet service: deliver data
- Most fundamental security issue: network availability
- Main attack is preventing communication, for example:
  - Disrupting routing system
  - Address hijacking
  - DDoS attack

BGP: Border Gateway Protocol

- Designed in 1989 by Lougheed and Rekhter [RFC 1105]
- BGP is a fundamental protocol to enable Internet communication
  - BGP is like the postal service: it finds the path to send network packets to the destination
- Perhaps the most important network protocol many people don't know about



Fundamental Limitations of BGP and BGPSEC

- Availability
  - Frequent periods of unavailability when paths change
  - **Slow convergence** during iterative route computation
  - Susceptible to attacks and **misconfigurations,** sometimes resulting in **global outages**
- Transparency: **poor path predictability and reproducibility**
- Control: Almost **no path choice** by end points
- Trust: Uses **very few trust roots** (RPKI / BGPSEC)
  - Single points of failure

Internet Attacks and Problems 1/3
BGP / Control Plane Issues

- Lack of fault isolation
  - Error propagation, potentially to entire internet, disruption of flows outside domain
  - Adversary can attract flows outside domain (prefix hijack/blackhole attacks)
  - Black art to keep BGP stable, manual rule sets, unanticipated consequences
- Lack of scalability, amount of work by BGP is O(N), N number of destinations
  - Path changes need to be sent to entire internet
- Dramatically higher router overhead during periods of route instability
  - Increased number of routing updates during DDoS attacks
- Short-term loops during periods of convergence, leading to outages during a few seconds (Katabi, "can you hear me?")
  - Intermittent routing loops during BGP convergence, need TTL to avoid packet looping
- Slow route convergence
  - Convergence attack
  - Network may require minutes up to tens of minutes to converge
- Lack of freshness for BGP update messages
- Cannot express any policies based on source of traffic
- Only single path, cannot use multipath
- No separation of routing and forwarding, forwarding may suddenly stop during route changes

Internet Attacks and Problems 2/3
BGPsec Issues

- Slower convergence than BGP
- Prefixes cannot be aggregated, much higher overhead
- RPKI needs connectivity to verify revocation status of a certificate, thus introducing a circular dependency between routing and cert validation
- Single root of trust for AS and address certificates, which leads to a powerful kill switch
- Path withdrawals are not secure, path oscillations can be induced by repeatedly announcing / withdrawing path
- New attacks are possible
  - Route flap dampening-based attacks:
    Y. Song, A. Venkataramani, and L. Gao. Identifying and addressing protocol manipulation attacks in secure BGP. ICDCS, 2013.
  - Q. Li, Y-C. Hu, and X. Zhang. Even Rockets Cannot Make Pigs Fly Sustainably: Can BGP be Secured with BGPsec? SENT 2014.

Internet Attacks and Problems 3/3

IP / Data Plane Issues

- Expensive forwarding table lookup for each packet, power-intensive if implemented with TCAM
- Bursting routing tables, especially with IPv6
- Lack of route transparency
- Lack of predictability for path availability
- Lack of route choice/control by senders and receivers

IP / BGP / Misc. Issues

- No path predictability due to inconsistency between routing table and BGP updates
- No isolation between control and data planes (routing and forwarding)
  - By attacking routing, prevent forwarding to work correctly
- Huge TCB (entire internet)
- Single root of trust for DNSsec, leads to kill switch
- Unauthenticated ICMP
- No clean global framework for PKI
- No network mechanisms to defend against DDoS attacks
- No path verifiability
- No mechanism to authenticate the source, easy to perform source IP spoofing

What Solutions are Ready?

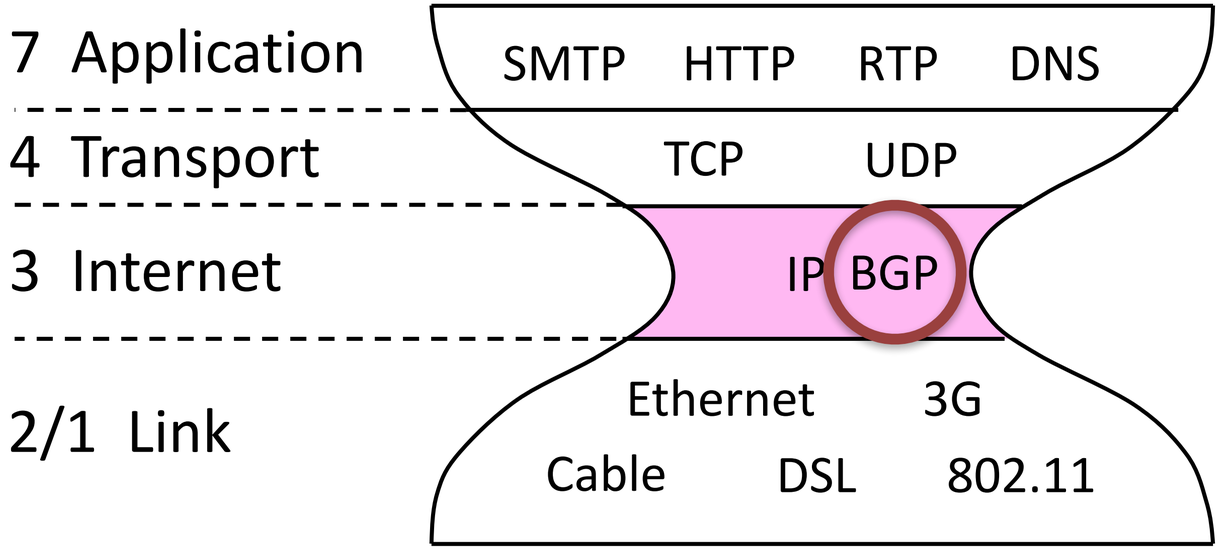
- Since the Internet is so important and people are aware of the problems, surely solutions are ready to solve the problems?
- Potential solutions many people think of:
  - SDN
  - Blockchain
  - Cloud computing

Proposed Future Internet Architectures

- **General FIAs**
  - **XIA**: enhance flexibility to accommodate future needs
  - **MobilityFirst**: empower rapid mobility
  - **Nebula** (ICING, SERVAL): support cloud computing
  - **NIMROD**: better scale and flexibility for Internet
  - **NewArch** (FARA, NIRA, XCP)
- **Content-centric FIAs**
  NDN, CCNx, PSIRP, SAIL / NETINF
- **Routing security**
  S-BGP, soBGP, psBGP, SPV, PGBGP, H-NPBR
- **Path control**
  MIRO, Deflection, Path splicing, Pathlet, I3, Segment Routing
- **Others**
  - SDN: flexible intra-domain networking
  - ChoiceNet, HLP, HAIR, RBF, AIP, PFRI, POMO, RINA, ANA, …

Absence of Inter-domain Routing Innovation

- Surprising fact: little changed in inter-domain routing over the past 15 years [Ken Calvert, Keynote @ ICNP 2016]
- Observation: Internet innovation happened at lower and upper layers, or in intra-domain routing



ETH zürich

SCION

Explanations why Problems are not Addressed

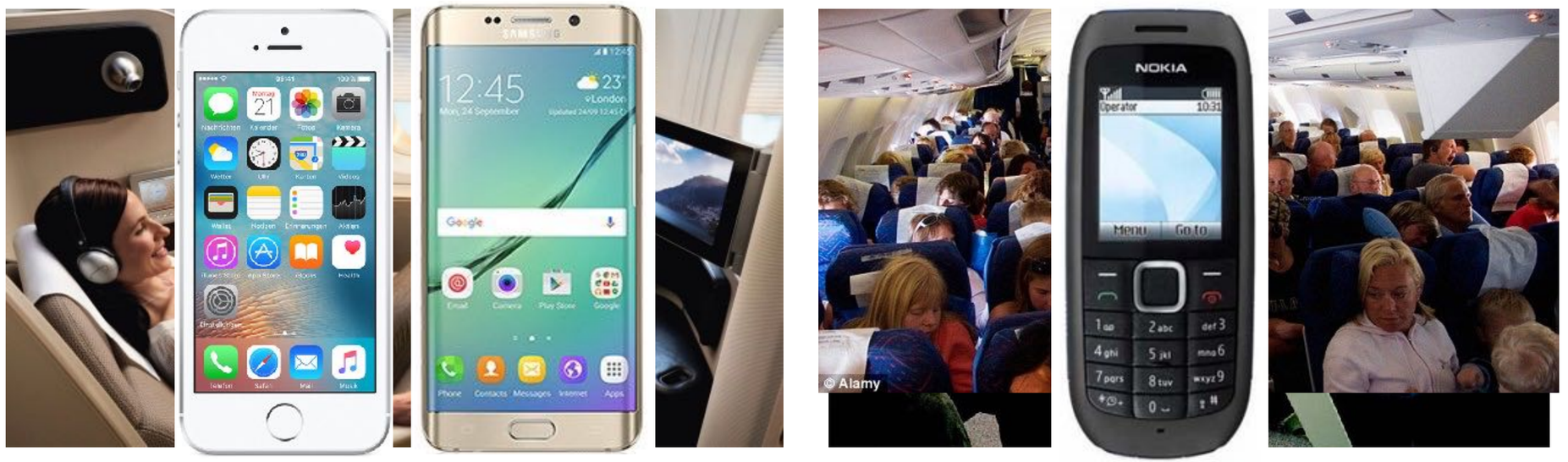
- Titanic scenario: we are overly confident that everything is fine
- Boiling frog scenario: we don’t realize severity of escalating threats

Sweat and Human Ingenuity

- Perhaps main reason why the Internet is not changing: sweat and human ingenuity of thousands of clever system and network administrators who are working hard to keep the Internet running

Belief that Internet is Immutable

- Evidence appears overwhelming that Internet is immutable: IPv6, BGPSEC, DNSSEC, etc.
- However, benefits are limited, esp. for early deployers
- Our goal: provide many benefits, even for early adopters, such that one cannot turn back



ETH zürich

SCION

Evolutionary vs. Revolutionary Change

- Revolutionary approach is **necessary**
  - Some problems are fundamental, not fixable through evolution
- Revolutionary approach is **desirable**
  - A fresh redesign can cleanly incorporate new mechanisms
- Revolutionary technology change is **easy** through evolutionary deployment
  - If IP is relegated to provide local (intra-domain) communication, only a small fraction of border routers need to change
  - Simultaneous operation with current Internet possible
  - Strong properties provide motivation for deployment

What Now?

Can we really change the Internet?

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