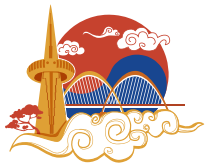
Why is Securing the Internet so Hard?

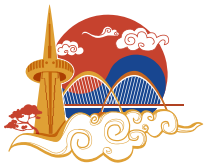
Geoff Huston
APNIC



Internet Issues

Why are some issues so challenging to solve, while others seem to be effortless?

Why was the IPv4 Internet an unintended runaway success in the 90's, yet IPv6 has been a protracted exercise in industry-wide indecision?

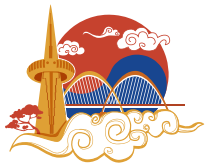


What makes a problem "hard"?

It might be **technically challenging**: While we understand what we might want that does not mean we know how to construct a solution

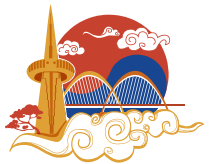
It might be **economically hard**: The costs of a solution are not directly borne by the potential beneficiaries of deploying the solution

It might be **motivated by risk mitigation**: We are notorious for undervaluing future risk!



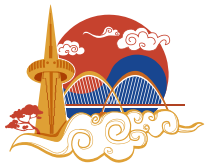
Internet Successes

- IPv4 (and datagram packet switching)
- Network Address Translators (perversely!)
- TCP evolution and adaptation
- Content Distribution Systems
- Streaming Services



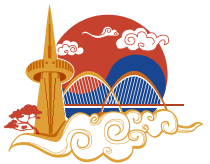
What are Internet success factors?

- Piecemeal deployment without the requirement for central orchestration
- Competitive advantages to early adopters
- Economies of scale as adopter numbers increase
- Alignment of common benefit with individual benefit



Failure Factors

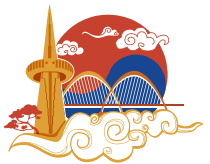
- Orchestrated actions
- Technologies that require universal or near universal adoption
- Where there are common benefits but not necessarily individual benefits
- Where there is no clear early adopter advantage



Internet Non-~~Successes~~ Failures!

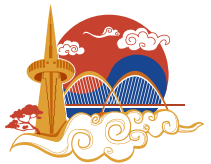
- SPAM
- DDOS defence
- BCP 38 deployment
- Secure end systems
- Secure networks
- Internet of Things

In short – we have failed at Security



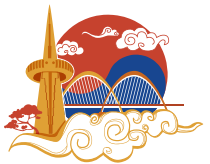
Why is Security a Failure?

- Here's a few suggestions …



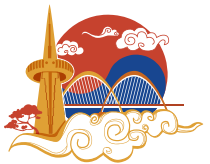
1. Noone is in charge!

- There is no single authority model for the Internet
- It's a decentralized distributed environment
- Which means there is no reference point for what is "right"
- Equally there is no clear way of understanding what is "wrong"
- There is no authority to direct anyone to do anything



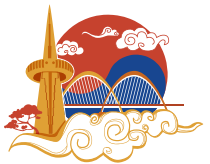
2. There is no authority

- See 1.
- Where is the point of authority to make the call of what's 'true' and what's 'false'?
- Could we all agree on a single source of authority of truth?
  - Google?
  - ICANN?
  - The CAB Forum?
  - The USG?



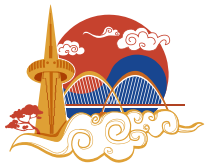
3. 'Success' is unattainable

- Any large scale complex system is prone to exhibit emergent behavior (which is part of what defines complexity)
- We don’t know how to create ordered predictable and stable systems from a clutter of loosely coordinated, numerous and diverse components
- So aberrant behavior is a constant factor
  - Whether its provoked (attack)
  - Or whether its unintended (accident)



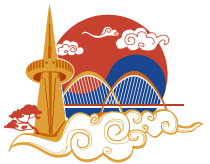
4. There is no wisdom in the crowd

- Just because we all do it does not imbue the activity with any magical property of security or safety
- Placing trust in a large set of sources allows any rogue individual source to mislead the rest
  - The WebPKI is a classic example of this
  - As is the routing system



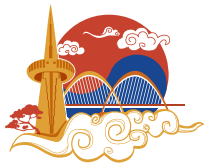
5. If we all cooperated with each other it would all be fixed!

- The basic issue with securing these systems is that their complexity creates unforseen vulnerabilities
- Markets tend to favor cheap products – particularly when robust security is an invisible and untested feature
- Talking to each other doesn't fix this



6. Attackers have an advantage

- Attackers are always at an advantage: defenders have to defend every point, while attackers have the luxury of selecting the point of attack

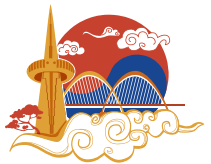


7. Partial Solutions are Failures

- Locking the front door while leaving the back door open does not improve the overall security of a house!
- Adequate security measures need to increase the cost / difficulty of attack, not just deflect it to another point of vulnerability

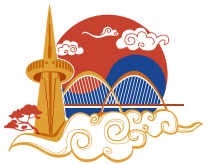
8. Shared problems are nobody's problem

- And security is a shared problem



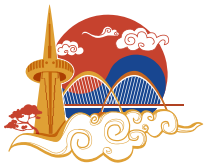
9. Because Risk is hard

- Taking measures to mitigate risk is like a lottery:
  - Everyone spends money to buy a ticket
  - But there is only one winner!
- But in this case the “win” is that the attack is deflected
  - And the potential victim does not even know that an attack was launched at them
- So everyone pays, but there are no visible winners!



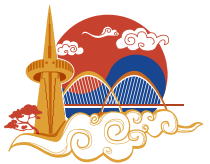
10. There is no Evil Bit

- In security system a “bad” data time does not identify itself as bad!
- All we can do is identify “good” data
- If we identify all the good data then what’s left is bad
- But if we only identify some good data then…



Because in security we really don't know what we want!

- We know instances of what we **don't** want - but that does not necessarily define what we **do** want
- It is challenging to identify a 'correct' Internet
- It is far easier to react when problems arise
- And that's likely to be as good as it gets!



Thanks