2STiC programme

Security, stability and transparency of inter-networking communication

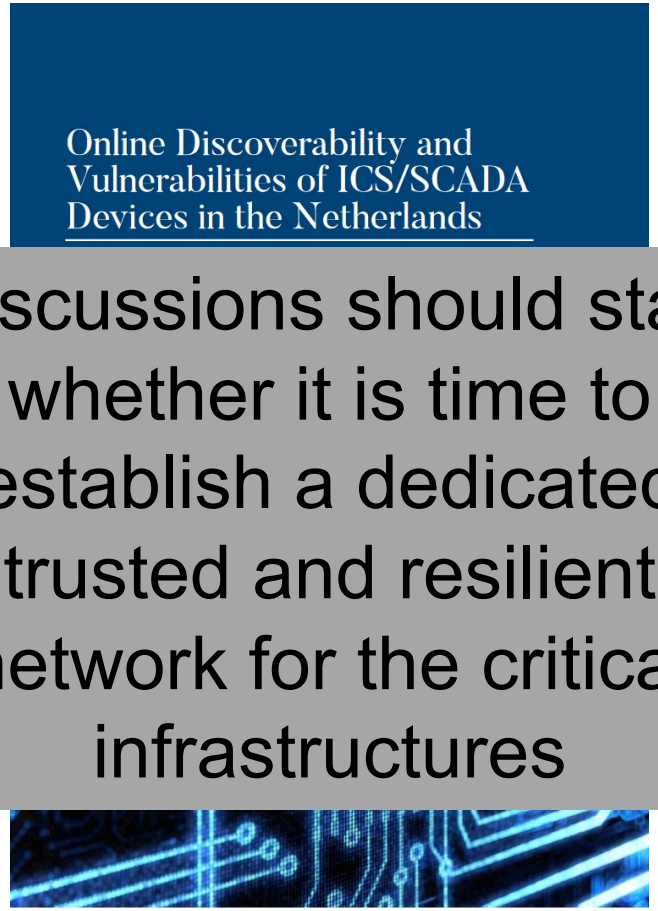
WWW.2STiC.NL

Recent public administration reports

Pay more attention to the network and supply chains which support critical processes

Recent public administration reports

Pay more attention to the network and supply chains which support critical processes



Discussions should start whether it is time to establish a dedicated trusted and resilient network for the critical infrastructures

Threat examples

Security

‘Nog eens honderden bedrijven onbeveiligd door lek in VPN-netwerk’

Om welke bedrijven het precies gaat, is om veiligheidsredenen niet bekendgemaakt. Het gaat om veel ICT-bedrijven, een groot ziekenhuis en een beursgenoteerd bedrijf.

Marissa van Loon 29 september 2019 om 17:05 Leestijd 1 minuut

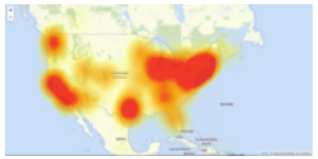
Threat examples

Stability

Distributed malware attacks Dyn DNS, takes down websites in US

Written by Wikinews, Oct 23, 2016, 0 Comments

Monday, October 24, 2016



The third attack distribution as provided by downdetector.com and OpenStreetMap.

On Friday, a network of diverse Internet-connected devices targeted the Dyn domain registration service provider. It took down Dyn clients, including several popular websites such as Twitter, Netflix, Spotify, Reddit, *New York Times*, and *Wired*.

The attack involved targeting Dyn's domain name system servers with a

Internet

Related stories

- Distributed malware attacks Dyn DNS, takes down websites in US
- Time magazine names Ahmed Mohamed to 'Most Influential Teens of 2015'
- Wikinews interviews painter Pricasso on his art and freedom of expression
- Texas student Ahmed Mohamed inspires social movement
- London court jails man after Dark Web ricin sting

Security

'Nog eens honderden bedrijven onbeveiligd door lek in VPN-netwerk'

Om welke bedrijven het precies gaat, is om veiligheidsredenen niet bekendgemaakt. Het gaat om veel ICT-bedrijven, een groot ziekenhuis en een beursgenoteerd bedrijf.

Marissa van Loon 29 september 2019 om 17:05 Leestijd 1 minuut

Threat examples

Stability

Security

Distributed malware attacks Dyn DNS, takes down websites in US

Written by Wikinews, Oct

Monday, October 24, 2016

The third attack distribution as
provided by downdetector.com
and OpenStreetMap.

On Friday, a network of diverse
domain registration service pr
several popular websites such
Times, and *Wired*.

The attack involved targeting

'Nog eens honderden bedrijven onbeveiligd door lek in VPN-netwerk'

denen niet bekendgemaakt. Het
beursgenoteerd bedrijf.

For two hours, a large chunk of European mobile traffic was rerouted through China

It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western countries."

By Catalin Cimpanu for Zero Day | June 7, 2019 -- 19:41 GMT (20:41 BST) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
Bitpoint cryptocurrency exchange hacked for $32 million

Security
US mayors group adopts resolution not to pay any more ransoms to hackers

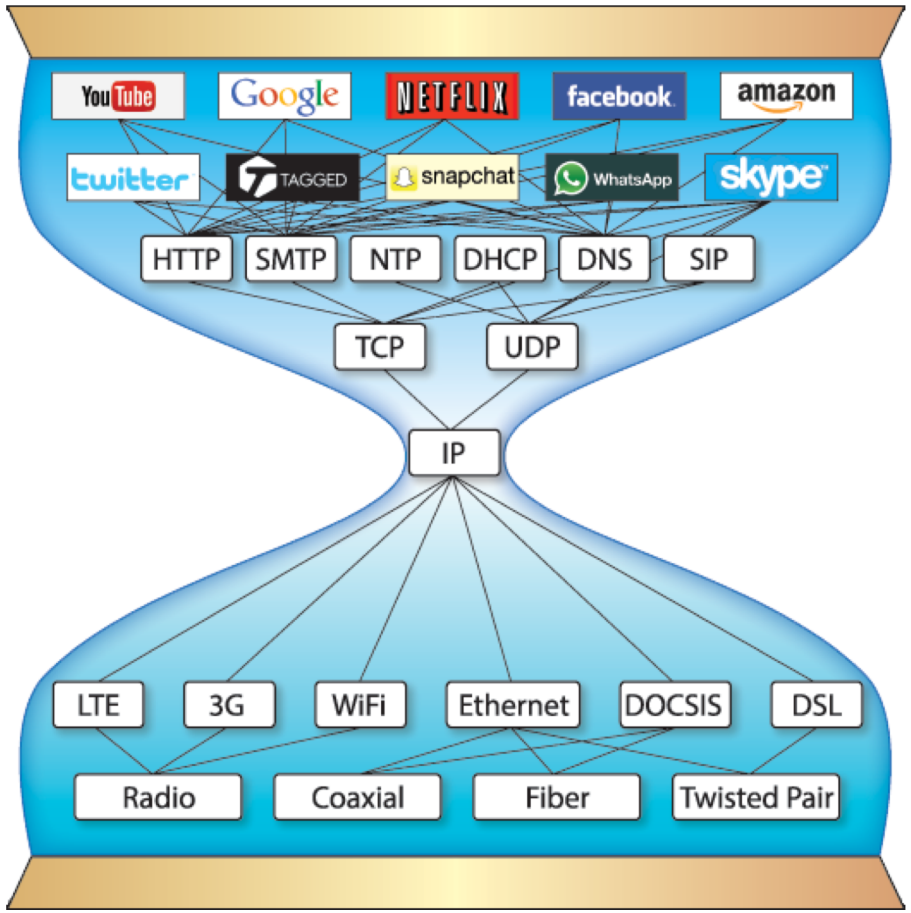
Security
German banks are moving away from SMS one-time passcodes

Security
Recent Windows zero-day used by Buhtrap gang for cyber-espionage

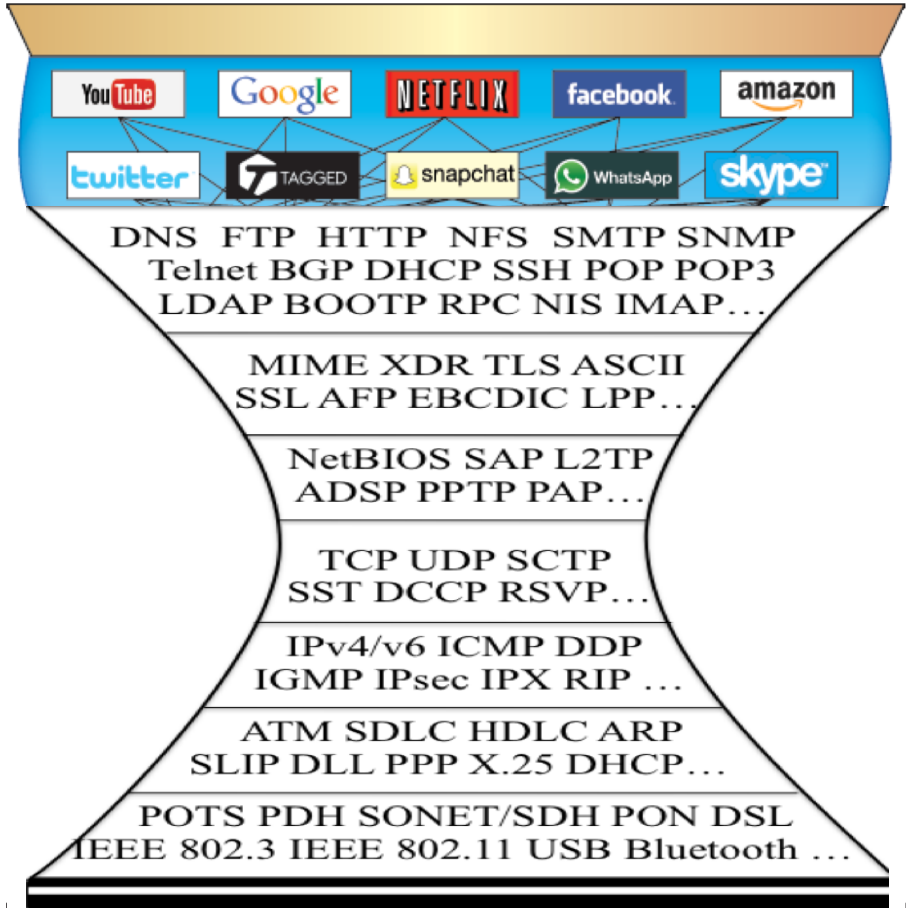
NEWSLETTERS

Transparency

Threats


YouTube
Google
NETFLIX
facebook
amazon
twitter
TAGGED
snapchat
WhatsApp
skype
HTTP
SMTP
NTP
DHCP
DNS
SIP
TCP
UDP
IP
LTE
3G
WiFi
Ethernet
DOCSIS
DSL
Radio
Coaxial
Fiber
Twisted Pair

Threats


YouTube
Google
NETFLIX
facebook
amazon
twitter
TAGGED
snapchat
WhatsApp
skype
DNS FTP HTTP NFS SMTP SNMP
Telnet BGP DHCP SSH POP POP3
LDAP BOOTP RPC NIS IMAP...
MIME XDR TLS ASCII
SSL AFP EBCDIC LPP...
NetBIOS SAP L2TP
ADSP PPTP PAP...
TCP UDP SCTP
SST DCCP RSVP...
IPv4/v6 ICMP DDP
IGMP IPsec IPX RIP ...
ATM SDLC HDLC ARP
SLIP DLL PPP X.25 DHCP...
POTS PDH SONET/SDH PON DSL
IEEE 802.3 IEEE 802.11 USB Bluetooth ...

Threats

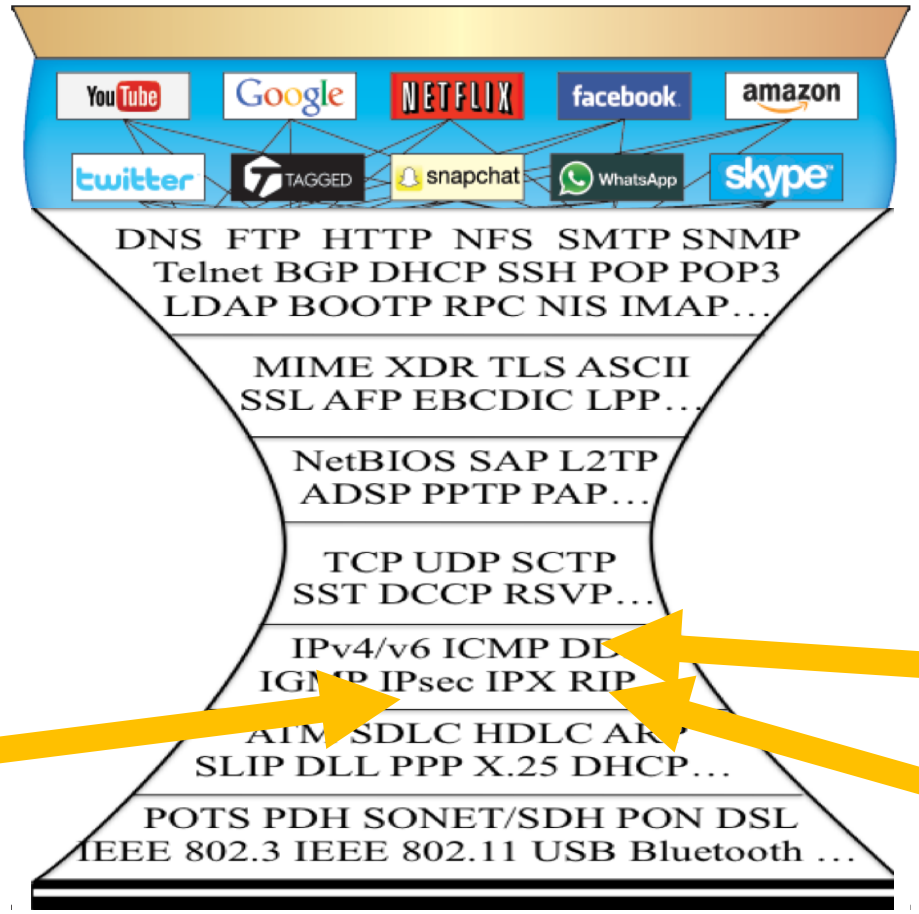
Decision

Malicious

Human error

Investigation

Threats

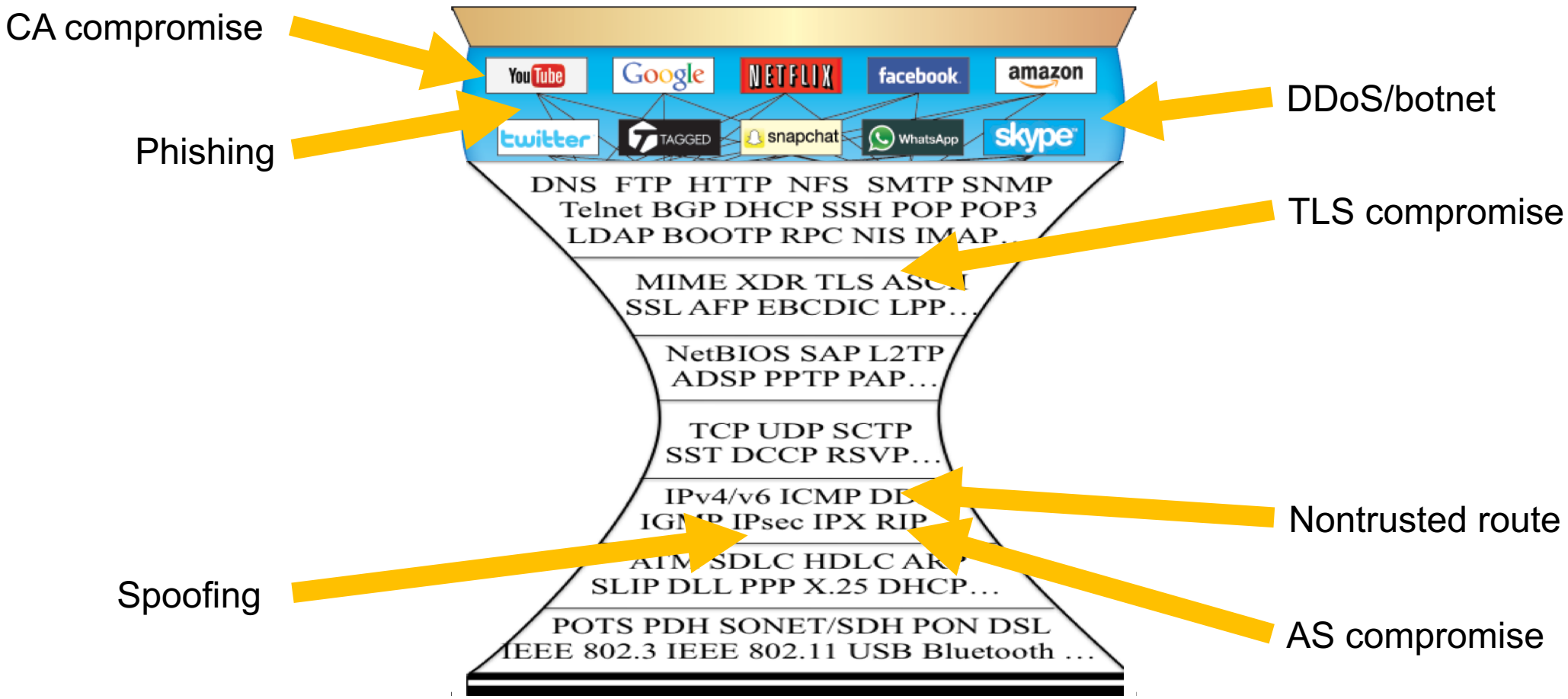


Spoofing

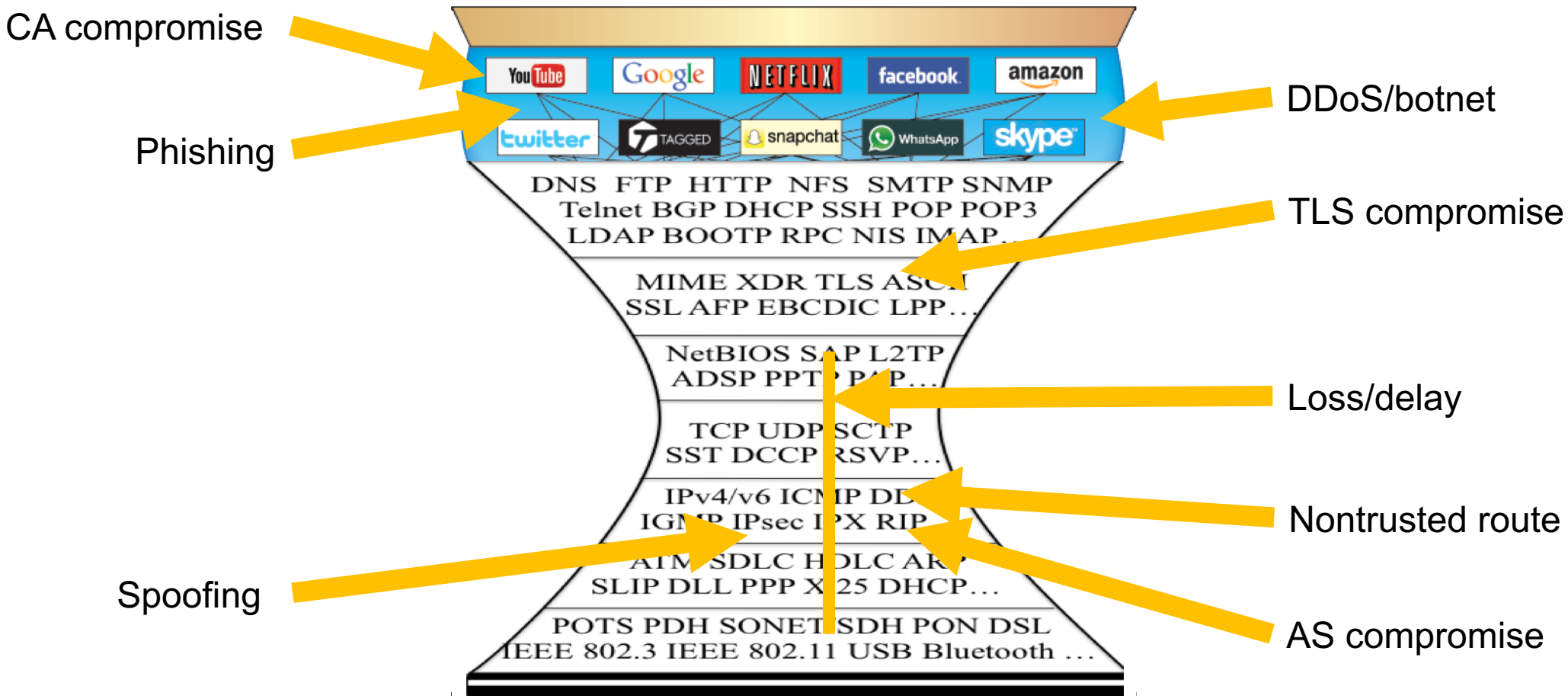
Nontrusted route

AS compromise

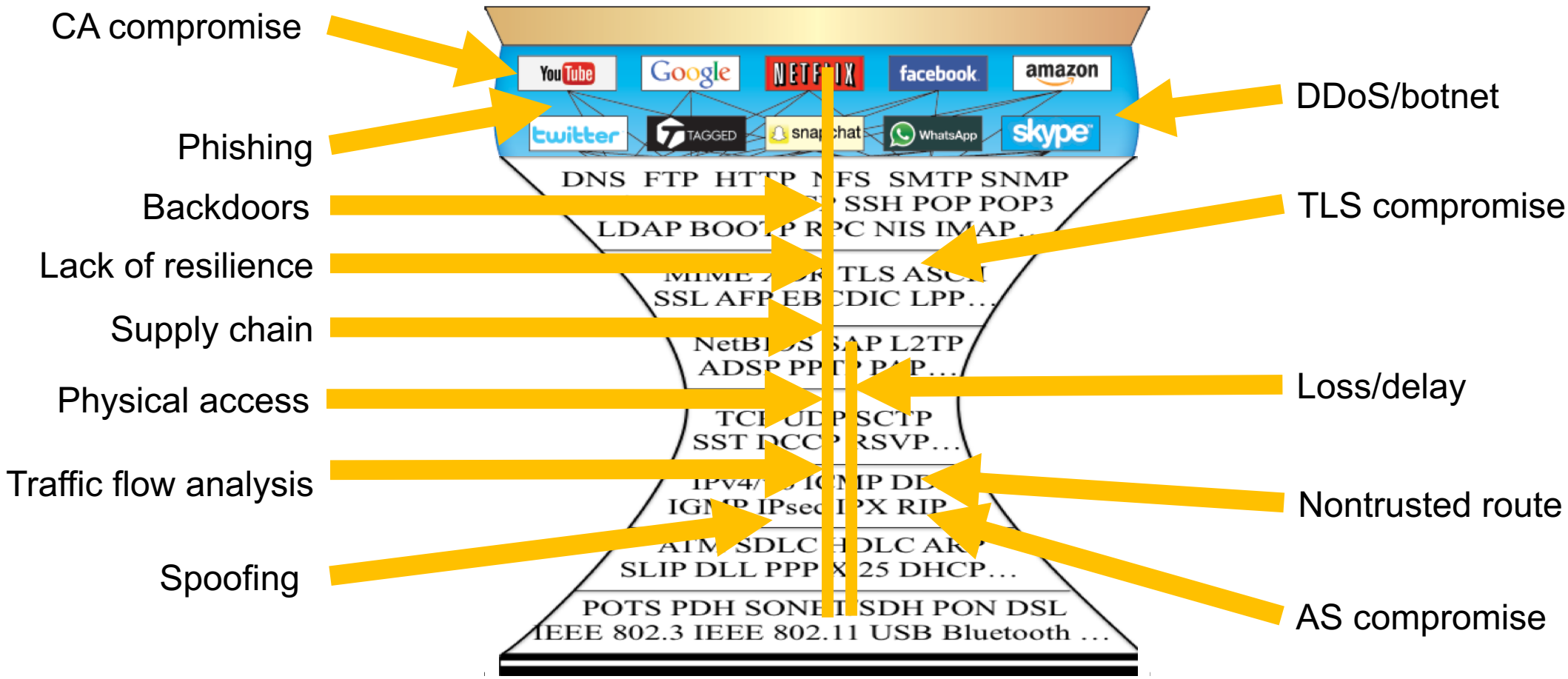
Threats


CA compromise
Phishing
Spoofing
DDoS/botnet
TLS compromise
Nontrusted route
AS compromise
YouTube
Google
NETFLIX
facebook
amazon
twitter
TAGGED
snapchat
WhatsApp
skype
DNS FTP HTTP NFS SMTP SNMP
Telnet BGP DHCP SSH POP POP3
LDAP BOOTP RPC NIS IMAP...
MIME XDR TLS ASCII
SSL AFP EBCDIC LPP...
NetBIOS SAP L2TP
ADSP PPTP PAP...
TCP UDP SCTP
SST DCCP RSVP...
IPv4/v6 ICMP DDP
IGMP IPsec IPX RIP
ATM SDLC HDLC ARP
SLIP DLL PPP X.25 DHCP...
POTS PDH SONET/SDH PON DSL
IEEE 802.3 IEEE 802.11 USB Bluetooth ...

Threats


CA compromise
Phishing
Spoofing
DDoS/botnet
TLS compromise
Loss/delay
Nontrusted route
AS compromise
YouTube
Google
NETFLIX
facebook
amazon
twitter
TAGGED
snapchat
WhatsApp
skype
DNS FTP HTTP NFS SMTP SNMP
Telnet BGP DHCP SSH POP POP3
LDAP BOOTP RPC NIS IMAP...
MIME XDR TLS ASCII
SSL AFP EBCDIC LPP...
NetBIOS SAP L2TP
ADSP PPTP PAP...
TCP UDP SCTP
SST DCCP RSVP...
IPv4/v6 ICMP DDP
IGMP IPsec IPX RIP
ATM SDLC HDLC ARP
SLIP DLL PPP X.25 DHCP...
POTS PDH SONET SDH PON DSL
IEEE 802.3 IEEE 802.11 USB Bluetooth ...

Threats


CA compromise
Phishing
Backdoors
Lack of resilience
Supply chain
Physical access
Traffic flow analysis
Spoofing
DDoS/botnet
TLS compromise
Loss/delay
Nontrusted route
AS compromise
YouTube
Google
facebook
amazon
twitter
TAGGED
WhatsApp
skype
DNS FTP
SMTP SNMP
SSH POP POP3
LDAP
NIS
SSL
SCTP
RSVP
SLIP DLL PPP
DHCP
POTS PDH
SDH PON DSL
IEEE 802.3 IEEE 802.11 USB Bluetooth

Lessons learnt over 50 years

- The Internet has come a long way: from small computer network to worldwide social environments

Lessons learnt over 50 years

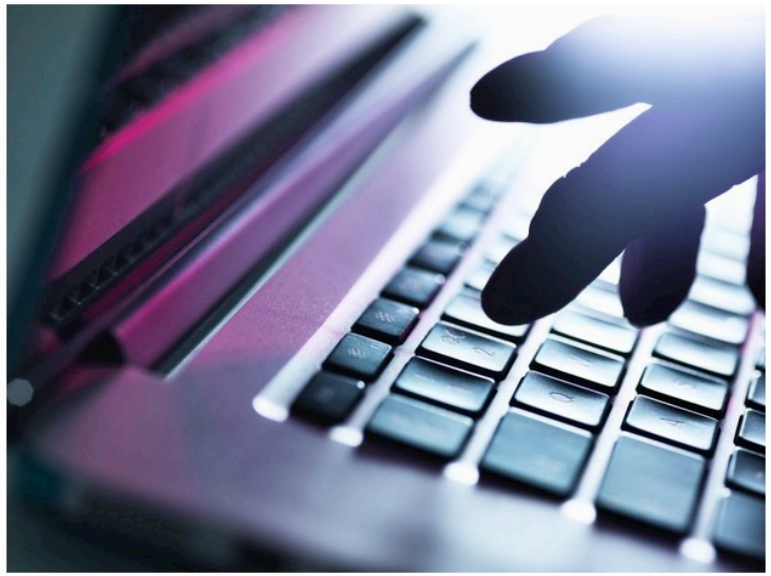
- The Interne
  from small
  worldwide s

Los Angeles Times

ADVERTISEMENT

OPINION

Opinion: 50 years ago, I helped invent the internet. How did it go so wrong?



Scientists inadvertently created the perfect formula for the "dark" side of the internet to spread like a virus by enabling anyone to reach millions of people inexpensively and anonymously. (Rafe Swan / Getty Images/Cultura RF)

By LEONARD KLEINROCK OCT. 29, 2019 | 3 AM

When I was a young scientist working on the fledgling creation that came to be known as the internet, the ethos that defined the culture we were building was characterized by words such as ethical, open, trusted, free, shared. None of us knew

ADVERTISEMENT

LATEST OPINION

OPINION
Letters to the Editor: Rep. Katie Hill has no one to blame but herself for using bad judgment
2 hours ago

OPINION
Letters to the Editor: Sorry, rich people, you'll pay more so we can have single payer
2 hours ago

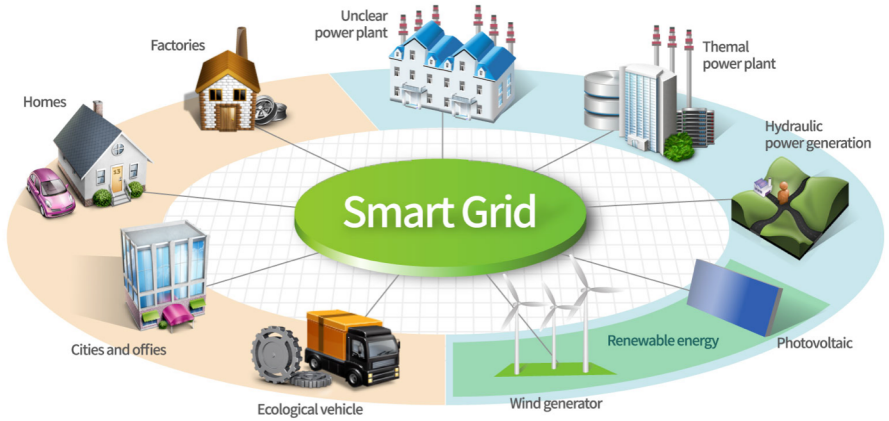
OPINION
Letters to the Editor: Imperiling Alaska's salmon by allowing the Pebble Mine would be a disaster
2 hours ago

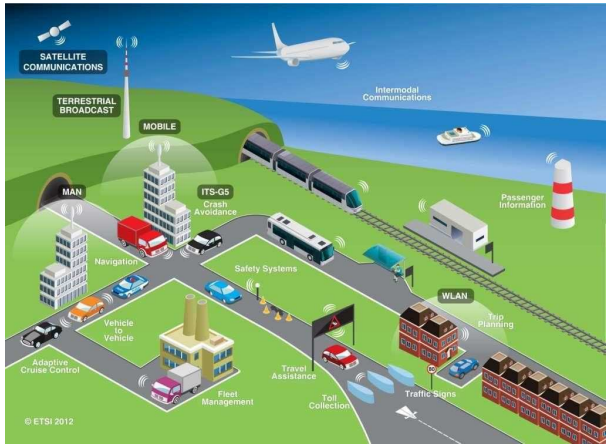
OPINION
Column: Facial ID recognition can help on your phone, but not so much in law enforcement hands
Oct. 30, 2019

OPINION
Opinion: A California gubernatorial candidate's campaign strategy? Lie on Facebook
Oct. 29, 2019

Lessons learnt over 50 years

- The Internet has come a long way: from small computer network to worldwide social environments
- QoS, scope, security, content delivery and mobility were though not part of initial Internet design





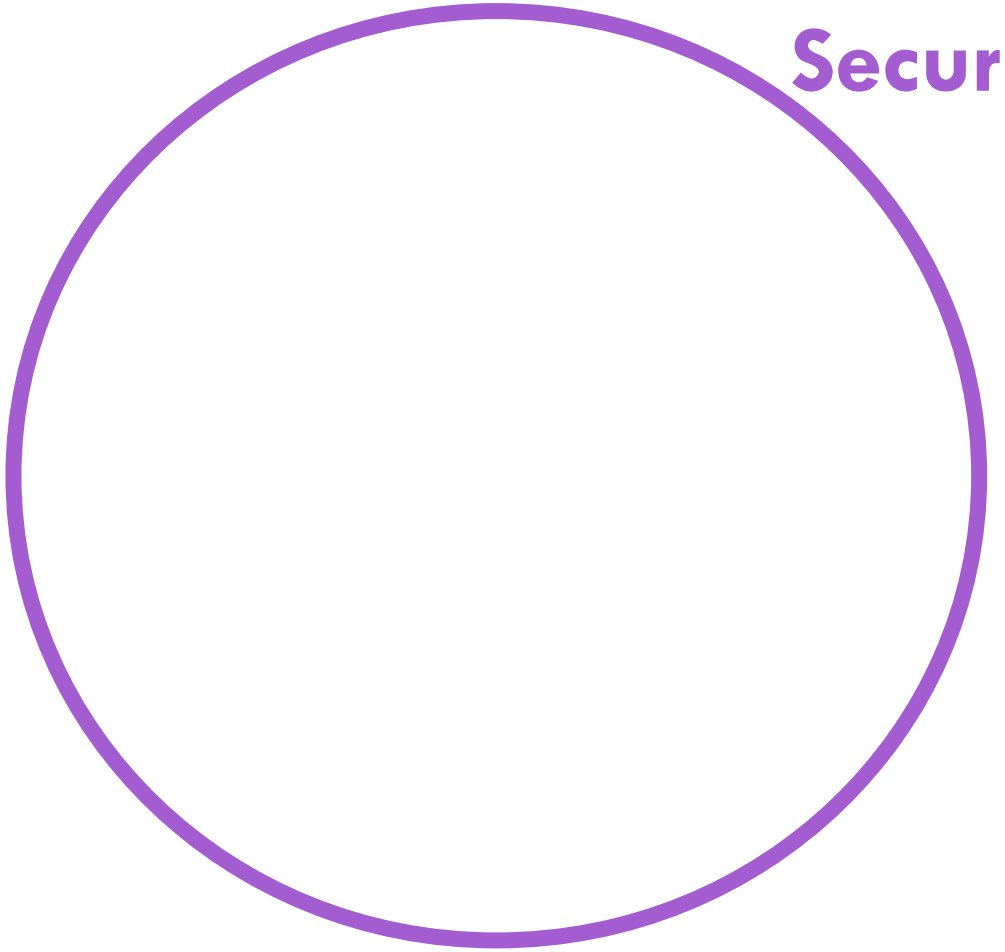
Several approaches to progress this

- Add essential functionality to Internet (reactive)
  - Important to keep Internet safe and providing compatibility is easy
  - Unknow effects of add-ons on security and transparency
- Investigate more fundamental approaches (proactive)
  - Include lessons learnt over 50 years
  - Transition is difficult, but easier for niche applications
- 2STiC programme will look at both in a practical approach…

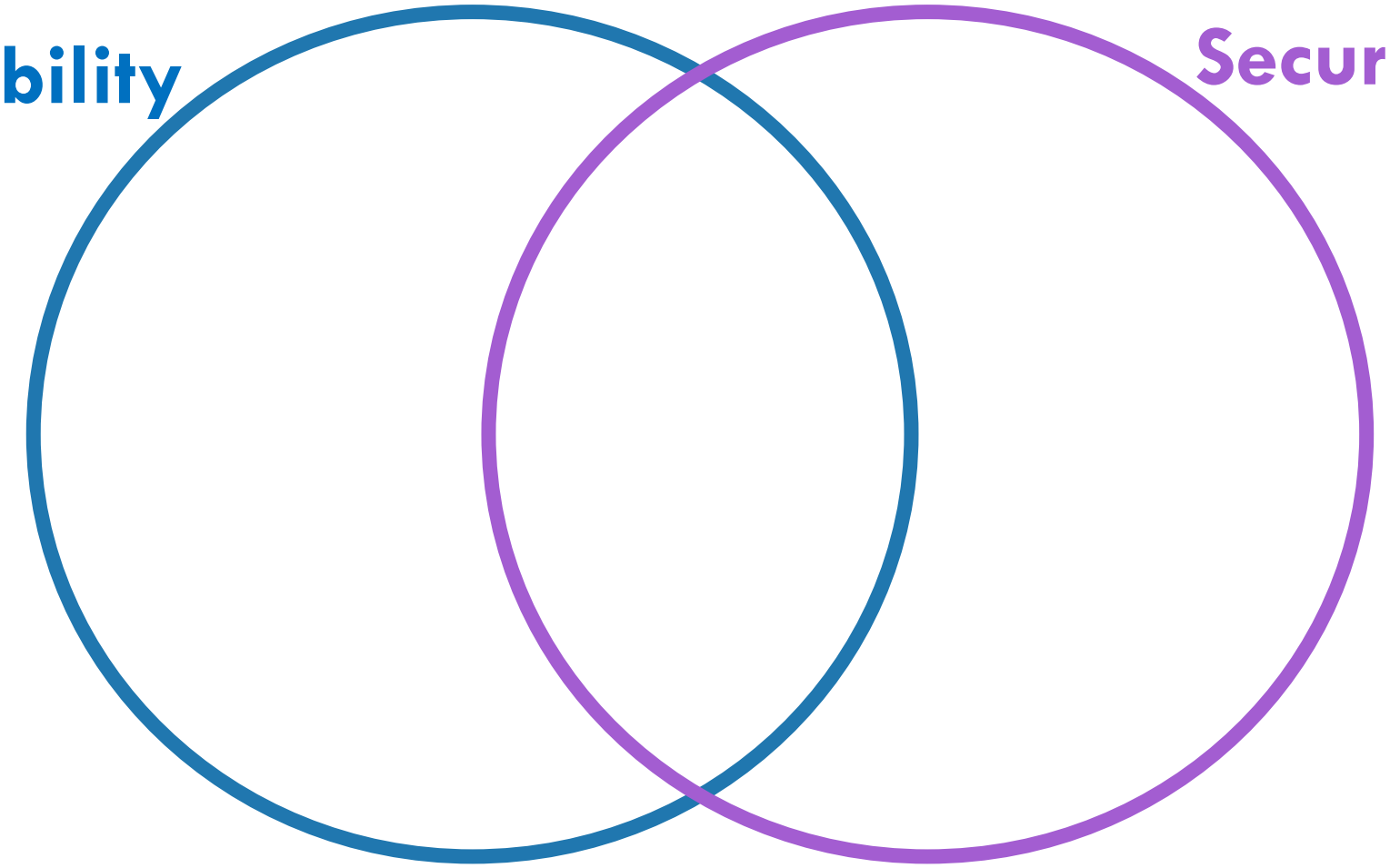
2STiC programme

Put Dutch and European internet communities in leading position of secure, stable and transparent inter-network communication

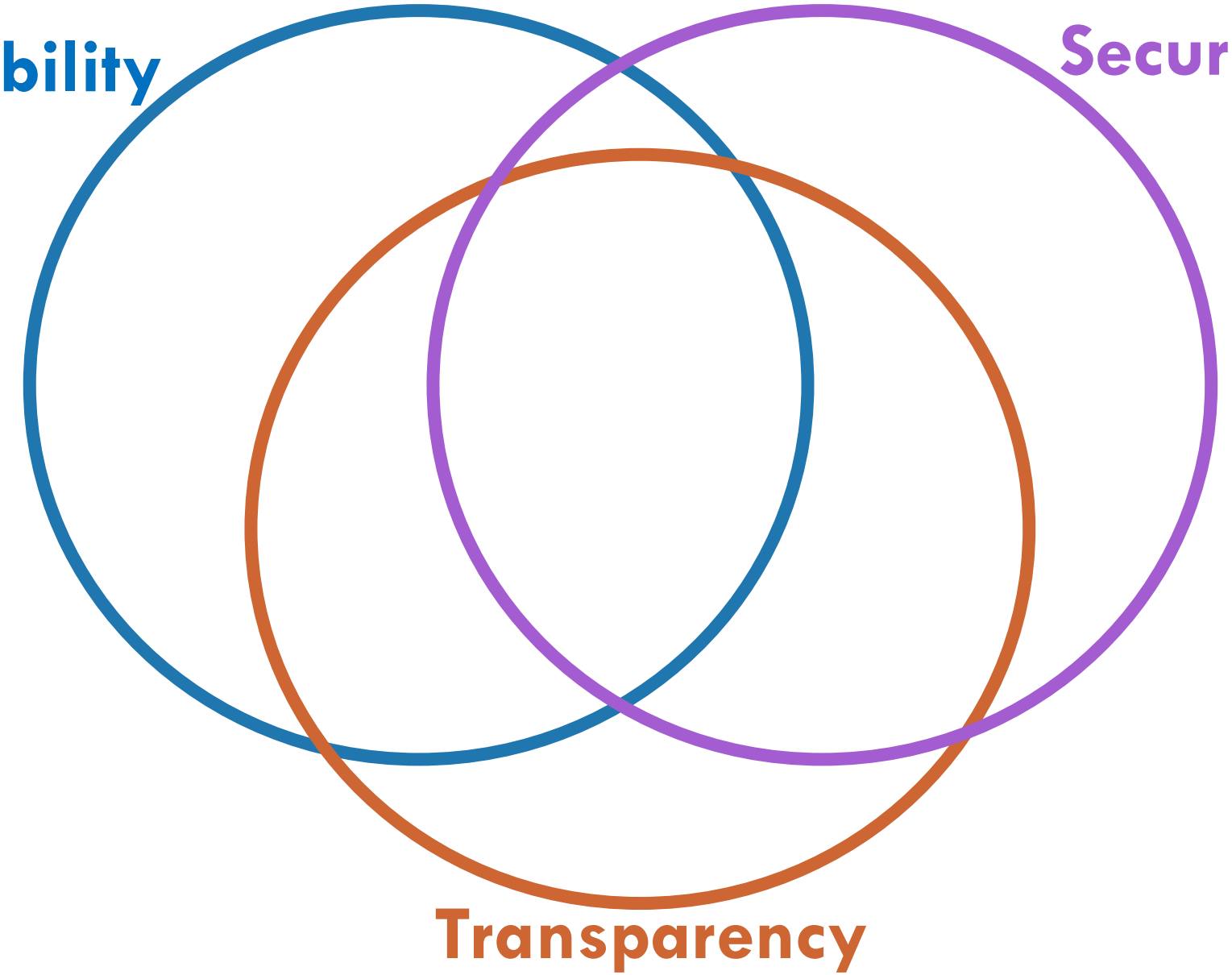
Security, Stability and Transparency are key



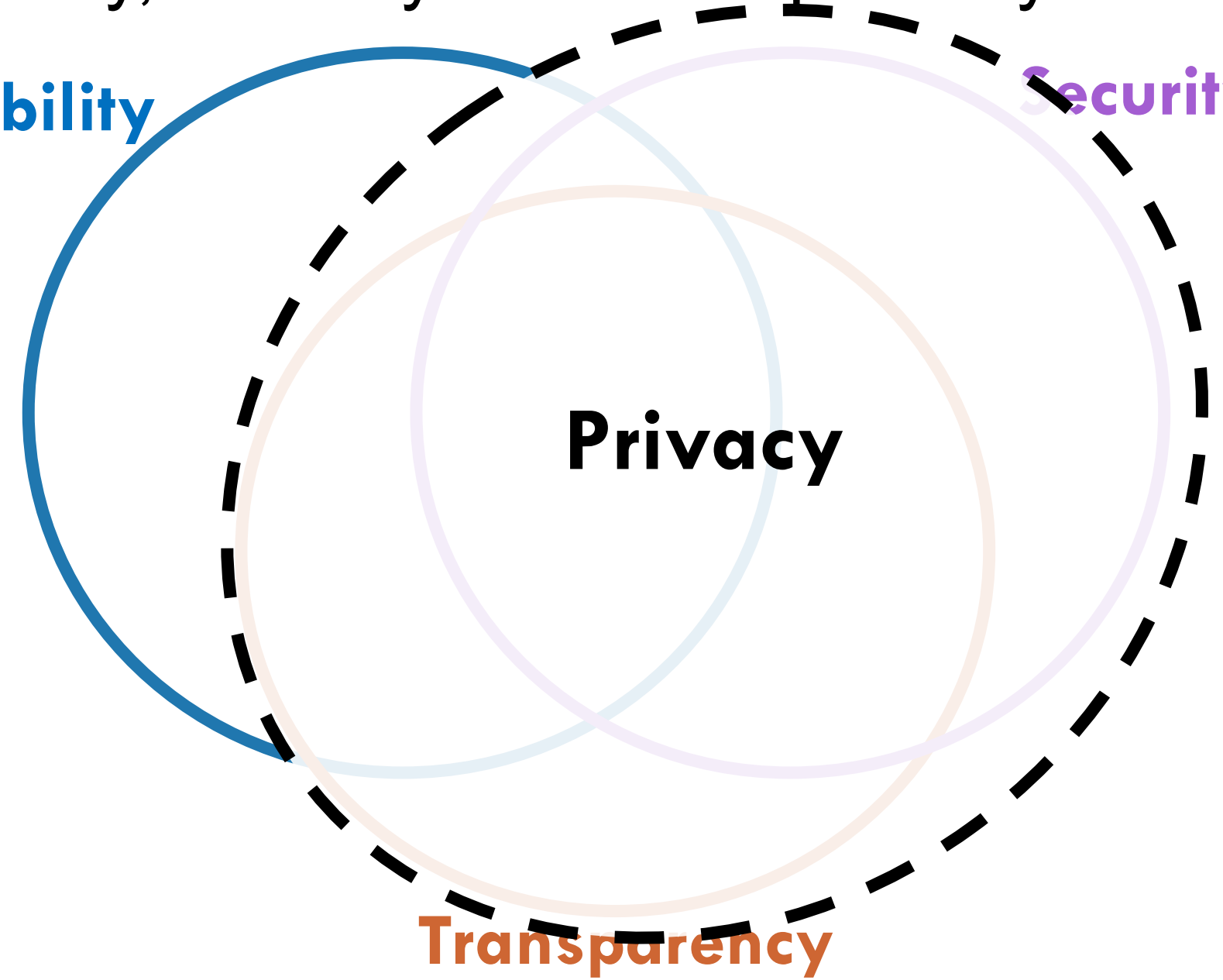
Security, Stability and Transparency are key



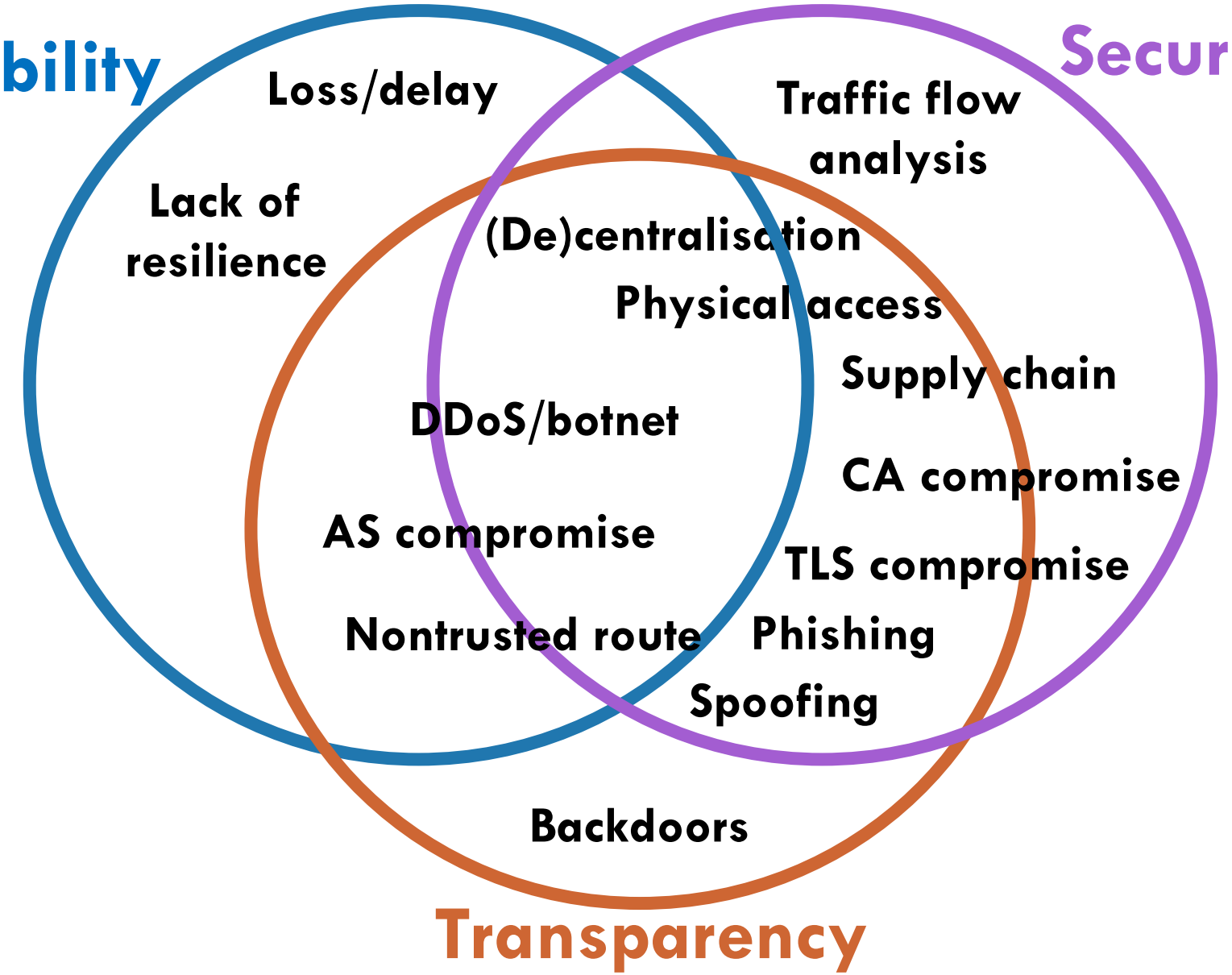
Security, Stability and Transparency are key



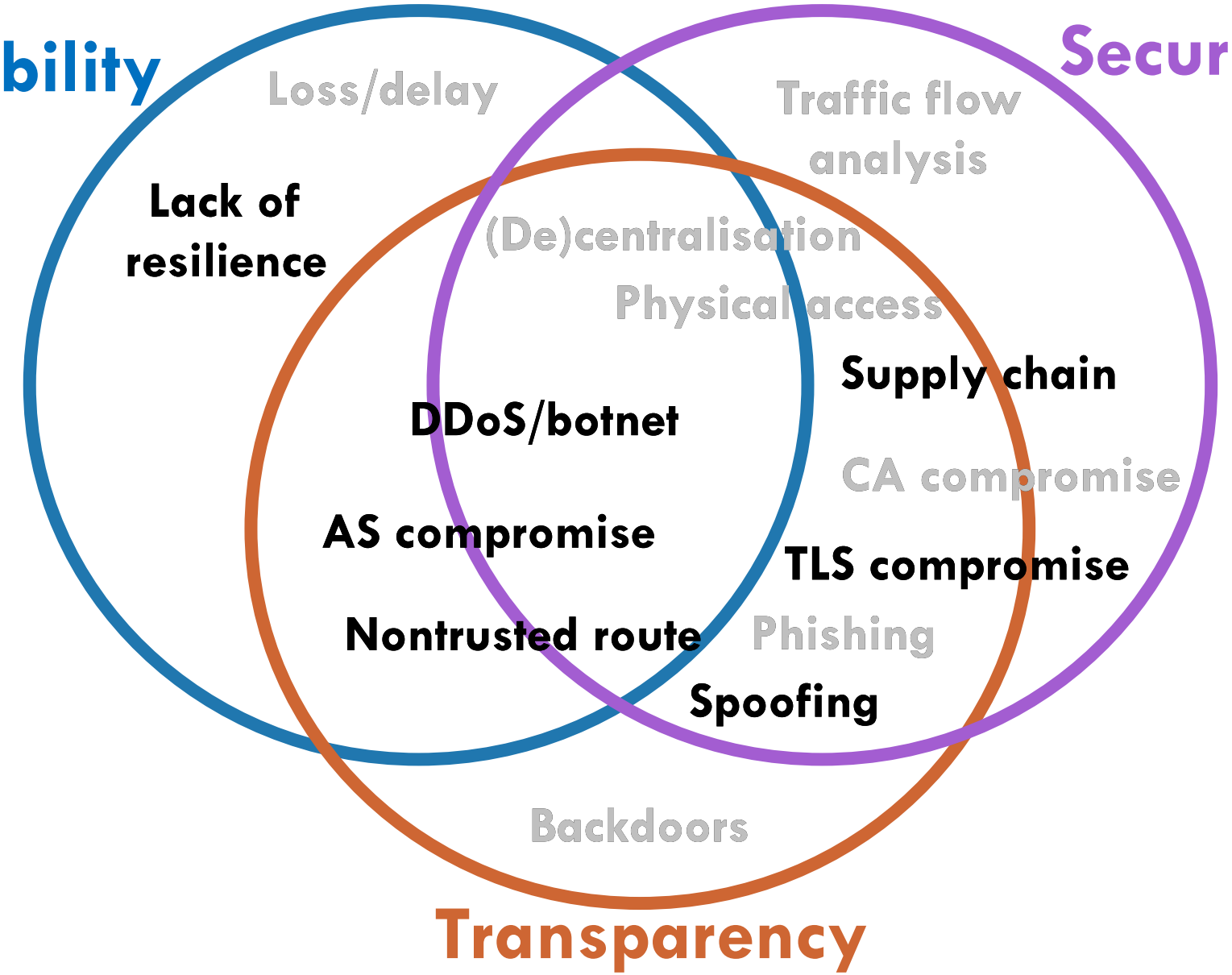
Security, Stability and Transparency are key



Security, Stability and Transparency threats



Security, Stability and Transparency priorities



Motivations for 2STiC programme

- New applications need new security, resilience and transparency requirements
  - More interaction with physical space (e.g., transport, energy grids, drones, remote healthcare procedures)
  - More insight in and control over who processes their (user) data
- Meet requirements through (multiple) shared internets
  - Applications will increasingly require ubiquitous computing and networking
  - Operating dedicated infrastructure might reduce value for money
- Open programmable network services become commercially available
  - Data plane, control plane and hardware programmability

Basic approach of 2STiC programme

- Act as an expertise centre
- Coordinate grant proposals
- Include multi-domain, governance, trust and deployment aspects from the start
- Evaluate future internet infrastructures that have active communities with testbeds and use open source code
- Learn by doing
- Focus on realistic/practical use cases and demonstrators

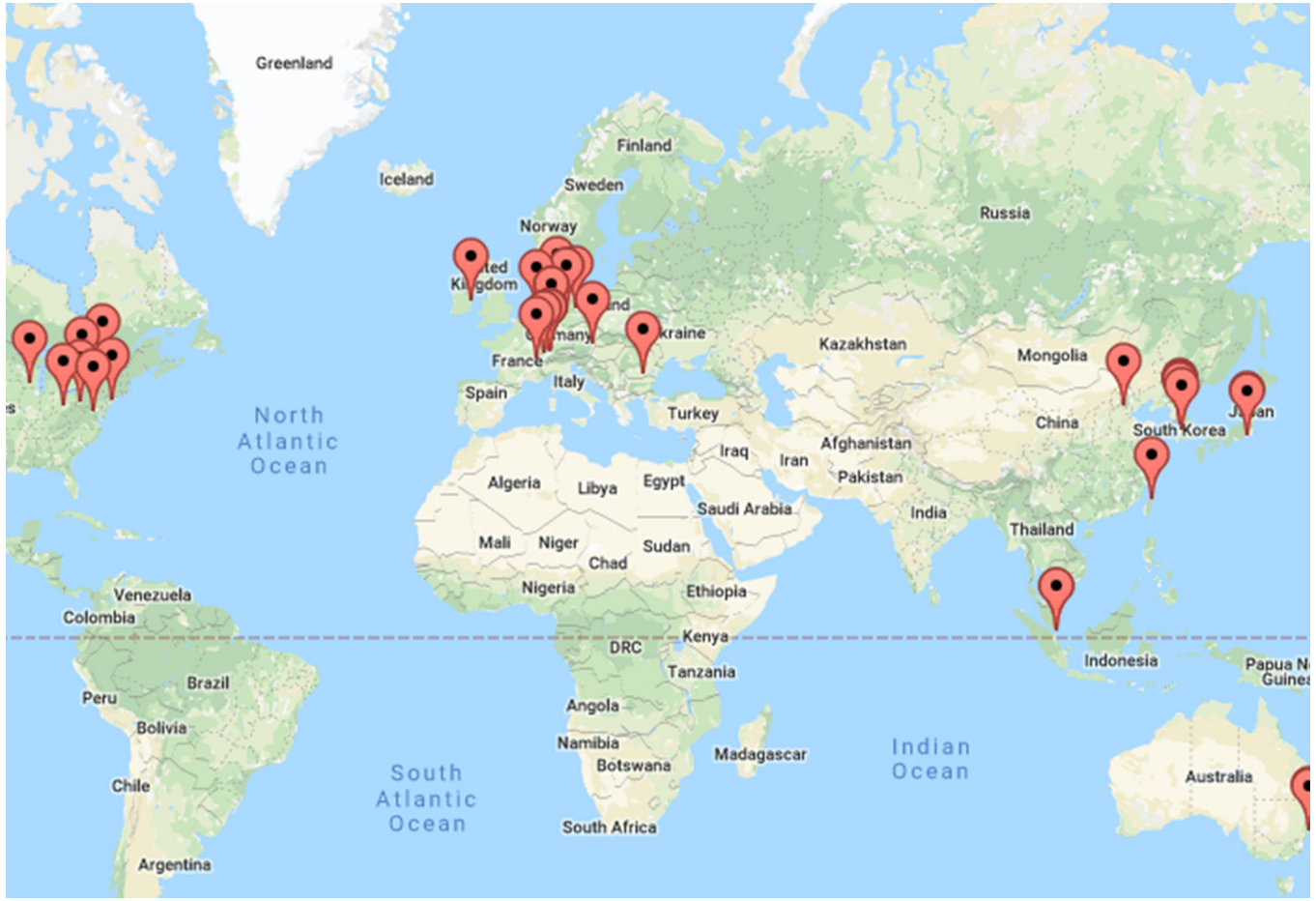
2STiC activities

Future internet infrastructures

- Current and past initiatives:
  - EC funded: Future Internet Research and Experimentation (FIRE), Next Generation Internet (NGI)
  - USA funded: NSF Future Internet Architecture
- Selection criteria:
  - Security, stability and transparency
  - Active community
  - Open community
- SCION, RINA, NDN

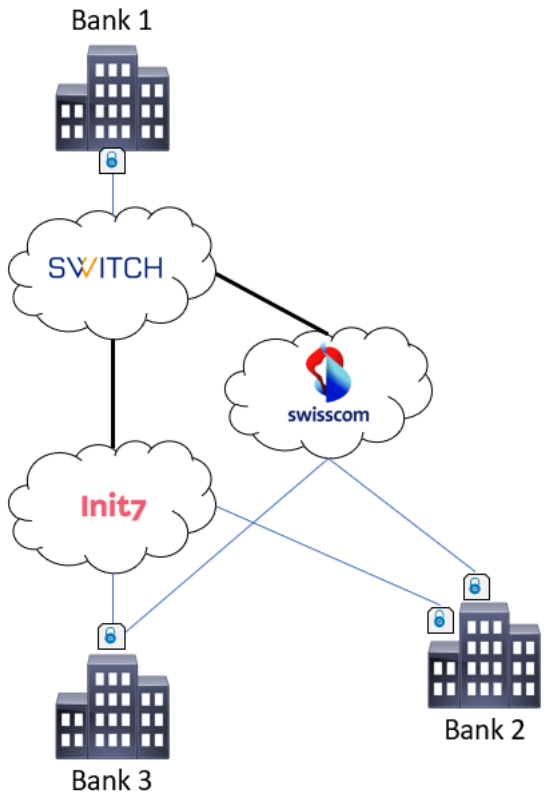
SCION

- SCION: Scalability, Control, and Isolation on Next-Generation Networks
- Network security group at ETH Zurich
- Goal: increase security of inter-domain routing
  - Path control
  - Resilience (e.g. redundant paths, no route hijacks)
  - Active research, e.g. into congestion control and QoS
  - Incremental deployment (e.g. SCION-IP gateway)
- Hands-on experience



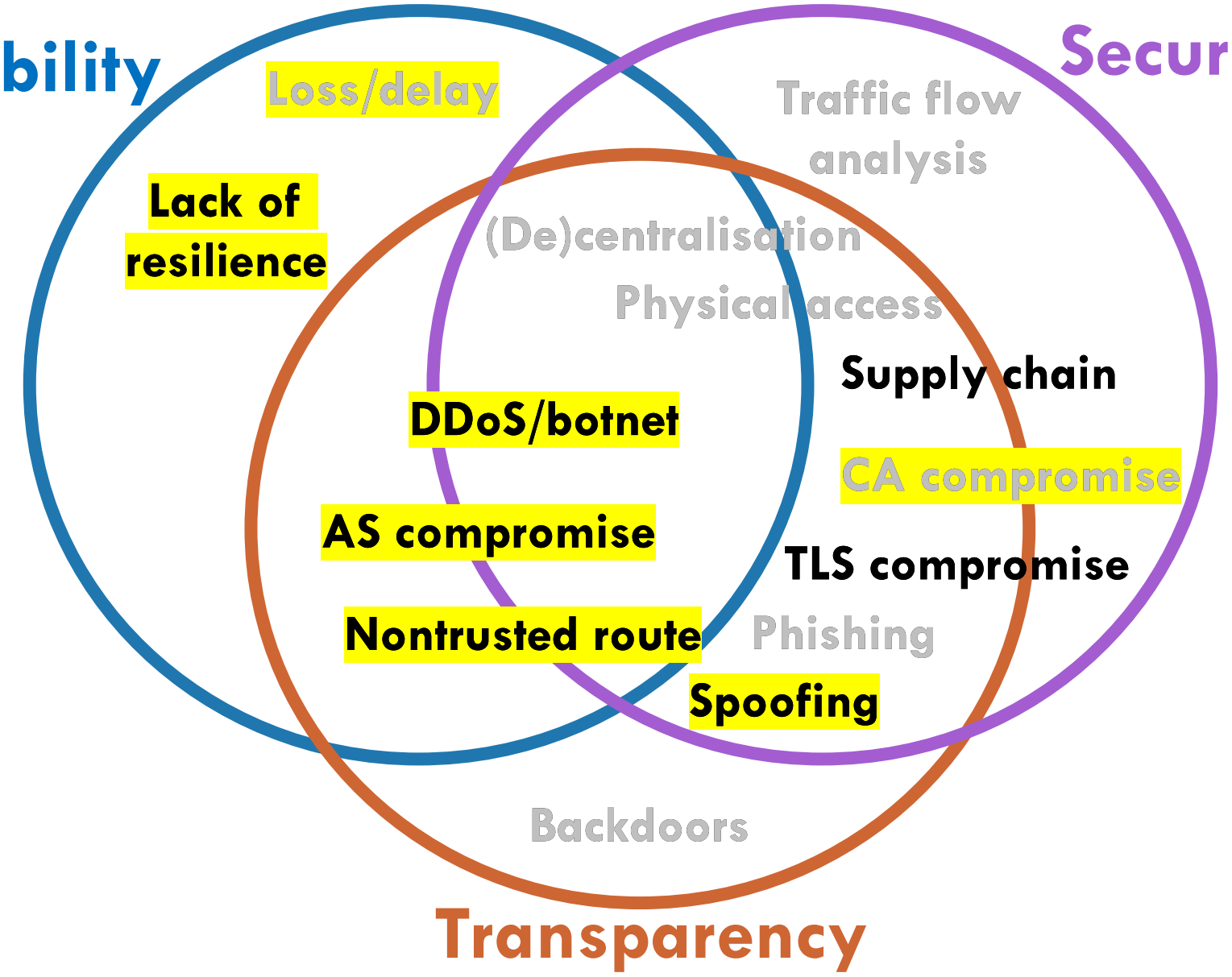
Using existing applications with SCION

- Incremental deployment
  - Run IP applications on SCION; currently testing/experimenting with DNS
  - No need to change user applications
- Benefits: no route hijacks, resilience through multiple paths, path control at network level



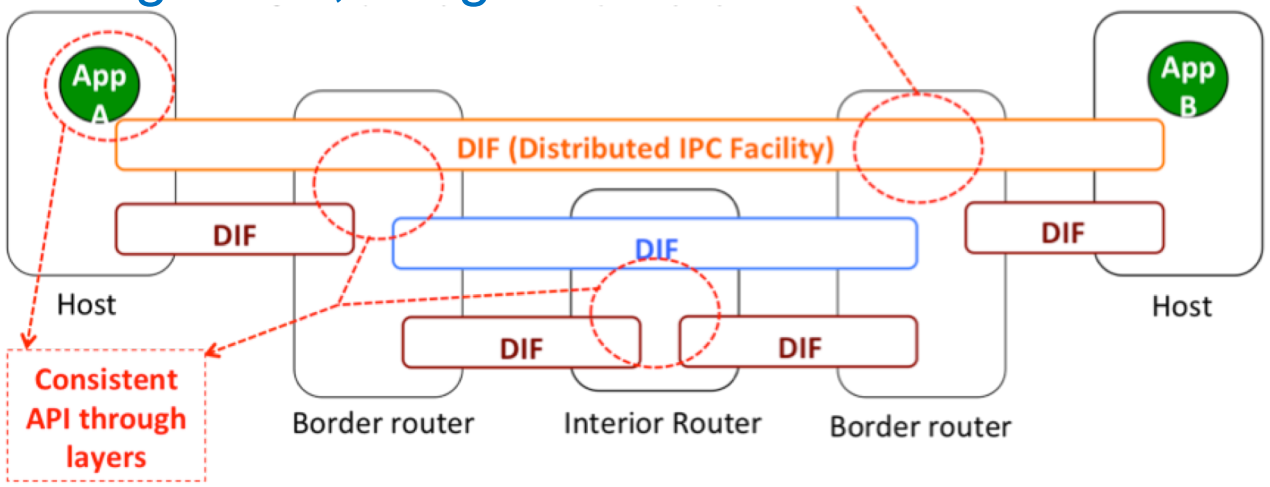
anapaya systems

Security, Stability and Transparency in SCION

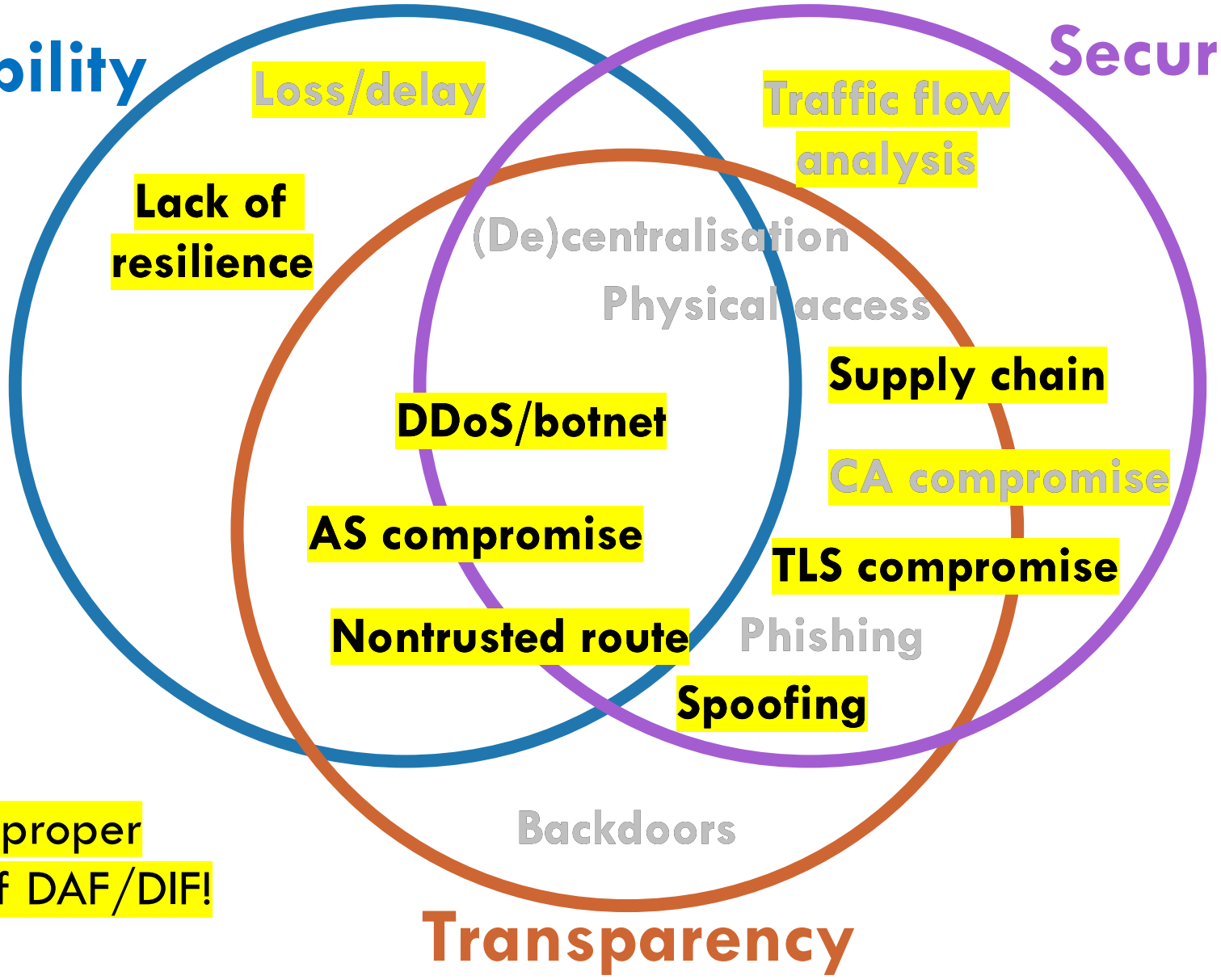


RINA

- RINA: Recursive InterNetwork Architecture
- Goal: address fundamental problems through a new architecture
  - An architecture: not a protocol
  - Provides mechanisms and policies (a toolbox) for network designers
  - Organize repeated functionality across layers
  - Idea is to standardize security, management, congestion
- Starting to look into RINA



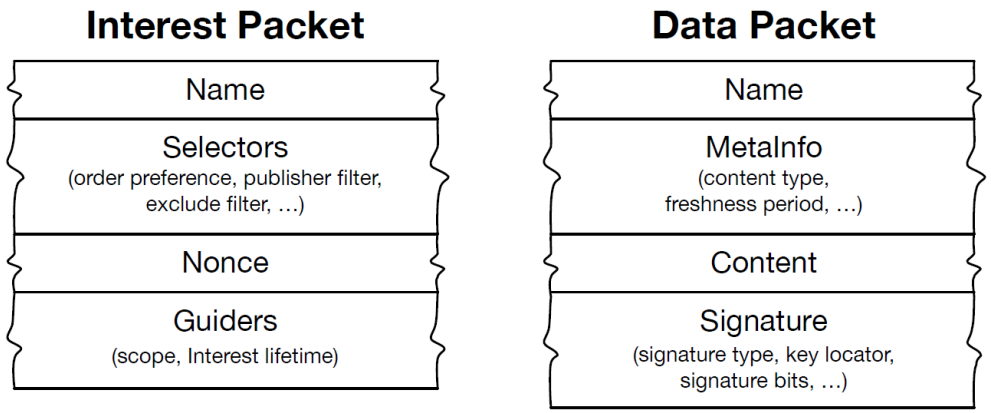
Security, Stability and Transparency in RINA



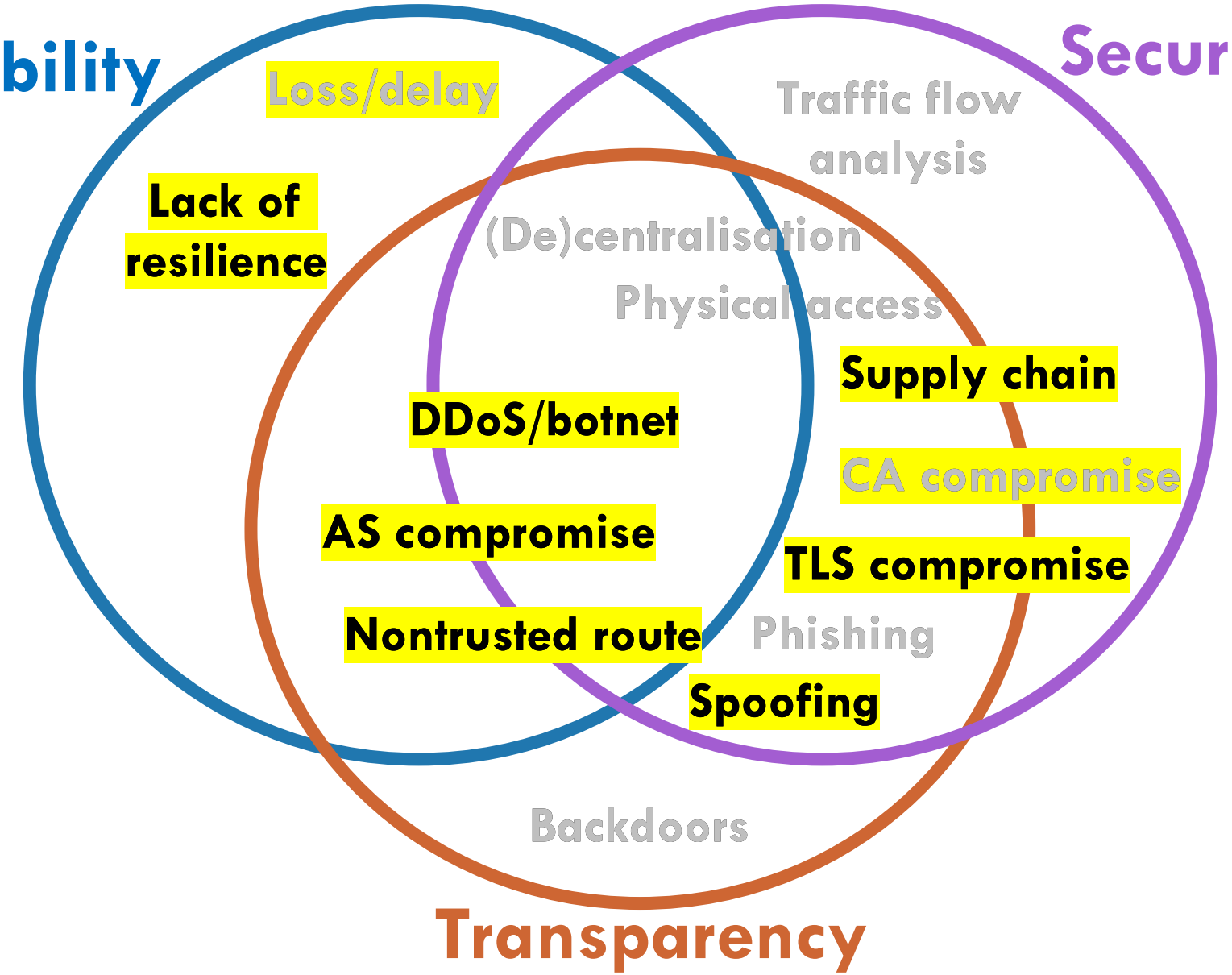
Depending on proper implementation of DAF/DIF!

NDN

- NDN: Named Data Networking
- Fundamental change: information-centric rather than host-centric
- Distribution of information, say from ICT/IIoT/IoT devices
- Little bit like Content Delivery Network (CDNs), but built into the network
- We'll look into NDN later



Security, Stability and Transparency in NDN



High level overview

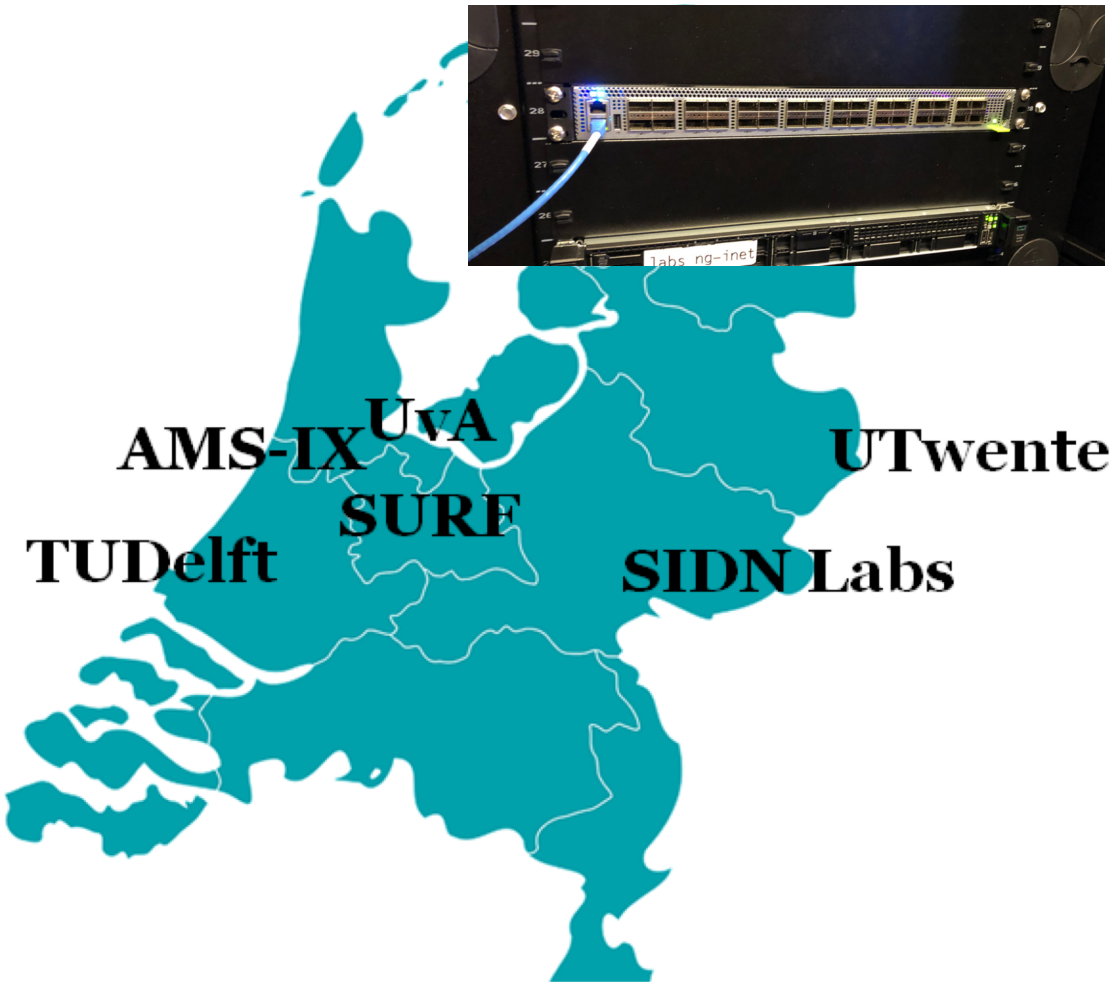
Aspect		IP	SCION	RINA	NDN
evolution	clean slate				
packet	chunk				
protocol	framework				
intra network	inter network				
operational	PoC				

Open programmable networks

- Networking hardware such as routers and switches
- Related to Software Defined Networking (SDN)
  - Control plane vs. data plane
- Allows us to implement and deploy new protocols

2STiC testbed

- Goal: evaluate future internet infrastructures, see how they perform "in real life"
- Open programmable networking hardware
- Experiment with P4-capable hardware (switches and network interfaces)
- Status: some partners connected, working on connecting the others



Applying our findings

- We are developing scenarios to experiment with those technologies:
  - What are interesting scenarios?
  - How do they perform in practice?
  - Do they solve our problems?
- Talking to various organizations from several sectors: transport systems, health, energy suppliers, monetary institutes, public administration, industrial control systems
- Can we help you?
  victor.reijs@sidn.nl