SHIELD

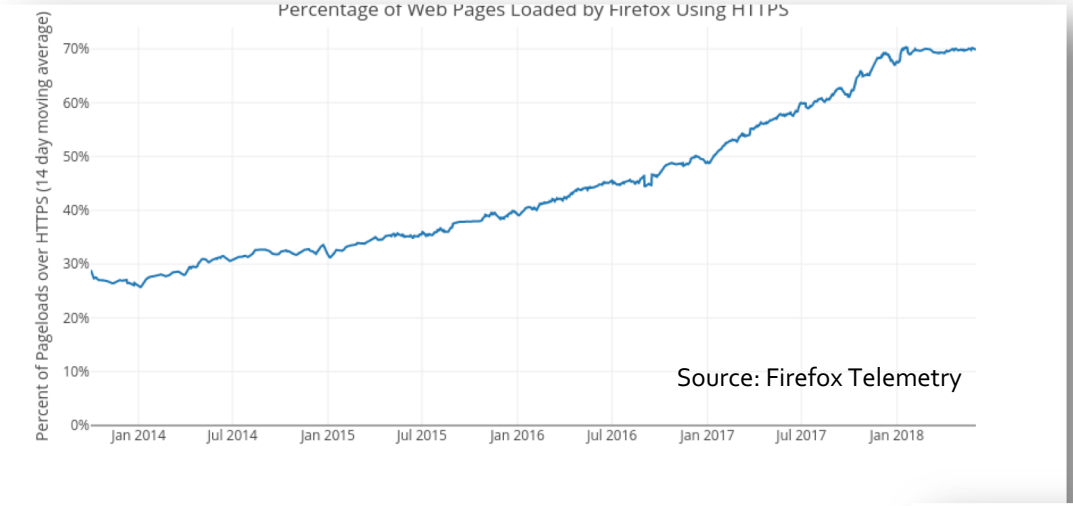
SECURING AGAINST INTRUDERS AND OTHER THREATS
THROUGH A NFV-ENABLED ENVIRONMENT
[H2020 - Grant Agreement No. 700199]

ACME STAR as an MSP enabler for TLS traffic

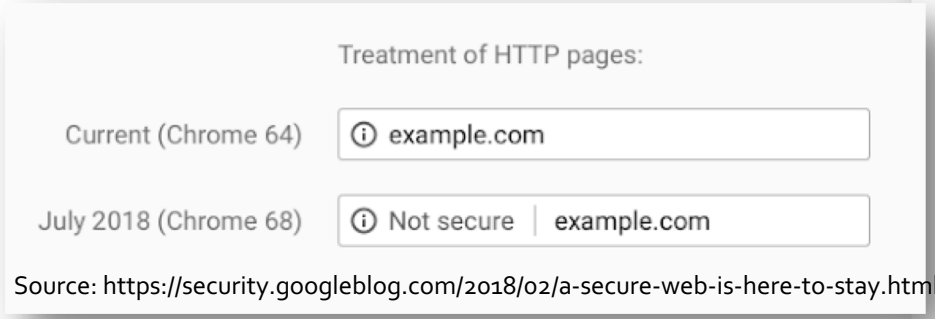
and its integration in a security Service

Antonio Pastor. Telefonica I+D.

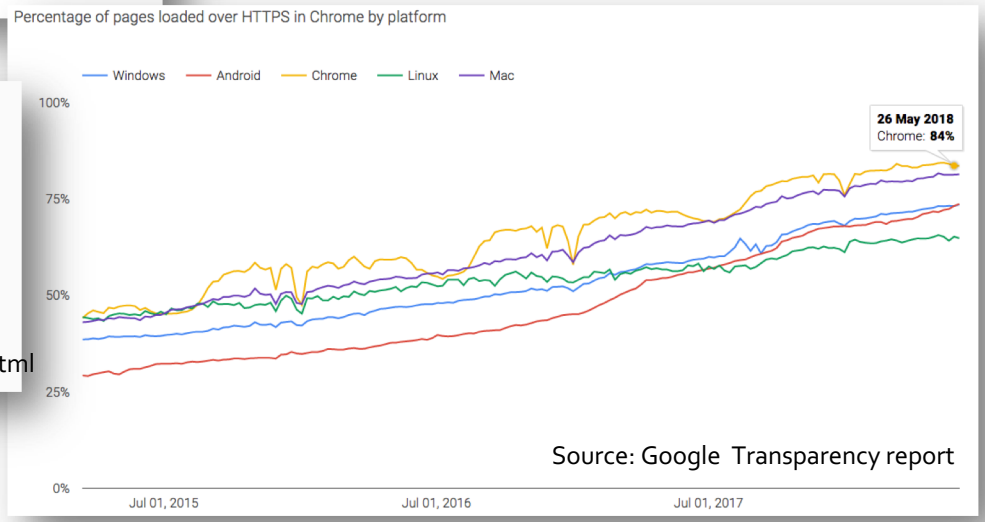
Pervasive encryption is a reality



- Pervasive Monitoring considered a real threat: (BCP 188)
- Now TLS is the rule
- Let's Encrypt helps
  - Certificates for everyone

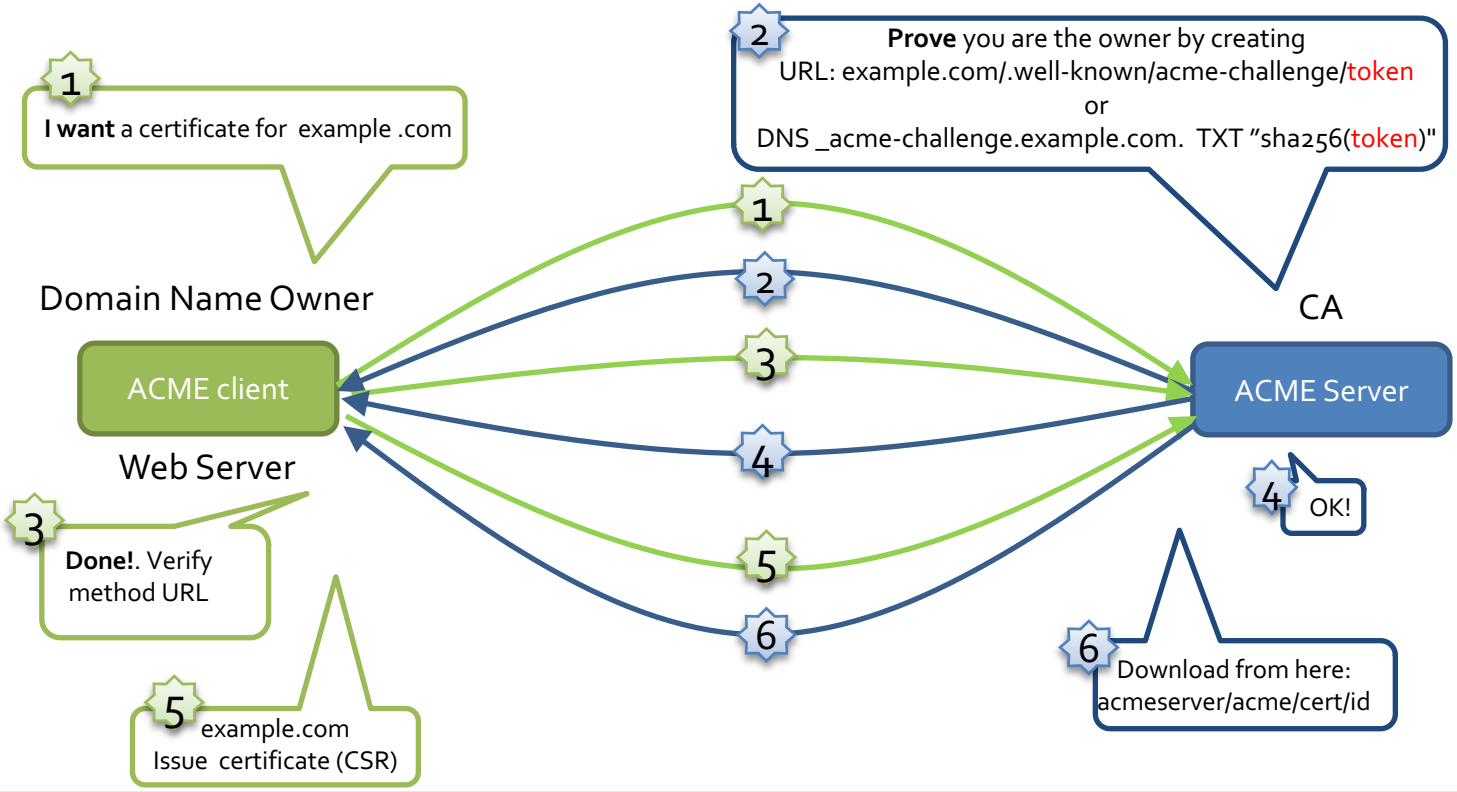


Source: https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html



Certificate delivery automation

- Let's encrypt is a CA
- *Automatic Certificate signing* request and delivery
  - Script/CLI based
- Based on **ACME** protocol (https://www.ietf.org/id/draft-ietf-acme-acme-12.txt)

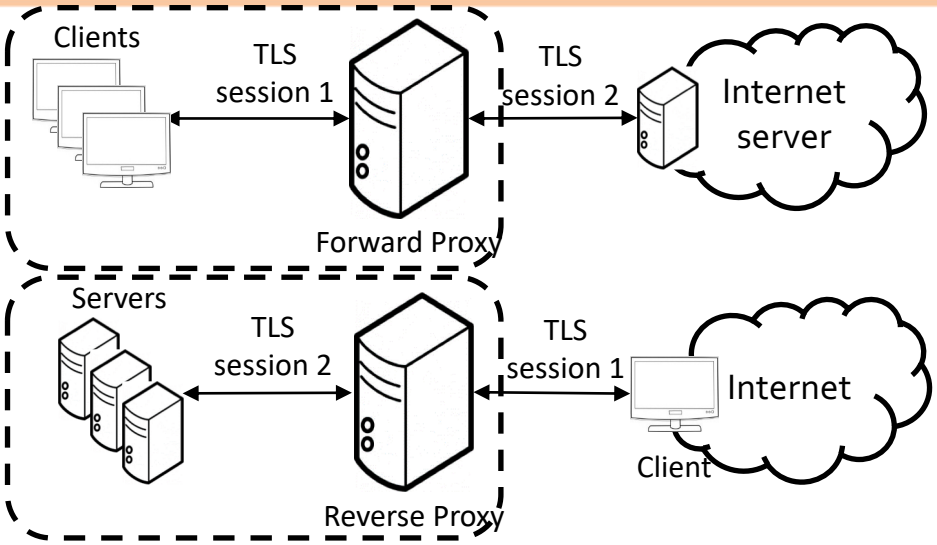


What's the problem with pervasive encryption?

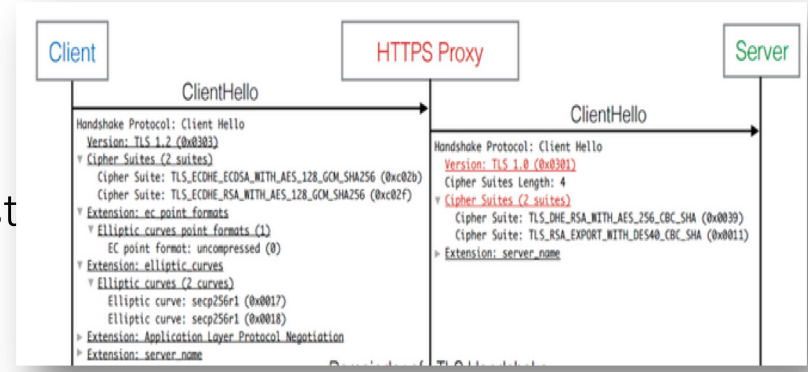
- Operational impact
  - Network planning and optimization
  - QoE based on applications / services
    - VoIP, OTT
  - Performance enhancing proxies
    - E.j: Telefonica Niji service
- Security impact
  - Commercial network security services
    - Content filtering, parental control
  - Regulatory
    - URL blocking (e.g. IWF)
  - Security monitoring
    - Malware, cyberattacks

TLS proxy case

- Direct proxy
  - You protect your users
    - Security monitoring
    - Enforce cypher suites, TLS
  - CA impersonation
- Reverse proxy
  - You protect your service
    - Monitor network activity
    - Regulatory (e.g. financial service)



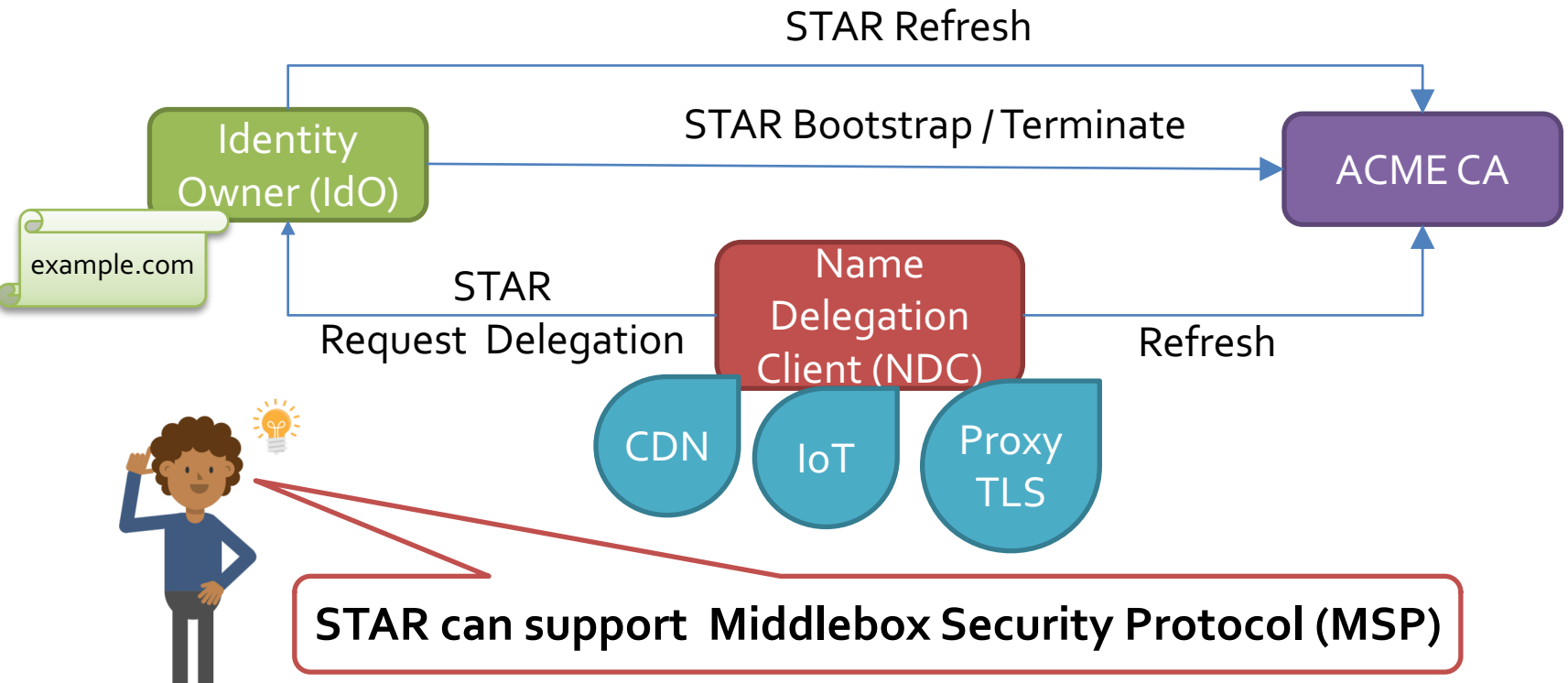
- What are the problems a TLS middlebox has to face?
  - Weak implementation:
    - Cypher suite or TLS version downgrade
    - New protocol support HTTP/2, TLS1.3
  - MITM certificate impersonation protections
    - HPKP (Certificate pinning) and preload list
    - Certificate Transparency Logs



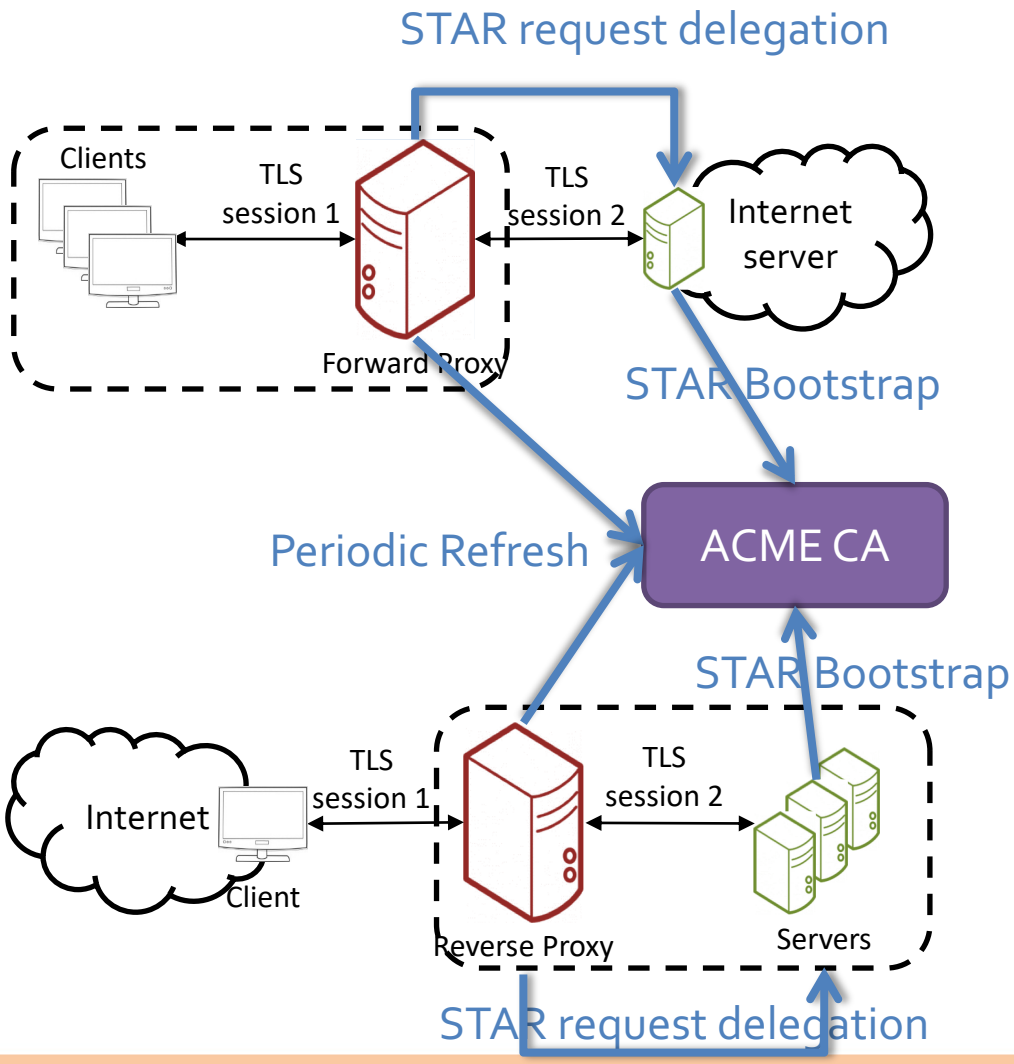
https://zakird.com/papers/https_interception.pdf

Short-Term Automatic Renewal (STAR)

- STAR in ACME (https://tools.ietf.org/html/draft-ietf-acme-star-03)
  - Owner authorizes 3rd parties to deploy very short lifetime certs
- Motivation:
  - **Delegate the authorization** to publish an Internet site
  - **Securely**: owner can **revoke** the authorization at any time



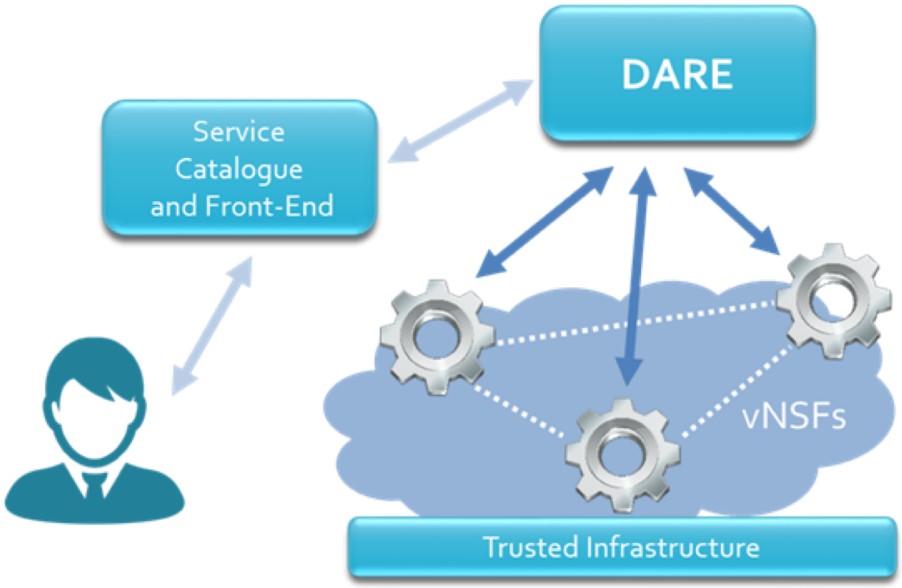
TLS proxy based on STAR



- Architecture
  - Proxy TLS →NDC
  - Web Server → IdO
  - ACME +STAR Server→ CA
- Process
  - Proxy request delegation for several domains (identities)
  - IdO accepts and supervise
  - CA generate periodic VALID certificates
- How to orchestrate this?

Implementation in SHIELD

- PoC in development
  - Using **SHIELD** for Security as a Service
    https://www.shield-h2020.eu/
- Workflow:
  - **TLS proxy** vNSF **detects** an **HTTPS malicious URL** in a CDN provider
  - **Artificial Intelligence** engine (AI) detects and **confirms anomaly**
  - Network manager **enforces a blocking policy**

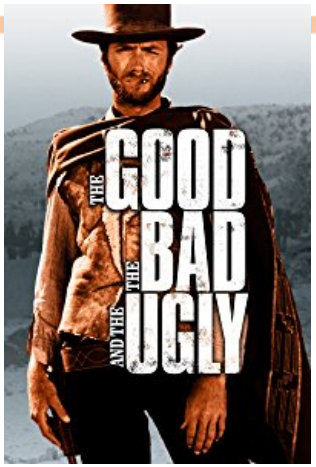


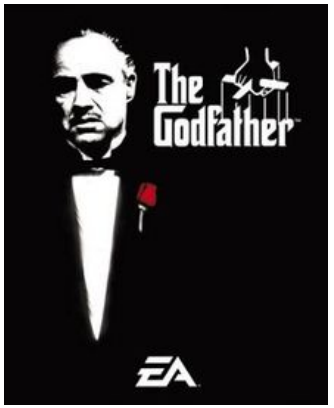
SHIELD is aligned with ETSI standards

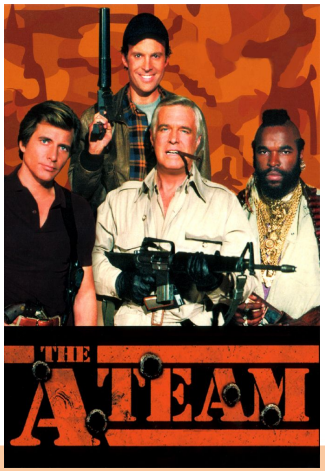
- ETSI NFV architecture..
  - ETSI Open Source MANO (vNSFO)
  - VNF (vNSF)
  - VNF & network attestation (Trust Monitoring)
- ETSI ENI Telco AI concepts -> (DARE)

Summary: Available strategies for a TLS middlebox

- E2E encryption (no middlebox)
  - Endpoint security is the only option (the good ones)
  - Pros:
    - Privacy is guaranteed (at least in transit)
  - Cons:
    - CDN security
    - Weak for restricted devices (IoT)
    - Operational impacts
- TLS proxy (middlebox) / Static TLS key-based Monitoring
  - You delegate to your network provider (the godfather)
  - Pros:
    - Operational impacts are reduced
    - Security /regulatory services are possible
  - Cons:
    - No privacy
    - Bad configuration can undermine security
- TLS proxy (middlebox) with STAR
  - Agreement between network and server (A team)
  - Pros:
    - Operational impacts are reduced
    - Security /regulatory services are possible
    - Transparent to client
    - Controlled by server not by network provider
  - Cons:
    - No privacy (but client aware)
    - Bad configuration can undermine security







Thank you