KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

07 Bezpečnostné aspekty protokolov aplikačnej vrstvy siete Internet

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnostné aspekty protokolov aplikačnej vrstvy siete Internet

- bezpečnostné aspekty protokolov aplikačnej vrstvy siete Internet
- DNSSEC

Aplikačná vrstva siete Internet

- Najvyššia vrstva modelu - priamo slúži aplikáciám
- protokoly: HTTP, DNS, SMTP, FTP, SSH, DHCP...
- mnohé pôvodné protokoly vznikli bez bezpečnostných prvkov
- dáta a prihlasovacie údaje sa často prenášali v otvorenej forme
- bezpečnosť sa rieši šifrovaním, autentizáciou a rozšíreniami

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťové protokoly

- HTTP → HTTPS (HTTP nad TLS)
- FTP → FTPS / SFTP (prenos súborov cez TLS / SSH)
- Telnet → SSH (šifrovaný vzdialený prístup)
- SMTP/IMAP/POP3 → STARTTLS / implicitné TLS
- DNS → DNS over TLS (DoT), DNS over HTTPS (DoH), DNSSEC

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Hrozby na aplikačnej vrstve

- odpočúvanie prihlasovacích údajov a citlivých dát
- phishing a sociálne inžinierstvo
- injekčné útoky (SQL injection, command injection)
- Cross-Site Scripting (XSS) a CSRF vo webových aplikáciách
- zneužitie a podvrhnutie DNS (cache poisoning)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Zabezpečenie e-mailu

- šifrovanie prenosu: STARTTLS, implicitné TLS (SMTPS/IMAPS)
- šifrovanie obsahu: S/MIME, PGP/GPG (end-to-end)
- autentizácia odosielateľa: SPF, DKIM, DMARC
- ochrana proti spamu a podvrhnutiu domény
- filtrovanie príloh a kontrola škodlivého obsahu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Zabezpečenie webu a HTTP

- HTTPS = HTTP nad TLS – dôvernosť a integrita prenosu
- HSTS vynucuje použitie HTTPS na strane prehliadača
- bezpečnostné hlavičky (CSP, X-Frame-Options)
- Cookies s príznakmi Secure a HttpOnly
- pravidelné aktualizácie a kontrola zraniteľností (OWASP)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnosť systému DNS

- DNS prekladá doménové mená na IP adresy
- pôvodný DNS nemá overenie pravosti odpovedí
- DNS cache poisoning – vloženie falošného záznamu do vyrovnávacej pamäte
- presmerovanie používateľa na podvrhnutý server
- riešenie integrity a autenticity odpovedí: DNSSEC

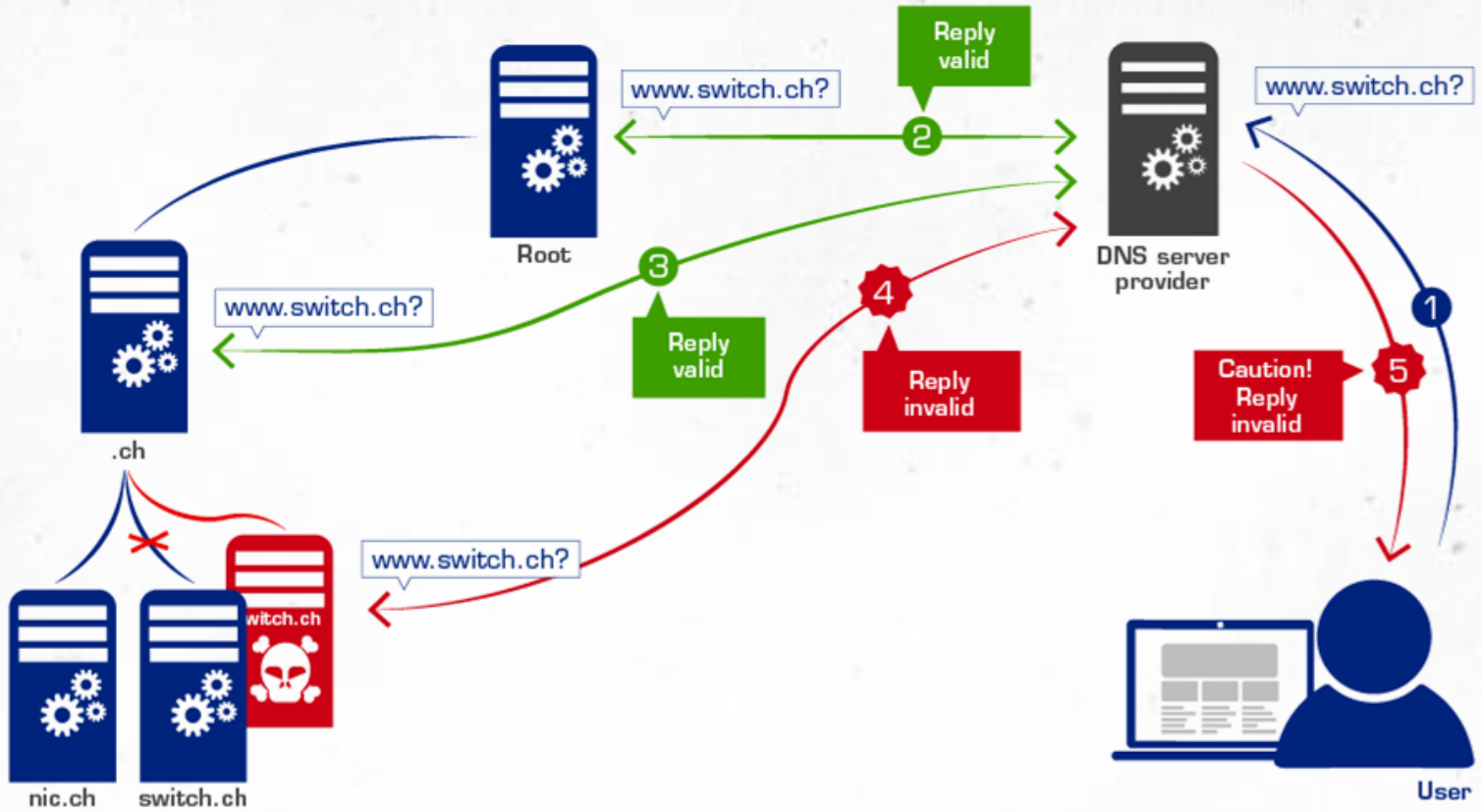
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

DNSSEC (I.)

- **DNSSEC** = DNS Security Extensions (RFC 4033–4035)
  - pridáva digitálne podpisy k DNS záznamom
  - zabezpečuje integritu a autenticitu odpovedí
  - nezabezpečuje dôvernosť - odpovede nie sú šifrované
  - klient (resolver) overuje podpisy verejnými kľúčmi zóny

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

DNSSEC (II.)



Zdroj: https://www.nic.ch/security/dnssec/details/

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

DNSSEC (III.)

- ZSK (Zone Signing Key) - podpisuje jednotlivé záznamy zóny
- KSK (Key Signing Key) - podpisuje kľúče zóny (DNSKEY)
- RRSIG nesie samotný digitálny podpis sady záznamov
- DS záznam v rodičovskej zóne overuje kľúč potomka
- NSEC/NSEC3 autentizovane dokazujú neexistenciu záznamu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

DNSSEC (IV.)

- vyžaduje podporu na strane zóny aj validujúceho resolvera
- zvyšuje veľkosť odpovedí a réžiu správy kľúčov
- rotácia kľúčov (key rollover) musí byť plánovaná
- nechráni „poslednú míľu“ – preto sa kombinuje s DoT/DoH
- postupné, ale rastúce nasadenie vo verejných doménach

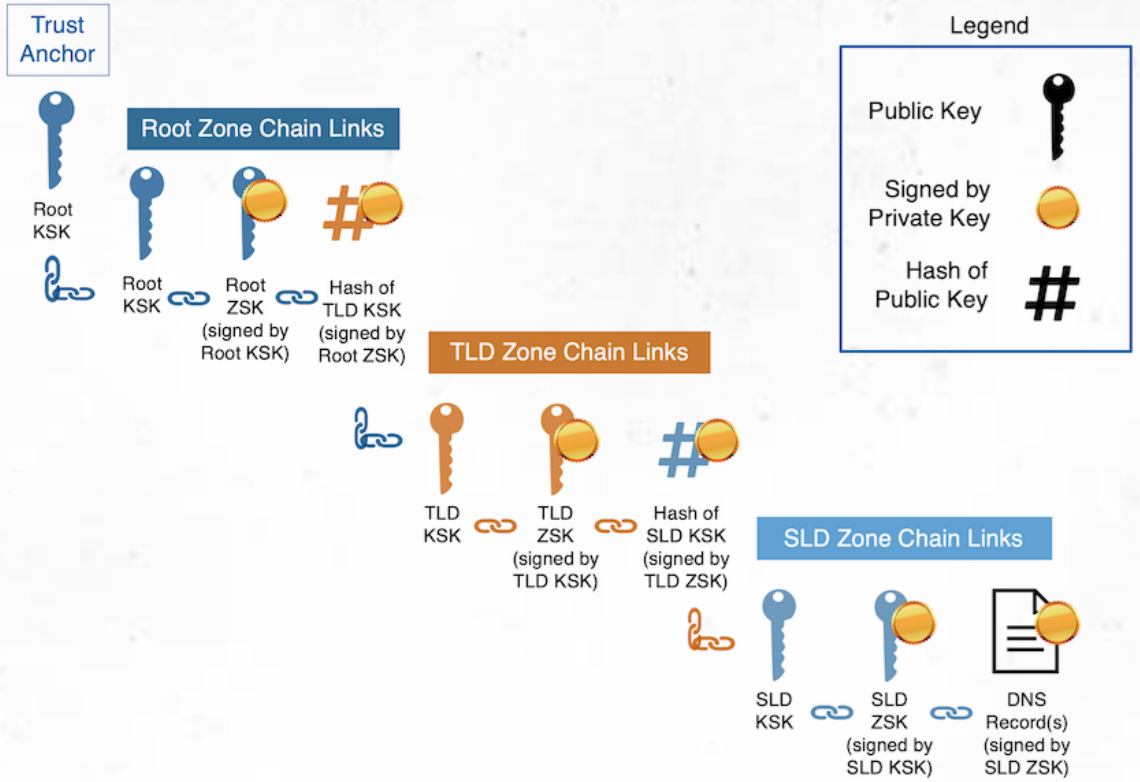
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Reťaz dôvery (chain of trust) (I.)

- dôvera začína v koreňovej zóne (trust anchor)
- každá úroveň podpisuje a delegáciou overuje úroveň nižšie
- resolver postupne overuje podpisy od koreňa po doménu
- narušenie podpisu v ktoromkoľvek bode preruší dôveru
- validujúci resolver odmietne neoverené alebo zmenené odpovede

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Reťaz dôvery (chain of trust) (II.)



Zdroj: https://blog.verisign.com/security/the-domain-name-system-a-cryptographers-perspective/

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť