Reevaluating The Adversary Model for DNS Security

Depending on The Kindness of Strangers

R. Harrison B. Benshoof

Department of Computer Science
Geoorgia State University

2/20/2014

Outline

SSL/TLS

Alice wishes to Start a communication with Bob.
Alice already knows the Certificate Authority's Public key: PK_C

- A$\Rightarrow$ B: "ClientHello" // Initiate exchange
- B$\Rightarrow$ A: PK_B signed by PK_C // Send the certificate
- A$\Rightarrow$ B: $E(PK_B$, NONCE) // Sends a key for the stream cipher

Certificate Authorities

DNSSEC

Key Exchange is Key

Trusted Third Parties solve everything

Trusted Third Parties are centralized points of failure

What is a Proof of Work

How does Bitcoin Work?

Modifcations to Bitcoin for a key exchange

- Limit the length of the blockchain to 1 year
- Add a 'physical' layer check to authenticate new transactions
- Consider alternative incentive methods

Research Directions

- Imropoved SSL
- New DNS distribution Options
- Improved Software Lisensing
- Greater avalibility of PGP style messaging
- Just about anything that needs a key exchange