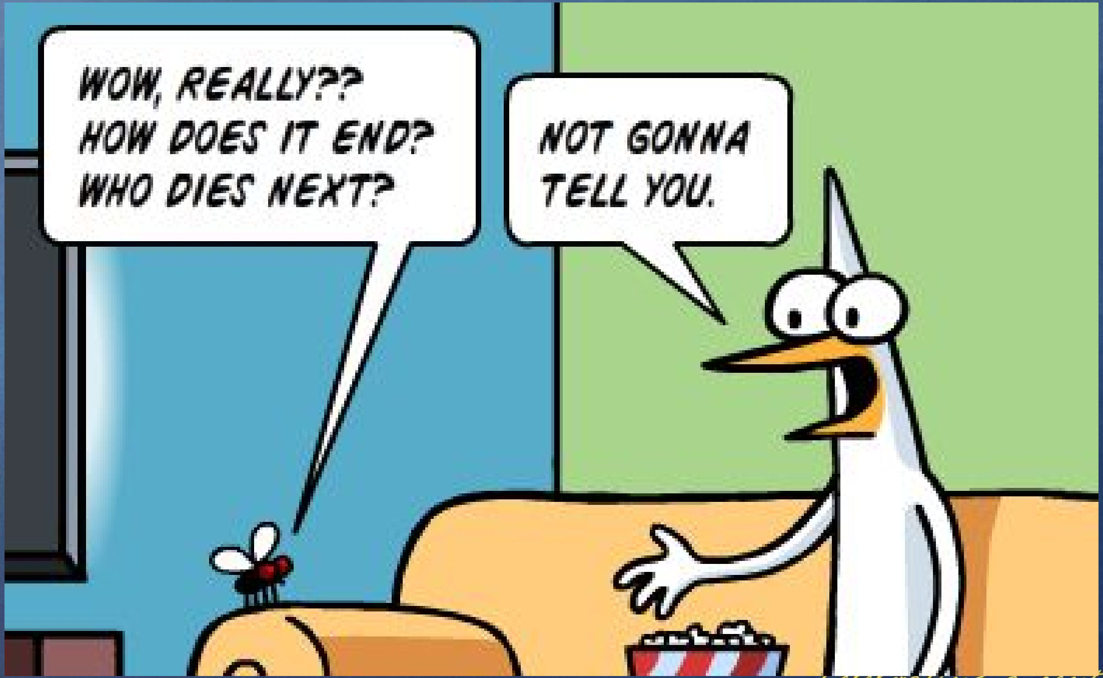
No Stranger Things discussions



What's up in Security

WPA 2 is broken (https://www.krackattacks.com/)

New IOT Malware (https://krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/)

UNIVERSITY OF ALASKA FAIRBANKS

Introduction to SSL and HTTPS

Arsh Chauhan

10/28/17

Celebrating a century 1917–2017

What is HTTPS?

HTTPS = HTTP + TLS (transport layer security)

What is HTTPS?

HTTPS = HTTP + TLS (transport layer security)

Take plain old HTTP and add some encryption on top of it

What is HTTPS?

HTTPS = HTTP + TLS (transport layer security)

Take plain old HTTP and add some encryption on top of it

See how it’s TLS?

What is HTTPS?

HTTPS = HTTP + TLS (transport layer security)

Take plain old HTTP and add some encryption on top of it

See how it’s TLS?

I.e. sits on top (or below) the application

Uses ?

Secrecy: Only client and server can understand the traffic.

Uses ?

Secrecy: Only client and server can understand the traffic. So mom can’t figure out you’re buying 55 gallons of lube

Uses ?

Secrecy: Only client and server can understand the traffic. So mom can't figure out you're buying 55 gallons of lube

Verification: Verify you're actually talking to Amazon and not Arsh pretending to be Amazon

So how does it work ?

Secrecy

Arsh doesn’t feel like explaining RSA math,so...

Secrecy

Arsh doesn’t feel like explaining RSA math,so…

We’ll say the secrecy is magic

Verification

This Arsh can explain (or try to ?)

Verification

This Arsh can explain (or try to ?)

HTTPS verification works due something known as the Certificate Authority (CA) system.

Verification

This Arsh can explain (or try to ?)

HTTPS verification works due something known as the Certificate Authority (CA) system.

The CA system is based on trust

Certificate Authorities

Chain of Trust

The CA system depends on a chain of trust

Chain of Trust

The CA system depends on a chain of trust

When I ask for a HTTPS certificate:

Chain of Trust

The CA system depends on a chain of trust

When I ask for a HTTPS certificate:

1. The CA verifies I own the site

Chain of Trust

The CA system depends on a chain of trust

When I ask for a HTTPS certificate:

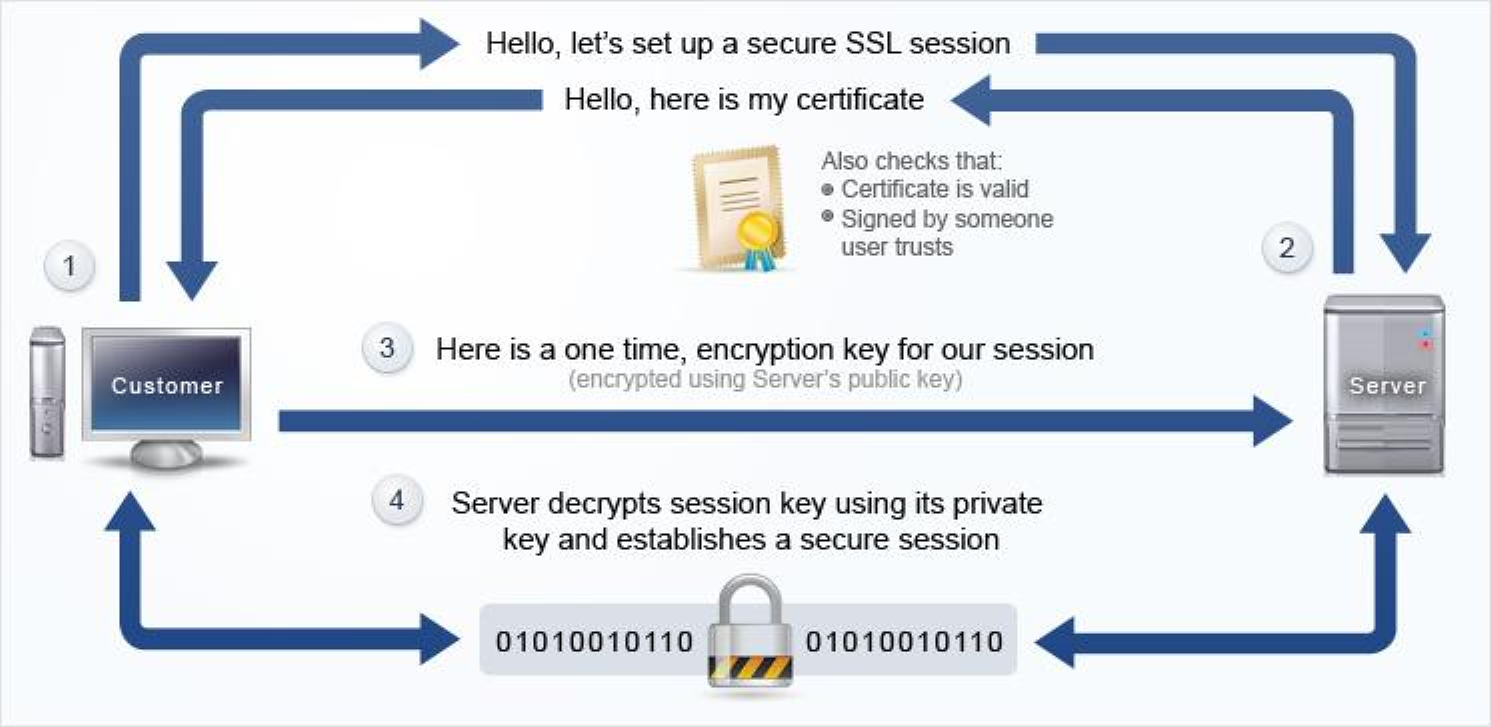
1. The CA verifies I own the site
2. The CA signs my cert with their key

Chain of Trust

The CA system depends on a chain of trust

When I ask for a HTTPS certificate:

1. The CA verifies I own the site
2. The CA signs my cert with their key
3. The CA's key is probably signed by a root CA


Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
● Certificate is valid
● Signed by someone user trusts
1
2
Customer
Server
3
Here is a one time, encryption key for our session
(encrypted using Server's public key)
4
Server decrypts session key using its private key and establishes a secure session
01010010110
01010010110

Site Verification

CA’s use various ways to verify the I’m authorized to request a key for the site. I’ve seen 4 common ones

Site Verification

CA’s use various ways to verify the I’m authorized to request a key for the site. I’ve seen 4 common ones

- Email Verification
- DNS Record
- File
- Enterprise

Establishing Trust

How is the CA trusted?

1. The CA's key is probably signed by a root CA
2. The browser trusts a list of root CA's

Establishing Trust

How is the CA trusted?

1. The CA’s key is probably signed by a root CA
2. The browser trusts a list of root CA’s

But can we really trust the CA

Establishing Trust

How is the CA trusted?

1. The CA’s key is probably signed by a root CA
2. The browser trusts a list of root CA’s

But can we really trust the CA

Short answer…

Establishing Trust

How is the CA trusted?

1. The CA’s key is probably signed by a root CA
2. The browser trusts a list of root CA’s

But can we really trust the CA

Short answer…Most of the time

The Flaws in the System

The CA system can be broken when there is a malicious trusted party

The Flaws in the System

The CA system can be broken when there is a malicious trusted party.This may be intentional or not

The Flaws in the System

The CA system can be broken when there is a malicious trusted party.This may be intentional or not

Chinese CA WoSign accidentally issued certs for Github (Link)

The Flaws in the System

The CA system can be broken when there is a malicious trusted party.This may be intentional or not

Chinese CA WoSign accidentally issued certs for Github (Link)

Superfish: Embedded malware in Lenovo computers

Can We Fix This

Yes…

Can We Fix This

Yes…become better as species not break trust other people put in us ???

Can We Fix This

Yes…become better as species not break trust other people put in us ???

That ain’t gonna happen, so we have technical solutions

Can We Fix This

Yes…become better as species not break trust other people put in us ???

That ain't gonna happen, so we have technical solutions

- DNSSEC
- HTTP Public Key Pinning (HPKP)
- DNS Certification Authority Authorization(CAA) record

Implementing SSL Lab

Celebrating a century 1917–2017

UNIVERSITY OF ALASKA FAIRBANKS