Web Security and the OWASP Top 10: The Big Picture

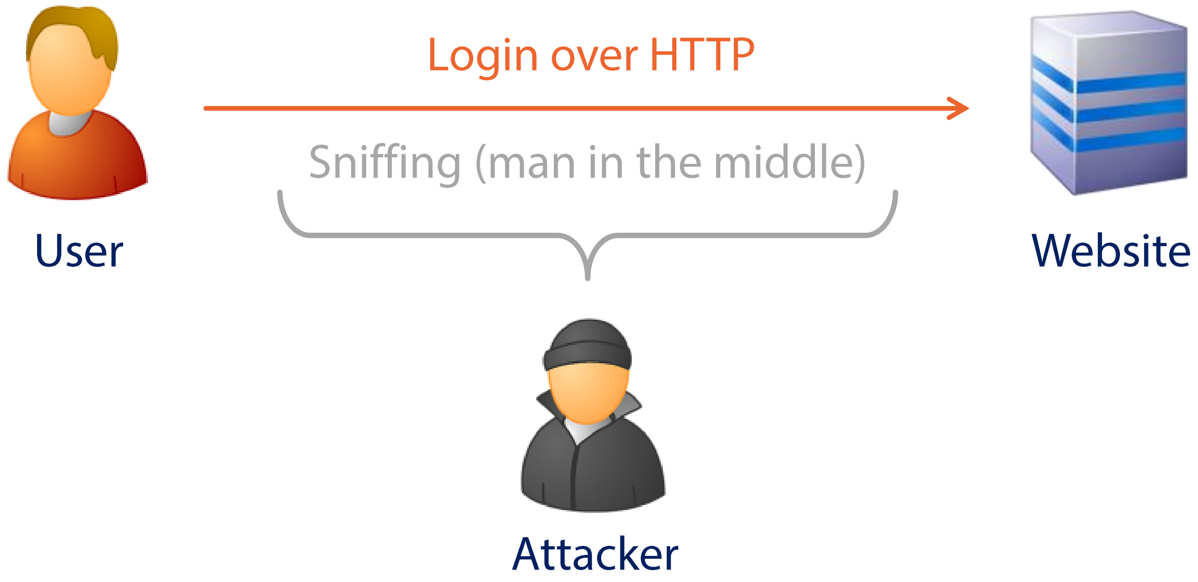
Sensitive Data Exposure

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Sensitive Data Exposure Overview

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Difficult	Prevalence Uncommon	Detectability Average	Impact Severe



User

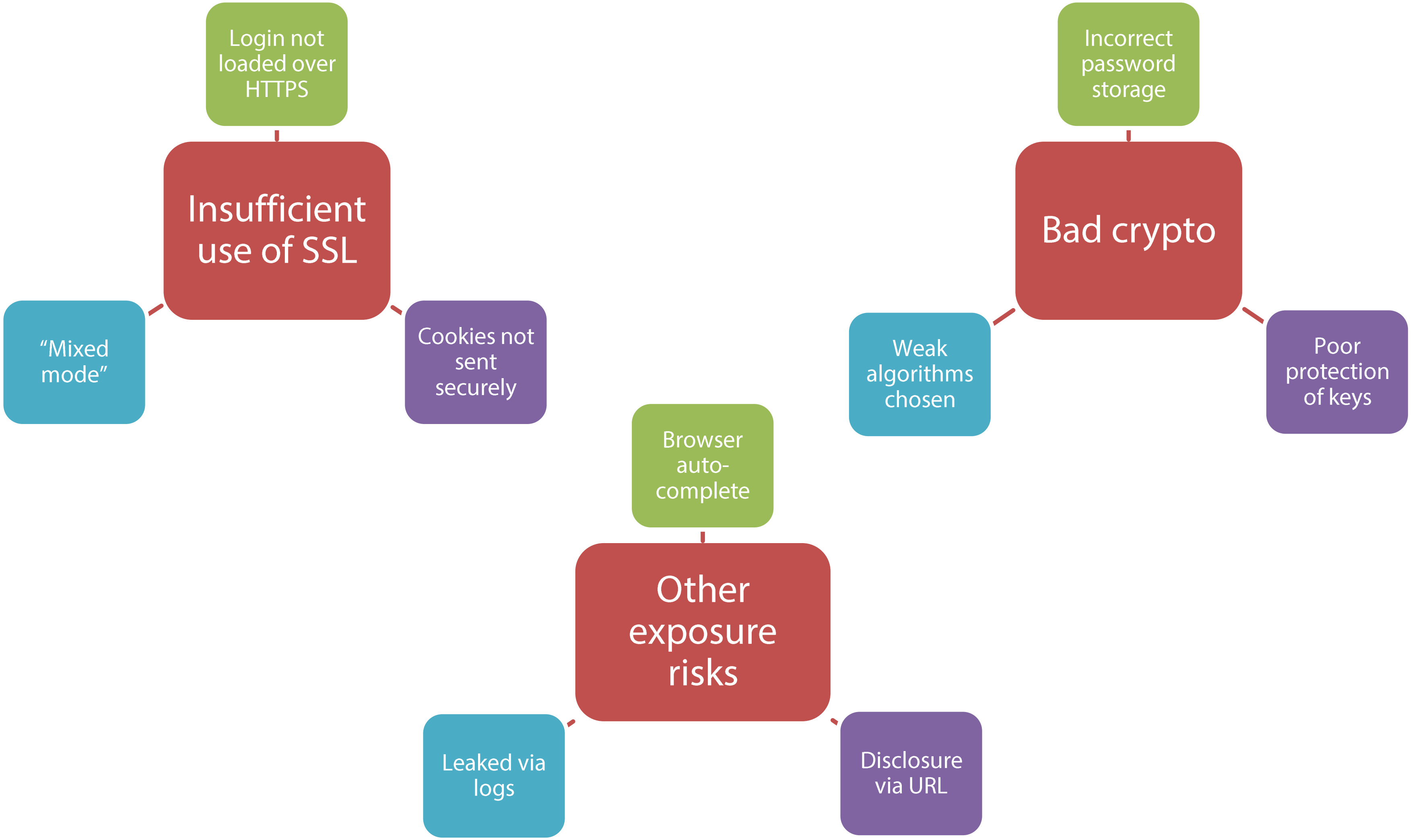
Login over HTTP

Sniffing (man in the middle)

Website

Attacker

Understanding Sensitive Data Exposure



Common Defences Against Sensitive Data Exposure

Minimise
sensitive data collection

- You can’t lose what you don’t have!
- Reduce the window of storage

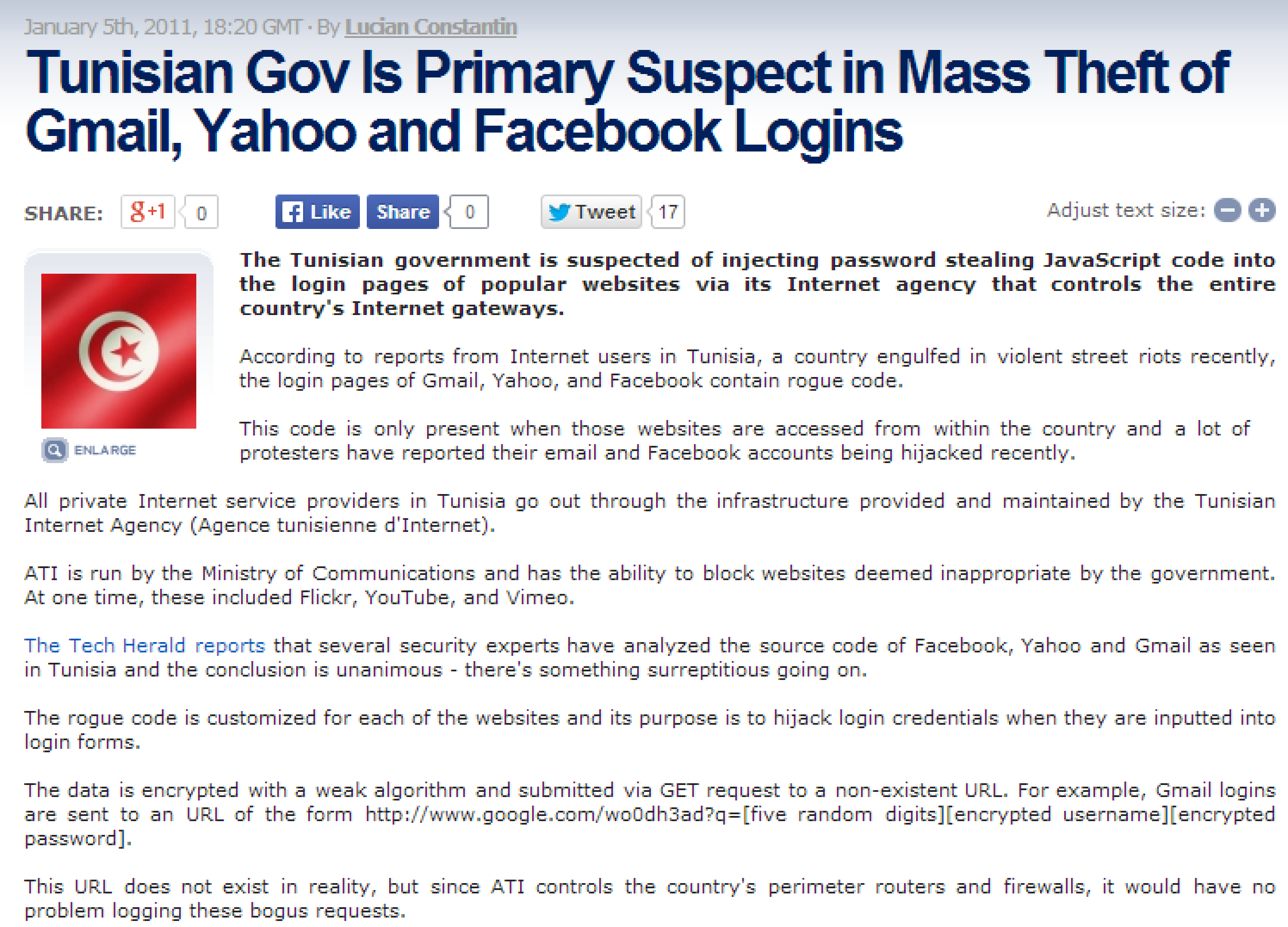
Apply
HTTPS everywhere

- It’s too easy to “insufficiently” implement
- Start with it everywhere – it’s easy!

Use
strong crypto storage

- Hashing algorithms designed for passwords
- Be very careful with key management

Sensitive Data Exposure in the Wild – Tunisia



January 5th, 2011, 18:20 GMT · By Lucian Constantin

Tunisian Gov Is Primary Suspect in Mass Theft of Gmail, Yahoo and Facebook Logins

The Tunisian government is suspected of injecting password stealing JavaScript code into the login pages of popular websites via its Internet agency that controls the entire country's Internet gateways.

According to reports from Internet users in Tunisia, a country engulfed in violent street riots recently, the login pages of Gmail, Yahoo, and Facebook contain rogue code.

This code is only present when those websites are accessed from within the country and a lot of protesters have reported their email and Facebook accounts being hijacked recently.

All private Internet service providers in Tunisia go out through the infrastructure provided and maintained by the Tunisian Internet Agency (Agence tunisienne d'Internet).

ATI is run by the Ministry of Communications and has the ability to block websites deemed inappropriate by the government. At one time, these included Flickr, YouTube, and Vimeo.

The Tech Herald reports that several security experts have analyzed the source code of Facebook, Yahoo and Gmail as seen in Tunisia and the conclusion is unanimous - there's something surreptitious going on.

The rogue code is customized for each of the websites and its purpose is to hijack login credentials when they are inputted into login forms.

The data is encrypted with a weak algorithm and submitted via GET request to a non-existent URL. For example, Gmail logins are sent to an URL of the form http://www.google.com/wo0dh3ad?q=[five random digits][encrypted username][encrypted password].

This URL does not exist in reality, but since ATI controls the country's perimeter routers and firewalls, it would have no problem logging these bogus requests.