# Information Security Abbreviation and Concepts flashcards

Browser Security 101

# Abbreviation List

**Owasp** - Open Web Application Security Project
**XSS** - cross  side scripting
**CSRF** - Cross Site Request Forgery
**SOP** - Same Origin Policy
**CSP** - Content Security Policy
**SSL** - Secure Sockets Layer
**TLS** - Transport Layer Security

# Some Example Attacks on Web Browsers

**POODLE -** Padding Oracle On Downgraded Legacy Encryption
**SLOTH -** Security Losses From Obsolete and Truncated Transcript
**CRIME -** Compression Ratio Info-Leak Mass Exploitation
**BEAST** - Browser Exploit Against SSL/TLS
**BREACH -** Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext

# Information Security Keywords and Definitions

**Threat:** Generic term for objects, People who pose a potential danger to an asset.
**Vulnerability:** Weakness or fault that can lead to an exposure.
**Risk:** Probability that “something bad” happens times expected damage
**Vector:** How the attack was carried out.

# Poodle Attack

The POODLE attack is a man-in-the-middle exploit, which takes advantage of Internet and Security Software clients fall to SSL 3.0

Prevention: Disable SSL 3.0 on the client side and the Server Side.

# FREAK

Factoring RSA Export Keys

The FREAK attack is possible because some servers, browsers and other SSL implementations still support and use the weaker export-grade cryptographic suites. Which lets a MITM force these clients to use export-grade keys even if they didn't ask for export grade encryption.

# FREAK

Contd...

Once the encryption of the session is cracked, the MITM can steal any ‘secured’ information from session.

It is possible

-at server: The Server must support RSA export cipher suites;

-at client: 1) Offers an RSA export suite

2) be using a vulnerable version of OpenSSL

# SLOTH

Security Losses from Obsolete and truncated hashes.
SLOTH can force clients/servers to downgrade to a weaker Hash algorithm.
TLS 1.2 introduced a new signature and Hash algorithm field in the serverkeyexchange message to allow the server to specify which signature and hash algorithms the client must use.

# SLOTH

contd...

Unfortunately, this also allows attackers to force the clients to downgrade to a weaker hash algorithm, like MD5


Thank You