**HOMEWORK 9**

**What is the error that was discovered?**

The “weak RSA moduli” bug is almost (and possibly) exclusively found within certificates that were already insecure (i.e. expired, or not signed by a valid CA).

**How serious is the problem in practice?**

Not very serious. Doesn’t affect single production website.

**What lessons did you learn from this incident?**

That there was never any security to be lost from crackable RSA keys. All of the affected keys were vulnerable to a Man-in-The-Middle Attack.

**What questions arose from your reading of the article?**  
Is this a website problem or a problem with web interface?

What is the *impact*, upon computer security? What is the *actionable intelligence* we can derive from these findings?

What are the other things that could happen due to this?

**DROWN ATTACK**

**What is DROWN Attack?**

- DROWN stands for Decrypting RSA with Obsolete and Weakened eNcryption.

- DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security.

- DROWN allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data.

**How serious is it?**

Very serious as all TLS dependent services are at a risk for DROWN attack, and many popular sites are affected.

**What factors contributed to DROWN?**

The U.S. government deliberately weakened three kinds of cryptographic primitives: RSA encryption, Diffie-Hellman key exchange, and symmetric ciphers. FREAK exploited export-grade RSA, and LogJam exploited export-grade Diffie-Hellman. Now, DROWN exploits export-grade symmetric ciphers, demonstrating that all three kinds of deliberately weakened crypto have come to put the security of the Internet at risk decades later.

**Questions I thought of**

Am I safe?

How do we prevent it?

If I update my web Browser, am i still vulnerable to the attack?Does DROWN allow an attacker to steal the server’s private key?