Cryptographic Vulnerabilities in Real-Life Web Servers

Eman Salem Alashwali
King Abdulaziz University
ealashwali@kau.edu.sa

Aim: We aim to: 1) shed light on the importance of proper implementation for SSL protocol; 2) raise awareness about the recently discovered prevalence of factorable RSA keys on the Internet by [2] and [3].

Our Motivation: How Secure Is the Internet?

- The Internet has become an integral part of everyone's daily life.
- With the growing number of users and the value of the data being transferred over the Internet, the number of threats and attacks has also increased. Therefore, Internet security has become essential.
- Secure Socket Layer/Transport Layer Security (SSL/TLS) is one of the most important network security protocols used to secure the Internet.
- However, SSL is only a communication protocol, and it has several limitations [1].

  1) It relies on different cryptographic algorithms. Therefore, SSL is only as strong as the cryptographic algorithms it employs [1]. For example, SSL can not secure a transaction that uses the broken DES algorithm.

  2) Another limitation arises from the implementation of SSL [1]. For instance, if the key size is not sufficient, or if the system's Random Number Generator (RNG) is faulty, SSL provides no security.

Questions

- To what extent are weak keys still used by real-life web servers?
- Are strong keys adopted in certain countries faster than others?
- Are weak keys more frequent in certain countries than others?
- Can we break real-life RSA keys?
- Does the problems detected of factorable keys on the Internet could also concern major e-commerce websites?
- Whether certain keys factored in the past are still in use today?

Related Work

Factoring RSA keys used by real web servers on the Internet has been a disturbing discovery which has received a lot of press in the recent months.

By / Year	Dataset	Factored Keys	Conclusion
Lenstra et al. / 2012	6,386,984	12,934	keys generated using "single-secret" algorithms based on DH such as ECDSA and ElGamal are more secure than keys generated using "multiple-secret" algorithms such as in RSA [2].
Heninger et al. / 2012	11,170,883	16,717	The main reason for widespread factorable keys is low entropy due to faulty implementation, not a cryptographic issue as Lenstra et al. concluded [3].

Table I. Summary of realted work.

Results:

A. Our Scan Results In a Nutshell

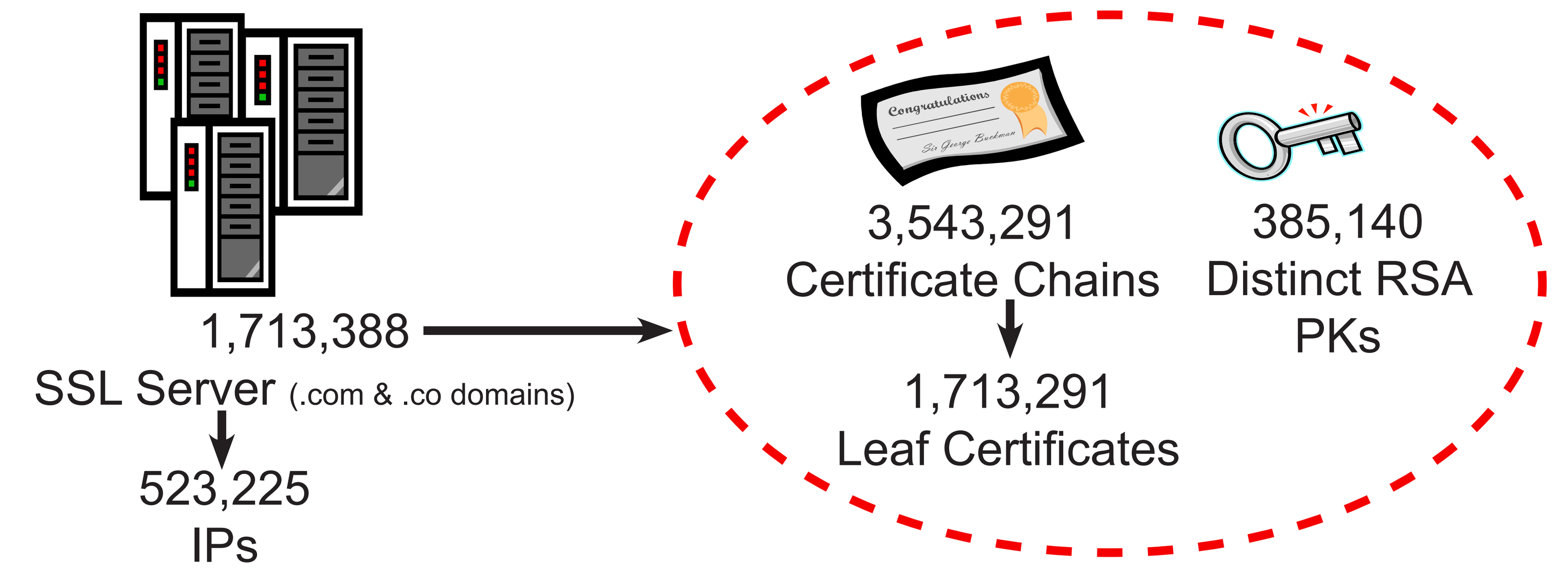

Figure 1. Our Internet scan results in a nutshell.

B. Weak Keys

Key Length	# and % of Weak Keys and the Affected Leaves		
	# keys	% keys	# affected servers (leaves)
<=512-bit	1,082	0.28%	5,003
<=768-bit	1,126	0.29%	5,532
< 1024-bit	1,140	0.30%	5,552
<=1024-bit	89,978	23.36%	406,698

Table II. Cumulative representation for weak keys.

Key Lengths Recommendations:

- NIST: >=2048-bit from 2011.
- FNISA: >= 2048-bit from 2010.
- Lenstra: > 1229-bit from 2006.

In our scan, we found 1024-bit keys still widely adopted, representing 23.36% of the keys and used by over 400,000 servers.

C. Keys Lengths Practices & IP Geolocation

Country	Distinct Keys				
	Total Keys	# Strong (>=2048-bit)	% Strong	# Weak (<=512-bit)	% Weak
US	247,307	196,250	**79.35%**	582	0.24%
UK	34,537	27,486	**79.58%**	89	0.26%
Germany	16,360	11,590	70.84%	36	0.22%
Canada	12,100	8,855	73.18%	37	0.31%
Australia	11,587	9,204	**79.43%**	35	0.30%
Japan	10,164	7,802	76.76%	23	0.23%
France	7,032	4,874	69.31%	50	**0.71%**
Netherlands	4,924	3,002	60.97%	6	0.12%
Spain	3,856	2,763	71.65%	14	0.36%
Italy	3,048	1,839	60.33%	22	**0.72%**

Table III. Weak vs. strong keys in the top 10 countries that showed the highest number of distinct RSA PKs.

The French Network and Information Security Agency (FNISA) has set 2048-bit as a minimal key length since 2010 [4]. However, there is no evidence that the industry is following these recommendations.

D. Can RSA Keys Be Broken?

- RSA security is based on the difficulty of factoring [5].
- There is a known vulnerability that leads to factoring a 1024-bit RSA modulus [3]. See Figure 2.
- It can be exploited if an adversary can find a pair of moduli that share a prime factor [3].

#	The Set		
	Our Set Only	Our Set + EFF Set	EFF Set
Distinct Keys	385,140	4,225,058	3,933,365
Factored Keys	7	6,513	6,508
Execution time (sec.)	286.075	3,381.675	2,890.326

TableIV. Factorable keys.

- We factored 6,513 RSA keys used in real-life web servers.
- In average, around 40% of the keys which known to be factored in the past are still in use today and some affected certificates will not expire until 2038.

RSA Public-key vulnerability can be exploited if two distinct moduli share a prime.

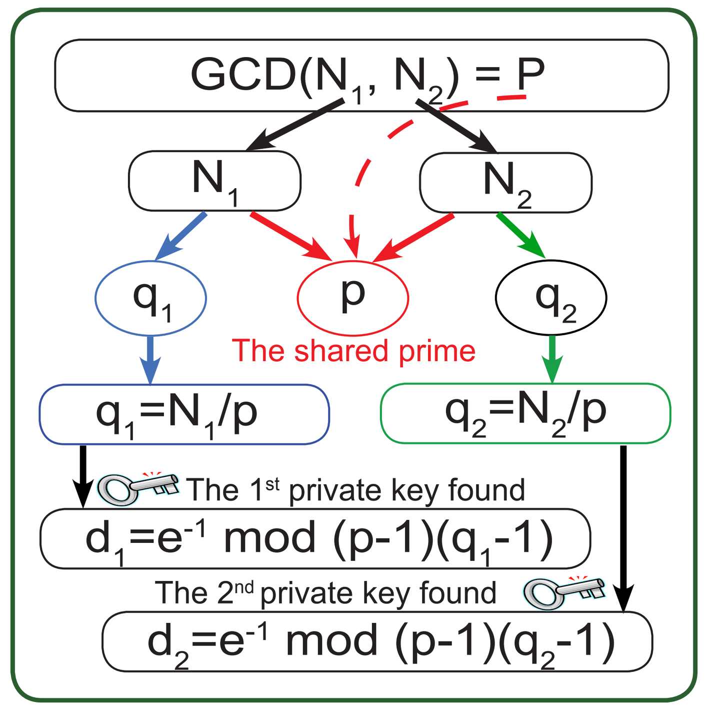

Figure 2. Illustration for the RSA-key vulnerability.

Conclusion

- Servers located in Italy and France showed the highest percentage of insecure keys (<= 512-bit), while servers located in the UK, US and Australia were leading in adopting secure keys (>= 2048-bit) out of all of the countries in the comparison.
- It is possible for an amateur with a single PC using publicly available information to break RSA keys in a reasonable amount of time.
- In the keys that we factored and for which we traced the web servers, there is no immediate threat to e-commerce websites. However, we report factored keys used by corporations but the certificates were deployed for Embedded Web Servers (EWSs) and not for an ordinary web server.
- Our results support the findings of [3] in that the vulenrability mainly concerns embedded network devices.

Acknowledgment: Part of this work has spanned from the author's MSc. thesis submitted to University College London. Special thanks go to Dr. Nicolas Courtois, the thesis supervisor.

References

[1] S. Thomas, SSL and TLS Essentials. New York, NY, USA: John Wiley & Sons, Inc., 2000.
[2] A. Lenstra, J. Hughes, M. Augier, J. Bos, T. Kleinjung and C. Wachter, "Ron was wrong, Whit is right," IACR Cryptology ePrint Archive, Report 2012/064, 2012.
[3] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices," in Proc. of the 21st USENIX conf. on Security symposium (Security'12), Berkeley, CA, USA, 2012, pp. 35-35.
[4] D. Giry. (2013, Feb.). Cryptographic Key Length Recommendations [Online]. Available: http://www.keylength.com.
[5] J. Katz and Y. Lindell, Introduction To Modern Cryptography. Boca Raton, FL: Chapman & Hall/CRC, 2008.