

**دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)**

**دانشکده‌ی مهندسی کامپیوتر و فن‌آوری اطلاعات**

**روش تحقیق و گزارش نویسی**

**تکلیف هفتم**

**سید محمد مهدی موسوی**

**(9231053)**

**استاد :**

**جناب آقای دکتر صفابخش**

**فروردین 95**

**IEEE**

[1] Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman, "Analysis of the HTTPS certificate ecosystem," presented at the Proceedings of the 2013 conference on Internet measurement conference, Barcelona, Spain, 2013.

[2] A. Goldberg, R. Buff, and A. Schmitt, "A comparison of HTTP and HTTPS performance," *Computer Measurement Group, CMG98,* 1998.

[3] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013, pp. 511-525.

[4] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol," *IEEE Security and Privacy,* vol. 7, pp. 78-81, 2009.

[5] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining your Ps and Qs: Detection of widespread weak keys in network devices," in *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*, 2012, pp. 205-220.

[6] D. Naylor, A. Finamore, I. Leontiadis, Y. Grunenberger, M. Mellia, M. Munafò*, et al.*, "The cost of the S in HTTPS," in *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, 2014, pp. 133-140.

[7] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography," *Mathematical Research Letters,* vol. 6, pp. 287-292, 1999.

[8] T. Chomsiri, "HTTPS Hacking Protection," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, 2007, pp. 590-594.

[9] D. Schatzmann, W. Mühlbauer, T. Spyropoulos, and X. Dimitropoulos, "Digging into HTTPS: flow-based classification of webmail traffic," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, 2010, pp. 322-327.

**Science**

1. Z. Durumeric, J. Kasten, M. Bailey, J. A. Halderman, paper presented at the Proceedings of the 2013 conference on Internet measurement conference, Barcelona, Spain, 2013.

2. A. Goldberg, R. Buff, A. Schmitt, A comparison of HTTP and HTTPS performance. *Computer Measurement Group, CMG98*, (1998).

3. J. Clark, P. C. van Oorschot, in *Security and Privacy (SP), 2013 IEEE Symposium on*. (IEEE, 2013), pp. 511-525.

4. F. Callegati, W. Cerroni, M. Ramilli, Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security and Privacy* **7**, 78-81 (2009).

5. N. Heninger, Z. Durumeric, E. Wustrow, J. A. Halderman, in *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*. (2012), pp. 205-220.

6. D. Naylor *et al.*, in *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. (ACM, 2014), pp. 133-140.

7. I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography. *Mathematical Research Letters* **6**, 287-292 (1999).

8. T. Chomsiri, in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*. (IEEE, 2007), vol. 1, pp. 590-594.

9. D. Schatzmann, W. Mühlbauer, T. Spyropoulos, X. Dimitropoulos, in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. (ACM, 2010), pp. 322-327.

**Annotated**

(Goldberg, Buff et al. 1998, Anshel, Anshel et al. 1999, Chomsiri 2007, Callegati, Cerroni et al. 2009, Schatzmann, Mühlbauer et al. 2010, Heninger, Durumeric et al. 2012, Clark and van Oorschot 2013, Durumeric, Kasten et al. 2013, Naylor, Finamore et al. 2014)

Anshel, I., et al. (1999). "An algebraic method for public-key cryptography." Mathematical Research Letters **6**: 287-292.

Callegati, F., et al. (2009). "Man-in-the-Middle Attack to the HTTPS Protocol." IEEE Security and Privacy **7**(1): 78-81.

Chomsiri, T. (2007). HTTPS Hacking Protection. Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, IEEE.

Clark, J. and P. C. van Oorschot (2013). SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. Security and Privacy (SP), 2013 IEEE Symposium on, IEEE.

Durumeric, Z., et al. (2013). Analysis of the HTTPS certificate ecosystem. Proceedings of the 2013 conference on Internet measurement conference. Barcelona, Spain, ACM**:** 291-304.

Goldberg, A., et al. (1998). "A comparison of HTTP and HTTPS performance." Computer Measurement Group, CMG98.

Heninger, N., et al. (2012). Mining your Ps and Qs: Detection of widespread weak keys in network devices. Presented as part of the 21st USENIX Security Symposium (USENIX Security 12).

Naylor, D., et al. (2014). The cost of the S in HTTPS. Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies, ACM.

Schatzmann, D., et al. (2010). Digging into HTTPS: flow-based classification of webmail traffic. Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, ACM.

**Chicago 16th Footnote**

Anshel, Iris, Michael Anshel, and Dorian Goldfeld. "An Algebraic Method for Public-Key Cryptography." *Mathematical Research Letters* 6 (1999): 287-92.

Callegati, Franco, Walter Cerroni, and Marco Ramilli. "Man-in-the-Middle Attack to the Https Protocol." *IEEE Security and Privacy* 7, no. 1 (2009): 78-81.

Chomsiri, Thawatchai. "Https Hacking Protection." Paper presented at the Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, 2007.

Clark, Jeremy, and Paul C van Oorschot. "Sok: Ssl and Https: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements." Paper presented at the Security and Privacy (SP), 2013 IEEE Symposium on, 2013.

Durumeric, Zakir, James Kasten, Michael Bailey, and J. Alex Halderman. "Analysis of the Https Certificate Ecosystem." In *Proceedings of the 2013 conference on Internet measurement conference*, 291-304. Barcelona, Spain: ACM, 2013.

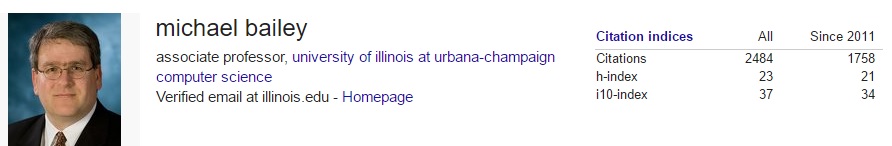
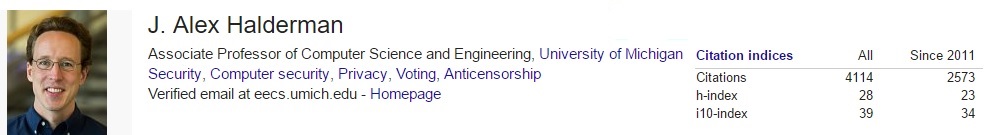
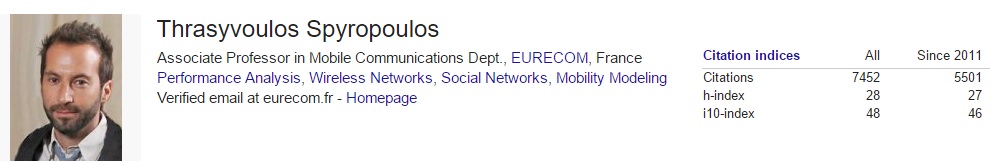
Goldberg, Arthur, Robert Buff, and Andrew Schmitt. "A Comparison of Http and Https Performance." *Computer Measurement Group, CMG98*  (1998).

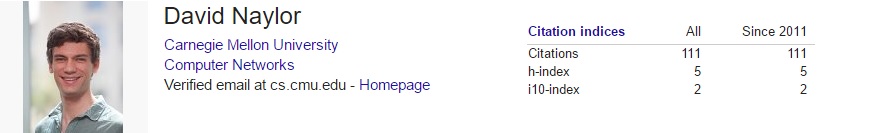
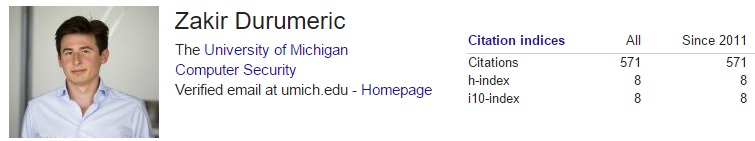
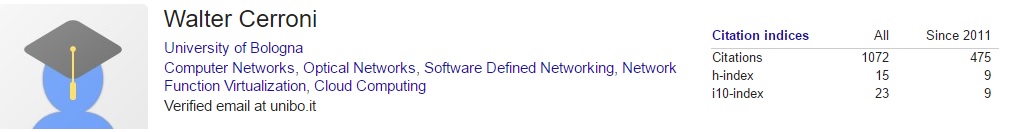
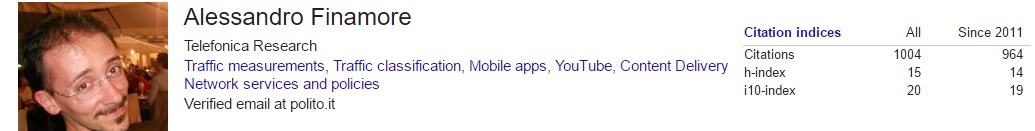
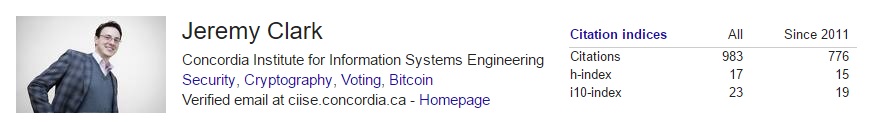
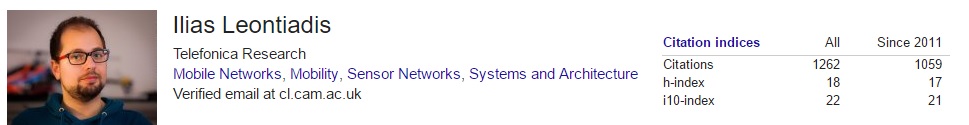
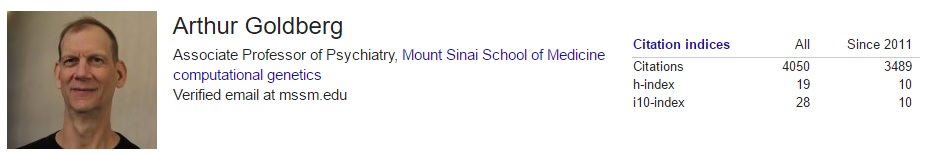
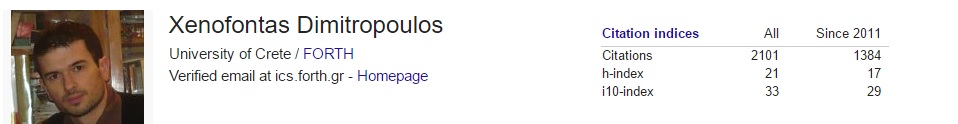
Heninger, Nadia, Zakir Durumeric, Eric Wustrow, and J Alex Halderman. "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices." Paper presented at the Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), 2012.

Naylor, David, Alessandro Finamore, Ilias Leontiadis, Yan Grunenberger, Marco Mellia, Maurizio Munafò, Konstantina Papagiannaki, and Peter Steenkiste. "The Cost of the S in Https." Paper presented at the Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies, 2014.

Schatzmann, Dominik, Wolfgang Mühlbauer, Thrasyvoulos Spyropoulos, and Xenofontas Dimitropoulos. "Digging into Https: Flow-Based Classification of Webmail Traffic." Paper presented at the Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, 2010.

حال نویسندگان مقاله ها را با معیار های # Of Citation و # h-index می سنجیم .





|  |  |
| --- | --- |
| عنوان مقاله | # Of Citation |
| Analysis of the HTTPS Certificate Ecosystem | Cited by 71 |
| A COMPARISON OF HTTP AND HTTPS PERFORMANCE | Cited by 19 |
| SSL and HTTPS:  Revisiting past challenges and evaluating certificate trust model enhancements | Cited by 61 |
| Man\_ In \_ The \_ Middle Attack To The HTTPS Protocol | Cited by 100 |
| The Cost of the "S" in HTTPS | Cited by 93 |
| HTTPS Hacking Protection | Cited by 30 |
| AN ALGEBRAIC METHOD FOR PUBLIC-KEY CRYPTOGRAPHY | Cited by 347 |
| Digging into HTTPS: FlowBased Classification of Webmail Traffic | Cited by 34 |

معیار سنجی توسط # of Impact Factor