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 .

Paul C. van Oorschot

Professor of Computer Science, Carleton University, Canada
authentication, information security, applied cryptography, computer security, cryptology
Verified email at scs.carleton.ca - Homepage

Citation indices	All	Since 2011
Citations	28153	11766
h-index	62	48
i10-index	125	106

Thrasyvoulos Spyropoulos

Associate Professor in Mobile Communications Dept., EURECOM, France
Performance Analysis, Wireless Networks, Social Networks, Mobility Modeling
Verified email at eurecom.fr - Homepage

Citation indices	All	Since 2011
Citations	7452	5501
h-index	28	27
i10-index	48	46

J. Alex Halderman

Associate Professor of Computer Science and Engineering, University of Michigan
Security, Computer security, Privacy, Voting, Anticensorship
Verified email at eecs.umich.edu - Homepage

Citation indices	All	Since 2011
Citations	4114	2573
h-index	28	23
i10-index	39	34

michael bailey

associate professor, university of illinois at urbana-champaign
computer science
Verified email at illinois.edu - Homepage

Citation indices	All	Since 2011
Citations	2484	1758
h-index	23	21
i10-index	37	34

Franco Callegati

Associate Professor
Software Defined Networking, Network Function Virtualization, Optical Networks, Network Security, Embedded Networking
Verified email at unibo.it - Homepage

Citation indices	All	Since 2011
Citations	3357	678
h-index	22	11
i10-index	38	14

Andrew L Schmitt

Brady Corporation
Verified email at bradycorp.com

Citation indices	All	Since 2011
Citations	1364	1009
h-index	17	16
i10-index	19	18

Xenofontas Dimitropoulos

University of Crete / FORTH
Verified email at ics.forth.gr - Homepage

Citation indices	All	Since 2011
Citations	2101	1384
h-index	21	17
i10-index	33	29

Arthur Goldberg

Associate Professor of Psychiatry, Mount Sinai School of Medicine
computational genetics
Verified email at mssm.edu

Citation indices	All	Since 2011
Citations	4050	3489
h-index	19	10
i10-index	28	10

Ilias Leontiadis

Telefonica Research
Mobile Networks, Mobility, Sensor Networks, Systems and Architecture
Verified email at cl.cam.ac.uk

Citation indices	All	Since 2011
Citations	1262	1059
h-index	18	17
i10-index	22	21

Marco Prandini

Assistant Professor, Bologna University, Italy
Network Security, System Security, System Administration
Verified email at unibo.it

Citation indices	All	Since 2011
Citations	133	74
h-index	6	5
i10-index	3	1

Jeremy Clark

Concordia Institute for Information Systems Engineering
Security, Cryptography, Voting, Bitcoin
Verified email at ciise.concordia.ca - Homepage

Citation indices	All	Since 2011
Citations	983	776
h-index	17	15
i10-index	23	19

Alessandro Finamore

Telefonica Research
Traffic measurements, Traffic classification, Mobile apps, YouTube, Content Delivery Network services and policies
Verified email at polito.it

Citation indices	All	Since 2011
Citations	1004	964
h-index	15	14
i10-index	20	19

Walter Cerroni

University of Bologna
Computer Networks, Optical Networks, Software Defined Networking, Network Function Virtualization, Cloud Computing
Verified email at unibo.it

Citation indices	All	Since 2011
Citations	1072	475
h-index	15	9
i10-index	23	9

Zakir Durumeric

The University of Michigan
Computer Security
Verified email at umich.edu - Homepage

Citation indices	All	Since 2011
Citations	571	571
h-index	8	8
i10-index	8	8

David Naylor

Carnegie Mellon University
Computer Networks
Verified email at cs.cmu.edu - Homepage

Citation indices	All	Since 2011
Citations	111	111
h-index	5	5
i10-index	2	2

James Kasten

University of Michigan
Security
Geverifieerd e-mailadres voor umich.edu - Startpagina

Citatie-indexen	Alles	Sinds 2011
Citaties	173	173
h-index	4	4
i10-index	3	3

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