Seminar on Strengthening Security

I Made Wiryana & Avinanta Tarigan

April - July 2004

Abstract

Security is more then just cryptography and patching vulnerability against exploit. In this seminar we try to explore one of important aspect of strengthening security: analysing system security in which we emphasize in verification of cryptographic protocol and analysis of security incident.

Aim

to introduce verification method of cryptographic protocol as one of important effort in stenthening security, as well as analysis on security system using WBA, Attack Graph-Attack Tree, and model checker for verification.

Prerequisit

basic knowledge of network, predicate logic, and security

Participants

Minimum 4, maximal 8 students

Time

12 Weeks, 1 day per week every Friday, 2-3 hours per day

Plan per week

Week	Subject	Activities	Homework
1.	Introduction to Security, Cryptography, and Security Protocol. How to specify security protocol in formal way.	Presentation by tutor, Discussion, Exercise	Papers to read
2.	Introduction to analysing security incidents with WBA, security model, attack model, and understanding security policy	Presentation by tutor, Discussion, Exercise	Papers to read, presentation to make
3.	Taxonomy and threat modeling	Presentation, exercise, discussion	Papers to read, presentation to make
4.	Attack Tree and Attack Graph	Presentation, discussion	Papers to read, presentation to make
5.	Risk assesment graph	Presentation, discussion	Papers to read, presentation to make
6.	Use of model checker for security verification	Presentation, discussion	Papers to read, presentation to make
7.	BAN Logic Basic: Basic notations, inference rules, idealization, proving simple protocol, TEXclass, and tools for BAN logic	Presentation Discussion, Exercise	Papers to read, protocol to proof
8.	Proofing protocol, revealing weaknesses : Otway Rees, Needham Schroeder	Presentation, Exercise, Discussion	protocol to proof
9.	Proofing protocol, revealing weaknesses : Kerberos Protocol, Andrew Secure Handshake, The Yahalom	Presentation, Exercise, Discussion	protocol to proof
10.	Proofing protocol, revealing weaknesses : Needham Schroeder Public Key, CIIT X509 Protocol	Presentation, Exercise, Discussion	protocol to proof
11.	Proofing protocol, revealing weaknesses : SSLv2, SSLv3	Presentation, Exercise, Discussion	Papers to read, presentation to make
12.	Limit and critique for BAN logic. Another methods on verification of security protocol	Presentation, Discussion	Papers to read, presentation to make

Material

1 BAN Logic basic

BAN Logic is one of the method in verificating authentication property of cryptographic protocol. It is relative easy and intuitive to understand and to apply in practise. BAN Logic consists of several inference rules and the idealization method. Using the inference rules, one tries to prove idealized protocol to achieve belief in both side. If this state is not achieved, then the flaw of the protocol being analyzed can be revealed.

References

[1] Martin Abadi (1997). Secrecy by typing in security protocols. Abaid, Takayasu Ito (Eds.) Theoretical Aspect of Computer Software. Third International Symposium, TACS '97 Sendai Japan, September 23-26. Springer Verlag, 611.-638

[2] Martin Abadi, Roger Nedham (1996). Prudent engineering practice for cyptographic protocols. IEEE Transaction on Software Engineering, vol 22 (1), p. 6-15. `http://www.cse.ucsc.edu/~abadi/Papers/gep-ieee.ps`

[3] Michael Burrows, Martin Abadi, Roger Needham (). A logic of authentication.

[4] Logical Systems for Security Protocol Analysis

[5] Sape J Mullender (). BAN Logic - A Logic of Authentication. `http://wwwhome.cs.utwente.nl/~sape/sse/ban.pdf`

[6] George Couloris, Jean Dollimore, Tim Kindberg (1994). Logics of authentication. `http://www.cdk3.net/security/Ed2/BANLogic.pdf`

[7] Annette Bleeker, Lambert Meertens (1997). A semantics for BAN logic. DIMACS Workshop on Design and Formal Verification of Security ProtocolsSeptember 3-5, 1997. `http://dimacs.rutgers.edu/Workshops/Security/program2/bleeker.ps`

2 BAN Logic example

Exercise will sharpen intutive. Analysing several known protocol using BAN Logic is very useful for knowing the common flaw which can be avoided in future protocol design process.

References

[1] Butler W. Lampson (199). Authentication in Distributed System.

[2] Rafael Accorsi, David Basin Luca Vigano (2001). Towards an awareness-based semantics for security protocol analysis. Workshop on Logical Aspects of Crpytographic Protocols 2001.

[3] Timo Kyantaja (1994). A Logic and Authentication by Burrows, Abadi, and Needham. Advances in Cryptology - Eurocrypt 93, Springer-Verlag, 1994, pp.240-247. http://www.tml.hut.fi/Opinnot/Tik-110.501/1995/ban.html

3 Tools for BAN logic analyst

In verification work, it is common to use automated theorem prover, to minimize error and time. Santoshi and Shreyas have brought their work on automated BAN analysis which is worthwhile to be learned.

References

[1] Santoshi D. B., Doshi Shreyas (2001). Automated BAN Analysis of Authentication Protocols. a graduate term paper for ICS 222- Formal Methods in Software Engineering, University of California, Irvine, 2001.http://www.ics.uci.edu/~sdoshi/w01/AutomatedBANAnalysis.pdf

4 Limit and critique for BAN logic

BAN Logic has several limitations. It runs on several condition or asumption to be fulfiled for that we are sure BAN Logic works. Knowing this limitation is important for the analist before making the conlusion.

References

[1] Colin Boyd, Wenbau Mao (). On a limitation of BAN Logic. http://sky.fit.qut.edu.au/~boydc/papers/euro93.ps

[2] Paul C. van Oorschot (1994). An alternate explanation of two BAN-logic "failures". Eurocrypt'93, LNCS vol. 765, pp. 443-447, Springer-Verlag .http://www.scs.carleton.ca/~paulv/papers/Euro93.pdf

5 Dialog model and user side security model

In a distributed system, every principals have their own model about state and state transitions of the system. Designer and user have their own perception. These differences might lead to insecurity. This condition is modeled in dialog model and user side security model.

References

[1] Anne Adams, Martina Angela Sasse (1999). Users are not the enemny. Communication of the ACM, vol 42 (12). December 1999, p. 41 - 45.

[2] Simon Hansman (2002). A Taxonomy of Network and Computer Attack Methodologies . Honours thesis University of Canterburry, http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/2003/hons_0306.pdf

[3] Jeffrey Undercoffer, John Pinkston. Modelling computer attacks : a target centric ontology for intrustion detection. http://www.csee.umbc.edu/cadip/2002Symposium/Ont-for-IDS.pdf

[4] Andy Bisste, Geraldine Sipton (2000). Some human dimensions of computer virus creation and infection. Int. Journal Human-Computer Studies, 52, p. 899 - 913.

[5] Ursula Holmström (1999). User-centered design of security software. http://www.hft.org/HFT99/paper99/Design/5_99.pdf

[6] Ellen Zurko, Mar, Richart T. Simon (). User-centered security. Proceedings of the UCLA conference on New security paradigms workshops September 17 - 20, 1996, Lake Arrowhead, CA USA, Pages 27-33. http://www.acm.org/pubs/citations/proceedings/commsec/304851/p27-zurko/

[7] Daniel Gord, Tom Markotten () User-Centered Security Engineering. Proceedings of the 4th EurOpen/USENIX Conference - NordU2002, Februar 2002. http://www.iig.uni-freiburg.de/telematik/forschung/projekte/kom_technik/atus/publications/Ge2002.pdf

[8] George Cybenko, Annarita Giani, Paul Thompson (2002). Cognitive hacking : a battle for mind. IEEE Computer, August 2002, p. 50 - 56.

[9] Alma Whitten and J.D. Tygar. Usability of security ; a case study, Carnegie Mellon School of Computer Science Technical Report, December 1998. http://reports-archive.adm.cs.cmu.edu/anon/1998/abstracts/98-155.html

[10] Jonathan J. Rusch. The "Social Engineering" of Internet Fraud. http://www.isoc.org/inet99/proceedings/3g/3g_2.htm

6 Attack Tree and Attack Graph

Many approachs in security analysis are based on the idea of modelling attacker's step in attacking the system. Attack Tree is one of such method in which nodes are attacker's goals, starting from leaves which are sub goals towards root which is main goal. Every possible actions are defined and compared to the security analysis of the system in order to find vulnerabilities.

References

[1] Paul Amman, Duminda Wijesekera, Saket Kaushik (2002)Scalable, Graph-based network vulnerability analysis. CCS"2002, November 18-22, 2002. pp. 217 - 224.

[2] Bruce Schneier (1999). Attack trees : modelling security threats. Dr Dobb Journal, December 1999, p. 21 - 29.

[3] Andrew P. Moore, Robert J. Ellison, Richard C. Linger (2001). Attack modelling for information security and survivability. Technical note CMU/SEI-2001-TN001. http://www.cert.org/archive/pdf/01tn001.pdf

[4] Frederick Moberg (2000). Security analysis of an information system using an attack tree-based methodology. Master thesis, Automation Engineering Program, Chalmers University of Technology. http://www.ce.chalmers.se/staff/jonsson/fredrik.moberg-thesis.pdf

[5] R. Dantu (An attack tree of Border Gateway Protocol. www.cs.unt.edu/~rdantu/An%20Attack%20Tree%20for%20the%20Border%20Gateway%20Protocol.htm

[6] Somesh Jha, Oleg Sheyner, Jeannette M. Wing (2002). Minimization and reliability analyses of attack graph. http://www-2.cs.cmu.edu/afs/cs/project/calder/papers/tr02-109/tr.ps

7 Vulnerability modelling and risk assesment

Nowdays, computer security tends to be stucked with the vulnerability and patching. This problem must be eliminated once and for all. The aim in this part is to learn the model of vulnerability and its application in distributed system. The result can be used to asses the risks of the system.

References

[1] Eric Knight (299). Computer vulnerabilities. http://www.fi.upm.es/~flimon/compvuln_draft.pdf

[2] Uttara Nerurkar (). Security Analysis & design. Dr Dobb Journal. November 2000. p. 50 - 56.

[3] Hubbert Common-Lundh, Veronique Cortier. Security properties: two agents are sufficient. In Proc 12th European Symposion on Programming (ESOP "2993), Warsaw Poland Apri 2003, vol 2618 of Lecture Notes i Computer Science, p. 99 -113, Springer. `http://www.lsv.ens-cachan.fr/Publis/`

[4] Taimur Aslam (1995). A taxonomy of security faults in the Unix operating system. Master thesis. Purdue University. `http://ftp.cerias.purdue.edu/pub/papers/taimur-aslam/aslam-taxonomy-msthesis.pdf`

[5] Robert A Martin (2001). Managing vulnerabilities in networked system. IEEE Computer, November 2001. p. 32 - 38.

[6] William A. Arbaugh, William L. Fithen, John McHugh (). Windows of vulnerabilits: a case study analysis. IEEE Computer, December 2002, p. 52 - 59.

[7] Chandana Lala, Brajendra Panda (2001). Evaluating damage from cyber attacks: a model and analysis. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol 31 (4), July 2001, p.300-310.

[8] Herbert H. Thompson, Scott. G. Chase (). Red-Team Application Security Testing. Dr Dobb Journal, November 2003, p 18 - 25.

[9] Herbert H. Thompson, James A. Whittaker (). Testing for software security, Dr Dobb Journal, November 2002, p. 24 - 34.

[10] Peter Herzog. Open Source Security Testing Methodology. `http://www.isecom.org/projects/osstmm.shtml`

[11] Amenaza, Understanding IT Risk Through Threat Tree Modelling.

[12] Ian Alexander (2003). Misuse cases: Use cases with hostile intent. IEEE Software, January/February 2003, p. 58 - 66

8 Use of model checker for security verification

Verification of security verification needs amount of work and time if it is done in ad-hoc way. Model checker provides a way to automate verification. It generates every possible states of the system and check wether unsecure state is reachable.

References

[1] Will Marrero, Edmund Clarke, Somesh Jha. A Model Checker for Authentication Protocols . DIMACS Workshop on Design and Formal Verification of Security Protocols, September 3-5, 1997 `http://dimacs.rutgers.edu/Workshops/Security/program2/marrero.ps`

[2] Dawn Xiadong Song. Athena: a New Efficient Automatic Checker for Security Protocol Analysis. `http://www.ece.cmu.edu/~dawnsong/papers/Athena.pdf`

[3] Hao Chen, David Wagner. MOPS: an infrastructure for examining security properties of software.

[4] Paul Ammann, Wei Ding, Daling Xu (). Using a model checker to test safety properties. Seventh International Conference on Engineering of Complex Computer Systems June 11 - 13, 2001 Skövde, Sweeden

[5] Paul Amman, Ronald W. Ritchey (). Model checking to analyze network vulnerabilities.