CS4103-DS: Security

Handout and Reading List

1 Aims and Objectives

- Gain an understanding of salient issues surrounding **Security** and Distributed Systems.
- Understand the issues associated with **authorisation** within a Distributed System, and ways in which it can be addressed.
- Understand issues associated with **authentication**, and how cryptographic techniques can be used to provide authentication mechanisms.

2 Summary

- Security is **hard**; Security is a socio-technical problem.
- Four main issues for Distributed systems:
  - **Data Security**: In Flight, At Rest.
  - **Identity Management**: Describing and managing entities.
  - **Authentication**: Verify entities identity.
  - **Authorisation**: Verify their permissions.
- Establishing *Secure Channels* often requires brokered authentication.
- Access Control Models help manage permissions at OS and Application Level.
- **Policy Enforcement Points** design pattern to provide distributed access control.

3 Notation

3.1 Key Notation

Symmetric Key K_{AB}

Public Key $\mathsf{Enc}_{pub}(Bob)$

Private Key $\mathsf{Dec}_{priv}(Bob)$

Signing Key $\mathsf{Enc}_{priv}(Alice)$

Verifying Key $\mathsf{Dec}_{pub}(Alice)$

3.2 Operations

Encrypt Encrypt(...)

Decrypt Decrypt(...)

Sign Sign(...)

Verify Verify(...)

3.3 Misc

Ctxt Sym $\{M\}_{\mathsf{K}_{Bob}}$

Hash $\#(msg)$

Concatenate $A \mid\mid B$

Ctxt ASym $\{|M|\}_{\mathsf{Enc}(Bob)}$

Send A to B $A \rightarrow B : msg$

Assignment $H_{msg} \leftarrow \#(msg)$

4 Chapter List

- Tanenbaum *et al.* [1, Chp. 9:§9.1-2, §9.2.1-2&4 §9.3.1, §9.4.1&3. §9.5]
- Coulouris *et al.* [2, Chp. 11:§11.1, §11.6.1&2]

Reading List

Required

[1] A. Tanenbaum *et al.*, *Distributed Systems: Principles and Paradigms*, English, 3rd ed. Pearson Higher Education, 2013, p. 633, ISBN: 1292025522. [Online]. Available: http://library.st-andrews.ac.uk/record=b1546370~S5.

[2] G. Coulouris *et al.*, *Distributed Systems: Concepts and Designs*, English, 5th ed. Pearson Higher Education, 2011, p. 927, ISBN: 0273760599. [Online]. Available: http://library.st-andrews.ac.uk/record=b1875791~S5.

[3] Y. Zhou *et al.*, 'Policy Enforcement Pattern', in *PLoP 2002*, 2002. [Online]. Available: http://hillside.net/plop/plop2002/final/ZZPerry_PLOP.pdf.

Recommended

[8] X. Jin *et al.*, 'A unified attribute-based access control model covering dac, mac and rbac', in *Proceedings of the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy*, ser. DBSec'12, Paris, France: Springer-Verlag, 2012, pp. 41–55, ISBN: 978-3-642-31539-8. DOI: 10.1007/978-3-642-31540-4_4. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-31540-4_4.

[10] R. N. M. Watson *et al.*, 'Capsicum: Practical capabilities for unix', in *Proceedings of the 19th USENIX Security Symposium*, 2010. [Online]. Available: http://www.cl.cam.ac.uk/research/security/capsicum/papers/2010usenix-security-capsicum-website.pdf.

[11] E. Rissanen, Ed., *Extensible access control markup language (xacml) version 3.0*, 2013. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[12] N. Unger *et al.*, 'Sok: Secure messaging', in *Security and Privacy (SP), 2015 IEEE Symposium on*, May 2015, pp. 232–249. DOI: 10.1109/SP.2015.22.

Further

[4] C. de Laat *et al.*, *Generic AAA Architecture*, RFC 2903 (Experimental), Internet Engineering Task Force, Aug. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2903.txt.

[5] J. Vollbrecht *et al.*, *AAA Authorization Framework*, RFC 2904 (Informational), Internet Engineering Task Force, Aug. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2904.txt.

[6] ——, *AAA Authorization Application Examples*, RFC 2905 (Informational), Internet Engineering Task Force, Aug. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2905.txt.

[7] S. Farrell *et al.*, *AAA Authorization Requirements*, RFC 2906 (Informational), Internet Engineering Task Force, Aug. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2906.txt.