Toward self-govern and self-protected data: A proposal

Kasra Madadipouya
kasra_mp@live.com

I. Problem statement

We live in an era of an explosion of data. The rate of generating data has been increased significantly in the last few years especially by popularization of Web 2.0 (Manno & Shahrabi, 2010; Madadipouya, 2013). In addition to that, our surrounding environments are becoming more dynamics and rapidly emerging as computing systems morph from monolithic and closed entities into globally disaggregated collaborating entities which require sensitive data sharing (Salim et al., 2010). As an instance content owners lose full control of their data once it is given away to consumers and hence data can be unlimitedly copied, access, modified and redistributed without data owner awareness (Chen et al., 2015). Moreover, authorized users or applications can maliciously or inadvertently compromise the confidentiality of the protected data by distributing (or leaking) the sensitive data to unauthorized users (Chen et al., 2012). Even during data transmission, sensitive and personal data can be compromised by third-parties or malicious users. Traditional solutions for these problems have proven not to be appropriate because they rely heavily on costly and centralized external systems or infrastructure (Konetski, 2014; Salim et al., 2010; Burnap & Hilton, 2009).

Hence, there is a need of having an automated mechanism for controlling of data in such dynamic and uncertain environments, where changes are frequent and there are unpredictable threats as well as opportunities (Zhao & Johnson, 2008; Lim et al., 2008). In other words, an appropriate data access control mechanism must be put in place in order to control how, where, when, by which data are granted to be accessed dynamically.

II. Proposed approach

One way to overcome with the above limitations is to make data self-protected and context-aware active that can act autonomously and protect itself against any unauthorized or unusual activity. Self-protected data acts autonomously on behalf of the content owner for continuous collecting, filtering, and processing of information as well as decision making.

To have active and self-protected data, access-control, different policies, processing of information and decision making algorithms can be embedded within data in the form of a security modular kernel which dynamically protects data throughout its lifetime, including when it is at-rest (i.e.,

in storage), in-transit, and during execution. Any action performed by the user, the kernel requests each security module to validate the action. Some modules will indeed confirm or deny the various actions (e.g. access control module). For instance, when a request is made to access the data for any purpose, the policy module translates the high-level usage policy into low-level hardware tags that define a memory region where the decrypted data will be placed. However, any attempt to transfer that decoded data into permanent storage on the recipient machine, or to send it out via a network, or do anything with it other than what is permitted in the usage policy will be blocked by access-control module.

Authentication keys are also provided to users which indicates their level though, policies associated with the data that specify which party can access the data for performing which actions. Environment attributes (such as location, IP address, time and date) also are utilized to define security level of access control. For instance, if an authorized user attempts to access to a document within an organization network, he may get unfettered access, however, if the same user tries to access to the same document in his phone from a cafeteria, he might not be able to access to sensitive portions of the document and perhaps visual filters put in place (blur, masking, wrong information, etc.). Furthermore, any unauthorized attempt to access, manipulation of individual kernel module for compromising data will trigger self-destruct kernel call which will destroy confidential content.

Utilizing the modular kernel can be highly beneficial since any entity in the model can be updated, replaced and modified independently from each other. This eliminates the need to rely on an online, trusted server to handle access control decisions and maintain record confidentiality since data itself provides its own security. Only a server will be used for monitoring, auditing and broadcasting updates (i.e., access-control, policy, encryption, etc.).

References

Burnap, P. and Hilton, J., 2009, February. Self protecting data for de-perimeterised information sharing. In *Digital Society, 2009. ICDS'09. Third International Conference on* (pp. 65-70). IEEE.

Chen, S., Thilakanathan, D., Xu, D., Nepal, S. and Calvo, R., 2015, May. Self Protecting Data Sharing using Generic Policies. In *Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on* (pp. 1197-1200). IEEE.

Chen, Yu-Yuan, Pramod A. Jamkhedkar, and Ruby B. Lee. "A software-hardware architecture for self-protecting data." In *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 14-27. ACM, 2012.

Konetski, D., 2014. *Today's disappearing security perimeter demands self-protecting data - David Konetski*. [online] Available at: https://powermore.dell.com/technology/todays-disappearing-security-perimeter-demands-self-protecting-data/ [Accessed 13 Mar. 2016].

Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C., 2015. *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*. Cryptology ePrint Archive, Report 2015/675,

2015. http://eprint. iacr. Org.

Lim, Y.T., Cheng, P.C., Clark, J.A. and Rohatgi, P., 2008, June. Policy evolution with genetic programming: A comparison of three approaches. In *Evolutionary Computation, 2008. CEC 2008. (IEEE World Congress on Computational Intelligence). IEEE Congress on* (pp. 1792-1800). IEEE.

Madadipouya, K., 2013. Survey on how Web 2.0 can facilitate knowledge management. IJCER, 2(6), pp.693-695.

Manno, A. and Shahrabi, K., 2010. Web 2.0: How It Is changing how society communicates. In *Annual National Conference, Louisville, KY, June*.

Salim, F., Reid, J. and Dawson, E., 2010. Authorization models for secure information sharing: A survey and research agenda. *The ISC International Journal of Information Security*, *2*(2).

Shebaro, B., Oluwatimi, O. and Bertino, E., 2015. Context-based access control systems for mobile devices. *Dependable and Secure Computing, IEEE Transactions on*, *12*(2), pp.150-163.

Zhao, X. and Johnson, E., 2008, June. Information Governance: Flexibility and Control through Escalation and Incentives. In *WEIS*.