Data Security and Privacy in 2025?

Matthias Schunter schunter@acm.org,
Intel Collaborative Research Institute for Secure Computing, Germany[1]

1 Data Security and Privacy in 2025?

Security research aims at reducing the risk of information technology. Based on the projection of current trends, this vision paper aims at identifying potential security research needs for the next 10 years.

Computing and Sensors Everywhere: The trend to connect computing devices including smartphones, tablets, and entertainment devices is expected to accelerate to include industrial equipment, vehicles, and wearables. Research cited by IBM predicts that "more than 22 billion web-connected devices by 2020 […] will generate more than 2.5 quintillion bytes of new data every day." If the technical progress continues at the pace of the last 15 years, a 2025 mobile device would have the performance of a 70 GHz processor, 256 TB of storage, and the size of 3×7 mm at a price tag of $16 [Sche11]. A likely consequence is that sensing will be ubiquitous. Personal devices permanently record ambient sounds, video, position, acceleration, and proximity to other objects and will interact with your vehicle, your appliances, and peers on a continuous basis and will be able provide real-time augmented reality to end-users [Bran13].

The Power of Analytics: This huge amount of data contains valuable information and enables real-time intelligent interaction with individuals. Applications for personal use include driver assistance, decision support, or augmented reality where people can obtain real-time and localized information through devices such as Google Glass and personal assistants. Similarly, enterprises have only explored a small subset of potential usages of this information and its value. Security technology has not even started to leverage recent advances in analytics to assess and mitigate risks.

Cyberphysical Systems: Besides sensing and analyzing, an important trend is the increased direct and automated control of the physical reality through actuators. Actuators include power grids controlling power consumers, intelligent transportation systems, management of cities, and control of home appliances. For instance, Wikipedia cites a prediction that 30 % of households will delegate selected tasks to intelligent robots in 2022.

What about Security and Privacy? The possibilities and the potential value acts as a strong incentive to maximize use of these technologies. On the downside, individuals are likely to accept the privacy loss for the convenience gained. The continued growth of complexity will ensure that all systems remain vulnerable. This in turn, may encourage industrial espionage for increasing the competitiveness of nations and enterprises.

2 Emerging Research Challenges

Huge amounts of data strive to be used (and mis-used). The overarching research challenge resulting from the outlined trend is: "How can society benefit from these capabilities without suffering the negative consequences." This holds even more since security and privacy risks may lead to rejection and pushback while the abundance of vulnerabilities may constitute a risk that may be unacceptable to enterprises and society.

2.1 Sensing, Computing, and Actuators Everywhere

The key research challenge is how to integrate privacy and confidentiality controls into a scenario where sensors are pervasive. The unlimited capability to sense and collect data allows computing devices to fully monitor and permanently record a given environment. They may learn the location and identity of persons and objects and record their behaviour without restrictions. One consequence of these abilities are unprecedented privacy and confidentiality challenges. For instance sensors that can record all activities in a

[1] To appear at 9th VLDB Workshop on Secure Data Management - SDM 2013, Springer, LNCS, 2013

building could void confidentiality for affected enterprises, or cameras in all mobile devices provide sufficient information to record the movements and behaviours of each individual.

Important questions are how can individuals control the sensed data derived from them, how can enterprises control the data generated from its behaviour, and how to generate insight in a way to protect privacy. While initial research (such as usage control) exists for controlling well-defined data streams, tackling the problem of privacy-aware sensing has not been resolved yet. Similarly, sensing systems that ensure that the insight does not trigger privacy concerns only exist for special circumstances such as video[2].

A second area of research is the scalability of security to billions of devices. Groundwork is the key- and security management of these devices without any human intervention under potentially adversarial conditions[3]. Related research includes multi-factor authentication of physical devices [DaZC12], intrinsic hardware identities such as Physically Unclonable Functions (PUFs), and end-user-managed security for mobile devices.

While protecting in-bound information is important, a second challenge is to ensure safety when controlling actuators that affect physical systems, in particular in safety-critical applications such as industrial control systems or automobiles. Again, adversaries may take over large portions of the infrastructure and a fail-safe mode of operation is often not available.[4]

2.2 End-to-end Data Confidentiality and Privacy

While securing sensors is difficult, a related challenge is how to protect data along its processing chain including the sensing end-nodes, edge devices providing network connections, aggregators, the cloud backend, and the network interconnections. Today's security mechanisms allow end-to-end protection of unmodified data streams (e.g., using authentication codes, encryption, or hardware security and usage control policies). How to allow data aggregation and analysis along this chain while keeping data confidential, proving the correctness of the results, and maintaining verifiable privacy are open problems. Research in this area includes multi-party computations [GoMW87], homomorphic encryption [Gent09], or trusted computing. In particular for cloud computing, these challenges gain relevance due to the increasing insider threats. In order to protect against individual cloud insiders, separation of duty can help [BKNS12]. However, if cloud providers as a whole may be dishonest, today's research results allow only cloud storage and requires the distribution of data across multiple clouds [BCQA11]. How to secure computation in the cloud against insiders is largely unsolved.

2.3 Failure-resistant Design

We believe that vulnerabilities will continue to grow and the corresponding risks will continue to increase. In particular for targeted attacks, we believe that a general defense is impossible and therefore these attacks will continue to be successful and their number will continue to grow.

A resulting research challenge is the failure-resistant design of security systems. Today, security mechanisms are designed with the assumption that they protect from given risks and that they usually do not fail. For targeted attacks, this assumption needs to be revisited. Surviving failures and successful attacks must receive more attention when designing individual security systems. The new challenge to address is "how to ensure that the damage of envisioned *successful* attacks is minimized?" Potential mechanisms to enhance the survivability of IT systems are the early erasure of data, multiple lines of defense, and hardware-based trust mechanisms as fallback that allow to re-establish the security of a system after a successful attack. Such fallback mechanisms are particularly important if systems are designed for a long life-time (e.g., monitoring systems for public infrastructures). One area of research on long-term security are Post-Quantum Cryptographic schemes that provide security even if the mathematical assumptions underpinning today's cryptographic systems are broken [BMV06].

---

[2] [SPHB05] describes surveillance cameras where persons are replaced by anonymized shapes at the source.

[3] Assume that each device requires 1 s of human intervention, then 1 B of devices require 32 person-years.

[4] For instance, in case of a fault (e.g., caused by an attack) in an automotive control system, the breaks may still slow down and stop the car while there is no fail-safe mode for the steering.

3 Conclusion

While the IT industry will continue to change at a rapid pace, the good news is that there already exists a vast amount of security and privacy research that can be used to address these new challenges. To some extent, translating research into usable real systems is one of the bigger challenges we face.

Besides addressing the research challenges that we have outlined, an interesting consequence of the emerging sensor/analytics/actuator trend that we have outlined is that we expect that security research will undergo a paradigm shift from black/white or trusted/untrusted towards a more analytics-based approach where all entities are somewhere on a continuum between trusted and untrusted. Failure and successful attacks are tolerated in this new approach. As a consequence, security-enhanced analytics will gain importance. This approach to analytics (also to be used for security purposes) will integrate trust assessment mechanisms along with data analysis to assess data based on its trustworthiness while automatically disregarding suspected outliers, untrusted data points, and data resulting from attacks.

4 Acknowledgements

This position paper solely reflects a subjective opinion of the author. Nevertheless, it was formed based on valuable input by my team at the Intel Collaborative Research Center for Secure Computing and at Intel Labs. In particular Christian Wachsmann of TU Darmstadt provided feedback on drafts of this position paper.

5 References

BCQA11 Bessani, A.; Correia, M.; Quaresma, B.; André, F. and Sousa, P. DepSky: Dependable and Secure Storage in a Cloud-of-Clouds. In 6th ACM SIGOPS/EuroSys European Systems Conference (EuroSys'11), ACM, 2011.

BKNS12 Sören Bleikertz, Anil Kurmus, Zoltán A. Nagy, and Matthias Schunter. 2012. Secure cloud maintenance: protecting workloads against insider attacks. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (ASIACCS '12). ACM, New York, NY, USA, 83-84. DOI=10.1145/2414456.2414505

BMV06 Johannes Buchmann, Alexander May, and Ulrich Vollmer. 2006. Perspectives for cryptographic long-term security. *Commun. ACM* 49, 9 (September 2006), 50-55

Bran13 Brandon, John: Top 5 Tech Predictions for 2023 (retrieved May 31, 2013) http://www.inc.com/john-brandon/top-5-tech-predictions-for-2025.html

DaZC12 Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On physical-layer identification of wireless devices. *ACM Comput. Surv.* 45, 1, Article 6 (December 2012), 29 pages. DOI=10.1145/2379776.2379782 http://doi.acm.org/10.1145/2379776.2379782

Gent09 Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In *the 41st ACM Symposium on Theory of Computing (STOC)*, 2009.

GoMW87 O. Goldreich, S. Micali, and A. Wigderson. How to play ANY mental game. In Proceedings of the nineteenth annual ACM conference on Theory of computing, pages 218-229. ACM Press, 1987.

Krin08 Axel Krings: Design for survivability: a tradeoff space. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (CSIIRW '08), ACM, New York, NY, USA, 2008, DOI=10.1145/1413140.1413154

RoNL11 Roman, R.; Najera, P.; Lopez, J., "Securing the Internet of Things," IEEE *Computer*, vol.44, no.9, pp.51,58, Sept. 2011. doi: 10.1109/MC.2011.291

Sche11 Rick Schetting: In your ear with intelligent super computers - by 2025, http://futuretimes.net retrieved May 31, 2013.

SPHB05 Senior, A.; Pankanti, S.; Hampapur, A.; Brown, L.; Ying-Li Tian; Ekin, A.; Connell, J.; Chiao-Fe Shu; Max Lu, "Enabling video privacy through computer vision," *Security & Privacy, IEEE* , vol.3, no.3, pp.50,57, May-June 2005, doi: 10.1109/MSP.2005.65