Quo Vadis “Data-Centric” Systems Security?

Neeraj Suri
Security Institute, Lancaster University neeraj.suri@lancaster.ac.uk

Modern society is inextricably driven and dependent on Information Technology (IT), be it at the computing, the communication or at the application level. This applies to safety-critical, service-critical and cost-critical services covering the entire spectrum of technical and societal needs. Naturally, the ever-increasing dependency on technology is driven by our trusting it to deliver the requisite services under all operational conditions irrespective of encountered perturbations, i.e., resilience to operational perturbations and secure to deliberate perturbations (attacks).

The security space is full of niche problems and niche solutions. Obviously, there is justifiable specificity to the application domains and technology though the goal of security needs also be to obtain security solutions that apply across the board. While we have innumerable accomplishments to take pride in, we are still failing to develop broad application/scale/technology & duration-invariant security solutions. *The imperative advocacy is for a data-level systems mindset to address the ever-evolving growth of security problems.*

It’s not just a technical issue, it’s a socio-technical “Systems” issue

A core limitation of our security approaches is not our innovativeness but the mindset of just finding a “solution to a problem”. As an analogy, we tend to patch leaks versus thinking of the holistic plumbing system. A Microsoft Windows, Amazon or iPhone vulnerability garners immediate attention and a corresponding point solution. Very often, we are liable to forget that security is NOT a discrete property. Security is an end-to-end “systems” property where the weakest part of the service chain attracts both the attacks and the solutions. For example, a security or privacy breach in a nuclear plant or a government database may happen discretely via a vulnerability in the Operating System (OS), the application or access control. However, it is a chain of technical-elements (deficient passwords, communication protocols, browsers…) and the user-elements (human or automation) that determine the compromisability of the system. Indeed, the user-level social and behavioral mores that result in a breach are often the ignored vulnerabilities. A single poor password can compromise the entire technical sophistication of the security solutions. *We explicitly need to consider security as an end-to-end socio-technical issue over a system-chain versus our traditional focus on mostly technical system-links.*

It’s all about data …in motion

To progress beyond technology, application and domain-specific (Cloud, Autonomous Systems, CIP…) point solutions, it befits to conceptually envision any computing infrastructure (e.g., Cloud, IoT, the upcoming Autonomous Systems) as a progression of data flows. Fundamentally, any IT system is a data-chain linking the elements of (a) **Data Acquisition** (the space of technical and user-level sensor inputs), (b) **Data Transportation** (the space of communication networks), and (c) **Data Usage** (the immense sprawl of services, applications, AI ML, NLP, Analytics…) enclosed in a regulatory envelope of Access Control, Repudiation, Compliance etc. *Addressing security at this level of data flows and information leakage helps develop fundamental security solutions that can consequently be tuned to specific applications and technologies.*

It will be about data …at rest

Data in the digital world is immutable. Unfortunately, we often tend to focus more on data in motion and less on the long-term storage of data. As multiple social media and governmental service breaches have amply highlighted, correlating data to profile for either “use or abuse” scenarios is often just a matter of developments in data analytics and technologies. A seemingly invulnerable RSA crypto-protected database becomes an open door as quantum computing technologies become viable. *We fundamentally lack technology-invariant solutions and the imperative need to think of such issues is now.*