TRUSTED IDENTITIES

A TOOL IN YOUR EUROPEAN GENERAL DATA PROTECTION REGULATION COMPLIANCE TOOLBOX

Tim Moses, Director of Security Technologies

Entrust Datacard™

THE GDPR—SETTING BOUNDARIES ON HANDLING & PROTECTION OF PERSONAL DATA

Large parts of the Internet are now funded by the trade in personal data. This has resulted in an unspoken bargain being struck between users and providers, in which users get free service in exchange for access to their personal data. While users seldom examine the terms of that bargain, they nevertheless have expectations for its limits. Too often, online service providers overstep those limits, either by taking insufficient care over the security of the data, or by deliberately exploiting the data in ways that the user did not anticipate.

The European Union recently introduced the General Data Protection Regulation (GDPR), which sets boundaries on the handling of personal data and harmonizes the protection of personal data across the Union, while ensuring its free flow between Member States. GDPR will replace the existing data protection directive in May 2018.

The European Union recently introduced the General Data Protection Regulation (GDPR), which sets boundaries on the handling of personal data and harmonizes the protection of personal data across the Union, while ensuring its free flow between Member States. GDPR will replace the existing data protection directive in May 2018. GDPR, being a regulation as opposed to a directive, applies throughout the Union without Member States having to implement compatible national legislation. GDPR sets a common minimum level of protection for personal data stored and processed by organizations located within the Union, and organizations outside of the Union that are offering goods or services to users in the Union.

GDPR lays down rules for collecting, processing and storing personal data, including data about the behaviour of individuals, whether supplied by the individuals themselves or obtained in some other way. Personal data is broadly defined and includes pseudonymous identifiers, as well as behaviour profiles and machine fingerprints. All such processing requires a legal basis. Common and long-standing privacy best practices deprecate the collection of unnecessary data, provide transparency to data subjects, ensure security at all stages of data lifecycle, and give data subjects the opportunity to examine and confirm data accuracy. GDPR incorporates foregoing concepts and also includes new data subject rights, such as "the right to be forgotten."

The potential penalties defined for violators of GDPR have grabbed attention at senior levels in the corporate world. This is understandable, considering how privacy requirements can have a far-reaching impact on the design and operation of a large-scale information system. Achieving a best-in-class privacy-respecting information system demands a comprehensive approach to technical and organizational design across multiple functions in the organization.

USER AUTHENTICATION & THE GDPR

The GDPR defines maximum levels for the administrative fines that may be imposed for infringement. For example, in extreme cases, infringement of the GDPR's provisions may attract a fine of up to the greater of 20 million Euros or 4% of total worldwide annual turnover.

Fine up to
20
million Euros
OR
4%
Total Worldwide
Annual Turnover

Under the GDPR, organizations are required to secure personal data using technical and organization measures that take into account the "state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for rights and freedoms of natural persons."[1] Information used to identify, authenticate and authorize users when they access resources and initiate transactions is especially critical, as it forms the basis for the security of all the most sensitive personal and corporate information assets in an organization. This requirement pervades every sizable organization, covering access to workstations, wireless access points, mobile devices, VPNs, Web applications, cloud infrastructure, customer and partner portals, and even administration interfaces for server-to-server and machine-to-machine communications.

Passwords have been the favourite authenticator since the beginning of the computer age. Now, despite their shortcomings, they are deeply entrenched in our computing infrastructure. Nevertheless, the industry has finally woken up to the fact that passwords are not secure enough for protecting the most sensitive resources found in the information environment. In a modern information environment, users demand access to dozens of information resources, at any time, from any location, and using whatever device is to hand. This has made the job of managing passwords nearly impossible for the user to achieve securely and reliably.

[1] **Risk, High Risk, risk Assessments and Data Protection Impact Assessments under the GDPR**, Centre for Information Policy Leadership, Hunton & Williams LLP, December 21, 2016

Organizations have much to consider:

- A breach may impact brand-loyalty and the future performance of the business.
- A breach may have financial impact. The maximum fine defined by the Regulation is quite severe; including forfeiture of profit and 4% of total annual worldwide turnover. Further penalties may include a ban on future processing.
- The burden placed on users by an authentication mechanism is a big consideration for operators. In other words, the authentication mechanism could cause friction and a less than desirable user experience.
- As time marches on, change will need to be considered in the IT strategy. The industry will develop best practices, codes of conduct, and certification programs that broadly reflect the judgment of experts concerning common types of interaction, and provide guidance to system architects on the suitability of particular authentication mechanisms.
- Authentication technology is a fast-changing field, as biometric and mobile technologies continue to provide a more attractive user experience at an ever more attractive price point.

Needless to say, for the reasons stated above, care is warranted in the design of systems and processes to minimize the probability of a breach now and into the future.

AUTHENTICATION SOLUTION CHARACTERISTICS

A suitable authentication solution should exhibit certain characteristics and features. An identity management system should support a variety of authentication methods, both on their own and in combination with other mechanisms. In this way, the system architect has flexibility in choosing the best mechanism for any particular situation; the one that provides the optimum balance between false-acceptance-rate, per-user cost, and acceptability of the authentication experience to the user. Preferably, users should be offered a choice, as, depending on cultural and generational factors, different users may have different mechanism preferences. Provided the choices achieve equivalent authentication strength, users should be offered a selection. Given the chance to choose their own username/password, users tend to select the same password for more than one service provider. In this way, a breach at a site with poor information security practices can result in the unauthorized disclosure of personal data at another site where the information security practices are sound. This argues strongly for the use of multi-factor authentication, in order to eliminate this flawed practice.

The suitability of any particular mechanism or combination of mechanisms may evolve over time as new attacks are discovered. And what is generally considered best practice today will likely evolve as (for instance) smartphone, wearable and biometric capabilities advance.

Authentication mechanisms are characterized by two parameters: false-acceptance-rate and false-rejection-rate. The design goal is to keep both of these parameter values below specified thresholds. But, generally, as the details of mechanisms are adjusted, one parameter decreases and the other increases. So, a mechanism with a highly secure (low) false-acceptance-rate can have an unacceptably high false-rejection-rate. And this can start to encroach on the user's goodwill. Operators cannot afford to strain user goodwill, as there will always be a competitor ready to compromise security in order to make the user's experience more pleasurable. (This is obvious in a consumer setting, but the same effect occurs in all other settings.) For this reason, false-rejection-rates must also be held to an acceptable level. And, strong, but convenient, recovery options must be offered to address situations where a primary authenticator fails.

Authentication mechanisms are characterized by two parameters: false-acceptance-rate and false-rejection-rate. The design goal is to keep both of these parameter values below specified thresholds.

HOW AUTHENTICATION SYSTEMS HELP ACHIEVE COMPLIANCE

Step-up authentication

Authentication systems can be used to validate the identity of data subjects exercising data subject rights under the GDPR. For example, when an organization receives a request to either delete all personal data of a particular data subject, or the data subject withdraws their consent to further processing, the organization will want to ensure that the request was issued by the correct data subject. So, this is a case in which a very low false-acceptance-rate is paramount, and step-up authentication is called for. Step-up authentication is a technique used within application logic before a particularly sensitive or irreversible operation is performed. Commonly, it confirms the data subject's approval for a specific action by presenting the details of the action and asking them to re-authenticate using a different (commonly more secure) mechanism.

Evidence preservation

From time to time, disputes may arise between a data subject and an organization handling their personal data. At such time, the controller may want to rely on the data subject having electronically agreed to a particular set of terms and conditions. And, it may become necessary to locate, assemble and deliver all the elements of proof required to demonstrate this, possibly many years after the fact. A variety of techniques are accepted as electronic signatures in the European Union. And digital signatures based on asymmetric cryptography can provide a reliable, and low-cost, solution. An advanced electronic signature with a standard secure document format, packages much of the necessary evidence in a single data item, thus simplifying the process of dispute resolution.

Transparency

Another requirement of the GDPR is to make the data subject aware of the legal entity to which they are entrusting their personal data. This helps to prevent inadvertent disclosure, and ensures that entities know where to seek redress in the event of a privacy violation. Browsers display site identifying information taken from the site's SSL certificate in their address bars. While Domain Validated certificates provide for encrypted communication, they don't support trusted display of the site operator's name. An Extended Validation SSL certificate, on the other hand, does contain the verified legal identity of the site operator, which will be displayed in the browser's address bar. For this reason, EV certificates are an accepted and cost-effective way of presenting the registered name of the organization with which the subject is entering into the consent contract in a trusted part of a browser's user interface.

Flexible authentication policy

While the front-door is the most obvious approach for an attack on a business system holding personal data, any such system also has administrative interfaces where much more powerful functions are exposed. These interfaces require authentication safeguards (Including intrusion detection/prevention and audit) that are the equal of, or superior to, the protections of the user interfaces. Additionally, processes, such as written scripts and workflow with multiple approval steps, are required to minimize the possibility of misconfiguration that could (in turn) lead to unauthorized disclosure. So, for these reasons, comprehensive authentication solutions have to be capable of supporting a range of security policies, depending on the sensitivity of the resource being protected, tipping the balance in favour of security and away from user acceptance in the case of administrative interfaces.

The challenge of erasure

Finally, business continuity considerations dictate that authentication databases be backed-up, archived, and replicated for load-distribution purposes. All the associated communications and stored copies of personal data must be secured, as attackers are naturally going to focus on the weakest point of vulnerability, and this may be it. Object-level encryption may be a cost-effective way of protecting such data, both when at rest and in motion.

Also, as part of its security and compliance program, an organization should maintain the ability to permanently delete a record from all copies of its authentication database, no matter where they might be. This feature may be used; for example, on the subject's authenticated request, where the organization does not have a lawful basis to further retain, or when the data is no longer required for the purpose for which it was collected. However, the organization may wish to securely preserve consent artifacts that it may require for future dispute resolution purposes. And object-level encryption may be a cost-effective solution to this requirement, as well.

THE BALANCING ACT: STRONG SECURITY & THE CUSTOMER EXPERIENCE

The GDPR provides a new data point in the search for the proper balance between user experience and privacy. Those who embrace it will distinguish themselves as a trustworthy and respectful custodian of their users' data.

Personal data plays an increasingly important part in providing the kind of appealing experience that brings users back time and time again. But, there's a balance to be struck; if a data controller (or processors acting on its behalf) were to misuse or take insufficient care with personal data, then users will start looking elsewhere. Strong security is the best tool available for navigating the dichotomy between an appealing user experience and the risk posed by data breach; it allows the collection and management of personal data in line with the user's expectations and without jeopardizing the trust that is so important between them and the provider. The GDPR provides a new data point in the search for the proper balance between user experience and privacy. Those who embrace it will distinguish themselves as a trustworthy and respectful custodian of their users' data.

The GDPR will come into effect in May 2018. Its impact is likely to be far-reaching for almost every enterprise that uses an information system to manage its relationships with customers, partners, and employees. European CIOs and CISOs are already acquainting themselves with the Regulation's provisions, and planning updates to their systems, organizational structures, and procedures in order to achieve compliance. And while the penalties for failure could be severe, the Regulation also represents a fine opportunity to reinforce these relationships, by demonstrating commitment to sound stewardship of personal data. And what better way to do this than to use the best available technology to protect the security of that data?

ABOUT ENTRUST DATACARD

Entrust Datacard is a leader in the business of securing access and information across enterprise, cloud and IoT networks and applications. Serving the world's most demanding organizations for over two decades, its trusted identity portfolio includes a comprehensive suite of advanced authentication, identity analytics and data security solutions that leverages the mobile and cloud computing models to address the demands of today's digital businesses. Whether an organization wants to avail itself of a traditional on-premise deployment, virtual appliance, or cloud service, Entrust Datacard has the ability to build an all-inclusive trust framework. Its goal is to cater to a wide range of use cases, whether internal, B2B or B2C. This means that the Entrust Datacard authentication solutions are able to evolve alongside an enterprise's digital transformation. In addition, Entrust Datacard ensures that the trust architecture can be managed seamlessly, despite the increased complexity that may result from digital change. Fundamentally, Entrust Datacard secures digital identities in an ever-changing corporate environment.

Disclaimer

This publication is provided "as is" and without warranty. In no event will Entrust Datacard have any liability arising from in connection with this publication.
The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.