Are you familiar with the phrase “data is the oil of the 21st century”? Let’s expand a bit further on it. Data pertains to everyone and anyone. You want your data to be protected at *all times.* When you're using it, but also when you aren’t. This need brings in the idea of security and privacy. They're related but not the same, and both are needed and expected in IBM Z® z/OS® environments.

THE DIFFERENCE

Security refers to how data is protected.

Security technology is commonly applied to data *at rest*.

Privacy relates to rights, control and how data is used.

Privacy technology is commonly applied to data *flowing* in a network.

Businesses protect security and privacy with a whole suite of tools like security management systems, encryption, digital certificates, strict audit practices, and real-time monitors.

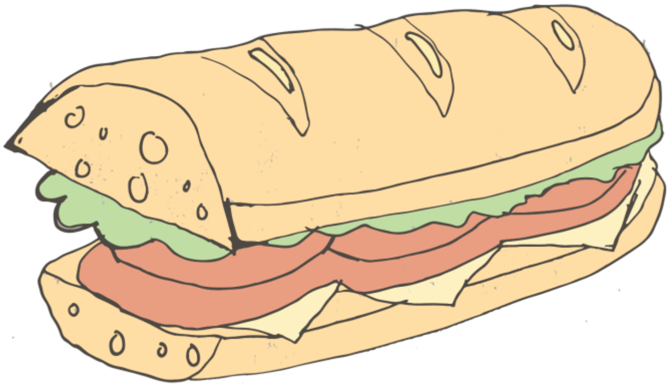
Remember when you use a social media application on your smartphone, and you click “I agree”? That’s you waiving your personal information privacy rights. While the data might be secured by whoever possesses the data, that *whoever* may make your data public or even sell it. Therefore, while data security is often maintained, data privacy is often compromised. The motive for securing the data while compromising individual data privacy is because the accumulated data has value to whoever possesses that data.

You’re probably more or less familiar with the security and privacy basics behind personal computers and smartphones. However, security and privacy practices are very different in z/OS software and IBM Z hardware.

HOW DO YOU MEAN?

IBM Z hardware and z/OS software includes integrated technology to meet the highest possible security and privacy requirements of business and governments.

Security and privacy are big topics. To simplify them, let's compare them to an Italian sub sandwich.



They have *a lot of layers*, without the smell of fresh bread. You wouldn't want an Italian sub if all you had were the slices of bread and nothing else, right? Similar to that, we wouldn't be doing our job if we only applied one layer of security to a system that contains something as important as financial, healthcare or engineering data.

We'll briefly explain the integrated IBM Z hardware and z/OS software technology.

z/OS environments are commonly configured for omni-present security, privacy, audit, and real-time monitoring. When they're all configured and working together, they make a beautiful, secured environment for the IBM Z hardware.

BUT WHY?

1. A security management started task such as IBM® RACF®, which stands for Resource Access Control Facility
2. Pervasive encryption built into the z/OS components
3. Best-of-breed hardware encryption accelerators and techniques
4. Communication server software sub-components enabling security and privacy for data in flight
5. Communication server and other software components enabling real-time monitoring and alerting of suspicious activity

Critical IBM Z data center locations are confidential and typically hidden from the public. They often have more physical security than a prison.

As threats evolve, so do the requirements for strong security. Until the end of the 20th century, previous generations of IBM mainframes effectively had an ocean around them. The public internet didn't exist, so data was only available and accessible to trusted employees. With the ever-expanding access to critical systems and data through the public internet came the ever-expanding need for security and privacy.

Security isn't just referring to making sure the physical box is protected. As nice as it would be to double lock the mainframe inside a cold, dark vault, it's just not enough. To ensure data remains protected, there needs to be security at all levels of the mainframe: the physical box, operating system and applications.

HOW THIS PROCESS WORKS

One of the most common ways that security is implemented on the IBM Z mainframe is through System Authorization Facility (SAF), which is *very* important to the security of data and information.

SAF is a built-in feature of the operating system and provides tools for managing the system security functions. Users don't interface directly with SAF. Instead, z/OS components, such as IBM CICS®, which stands for Customer Information Control System or Time Sharing Option (TSO), can be enabled to communicate with SAF through a security manager component. These security managers, such as RACF (Resource Access Control Facility), contain the security rules used by the z/OS components.

IBM RACF

RACF stores IDs and passwords of users allowed to access the system. It also stores the names of objects, such as data sets, files, programs and so on, along with information about which users are allowed to access the protected objects for either read only or read/write.

An ID defined by RACF can be assigned to a person or process. If a z/OS batch job or started task requests access to a protected resource, RACF will *allow* or *deny* access based upon the security rules defined by the RACF. Access to protected objects frequently includes RACF multi-factor authentication, RACF digital certificates, and long complex RACF password strings.

Too lazy, didn’t read (TL:DR):

1. A user attempts to access a resource.
2. The operating system calls a security manager to say, “hey I know this user, they have permission to access”, “yeah, I know this user, they definitely don't have permission to access” or “hmm I am not familiar with this user, they can’t have access”.
3. Based on the security manager’s answer, the operating system will *allow* or *deny* access to the user.

IN SUMMARY

Security and privacy are built into the hardware, the operating system and the applications inside the z/OS operating system to make sure that not only the data the system is being protected, but ensuring data being transferred in and out is kept confidential and safe as well.

So, next time you are thinking about all the various data that each individual or company holds, remember all the security and privacy functions that are set in place to ensure that what and is kept out of the hands of those that don't have permission.

We’ve covered a lot of topics but have only touched the surface of the security and privacy capabilities of the IBM Z mainframe. If you would like to learn more, visit the Enterprise Knights of IBM Z video library. There are videos on various aspects of security concepts, code and configurations so you can learn more about how your data is being protected, and even get a chance to earn a professional badge.