Information Integrity, The Final Frontier

It is an axiom that good IT security is based on the analysis of threats and defences and the potential impact to information integrity, availability and confidentiality. We have been defending against availability attacks for over 20 years, not least because of unreliable hardware. Confidentiality has been in focus for a similar period of time, protecting against hackers and information thieves who look to compromise confidentiality, steal secrets and often looking to find access credentials for more valuable sites. The final frontier of IT security defence though is Integrity. Information integrity requires an accurate representation of the state of the business and the audit records as to how it got there. Modern systems need to record both; it's not enough that the system is provably accurate, records are required to ensure that transactions and changes are appropriately authorised. The key questions are "does the system tell the truth?" and "can we prove that the accurate state of the business has been authorised?".

Information integrity failures can be the result of bugs, design flaws and also of malicious action. Bugs & design flaws can be addressed by strong requirements management and good testing. Malicious action is defended using the classic tools of:

- an effective boundary defence
- adequate technical protection based on a "defence in depth" cybersecurity implementation and effective internal controls that reinforce the defence in depth such as the segregation of duties and enabling the principle of least privilege
- application and error logs beyond the classic write-ahead log (to prove appropriate authorisation). Error logs are fairly common in modern software design, application logs less so.

Encryption & authentication are classic confidentiality defences, yet the problems that PKI was designed to solve were that of authentication and non-repudiation. Digital signatures can therefore be used to sign checksums and/or even complete feeds or files. In this light, the use of encrypted messaging inside the firewall, which may seem to be an excessive overhead if only considered as confidentiality defences, actually delivers information integrity defence benefits because it guarantees the legitimacy of source data. The use of digital signatures and encryption is not a silver bullet, it must be used in conjunction with a strong "zones of control" architectures and countervailing controls need to be In place to ensure that network intrusion countermeasures remain effective. It should be obvious really, encryption is at the heart of PKI and is used to guarantee both the source and content thus the use of encrypted digital signatures on feeds carrying data between applications, even inside the firewall, ensures their integrity as it validates both the content and the source system. It's highly unusual that an unsigned and unencrypted feed would be taken from outside the firewall; using this technology inside the firewall is an important part of defending information integrity.

Dave Levy
London, March 2017

ooOOOoo

https://www.citihub.com/insights/our-blog/information-integrity-the-final-frontier/