Austin Hunt
CS 6387 – Homework 2 (Crypto Homework) Part 3: Digital Signatures Paper
Sept 17, 2022

Breaking Down Modern Trust: Digital Signatures and their Impact on Business

Running a successful business, whether in finance, education, health, manufacturing, retail, or even doomsday prep gear distribution (that's real), requires trust – trust between the business and other businesses providing third party services (or investors providing money), trust between the business and their clients using *their* service, and trust within the business itself. Without inter-business trust, an organization cannot fully leverage the services provided by others; without client trust, the services provided by a business have no value; without intra-business trust – that is, trust among the internal units of the organization – communication channels that allow for internal productivity fail and services cannot be provided, which then can collapse both client and inter-business trust. As Bruce Nolan would say, "that's the way the cookie crumbles."

Extending this idea to the modern world, in which a business's success increasingly requires a digital presence, we can begin thinking about the value of digital signatures in bolstering the architecture of that trust triangle in a digital context.

What Do Digital Signatures Provide?

In a nutshell, digital signatures provide proof that something digitally received is coming from the expected sender and has not been tampered with during its transmission. This means that when using digital signatures, we can receive information and files over the internet without losing our trust in the integrity and authenticity of what we are receiving. On the other side of that same coin is non-repudiation, or the guarantee that the sender cannot deny their authorship of the item received since their digital signature (ultimately, their private key) is unique to them.

How Do They Work?

On the sender side, the message being sent (which could simply be text or perhaps a file) is first hashed to produce a *message digest*. That message digest is then encrypted using the private key (assumed to be truly private and unique to the sender). The output of that encryption, which *is* the **digital signature**, gets appended to the original message being sent. Note here that the original plaintext message is not encrypted by the creation of a digital signature, so encrypting the message is a separate optional step that can be taken pre-transmission for confidentiality purposes. More details about this step are provided in the What Digital Signatures Do Not Provide section.

Upon receiving the message, the receiver uses the public key owned by the sender to decrypt the digital signature, which produces the message digest (i.e., the hash output). Since public key infrastructure is built on the idea that something locked with a private key can only be unlocked with the corresponding public key and something unlocked with the public key *must* have been locked by the corresponding private key, the receiver can trust that the *message digest* came from the expected sender who owns the private key. Knowing the message digest, the receiver then hashes the plaintext message (possibly after decrypting it if it

was encrypted pre-transmission for confidentiality) to produce their own message digest. To do this, they use the same hash function that was used by the sender. If *their* message digest matches the message digest produced from *decrypting the digital signature*, then the message is guaranteed to have come from the expected sender without tampering from a middleman. The key assumptions here are the true privacy of the sender's private key and the use of a cryptographically secure hash function that will not produce the same message digest for two distinct messages. For example, you wouldn't want a hash function that produces the same digest for a) a malicious message linking to fake a website and b) a real, non-malicious message with information about a policy update.

What Digital Signatures Do Not Provide

While digital signatures do guarantee the integrity of received digital content and provide non-repudiation (i.e., the author of the signed content received cannot deny their authorship as the sole owner of the private key used to generate the signature), they do not inherently guarantee confidentiality. Digital signatures do not necessitate the encryption of the message whose integrity is being validated. Rather, the message *digest* (the hashed value of the message) is encrypted with the private key and that encrypted value is appended to the *plaintext* message before transmission. To achieve confidentiality as well, the message itself would also need to be encrypted by the sender with the *public key* of the receiver pre-transmission and then decrypted by the receiver with their own private key. Note that these "guarantees" assume that private keys are truly kept private, which is the assumption underlying public key infrastructure as a whole.

A Real-World Example from My Own Experience

Consider a higher education institution (which, indeed, is a business) which pays for a Microsoft 365 tenant that provides all faculty, staff, and students with the Office 365 suite of tools for file sharing, emailing, chatting, and generally collaborating both within the organization and with external users, groups, and vendors. In this scenario, through the lens of the previously discussed trust triangle, we consider students (prospective and current) as customers, faculty and staff as the internal business actors, and entities like vendors and donors as external stakeholders on the inter-business edge.

The day-to-day business processes of each administrative and academic department, each office, and generally each team within the organization are critical to its overall success, and many of those processes heavily involve consistent internal sharing of (and acting upon) information in the modes of emails, forms and files representing various aspects of student (customer) statuses from academic standings to financial aid eligibilities to degree audits and so on. Thus, the trust in the integrity of digital information is critical to those various processes; a loss of trust removes "actionable" from "actionable information." A loss of action is a loss of productivity, which crumbles the cookie.

Austin Hunt
CS 6387 – Homework 2 (Crypto Homework) Part 3: Digital Signatures Paper
Sept 17, 2022

Moreover, higher education institutions significantly depend upon external vendors for managing things like events, facilities, software, websites, IT infrastructure, and more. While the initial touchpoints with such vendors certainly require trustable communication, especially when regarding expensive services, the ongoing relationships between the organization and those parties often involves more intensive file sharing, emailing, and collaboration that requires both sides to trust in their digital exchanges. Losing faith in the integrity of files or software shared by a software vendor, for example, could have expensive negative implications resulting in the termination of a contract, and perhaps the loss of a student-facing service which affects *their* trust as customers.

Of course, students need to be able to trust the school they're attending or considering attending, and a big factor in that trust is the communication they receive (or don't receive). A majority of the communication students do receive is sent via email (though the effectiveness of this channel is questionable, but that is a rabbit hole that we can avoid here). Let's say a student enters their contact details into a "request more information" form on the school's public website. Then, the school adds them to a communication plan, and they begin receiving spammy or malicious-looking emails from what *appears* to be that school – or worse, they get a virus – because of the email content being tampered with during transmission. If a student doesn't trust information shared by a school, the chance of that student crossing that school off their list increases; at scale, that gets expensive for the institution.

Fortunately, the Office 365 suite on which the institution's faculty and staff rely for file and information sharing offers methods for adding digital signatures both to emails sent via Outlook (in addition to those regular signatures) and to files created with Office apps like Word and Excel. This means receivers of files and emails sent by people *who use those digital signatures* can be confident in their content, whether the receiver is a faculty member, a staff member, an external party, or a student. Unfortunately, these signatures are *optional,* and their additions are up to the individual authors. It doesn't look like Microsoft tenant admins are able to establish a domain-wide policy requiring their use. Rather, an issue like this prompts a need for communication across the organization about the importance of email security and integrity that includes instructions for enabling and using digital signatures when authoring content – especially important content.