How much do you trust your inactivity timer?

By Anthony Dibble, Middle East Senior Technical Services Consultant

In today's world of healthcare regulation, privacy requirements, and cyberattacks, those who are part of the C-suite, such as CISOs, CIOs, and CMIOs, are faced with the problem of balancing a complex variety of risks.

As our existing customers already know, Imprivata solutions are designed to help solve those problems. However, in talking to prospective customers, a question I'm often asked is:

"How can we be sure that the Imprivata proximity card modality is sufficiently secure, because a card and PIN can be shared? Surely we should opt for a biometric solution?"

Of course, Imprivata offers a fingerprint biometric modality, and I use it every day on my own workstation. So why do we always recommend the proximity card modality, and why do the vast majority of our customers follow that recommendation?

The answer is based on the fact that a security solution is only as strong as its weakest point, and the weakest point will always be the human being.

A clinician's dilemma

In healthcare, the people who are most likely to de-prioritise security are clinicians. They work in a highly time-sensitive environment where seconds and minutes can significantly affect clinical outcomes. Therefore, faced with balancing time and the wellbeing of a patient against security, clinical professionals will always err on the side of the patient, which may translate into security workarounds.

Healthcare security challenges

Clinicians typically are mobile, using multiple workstations in numerous locations like nursing stations, patient rooms, and computers on wheels. These workstations are usually shared, each being used more than fifty times per day.

In that context, let's examine the issues faced by a clinician that could affect security:

- Time taken to log in to Windows – around one minute, often considerably more
- Accessing multiple individual applications (EHR, PACS, RIS, etc.) – Requires users to remember multiple complex passwords
- Locking Windows – desktop is unusable for other users unless they:
  - Use switch users capability – which can cause the machine to overload
  - Reboot the computer – a surprisingly common workaround
- Unlocking Windows – typically 20-30 seconds
- Time taken to log out of Windows
  - A few seconds to initiate the process
  - Logging out requires logging in again – which can deter clinicians from wanting to log out in the first place

Faced with this, it's unsurprising that a walk around a typical hospital will show an array of unlocked workstations, hidden post-it notes containing passwords, application credentials written on the wall or notice board, and other unsecure practises.

In addition, credential sharing is not uncommon. As an example, at one hospital Imprivata worked with, a head of department explained that all clinicians in his department had a photocopied sheet listing all usernames and passwords of people working there. If a workstation was found locked, it could thus be unlocked by anyone without having to power down the computer or switch users.

Strong authentication – on its own...

Let's imagine that at this point we add a strong authentication modality such as fingerprint or smart card. We've strengthened the security of our front door, but has it improved the situation? The answer is "no," because all of the above challenges remain. As a result, when a clinician walks away from a workstation, they will undoubtedly leave it unlocked, perhaps switching off the monitor as a nod to data privacy.

At this point, your security is in the hands of your automated inactivity timer.

Cue the inactivity timer

So, while we have a strong authentication mechanism, it doesn't solve the usability challenges as users work around it by avoiding locking the workstations. We are now relying on an activity timer. Let's examine what that means:

- Inactivity timers are typically set to lock the workstation after a delay of at least 10 minutes. Any less and clinicians complain that the timer is too aggressive. Much more than 20 minutes and most security officers get nervous
- Unattended workstations are therefore fully accessible for a period of between 10-20 minutes
- If the workstation is accessed during this period, the timer is reset. In effect this means the workstation could be accessible indefinitely

Based on this, we can agree that an inactivity timer may be of some effect in preventing casual misuse of a workstation, but not against a more determined attack.

It's all about the workflows

So what's the answer? In short, strong authentication solutions in healthcare typically fail unless deployed in conjunction with a solution that solves the usability challenges and takes into account the day to day workflows of the clinical staff.

This is why Imprivata offers three different workstation configurations which, together, solve healthcare security challenges. So, even in the absence of a strong authentication mechanism, users are happier to lock unattended workstations because unlocking them takes significantly less time.

Imprivata's strong authentication solution is designed to be an integral part of the overall Imprivata healthcare solution. Combined with the appropriate workstation configuration, authentication becomes both fast and secure.

Modality

So let's return to the original question of modality. Why proximity card?

- It's easy – In the same way the clinician taps the card on the door entry panel for physical access, they tap it on the card reader for workstation access
- It's reliable – Unlike fingerprint, it doesn't matter if the clinician is wearing gloves or has made his fingerprint temporarily unreadable through manual tasks or injury. The proximity card will work every time
- It can lock, as well as unlock – Tap to login, Tap to lock. An easy habit. In contrast, the fingerprint modality cannot be used to lock a workstation

For workstation authentication, these features, in conjunction with the Imprivata workflow enhancements, actually make the proximity card more secure, not less secure than a fingerprint scan. Why?

- The Imprivata-accelerated workflow enhancements have removed the need to leave workstations unlocked or to share credentials – it is now fast enough for the clinician not to require an unsecure workaround. Clinicians have no need to share their proximity card, in the same way that they have no need to do so for physical access
- The proximity card is, of course, always configured to work with a second factor (password or PIN) to protect against accidental loss. This second factor is configured with a grace period so that it's only required at configurable intervals, thus maintaining convenience
- Occasional failures to read a fingerprint can increase reluctance of clinicians to lock their workstation – taking us back to the inactivity timer
- Clinicians are more likely to forget to lock the workstation when using fingerprint modality (tap on, tap off is an easier habit to create) – again taking us back to the inactivity timer

Of course, fingerprint has its place – for example in US electronic prescribing of controlled substances (EPCS) workflows, or for signing medication orders – in which case readers can be procured for those specific purposes.

But for the basic 50-100 times per day task of workstation authentication and securing the workstation, proximity card wins based on convenience and reliability. The human being is now working with your security solution, not around it.

imprivata®