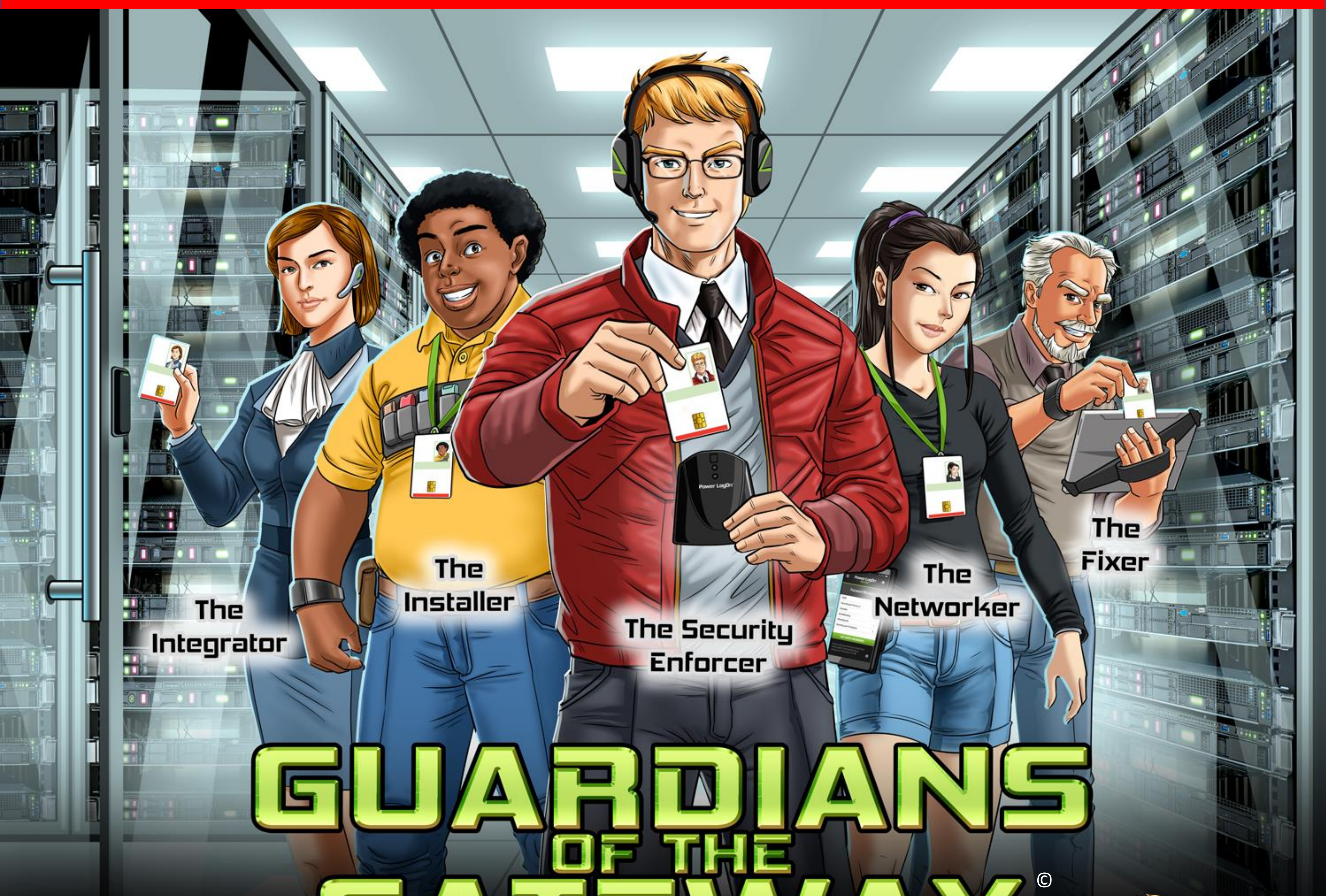
Is PKI better than Passwords?



The Security Enforcer: I'm looking into securing our company with PKI because I've been told it is far more secure. What do you think?

So, which is faster, a bicycle or a Ferrari?

That's obvious, a Ferrari

Really? What if the Ferrari is on the I-405 in LA at 5pm on a weekday? It can only move as fast as the rest of the traffic. So, who's passing who?

One solution is not better than another. It's all about the context and what you are trying to achieve. PKI relies on a 256 character (2048-bit) private key for security. What makes PKI secure is how that key is protected from outside attackers. If you incorporate the same security methodologies as PKI (encryption, MFA and smartcards) with a 300-character password that changes weekly, would PKI still be more secure?

The only thing PKI adds that a secure, multi-factor password manager doesn't is the ability to digitally sign legally binding documents. What percentage of employees have authority to sign legally binding contracts?

What you really want is authentication, authorization and non-repudiation logon. You need a solution that solves your problem based on risk, time to implement and budget.

PKI and passwords are both viable solutions. Passwords that are managed correctly are secure when using the same technologies as PKI, and cost a whole lot less to implement. The take away is that security is weakened when employees manage authentication secrets. The authentication method I'll choose will be based on what the employee needs. The low cost on managing passwords also keeps our overhead costs low.

Power LogOn works side by side with PKI. Or, it can be deployed by itself. The security of Power LogOn is that employees don't have to remember, type, know, generate, or manage any passwords. By leveraging your existing security is a major cost savings.

www.access-smart.com

The_Security_Enforcer@access-smart.com

Smart Access
Cyber Access Control