



Hidden Threats: A 1 Step Plan To Global Failure

Security threats to global cryptographic infrastructures

Jürgen Pabel, CISSP

An announcement this week about the new generation of passports, the ones that store biometric data and feature components automated data extraction, lead me to question the adequacy of technical aspects of modern infrastructures employing cryptographic components. It's not that these systems don't hold up to the current security standards, it's whether they will still be on par with security evaluations of tomorrow.

Modern electronic infrastructure systems are global in nature and therefore globally vulnerable: proper steps must be taken in order to improve the resilience against catastrophic failures. However, the infrastructure that is devised for modern passports has a significant weak spot: the dependence on a single cryptographic algorithm. It's not that the algorithm is currently considered unsafe – it's that this may change suddenly and completely. Over the last months, there have been several key advances against some major cryptographic algorithms, that were previously seen as completely secure; in the field of cryptography, a classification of “secure” only means that no one has yet found a weakness. The discovery of a cryptographic weakness may quickly lead to the total collapse of the security properties upon which the infrastructure was build. Yet, modern information infrastructures almost universally abstain from incorporating redundancy in their cryptographic schemes. Should those single cryptographic components ever be broken, entire systems would probably be rendered vulnerable to severe manipulation. Incorporating cryptographic redundancy provides a transition period for the case in which a cryptographic component has been compromised; a replacement cryptographic component can than be evaluated and deployed without having lost the system entirely.

Bruce Schneier addresses the combination of multiple cryptographic algorithms in *Applied Cryptography*, but questions its practicality¹; while this may be valid for environments with small and/or short term security requirements, it's a completely different situation when dealing with global infrastructures of vital importance.

¹ Schneier, Bruce (1996). *Applied Cryptography*, second edition (368). New York: John Wiley & Sons, Inc.