Rethinking Information Security

Michael Barwise

I was reminded the other day that the World Wide Web is 20 years old this month, and it came as a shock to realise I've been involved with it for all but the first three years.

Things move very fast in IT: ten years is a lifetime, and 20 is a whole era. Why then, after more than 15 years of general public access to the web and almost as much of burgeoning web services for business, is the infrastructure less secure and resilient today than it was back then? I believe it's primarily due, not to technological issues, but to the psychology that underpins the dominant security paradigm. We've so far consistently taken the defensive in a guerrilla war against a proactive enemy who is at least as competent and determined as ourselves, and we have almost exclusively used technology-driven reactive tactics.

We generally assume that "until it's attacked it's secure", so post-hoc tests that (possibly fortuitously) come up clean are construed as a indicator of robustness, and protection measures get deployed only once the calibre of the flying bullets has been recognised. As a result, lots of us get shot. This is typified by the Citigroup breach discovered in early May this year, in which some 200,000 customer accounts were illicitly accessed via a trivial and well-known URL parameter tampering attack. More recently, it was reported that a 3G femtocell base station could be breached via a flaw in its remote firmware update system - the update image was digitally signed, but the public signing key was stored in an unencrypted file on the device, and it was apparently also possible to download an unencrypted backup image from the device, making plaintext attacks on the encryption possible. As a result of these rather obvious flaws, malicious updates could be made to the firmware. Then of course we have the constant stream of patches from every software vendor on Earth - something we've come to accept as normal.

But a change of emphasis is long overdue. For commerce and government to survive online we need a robust infrastructure that will remain resilient in the face of the unexpected, not a fragile one that constantly needs fixing in the aftermath of attacks. If you were driving into a war zone, would you travel in a Ford fiesta with a load of armour plate tiles and a welding kit on the back seat, and every time a bullet hole appeared rapidly weld a patch over the hole? I think not - not if you wanted to survive. You'd go in an armoured personnel carrier if you had even half a brain.

So why do we accept the "Ford fiesta" in the world of IT? I don't believe it's because systems and software developers don't care. After all, there's no money to be made out of patches - they're a drain on resources and they damage reputation. I think it's because IT is not yet a real engineering discipline. To make it one, we need to accomplish two things. Instead of relying on the rote dashboard knowledge currently prevalent, we must educate both developers and implementers in first principles so they can identify and pre-empt issues before they become manifest as faults. And we must instil in the same people an adequate grounding in the theory of risk - probability, uncertainty and heuristic biases - so they can reliably and accurately assess the relative significance of the issues they identify.

The necessary prerequisites for the creation of a robust inherently attack-resistant infrastructure are rigour, consistency, objectivity, evidential support for decision-making, and assurance of the expertise of all involved parties. These prerequisites may seem hard to achieve, but they are fundamentally necessary. If they seem unattainable, remember that the only penalty for failure is to remain insecure. That's not illegal (yet).

Originally appeared on the Infosecurity Network, August 2011