Riscos de Segurança das Infraestruturas de Informação Crítica
ou porque Bang! é diferente de Crash

Paulo Esteves Veríssimo

LaSIGE, Faculdade de Ciências da Univ. Lisboa, Portugal

Esta palestra será inspirada numa intervenção recente na revista IEEE Security & Privacy, January 2008, em resposta a uma pergunta no "Information Assurance Technology Forecast 2008":

Sec&Priv: What's the nature and magnitude of risk that critical information infrastructure (CII) faces over the next 15 years? By "critical," I mean the part whose failure would have major effects on the nation, such as economic loss or loss of life.

Paulo Verissimo: Large and ever increasing. Moreover, the objective risk is amplified by the lack of perception of the risk itself existing, by citizens, policy makers, and CII manufacturers and operators. There's still a belief that the SCADA [Supervisory, Control and Data Acquisition] systems controlling these infrastructures are legacy, closed, obscure, and thus unattackable, or that it suffices to just use a firewall and an intrusion detector. But normal ICT systems protection won't be enough. To keep a long story short: Ctl-Alt-Del isn't a remedy for things that have worked continuously for more than 20 years, many security techniques hamper real-time operation, and there's still a difference between erasing a database and setting a generator on fire. This should be understood immediately or else we should get prepared for the next generation of mass hacking. Maybe all it takes for people to get serious about this is a www.scada_rootshell.com (Google the remainders of the classical www.rootshell.com to grasp the basic idea). It might be a good idea for policy makers and CII manufacturers and operators to learn the difference between crash and bang.

Artigo completo na BD do IEEEexplore. Information Assurance Technology Forecast 2008, Steven M. Bellovin, Terry V. Benzel, Bob Blakley, Dorothy E. Denning, Whitfield Diffie, Jeremy Epstein, Paulo Veríssimo. IEEE Security & Privacy, vol. 6, no. 1, pp. 10-17, January/February, 2008.