Chapter 15

Next Generation Information-Based Infrastructures: New Dependencies and Threats

Eric Luijff
TNO, The Netherlands

ABSTRACT

Advancements of information and communication technologies (ICT) cause infrastructure owners to augment current infrastructures with such ICT. The creation of more efficient and effective end-user services provides economical benefits and increases customer satisfaction. Concurrently, ICT advancements allow governmental and industrial sectors to develop complete new infrastructures and infrastructure services, the so called Next Generation Infrastructures (NGI). NGI will offer new services to society, end-users and the supply-chain of organisations and linked, dependent infrastructural services. For over fifty years, the introduction of new ICT-based services and infrastructures has been tightly coupled with failures in ICT-security. This chapter on NGI discusses the root causes of these security failures. Based on historical experiences, this chapter predicts threats and cyber security failures alike for the envisioned NGI such as smart (energy) grids, smart road transport infrastructure, smart cities, and e-health. This prediction will become reality unless fundamental changes in the approach to security of ICT-based and ICT-controlled infrastructures are taken.

INTRODUCTION

Advancements of information and communication technologies (ICT) cause infrastructure owners to augment current infrastructures with such ICT. The creation of more efficient and effective end-user services provides economical benefits and increases customer satisfaction. Concurrently, ICT advancements allow governmental and industrial sectors to develop complete new infrastructures and infrastructure services, the so called Next Generation Infrastructures (NGI). NGI will offer new services to society, end-users and the supply-chain of organisations and linked, dependent infrastructural services. Examples discussed below comprise Smart (energy) Grids,
Smart Cities, Smart Road Transport Infrastructure, and e-Health.

For over fifty years, the introduction of new ICT-based services is tightly coupled with the reinvention of previously made ICT-security failures. Below, the root causes of these cyber security failures are discussed which includes the organisational failure to learn from lessons identified in the past. Based on historical experiences, this chapter predicts alike cyber security threats for the NGI ICT-based services unless the lessons from the past are really learned. The current risk-based approaches turn out to be only a part of the protection puzzle. Dynamic, well-trained and knowledge based operator integrator intervention to deal with unexpected and unpredicted incident situations is another one. At the end of this chapter, a set of recommendations is presented.

BACKGROUND

Cyber Attacks

Before we discuss NGI, it is worthwhile to look back into the relative young history of information and communication technologies (ICT). Since the 1950s, one can recognise a number of ICT-adoption waves which followed the (Bohlen, 1957) technology adoption lifecycle model. This model recognises an innovation phase, followed by early adopters of new technology. When the new technology breaks through, an early majority phase is recognised, followed by the mainstream phase of technology adoption. Often, some setbacks mark the step between the early adoption and early majority phases. According to (Venkatesh & Bala, Technology Acceptance Model 3 and a Research Agenda on Interventions, 2008) these setbacks in acceptance of new ICT comprise either a lack in the perceived ease of use of the new technology, or a lack of perceived usefulness to individuals and organisations. TAM 3 is one of the models which relates to the Unified Theory of Acceptance and Use of Technology (UTAUT) by (Venkatesh, Morris, Davis, & Davis, 2003). Interestingly, neither TAM 3, nor UTAUT take the security posture of ICT and the user perception of security as a major factor for the acceptance of ICT into account. However, the lack of real and perceived security is one of the setbacks for users and organisations to move to the majority adoption phase of new ICT.

Examples of Cyber Attacks and New ICT Adoption Waves

In the 1960s, passwords were stored on mainframes in clear. The password file was accessible to all legitimate users. Only after a number of break-ins and stolen data sets, tighter control was added. From the early 70’s, mini and midi computers took off. They were often deployed in a closed community area. Passwords, if required, were used for user data separation. The initial versions of the Unix operating system used a single password file that could be read by all users and applications. The password file stored information like the user name, user id, start shell, and the related one-way encrypted passwords. As the recreation of the plaintext password after the one-way encryption process was considered mathematically infeasible, the designers had no reason to hide and protect the one-way encrypted password data. As an additional security measure, a random number (‘salt’) added to the plaintext password caused different outcomes in case different users selected the same password. For that reason, the password file was made read-accessible to all.

The security design, however, did not take into account Moore’s law (Moore, 1965). The yearly doubling of computer speed and memory size made it feasible to apply the password algorithm either in a brute force way or by using dictionaries. That made it easy to verify whether the one-way encrypted result matches one of the stored, publically readable set of encrypted passwords.