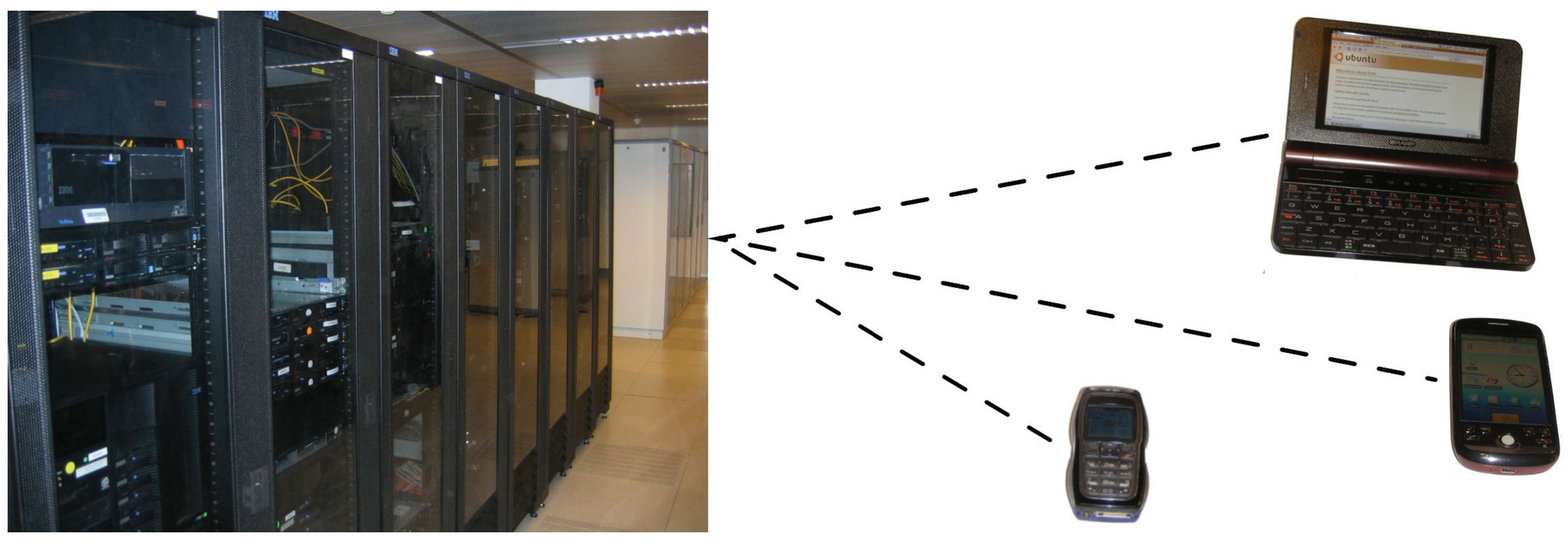
Cryptanalysis

NCF

Cryptography is critical to secure eCommerce and Internet banking and to keep confidential data safe. But establishing the security of cryptosystems is difficult. Predictions about the complexity of attacks rely on mathematical estimates and cryptanalytic experiments. Attackers sometimes have orders of magnitude more computer power than the experimenters, but often it is possible to gain information by attacking scaled-down versions of the actual cryptosystems. The resulting security predictions become more accurate with more data points over a larger range of system parameters; large parameters require high performance computations.



Most cryptosystems can be scaled to very large key sizes, making them very difficult to break. But paranoia is expensive. Cryptosystems that do not provide good performance are not deployed and even cryptosystems that achieve reasonable performance are often considered too expensive for the benefit they bring. Google has recently added cryptographic protection for text search but turns it off for image and video search. Most web servers have even less protection, as illustrated by the Firesheep hijacking tool. The cost of cryptography is also important for small devices that run at low speed and are constrained by battery life.

The most widely deployed public-key cryptosystem on the Internet is 1024-bit RSA, achieving an unhappy balance between poor efficienc and poor security: 1024-bit RSA is too slow for most sites to deploy, and its safety is increasingly unclear. The invention of botnets has dramatically increased the power of a low-budget attacker: with a laptop and an Internet connection a skillful attacker can infect and "own" millions of computers. The Conficker worm seized control of more than ten million computers around the Internet, assembling them into an inhomogeneous but powerful grid.

Understanding how much security is being compromised for cryptographic performance requires understanding the cost of an attack. Mathematically modelling and analyzing the scalability of attacks is difficult and error-prone; to make reliable predictions and verify previous predictions we are carrying out a series of larger and larger attacks against various cryptosystems, optimizing the mathematical aspects of the attack algorithms and at the same time making them more suitable for modern computer architectures such as GPUs. This work improves our understanding of the scalability of the attacks and allows us to make confident recommendations to users regarding safe key sizes, increasing the speed of Internet cryptography without compromising security.

UIC University of Illinois at Chicago

TU/e Technische Universiteit Eindhoven University of Technology

AUTHORS TANJA LANGE (TU/E) | DANIEL J. BERNSTEIN (UIC)