Real World Protocol Analysis
Cryptography Group, Department of Computer Science, University of Bristol

Securing Online Payments

Cryptography plays a vital role in the modern world. Security protocols are involved in many everyday actions e.g. phone calls (GSM/UMTS) and monetary transactions (EMV). Combining cryptographic primitives to create secure protocols is an inherently difficult task. Many subtleties regarding how the scheme is used in practice must also be considered when evaluating a protocol's security.

Research in this area can take one of two roots:
▶ Searching for vulnerabilities in existing schemes.
▶ Providing formal guarantees that a particular protocol or generic construction is secure.

There are two branches of research which provide such formal guarantees:
▶ Practice-Oriented Provable Security.
▶ Formal Methods.

On going research in this area is vital to ensure that the protocols we use everyday are secure.

Motivation

Contribution and Outlook

The range of protocols studied by members of the group include:

SSL/TLS – One of the most widely used secure network protocols. Most famously it is used to secure credit card transactions made over the Internet. Dr. Dan Page was recently involved in analysing features of OpenSSL which led to the discovery of an ECC-related software bug attack.

EMV – More commonly known as Chip-and-Pin; the system used throughout Europe to secure credit/debit card payments. Prof. Nigel Smart co-authored a paper provided a formal security analysis of the currently used and future algorithms in the EMV standards.

SSH – Another important network security protocol, used primarily for remote login. Detailed analysis of the SSH key exchange was performed by a PhD student in the group.

We continue to analyse existing protocols against formal security requirements; our ongoing projects relate to a variety of topics including Access Control, CDA protocol, UMTS and many more.

Everyday Devices

Funding and Collaboration

▶ EPSRC via grant EP/H043454/1.
▶ EPSRC via the CryptoForma network.
▶ European Commission via ECRYPT II.
▶ ERC via Advanced Grant CRIPTO.
▶ Academic Collaborators:
▶ Industrial Collaborators:
▶ Cryptomathic, EMVC, Hewlett Packard, Google, IBM Research Zurich, Microsoft, Trend Micro.