3.14 Security of Symmetric Encryption against Mass Surveillance

Kenneth G. Paterson (Royal Holloway University of London, GB)

Motivated by revelations concerning population-wide surveillance of encrypted communications, we formalize and investigate the resistance of symmetric encryption schemes to mass surveillance. The focus is on algorithm-substitution attacks (ASAs), where a subverted encryption algorithm replaces the real one. We assume that the goal of “big brother” is undetectable subversion, meaning that ciphertexts produced by the subverted encryption algorithm should reveal plaintexts to big brother yet be indistinguishable to users from those produced by the real encryption scheme. We formalize security notions to capture this goal and then offer both attacks and defenses. In the first category we show that successful (from the point of view of big brother) ASAs may be mounted on a large class of common symmetric encryption schemes. In the second category we show how to design symmetric encryption schemes that avoid such attacks and meet our notion of security. The lesson that emerges is the danger of choice: randomized, stateless schemes are subject to attack while deterministic, stateful ones are not.

3.15 Privacy as a Social Value and as a Security Value

Charles Raab (University of Edinburgh, UK)

Privacy and security (national security, public safety) have no agreed singular meanings.

Law and conventional wisdom: Privacy is only an individual right.

But the social and public interest value of privacy is insufficiently recognized: it can be construed as a constitutive public good and as part of the public interest as well as being an individual right.

Across and within societies, different people construe, and value, privacy differently, and privacy has to be seen contextually.

Security is also a slippery term, and can refer to different levels of social scale: individual, neighbourhood, local community, a whole country or society, a region, the world. ‘Safety’ is a related concept (and in today’s world, has become a pre-eminent value, along with ‘security’).

These definitional and conceptual ambiguities and variations are not necessary a problem, except when – in legal, political, social, and medial parlance—it is said that (e.g.) ‘privacy’ conflicts with ‘security’ and must be ‘balanced’.

The concept of ‘balance’ is conceptually and empirically flawed; ‘balancing’ (individual) privacy and (national) security is a rhetorical and tendentious proposition.
We need to think more imaginatively about the relationship between privacy and security, especially if we are to avoid security (almost always) trumping privacy in public policy, surveillance practice, and in popular parlance.

It is helpful to consider that privacy and security have closer affinities than the ‘versus’ rhetoric allows. An important part of the value of privacy is that it affords a zone of security or safety. If so, the relationship between the two values is much more interesting and complex, and points to a need for a creative policy discourse.

In addition, if privacy is an element of the public interest and a foundational principle of social relationships, for which there is considerable psychological and sociological support, then a relationship between privacy and security (or safety) as also public-interest values, becomes more complex and requires more subtle public-policy approaches.

3.16 End-to-end encrypted mail made easy for users

Mark D. Ryan (University of Birmingham, GB)

The certificate authority model for authenticating public keys of websites has been attacked in recent years, and several proposals have been made to reinforce it. We develop and extend certificate transparency, a proposal in this direction, so that it efficiently handles certificate revocation. We show how this extension can be used to build a secure end-to-end email or messaging system using PKI with no requirement to trust certificate authorities, or to rely on complex peer-to-peer key-signing arrangements such as PGP. This makes end-to-end encrypted mail possible, with apparently few additional usability issues compared to unencrypted mail (specifically, users do not need to understand or concern themselves with keys or certificates). Underlying these ideas is a new attacker model appropriate for cloud computing, which we call “malicious-but-cautious”.

3.17 Data Obfuscation/Pollution: adapting TrackMeNot to counter surveillance

Vincent Toubiana

TrackMeNot is a browser extension designed to pollute the web search profile and web search history of users. Initial design of TrackMeNot considered search engines as the main adversaries. However, recent revelation about the NSA program XKeyScore highlights that surveillance can be triggered by specific search queries. This revelation raises the question “Could data pollution be used to make bulk collection inefficient?”. Addressing this question implies to adapt the threat model to consider an adversary that uses less accurate profiles. Furthermore, in order to adapt to this type of adversary it is necessary to find new sources of keywords like the list released by DHS in 2012. The open question is could data pollution have a positive outcome and could it be extended to other services than search.