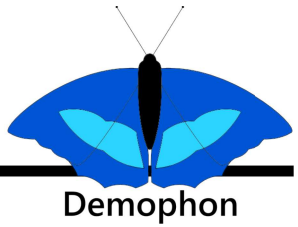
T-110.6000 Internet and Computing Forum
16 March 2015

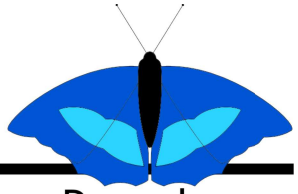
Open-source cryptography for communications

Arto Karila <arto.karila@demophon.com>



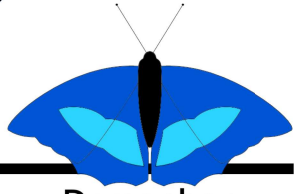
Threats to information security

- Signal intelligence has been a hot topic ever since WW2
- The private information of companies, governments and private people is valuable and the target of cyber criminals
- Over the past couple of years, it has become evident that many of the widely used IT and security solutions not only are insecure but in fact contain Trojan horses and backdoors planted there by various intelligence organizations
- Organizations and people who have taken precaution to protect their information have had a totally wrong conception of both the level of their security and the level of surveillance
- It is impossible to verify the security of any closed solution
- Fully open, auditable security solutions are needed!



Role of cryptography

- Cryptography is only a small part of information security
- However, it is a necessary part of the security of any security solution in an open network
- The security of a crypto system can only be based on the strength of its design and the secrecy of its keys
- Crypto mechanisms needed:
  - Secret key crypto systems
  - Public key crypto systems
  - Key generation
  - One-way hashes
  - Crypto protocols
  - Public Key Infrastructure (PKI)
- The implementation of strong crypto solutions is very difficult
- The system is only as strong as its weakest link



Demophon's business idea

- Currently there is no commercial supply of open, integrated solutions for corporate communications
- Demophon (https://www.demophon.com) was founded to develop an open-source security solution for corporate, private and M2M communications
- At the first phase, the system will offer secure VoIP, IM, E-mail, and file sharing & storage (private cloud)
- The service can be used from portable and fixed devices
- Security is implemented with strong cryptography end-to-end
- Our plan is to first develop a product in customer projects with a few pilot customers and also get paid for support
- The next step is to develop a full product, which will be put to global distribution via the Internet
- Even though all the software is open-source, not all of it is necessarily free (in the GNU sense of the word)

Demophon's solution

- We are basing on existing protocols and crypto systems (such as XMPP and AES)
- Problems with security standards:
  - Lots of old, broken standards/versions still in use
  - Insecure options even in current standards
  - Very easy to choose insecure combinations of features
- We select reasonable and safe features and default options (e.g. no support for ancient SSL/TLS versions)
- Both our design and implementation are totally open for audit
- Simple user interface to avoid human errors

Opportunities & Challenges

Opportunities:

- **Trust to both governments and corporations should be gone**
- **There is a real and growing need for open, auditable security**
- **IoT will make security even more ubiquitous and critical**
- **This can open a window of opportunity for new, agile players**

Challenges:

- **Many people, companies and governments are still not awake**
- **The bearer of bad news risks getting shot**
- **How to make business with open source?**