

Swiss Open Source Security Software for the World Market

Polish-Swiss ICT-Sector Meeting, September 2nd 2015

Prof. Dr. Andreas Steffen
Institute for Internet Technologies and Applications
HSR Hochschule für Technik Rapperswil
andreas.steffen@hsr.ch

HSR - Hochschule für Technik Rapperswil

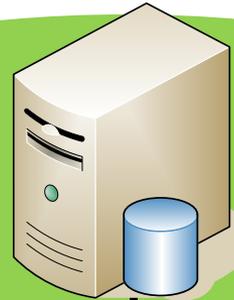
- University of Applied Sciences with about 1500 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)



strongSwan – the OpenSource VPN Solution



Windows Active Directory Server

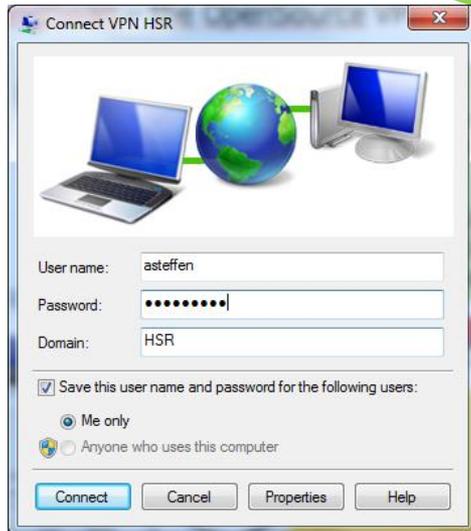
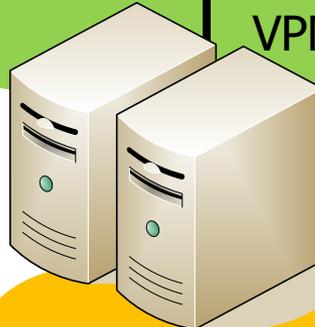
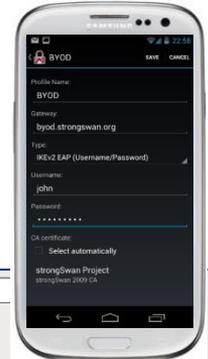


Linux FreeRadius Server



Corporate Network

High-Availability strongSwan VPN Gateway

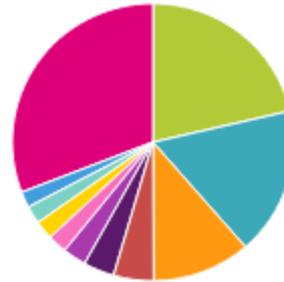
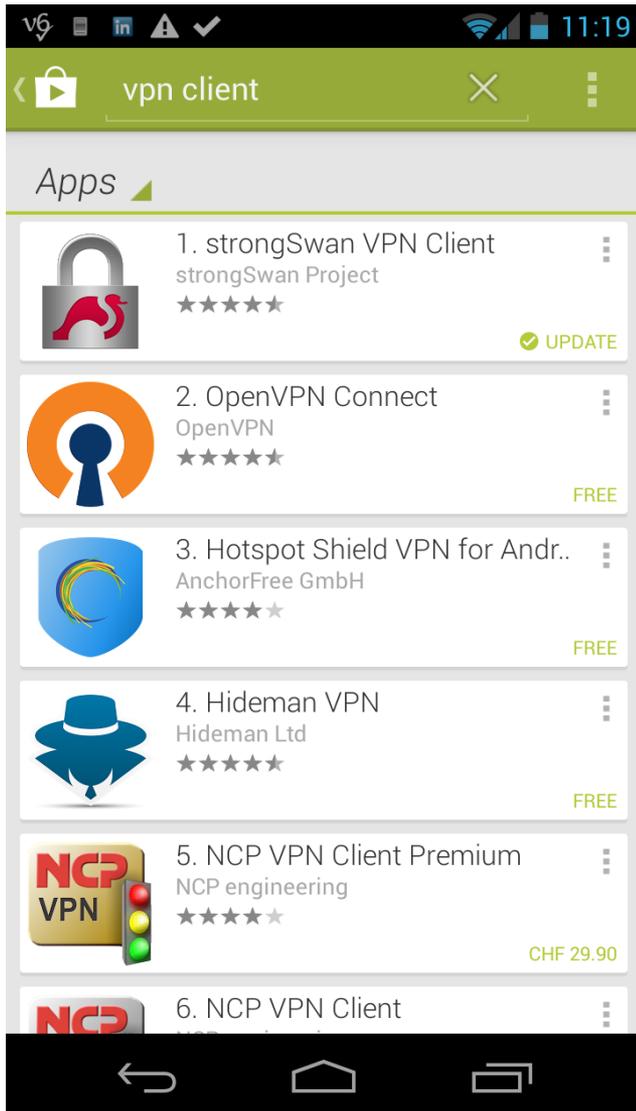


Windows 7/8/10 Agile VPN Client



strongSwan Linux Client

Free Download from Google Play Store



August 27, 2015:
13'254 installations

<input checked="" type="checkbox"/>		United States	2,833	21.37%
<input checked="" type="checkbox"/>		China	2,283	17.22%
<input checked="" type="checkbox"/>		Germany	1,501	11.32%
<input type="checkbox"/>		United Kingdom	608	4.59%
<input type="checkbox"/>		Russia	471	3.55%
<input type="checkbox"/>		Canada	359	2.71%
<input type="checkbox"/>		France	294	2.22%
<input type="checkbox"/>		Australia	290	2.19%
<input type="checkbox"/>		Japan	277	2.09%
<input type="checkbox"/>		Italy	246	1.86%
<input type="checkbox"/>		Others	4,092	30.87%

strongSwan Downloads from Polish Domains

Domain	Downloads	Organisation
agh.edu.pl	47	Akademia Górniczo-Hutnicza w Krakowie
cryptotech.com.pl	25	CryptoTech eSecurity Solutions, Kraków
gamrat.pl	29	GAMRAT SA, Jasło
pacomp.pl	32	PACOMP, Warszawa (fuzja z ENIGMA SOI)
pie.edu.pl	11	Przemysłowy Instytut Elektroniki, Warszawa
polmoauto.com.pl	8	POL-MOT Auto, Warszawa
rst.com.pl	4	RST Wrocław / Świdnica
wp-sa.pl	18	Wirtualna Polska

Multiple downloads from download.strongswan.org over the last two years indicate active use of the strongSwan software.

Swiss Open Source Security Software for the World Market

Polish-Swiss ICT-Sector Meeting, September 2nd 2015

How to launch a successful Open Source Project

The strongSwan Project takes off

- In December 2005 the second generation IPsec Internet Key Exchange protocol (IKEv2) is published as RFC 4306.
- As part of their diploma thesis the two HSR students Jan Hutter and Martin Willi implement a rapid prototype of the IKEv2 protocol in just **8 weeks**.
- The IKEv2 software is written in the **C** language but with a modern, **object-oriented, modular** and **multi-threaded** architecture.
- Thanks to an **initial project funding** by **HSR**, Martin Willi stays on as a research assistant and implements most of the IKEv2 standard over the next 18 months.
- In December 2006 the **first customer** orders an IKEv2 feature extension.
- **Two years** after its inception the strongSwan project becomes financially **self-sustaining**.

IKEv2 Interoperability Workshops



Spring 2007 in Orlando, Florida
Spring 2008 in San Antonio, Texas

- **strongSwan** successfully interoperated with IKEv2 products from Alcatel-Lucent, Certicom, CheckPoint, Cisco, Furukawa, IBM, Ixia, Juniper, **Microsoft**, Nokia, SafeNet, Secure Computing, SonicWall, and the IPv6 TAHI Project.

The strongSwan Business Model

- There are two basic sources of income:
 1. Development of additional VPN standard features or customer-specific plugins, usually on a fixed price basis.
Main focus during the first 5 years
 2. Licensing of the strongSwan source code under a commercial [closed] source license instead of the public open source GPLv2 license.
Main focus during the second 5 years
- Professional consulting and training for key customers only
- Some strongSwan users and customers:
Alcatel-Lucent, Cisco, Clavister, Ericsson, Freescale, Google, Intel, Nokia Solutions Network, Samsung, secunet, Sophos, Swisscom, Swiss Post, U.K. Government, U.S. Government, ...

Swiss Open Source Security Software for the World Market

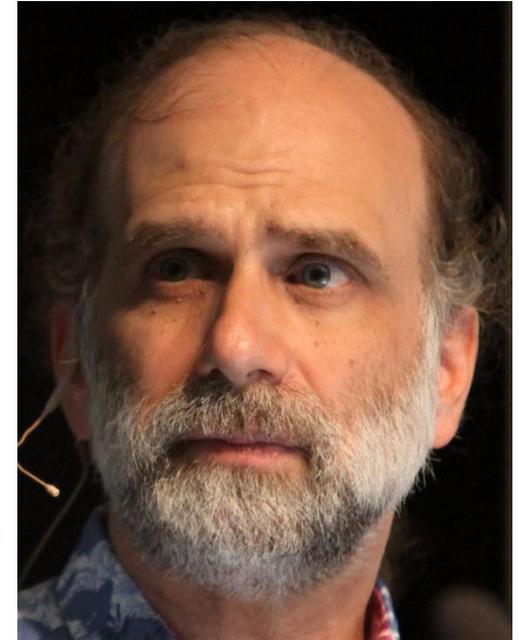
Polish-Swiss ICT-Sector Meeting, September 2nd 2015

2014 – The Year of Encryption

The Snowden Documents – Fall 2013



Edward Snowden



Bruce Schneier



Laura Poitras



Glenn Greenwald

- Bruce Schneier in his September 2013 Guardian article:
“Be suspicious of commercial encryption software,
especially from large vendors”
- Consequence:

Many companies (especially in the U.S.) switched to a
strongSwan VPN solution in 2014 and 2015.

- In 2008 strongSwan adds support of **Elliptic Curve Cryptography**.
- In 2011 the U.S. Government orders an open source strongSwan-based IPsec **Suite B Elliptic Curve Cryptography** reference platform for compliance testing of third party VPN products.
- In 2013 documents leaked by Edward Snowden hint at possible **weaknesses** in standard **cryptographic protocols** and the possibility that the NSA might have an operational **quantum computer** soon.
- In 2014 strongSwan hardens its crypto parameters and adds support of lattice-based **quantum resistant** encryption and signature algorithms.
- In August 2015 the NSA publishes the following statement:

*“For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming **quantum resistant** algorithm transition.”*

Swiss Open Source Security Software for the World Market

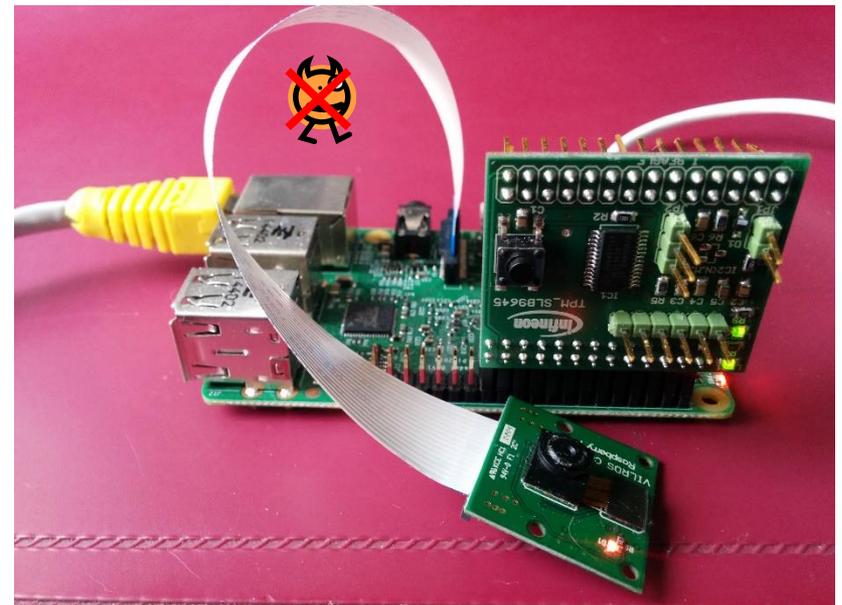
Polish-Swiss ICT-Sector Meeting, September 2nd 2015

Mutual Attestation of IoT Devices
based on the Trusted Network Connect (TNC)
IETF Internet Standards

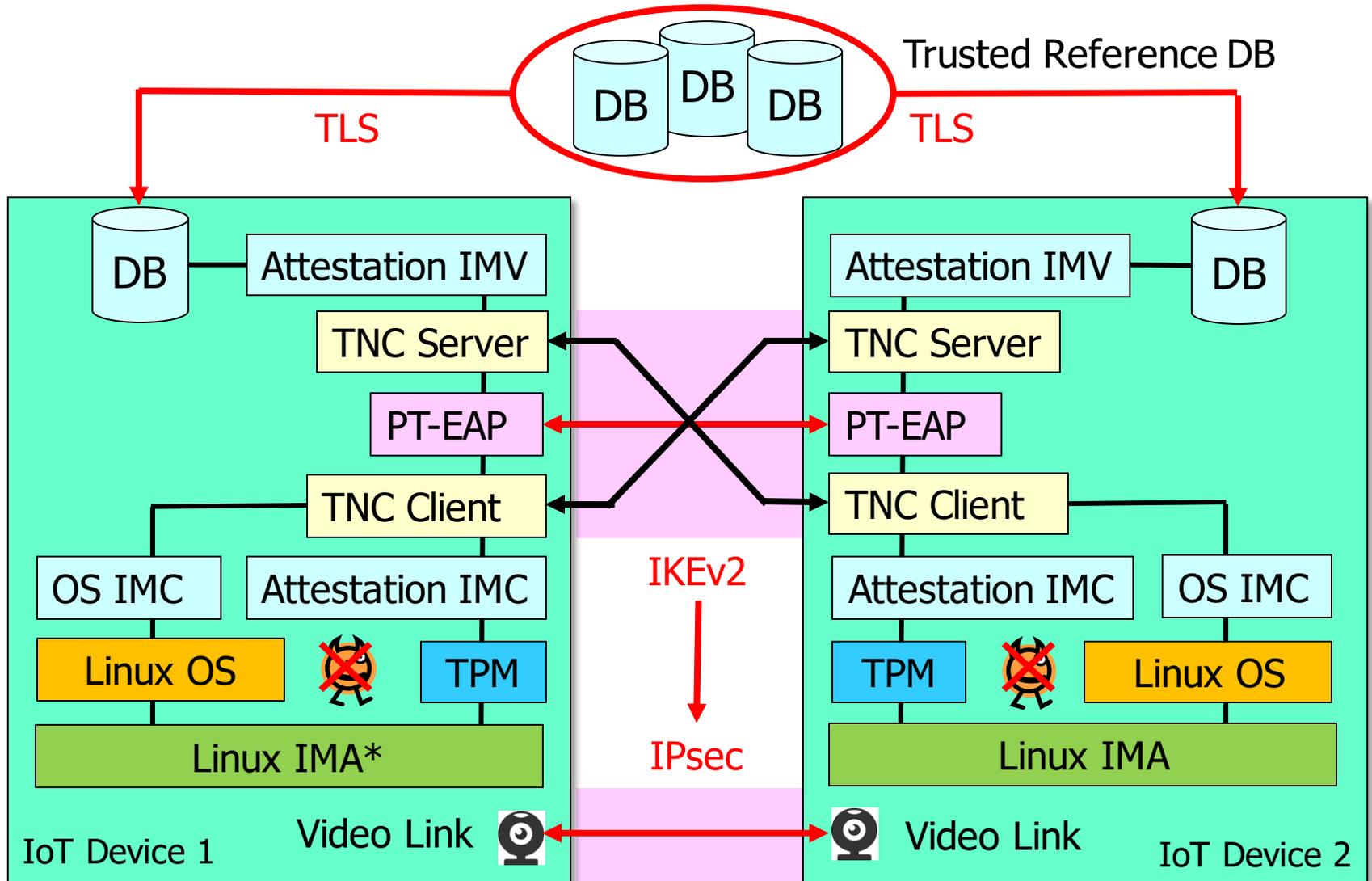
IoT Demo: Mutually Trusted Video Phones



Joint IoT Demo by
Cisco, Infineon & Intel
at **RSA 2015 Conference**
in San Francisco



Mutual Attestation of IoT Devices based on TNC Internet Standards



* IMA: Integrity Measurement Architecture

- It is possible to gain a large share of the world market with a specialized open source security product.
- Open source software is very popular in a security environment because the source code can be readily inspected at any time.
- Modular open source software is very popular because it can be easily modified and extended according to customer requirements.
- But, ...
every open source product needs a constant source of income in order to survive and keep up its quality level (see e.g. the financial problems of the OpenSSL and GnuPG projects).

Thank you for your attention!

Questions?

www.strongswan.org

