PERFECT FORWARD SECRECY FOR EAP-AKA’

or

THE SPIES ATTACKED MY PROTOCOL, I WANT A DEFENCE :-)

Jari Arkko, Karl Norrman, Vesa Torvinen
Ericsson Research

*draft-arkko-eap-aka-pfs-01.txt**

*) Has an IPR notice

Background

- Revelations lead to improvements at card manufacturers, operators & GSMA

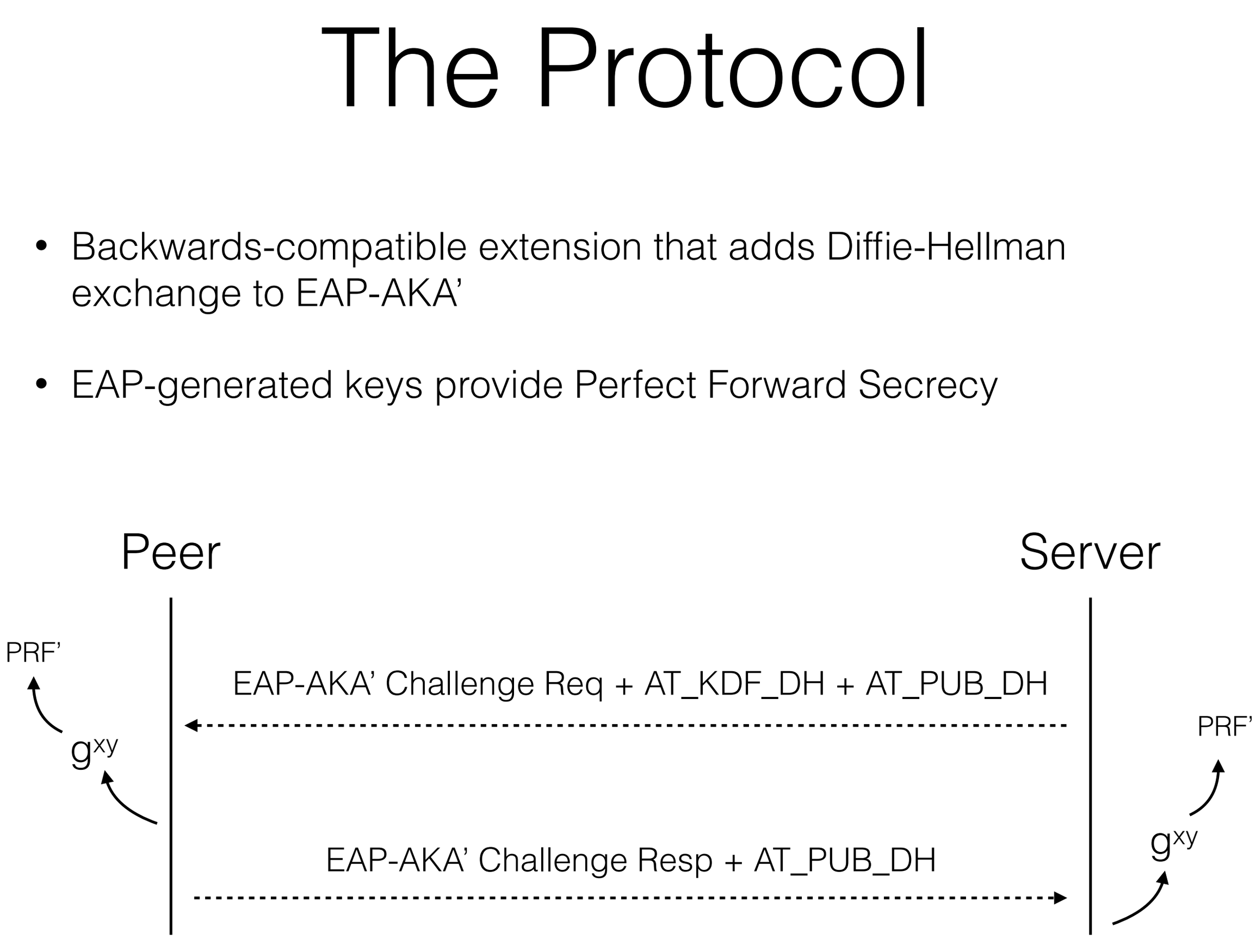
- … but vulnerabilities cannot be ruled out

- Perfect forward secrecy defends against this

- If there is a compromise of smart card long-term keys, the use of EAP AKA' PFS protects against passive attackers (or forces active attack)

The Protocol

- Backwards-compatible extension that adds Diffie-Hellman exchange to EAP-AKA’
- EAP-generated keys provide Perfect Forward Secrecy



More Details

- Interfaces to SIM card and to HSS are kept unchanged; Diffie-Hellman is performed on the phone/authentication server

  => no changes to credentials or key parts of infrastructure, only EAP implementations

- Anything that runs of the EAP keys benefits from the high-quality keying material produced by Diffie-Hellman keys

Why Do This?

- My protocol is broken, please let me fix it :-)
- RFC 7258 requires that pervasive monitoring attacks be taken into account in IETF protocols, and defences considered
- Modern cryptographic protocols generally try to provide PFS
- Support for PFS is part of the agreed plans in the next 5G development (phase 2)

Next Steps

- A specification that is available now can meet industry needs in 2019
- Ongoing implementation efforts
- Consider for WG adoption?