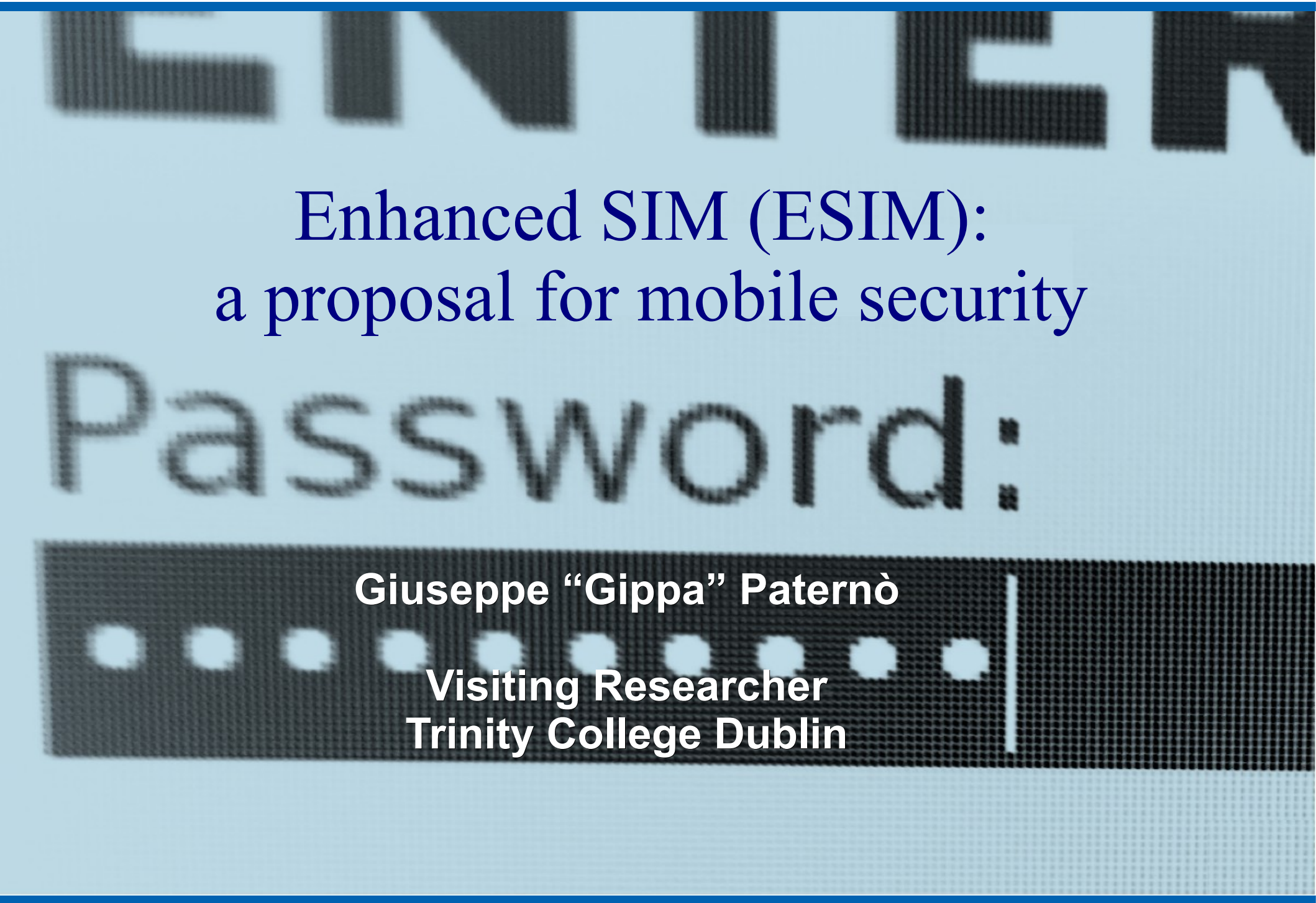

Enhanced SIM (ESIM): a proposal for mobile security

Giuseppe "Gippa" Paternò

Visiting Researcher
Trinity College Dublin

Fàilte

(welcome)

Who am I

- Visiting Researcher at Trinity College Dublin (Ireland)
- Solution Architect and EMEA Security Expert in Red Hat
- Previously Security Solution Architect in Sun and also in IBM
- Red Hat Certified Security Specialist (RHCSS), Red Hat Certified Architect (RHCA) and Cisco Certified Network Professinal (CCNP)
- Part of the italian security community *sikurezza.org*
- Published books and whitepapers
- Forensic analisys for local govs
- More on:
  - http://www.scss.tcd.ie/Giuseppe.Paterno/
  - http://www.gpaterno.com/
  - http://www.linkedin.com/in/gpaterno

Current authentication issues

- Increasing number of websites and intranet/extranet lead to:
  - Increase of username/password combinations to remember
  - Increased number of OTP tokens
- With the following issues:
  - You end up writing the username/password somewhere
  - You can have multiple OTP tokens to carry (I have **three**!!)

The idea

Too many things to carry and a lot of things to remember but .... is anything I carry always with me?

My mobile phone

Enhanced SIM (ESIM)

- SIM/USIM are smartcards that contains:
  - IMSI
  - Security authentication for mobile network
  - PIN protected
  - Not different from any other smartcard
- **Embed a cryptographic engine in a SIM to hold X.509 and corresponding private key.**
- Pre-loaded keypair with Mobile Operator's own CA

ESIM advantages

- Provide the following security services:
  - Website authentication and authorization
  - Corporate logon to resources (Web, Windows Network, …)
  - Bank/financial services for mobile
  - Any other use that require confidentiality
- No need to reissue a smartcard and/or a keypair for each user: any corporate or website only need to authorize, no more authentication hassle!

ESIM advantages

- No need to modify current software:
  - Most webservers has SSL authentication
  - Microsoft Windows allows PKI log-on
  - Kerberos PKINIT can provide smartcard authentication for corporate/kerberized environment
  - Adobe(tm) PDF can use X.509 to crypt documents

ESIM proposed specs

- Two parts are involved, the SIM itself and the mobile device that provides access:
- SIM:
  - JavaCard holding MUSCLE card applet
  - Contact or contactless
- Device: CCID smartcard specifications over USB or bluetooth

Certificate Lifecycle: CA

- Each operator must have a Certification Authority (CA) that mets common criteria
- Must publish the following information:
  - CA root certificate URL
  - Certificate Revocation List (CRL) for offline
  - Online Certificate Status Protocol (OCSP) responder is a plus
- SIM can optionally hold a list of "preferred" CA roots
- Hold the public key for lawful interception

Certificate Lifecycle: ESIM

- SIM preloaded with an X.509 keypair at the factory
  - Key generation command issued
  - Signing of the public key
  - Common Name (CN) set to IMSI value
  - Renewals through the SCEP protocol
- Provisioning
  - The lifecycle must be integrated with operators' provisioning system to revoke the ESIM certificate if needed

API/Crypto Engine Access

Phone manufacturer must:

- Publish APIs to access the key infrastructure for both internal and external applications
- Leverage the existing APIs if possible:
  - Windows Mobile CertificateStore
  - Iphone keychain service
- Enable access to standard computer through USB CCID standard
  - CCID is easy available and requires no drivers

Application Scenario

- VPN access
- Short Messaging Service (SMS) encryption
- Remote device wiping
- IP-based telephony security (SRTP)
- IEEE 802.1x access (EAP) for WiFi and WiMAX
- Financial transactions (security and non repudiation)

Lawful interception

- Required in some countries
- ESIM can be an obstacle to lawful interception
- Home operator must hold a keypair for lawful interception
  - any “network” services should be encrypted with the operator keypair (ex: SMS)
  - Ensure that the “home” country is responsible for crimes, to protect users' rights when roaming
- For other applications, the service provider is responsible for providing the required info.

Criticism

- Public key (X.509) never "took off" apart from government agencies/military
  - Maybe due to costs related in maintaining the infrastructure
- Peer-to-peer crypto is still strong in vertical enviroments (PGP, SSH)
- Usability is a must for the end-user
  - Can lead to a real "flop" if is not easy to use
- In some countries (ex: Ireland) ID is not required to purchase a SIM

Project status

- Some tests have been done, but not the "full chain"
- Talking and investigating in building the chain, but mostly lack of cooperation from manufacturers/vendors and mobile operators
- Exploring other possibilities as well (such as peer-to-peer crypto)
- Your feedback is well-appreciated!

Thank you!!

Giuseppe “Gippa” Paternò
Visiting Researcher
Trinity College Dublin

paternog@cs.tcd.ie
http://www.scss.tcd.ie/Giuseppe.Paterno/
http://www.gpaterno.com/