Security Level:

(U)SIM usage in OTT authentication

Jing Chen & Marcus Wong

www.huawei.com

Email: eric.jingchen@, mwong@huawei.com

Version: V1.0(20131022)

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Agenda

- (U)SIM basics
- Current State of OTT
- (U)SIM for OTT

SIM & USIM

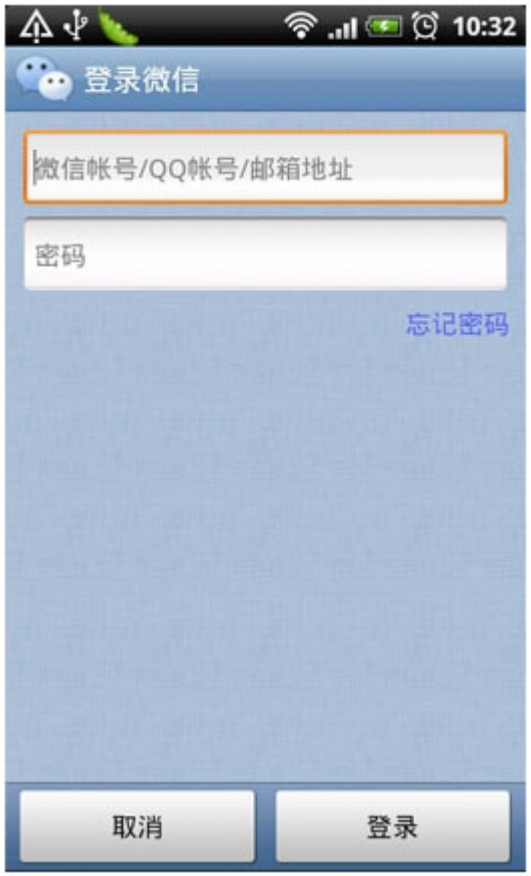
- SIM
  - Subscriber Identity Module
  - can be used to access GSM and UMTS
  - One-way authentication
- USIM
  - Can be used to access UMTS and LTE
  - Two-way authentication, basis for Authentication and Key Agreement protocol (AKA)
- (U)SIM based authentication
  - has worked well for quite a long time and provided secure and easy access for billions of subscribers.

explosive growing OTT services

- OTT – Over-the-Top
- Third party applications that run on top of telecom's pipe

Authentication mechanisms of OTT

- Username and password + dynamic verification code or CAPCHAR (optional)
  - Created between user and server during service sign-up using a mobile number to receive confirmation via SMS
  - Mobile number bound to the OTT service
  - Users likely to choose easy to remember password
  - Same password for different OTT



Password reset or retrieval

- For difficult to remember passwords
  - Easy to forget
  - Reset or retrieval service provided by OTT server
- Password retrieval based on SMS on the Mobile registered with OTT server
- Risk
  - Operator reclaims mobile number
  - Operator assigns to a new user
  - Former owner of the number forgets to cancel OTT service
  - New owner resets password via SMS

Actual attack

- Fuzhou, China

You are here Home >> North police station >> Text

Abandoned phone number, Paypal stolen brush on a million

[Source: Site | Author: Original | Date: September 30, 2013 | Read 19 times] Fonts: [big middle small]

[Deprecated phone number, Paypal brush on the yuan] Kobayashi stolen bank card and Paypal bindings and applied for a "fast pay" function, simply enter the online shopping Paypal password, you can consume. Meanwhile the phone number and Alipay binding. Kobayashi abandoned after the phone number, but forgot to unbind, was fraudulent 12,000 yuan. It turned out that Yang is now using this number, through the "phone number located Password" changed the original PayPal account password.

Editor: wusheng School Policing

Previous: phone a jacket pocket most dangerous Xiecha
Next: alert! New viruses appear to steal cell phone privacy

Related Articles

- There is no related articles

Related Topics

- Thematic an information No
- Theme 2 info

Natural choice for OTT authentication

(U)SIM

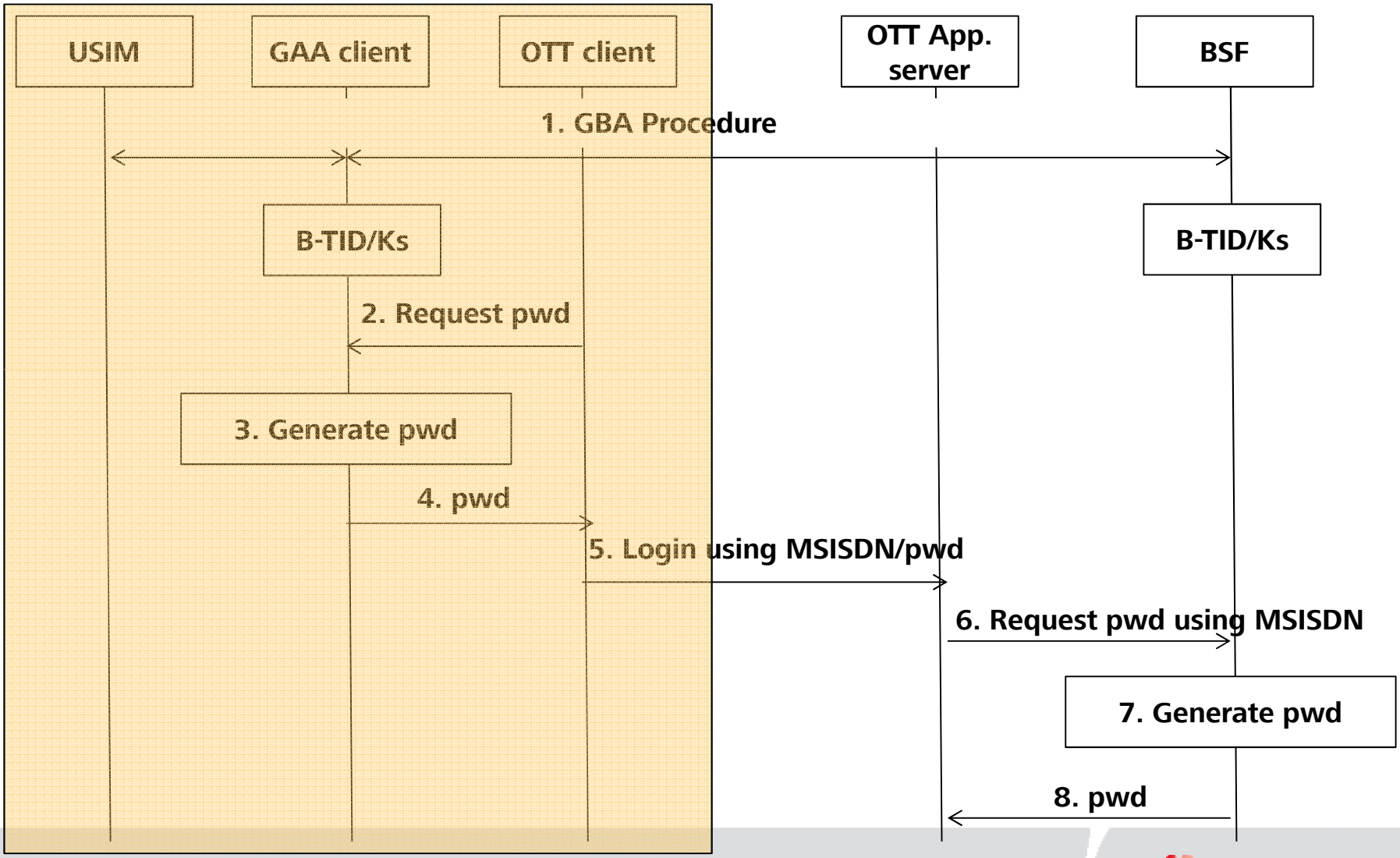
Benefits

- user does not need to create, remember, and type in the username/password
- (U)SIM based authentication has been proven secure in its current form and has been future-proofed as a secure authentication solution in the long run
  - Supports 128-bit security in 3G and 256-bit in LTE
- reclaimed mobile phone number attack can be prevented since mobile network operators are involved
- Mobile operator can offer value-added service
- OTT service provider can simplify operations and minimize maintenance/management of passwords

Business opportunities

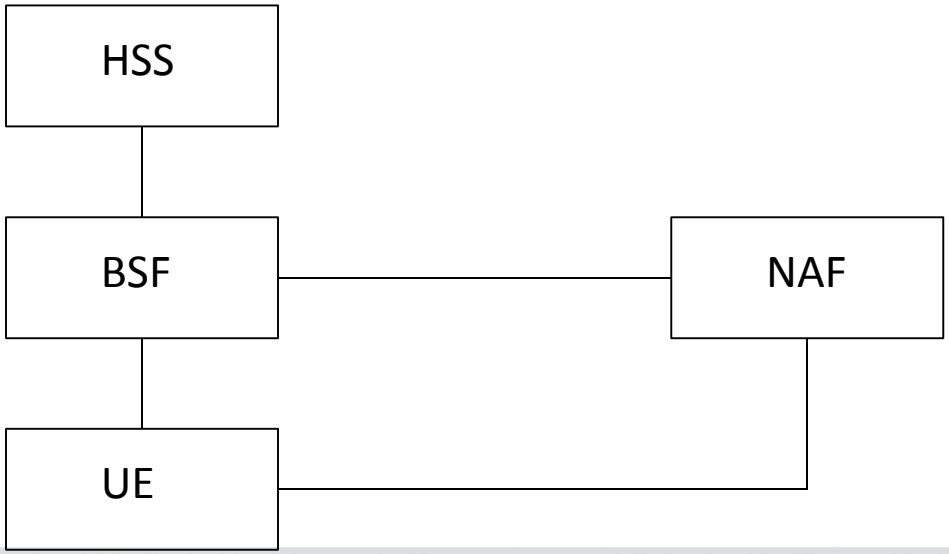
- End users
  - Easy with nothing to remember
  - confident
- Mobile operators
  - offer VAS using their already deployed infrastructure
  - bring in extra revenues for the mobile network operators
- OTT service providers
  - Counter the attack on reclaimed mobile number threat
  - escape from heavy identity management burden
  - attractive user base for the OTT application provider
  - improve the experience of end users

Potential Solution

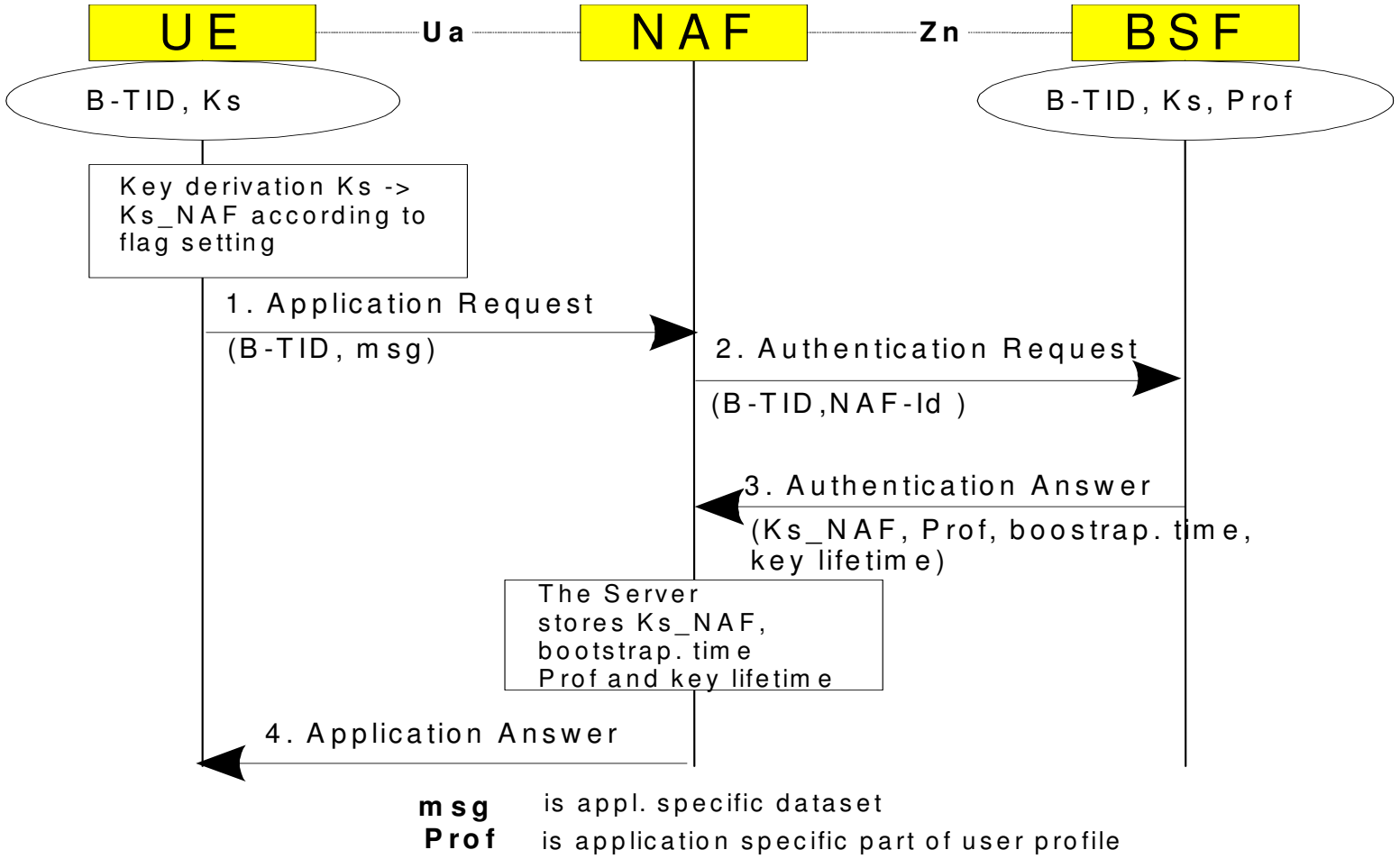


How GBA Works

- Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and an operator-controlled Network Application Function (NAF).
- After the bootstrapping, the UE and NAF can run some application-specific protocol where the authentication / encryption of messages will be based on those session keys generated



GBA Protocol in 3GPP



Conclusion

- Using (U)SIM in OTT application authentication can bring benefits to the end user, the operator and the OTT application provider.
- It can also create business opportunities as value-added services to both mobile network operators and OTT application providers.
- A potential solution based on GBA is also presented.

Thank you

www.huawei.com

Copyright©2011 Huawei Technologies Co., Ltd. All Rights Reserved.
The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.