Breaking Cell Phone Authentication: Vulnerabilities in AKA, IMS, and Android



Berkeley
UNIVERSITY OF CALIFORNIA

Jethro G. Beekman ←
Christopher Thompson

{jbeekman@eecs,cthompson@cs}.berkeley.edu

7th USENIX WORKSHOP ON OFFENSIVE TECHNOLOGIES

AUGUST 13, 2013

New phone, now what?



Hack it.

Outline

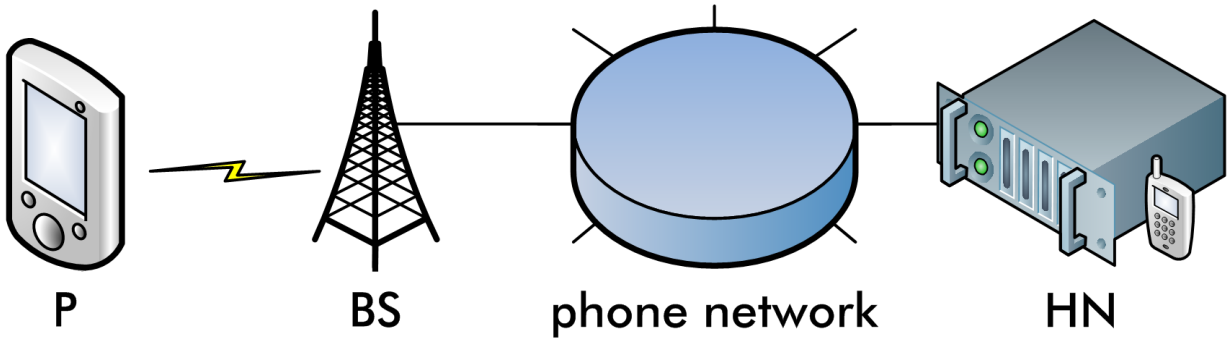
- Introduction
- Background
- Attack vectors
- Solutions
- Conclusion

Background

Authentication and Key Agreement
IP Multimedia Subsystem

- Introduction
- **Background**
- Attack vectors
- Solutions
- Conclusion

Authentication and Key Agreement[1]



identity →

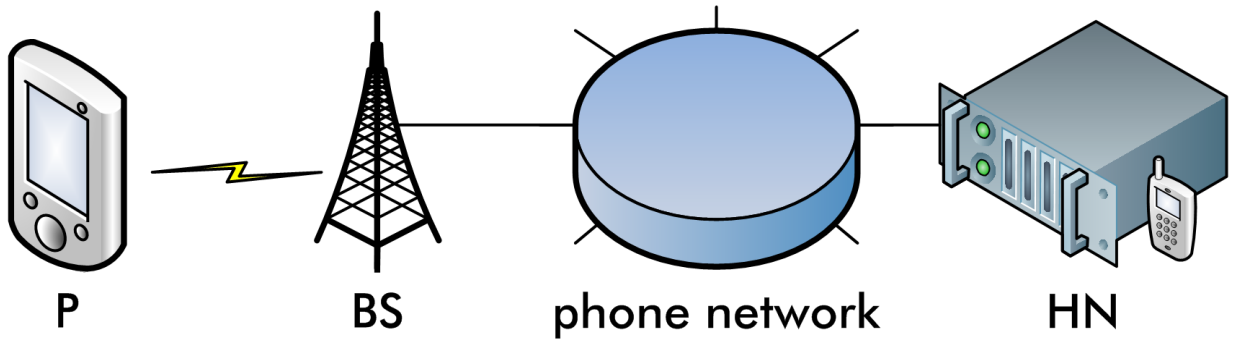
RAND,sequence#,MAC_{K1}(rand,sequence#) ←

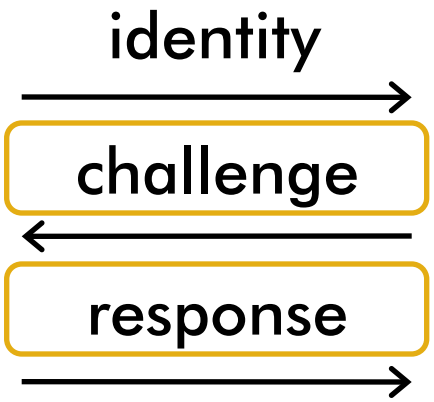
MAC_{K2}(RAND) →

$CK = MAC_{K3}(RAND)$
$IK = MAC_{K4}(RAND)$

[1] 3GPP TS 33.102

Authentication and Key Agreement[1]



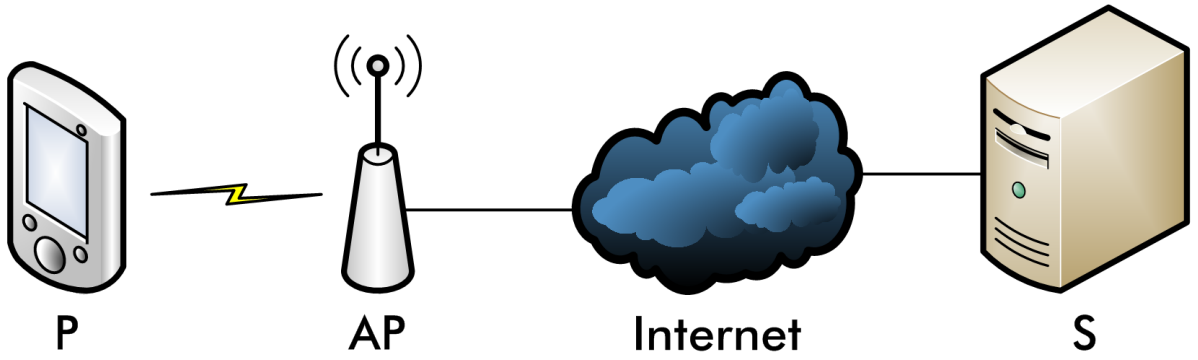


$CK = MAC_{K3}(RAND)$
$IK = MAC_{K4}(RAND)$

[1] 3GPP TS 33.102

IP Multimedia Subsystem

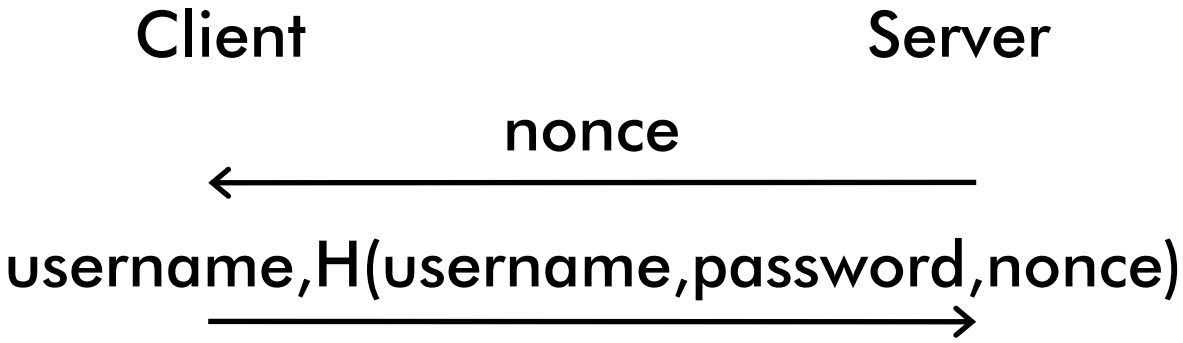
- Telephony using Internet standards



- SIP, TLS, etc.
- Digest Authentication (as in HTTP)

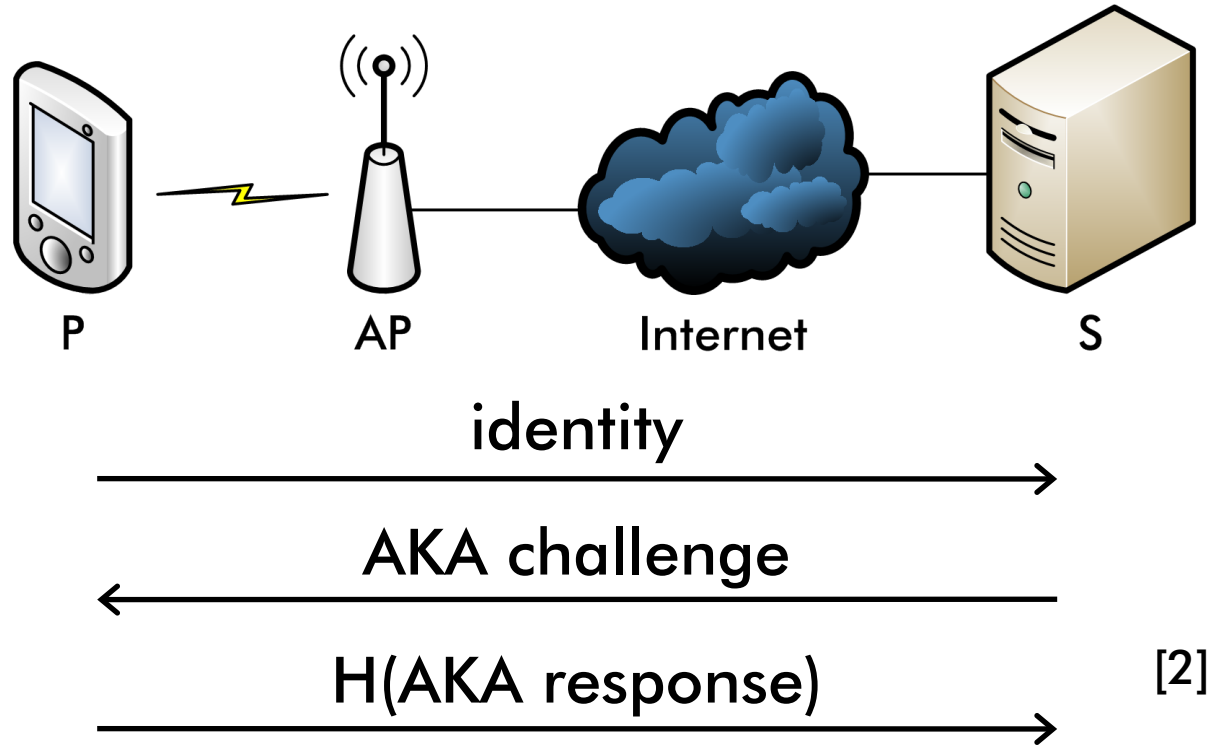
Digest Authentication (HTTP)

- Challenge-response protocol designed to not send HTTP passwords in the clear



Digest AKA[2]

- Overload nonce as AKA "challenge"
- Overload password as AKA "response"

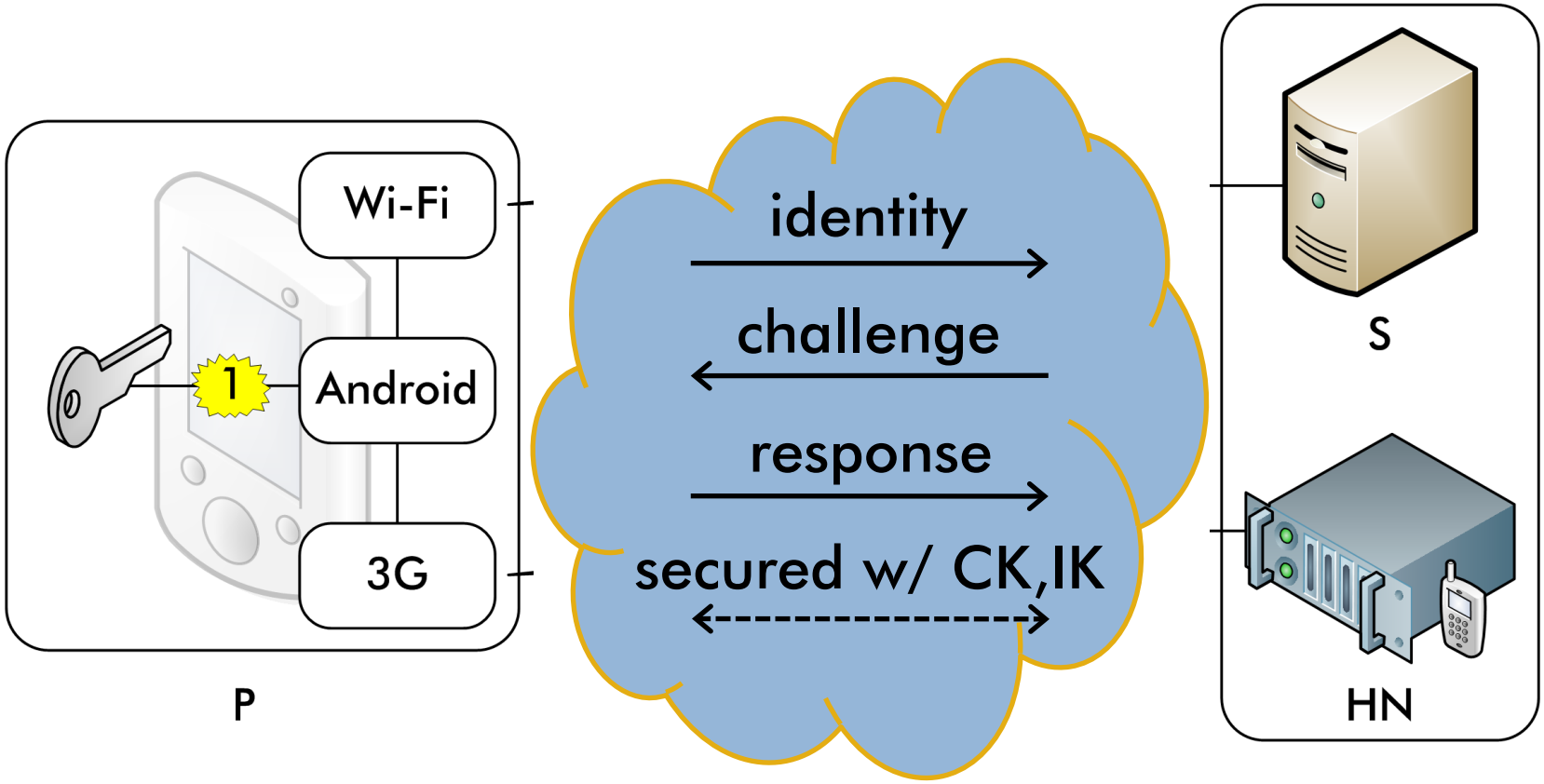


[2] RFC 3310

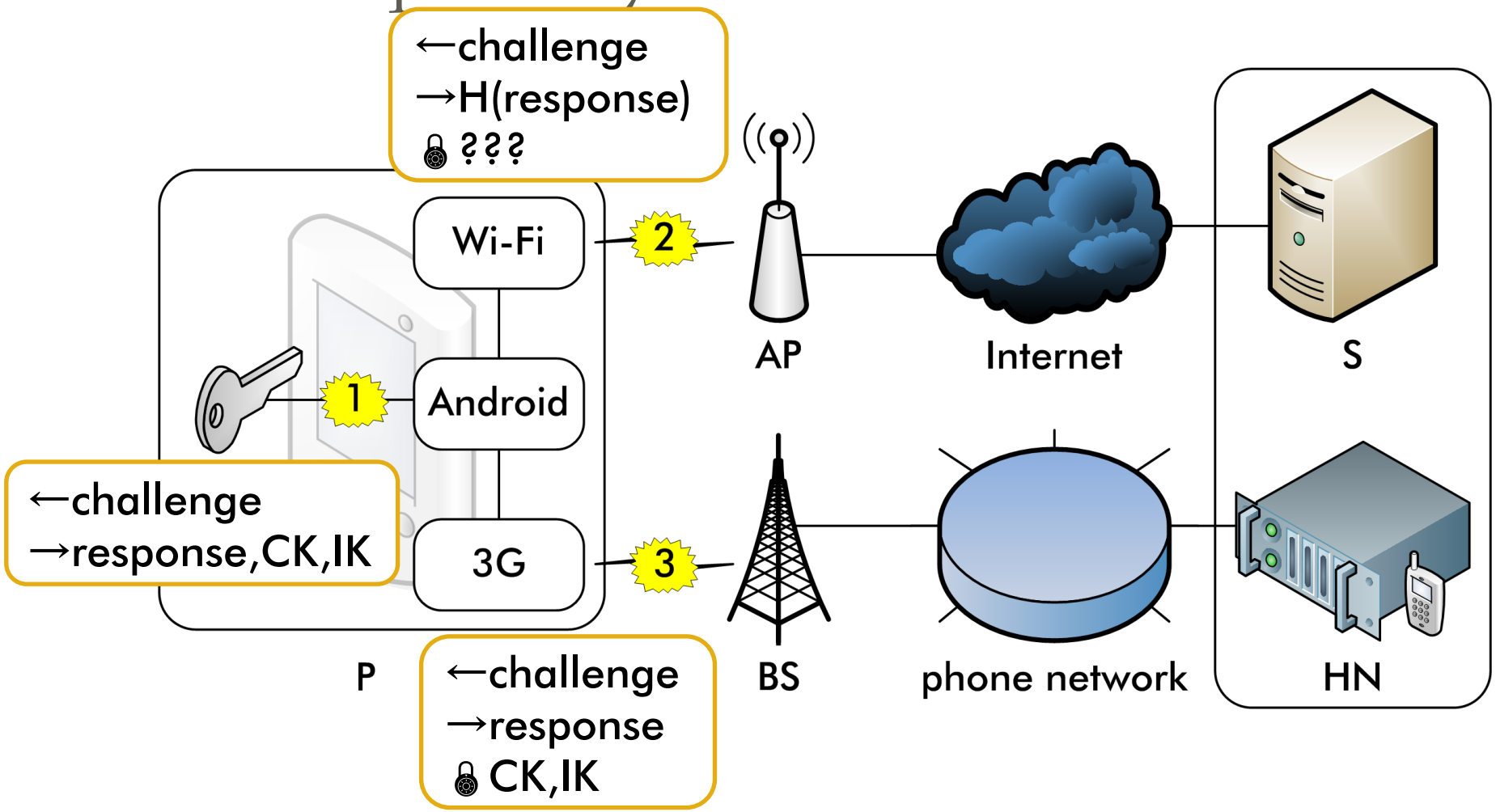
Attack vectors

- Introduction
- Background
- Attack vectors
- Solutions
- Conclusion

The complete system



The complete system redux



Digest AKA is not enough!

- RFC about Confidentiality and Integrity keys:

  "[…] this document does not specify the use of these additional keys, they may be used for […] additional security [with some undefined] security mechanism."

- "Additional security"?

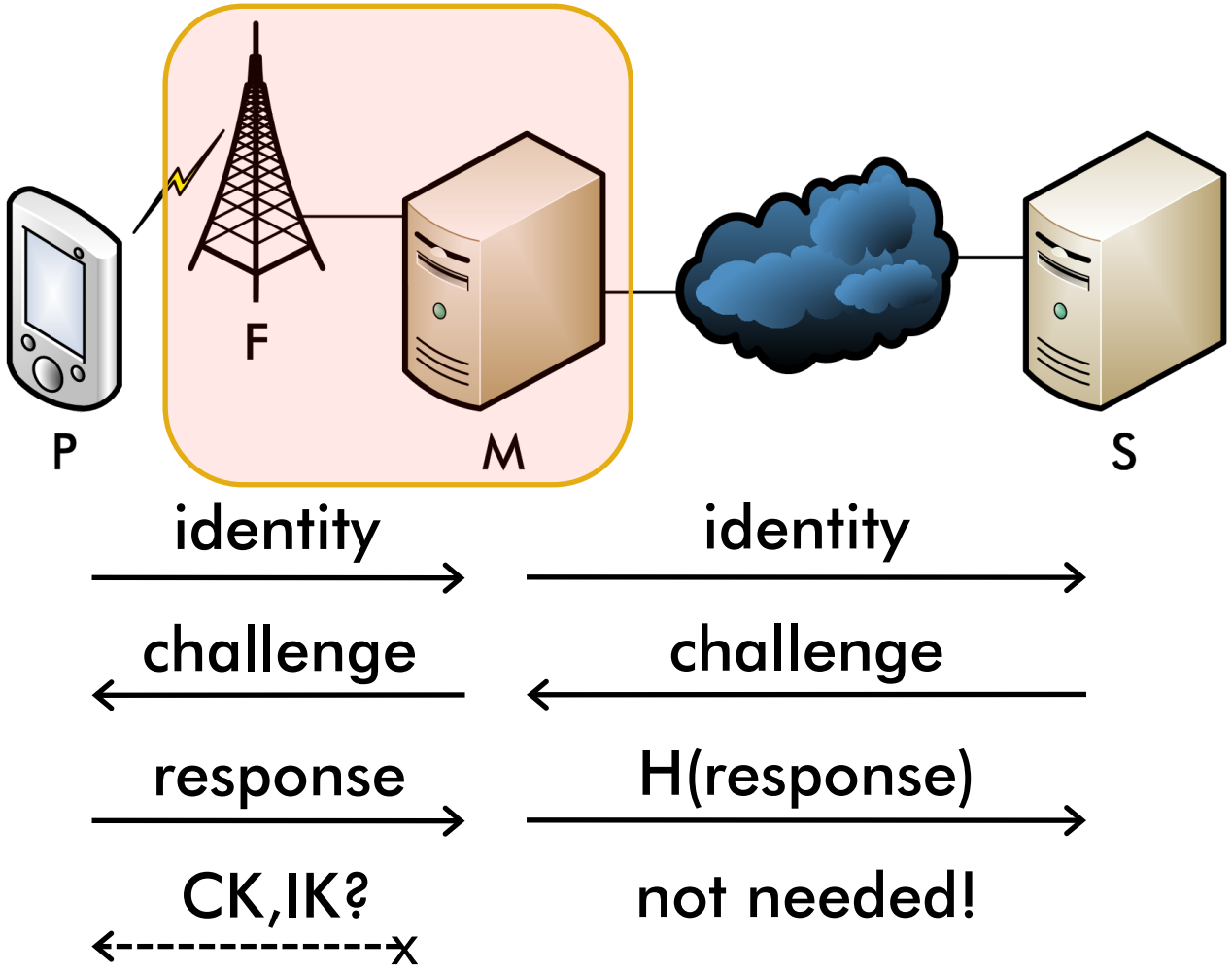
  Without CK/IK, you get *no* security!

SIPS (TLS)

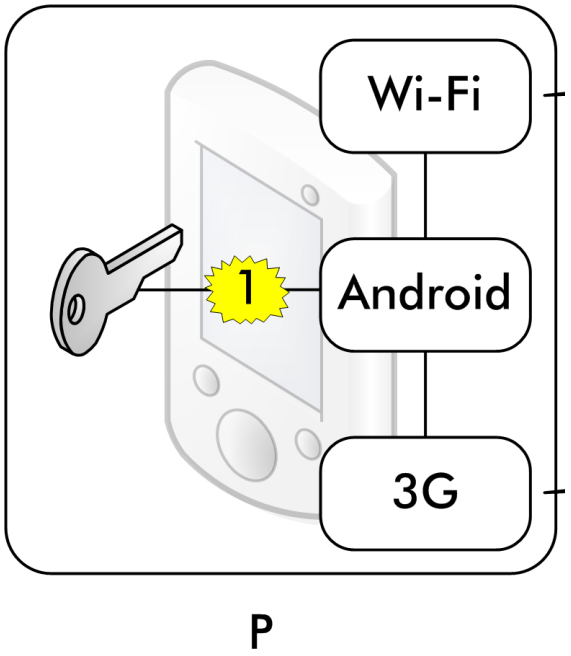
- What if channel security depends on TLS?
- Example: T-Mobile Wi-Fi Calling
  - SIP server cert chain root not standard…
  - …and not included in app → classic MITM
  - Android apps commonly flunk TLS security[3]

[3] Fahl et al., ACM CCS 2012

False base station attack

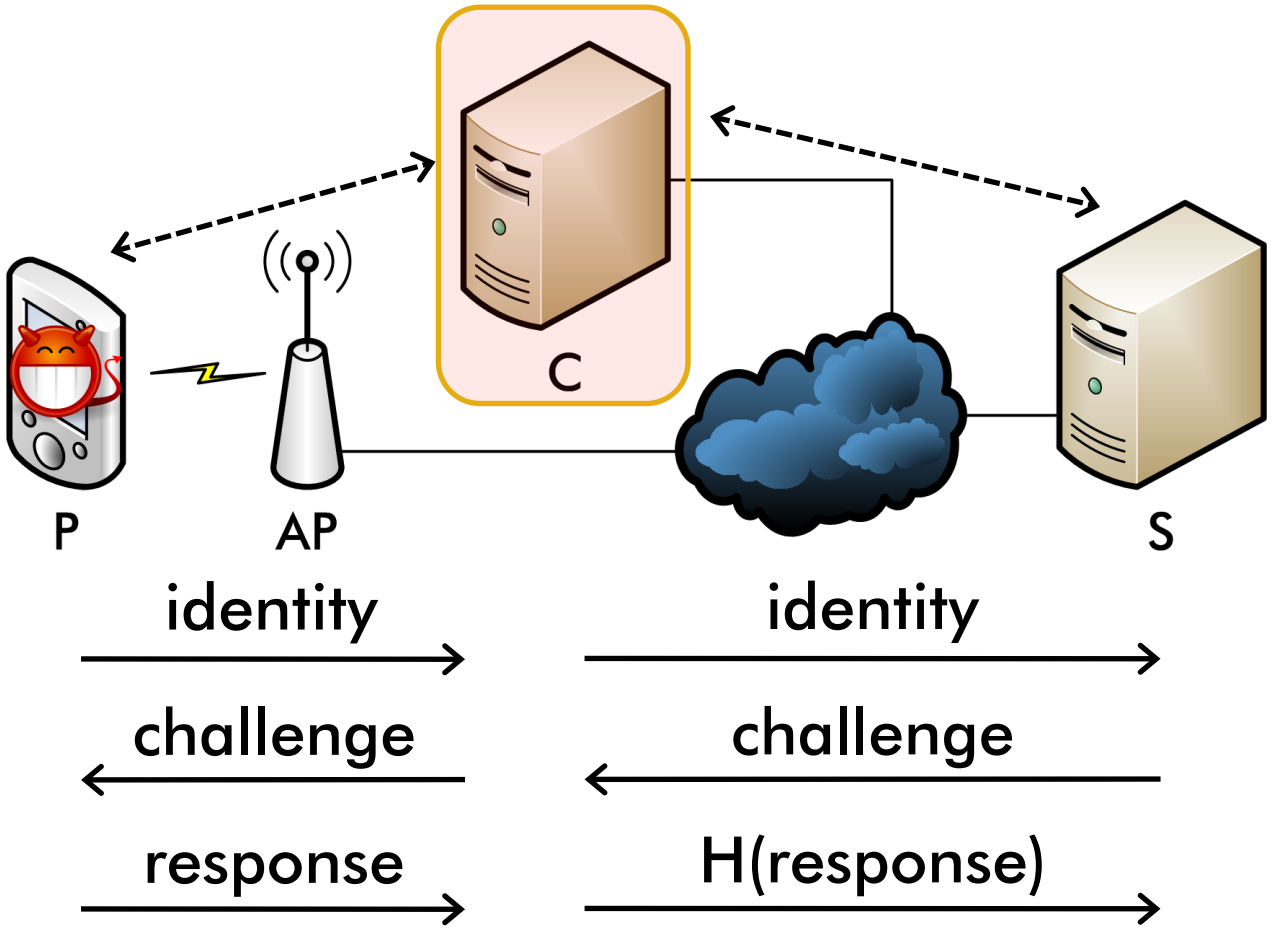


Android SIM card interface

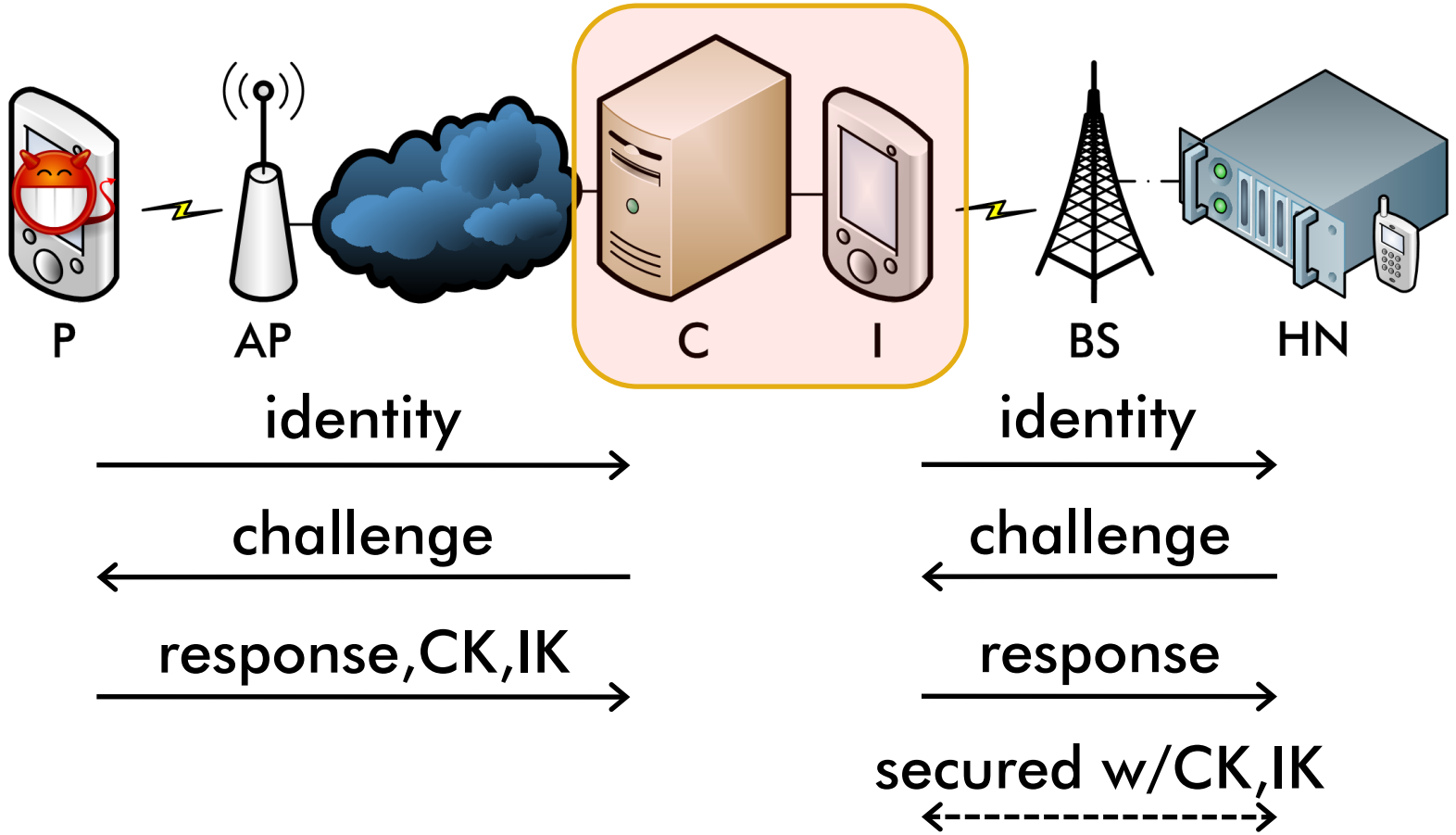


- requestIsimAuthentication
  - ←challenge
  - →response,CK,IK

Malware attack



Imposter attack



requestIsimAuthentication permissions

- READ_PHONE_STATE

  PHONE CALLS *Read phone state and identity*

  Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.

  – ⅓ of apps request this[4]

[4] Felt et al., USENIX WebApps 2011

Impact

- Classic MITM attack
  - T-Mobile customers with Wi-Fi Calling (before update)
- Fake base station attack
  - 3G/IMS providers that use AKAv1
- Malware attack
  - 3G/IMS providers with Android 4.0+ customers
- Imposter attack
  - 3G providers with Android 4.0+ customers

Solutions

- Introduction
- Background
- Attack vectors
- Solutions
- Conclusion

T-Mobile Wi-Fi Calling
(Classic MITM attack)

- TLS problems[5] reported December 2012
- Fixed (OTA update) March 2013
  - Fix looks ok

[5] Beekman, Thompson, UCB/EECS-2013-18

Digest AKAv1

(False base station attack)

- Confidentiality and Integrity keys MUST be used
  - e.g. TLS renegotiation with pre-shared key
- AKAv2[6] uses CK,IK in hash
  - IMS specifies use of AKAv1[7]
  - TLS and Digest AKAv2 should suffice if server is authenticated another way
  - Does not protect against malware attacks

[6] RFC 4169
[7] 3GPP TS 33.203

requestIsimAuthentication

(Malware and Imposter attacks)

- API should not be accessible
- At least require appropriate permissions
  - e.g. "Services that cost you money"
- Reported to Google June 2013
  - Current status unknown

Conclusion

4 attacks
- 3 implementation errors
- 1 cross-protocol issue

4 solutions

- Introduction
- Background
- Attack vectors
- Solutions
- Conclusion

Breaking Cell Phone Authentication: Vulnerabilities in AKA, IMS, and Android



Berkeley
UNIVERSITY OF CALIFORNIA

Jethro G. Beekman ←
Christopher Thompson

{jbeekman@eecs,cthompson@cs}.berkeley.edu

7th USENIX WORKSHOP ON OFFENSIVE TECHNOLOGIES

AUGUST 13, 2013