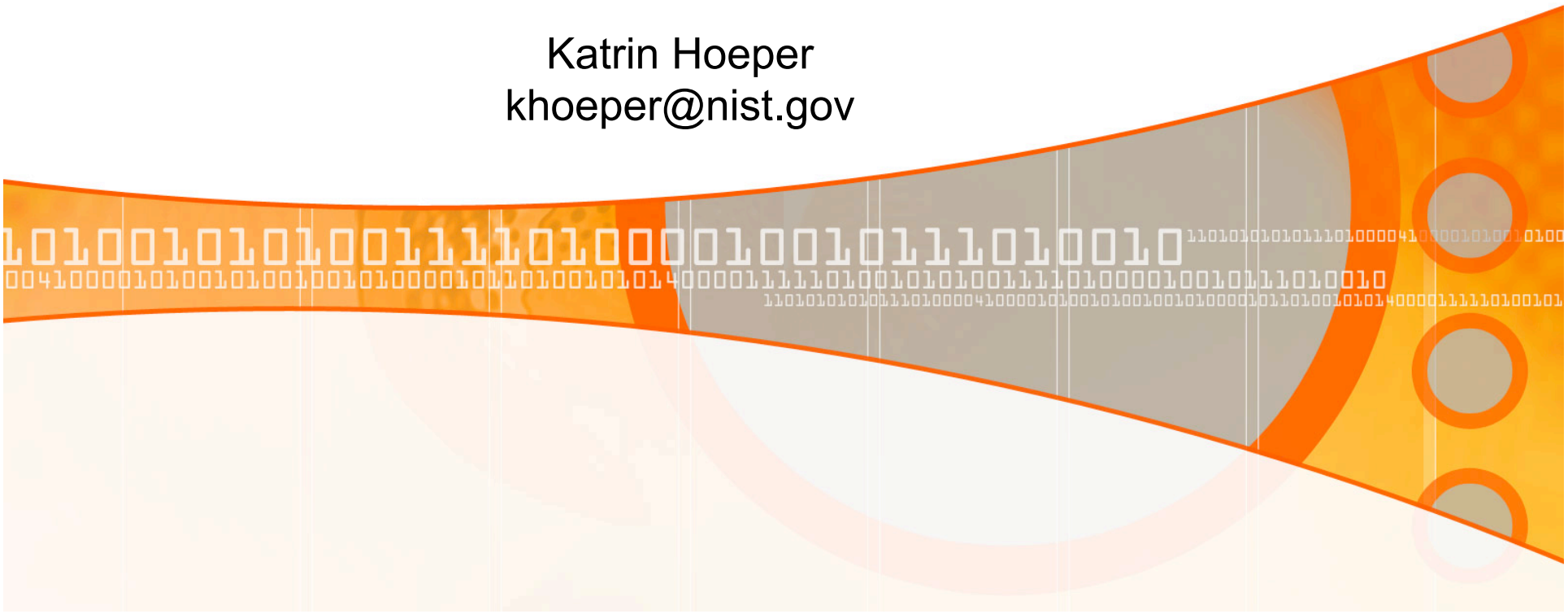
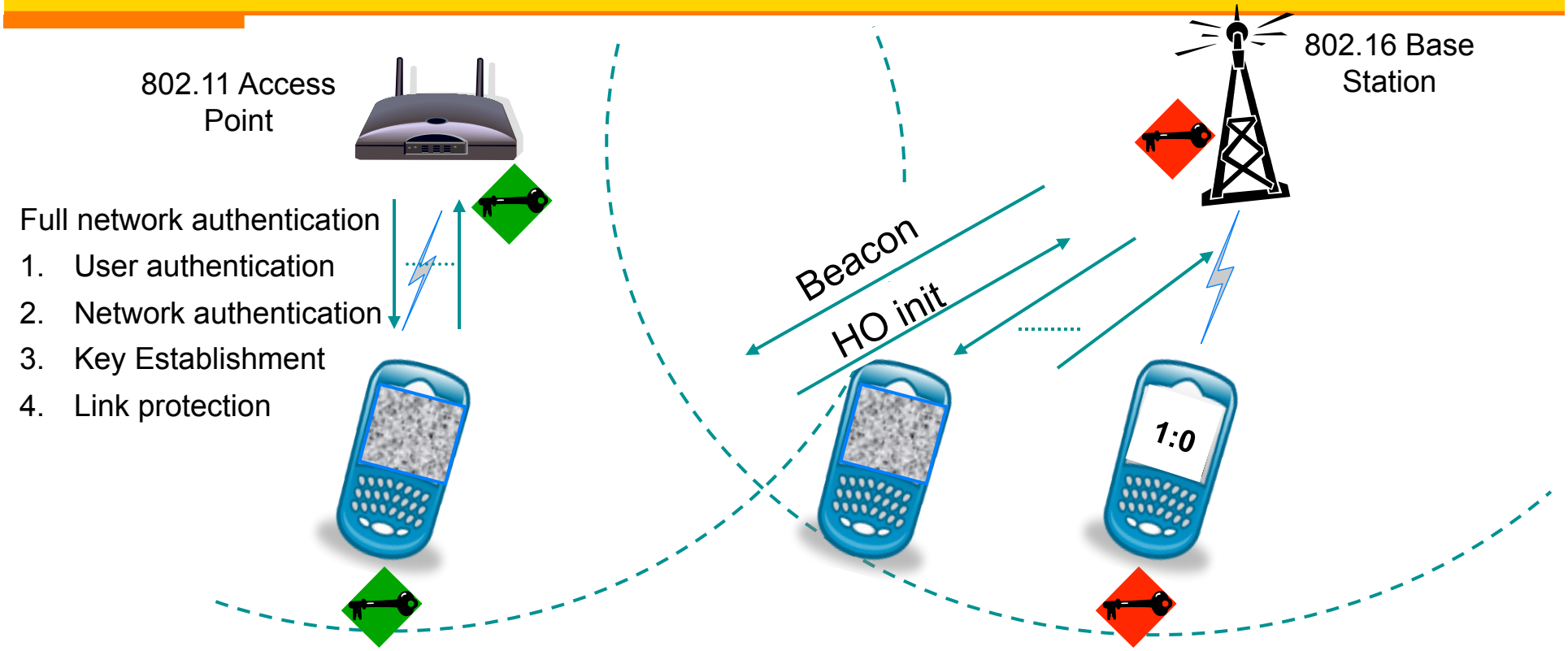
NIST
National Institute of Standards and Technology

Challenges in Key Management for Seamless Mobility

Katrin Hoeper
khoeper@nist.gov

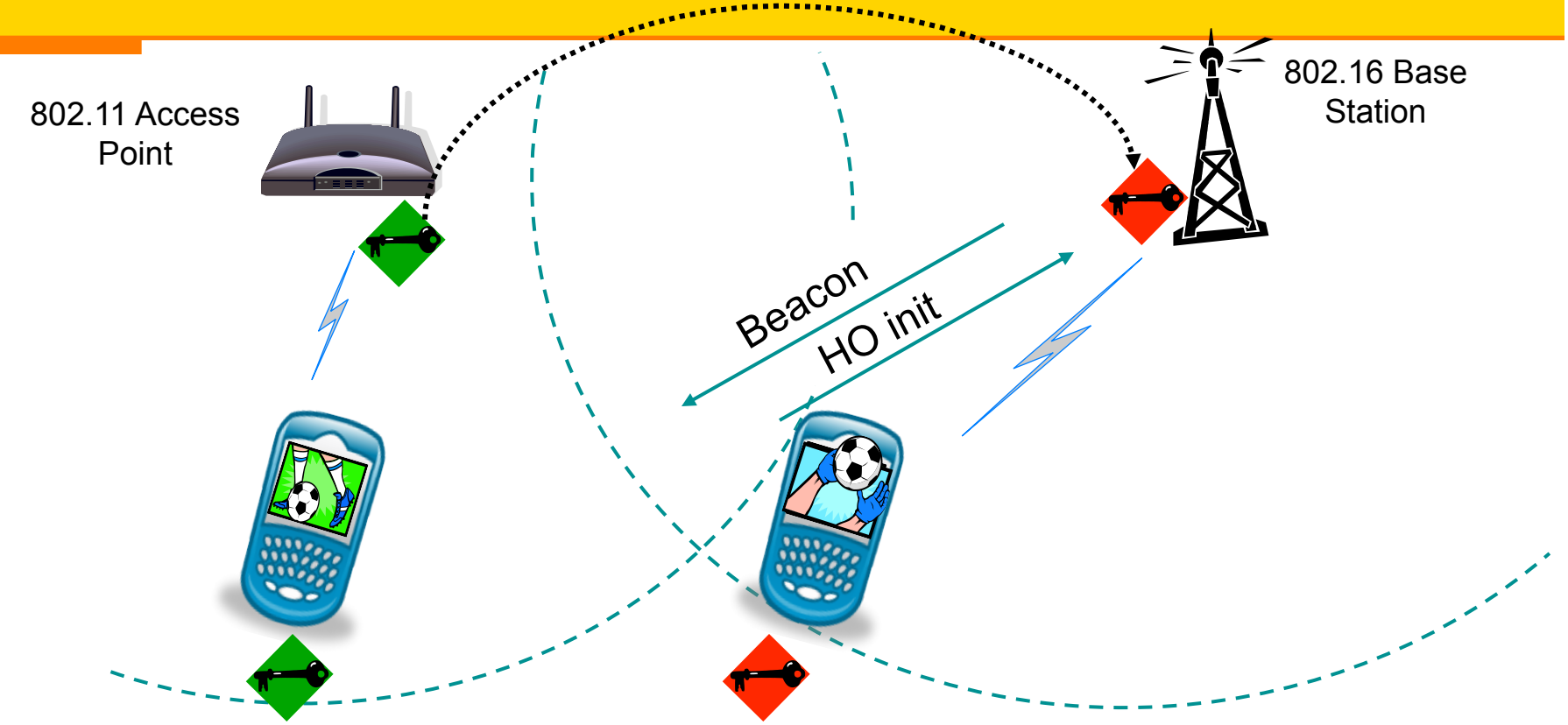


Roaming in Heterogeneous Networks



- (Secure) network entry has large computation and communication overhead
  - likely to lead to service disruptions

Seamless Handovers



- Seamless handovers demand key management solutions that enable expedited network entry

Seamless Mobility

- Goals
  - improve network accessibility and QoS while maintaining connectivity during roaming

1. Roaming in heterogeneous networks
   - e.g.: IEEE 802.11, IEEE 802.16, 3GPP
2. Handover without disconnection
   - timely initiation of handover (HO)
   - expedited network access

Approaches

- Full network authentication
  - too slow!
- Pre-authentication
  - full network authentication executed ahead of time through serving network
  - requires smart triggers and network information
- Re-authentication
  - re-uses keying material from full network authentication for expedited authentication and HO key derivation
  - computationally most efficient
  - requires HO key management

HO Scenarios

	Intra-domain (PoAs operated by one provider)	**Inter-domain** w/ roaming agreements (PoAs operated by different providers)	**Inter-domain** w/ o roaming agreements (PoAs operated by different providers)
Intra-technology (e.g. IEEE 802.11 → IEEE 802.11)	Re-authentication	Re-authentication	Pre-authentication
Inter-technology (e.g. IEEE 802.11 → IEEE 802.16)	Re-authentication	Re-authentication	Pre-authentication

Existing Work

- Each wireless technology
  - specifies HO key hierarchy for intra-technology & intra-domain HOs
- IETF HOKEY WG
  - specifies HO key hierarchy and re-authentication for EAP-based technologies
  - key distribution protocol and pre-authentication are work in progress
- IEEE 802.21 SSG
  - enable secure HO and interoperability between heterogeneous network types including both 802 and non-802 networks
  - draws from HOKEY: pre- and re-authentication work in progress

Key Management Challenges

1. Key distribution infrastructure
2. Secure re-use of keying material
3. Key update and synchronization
4. Trust models and server-centric trust

1. Key Distribution Infrastructure

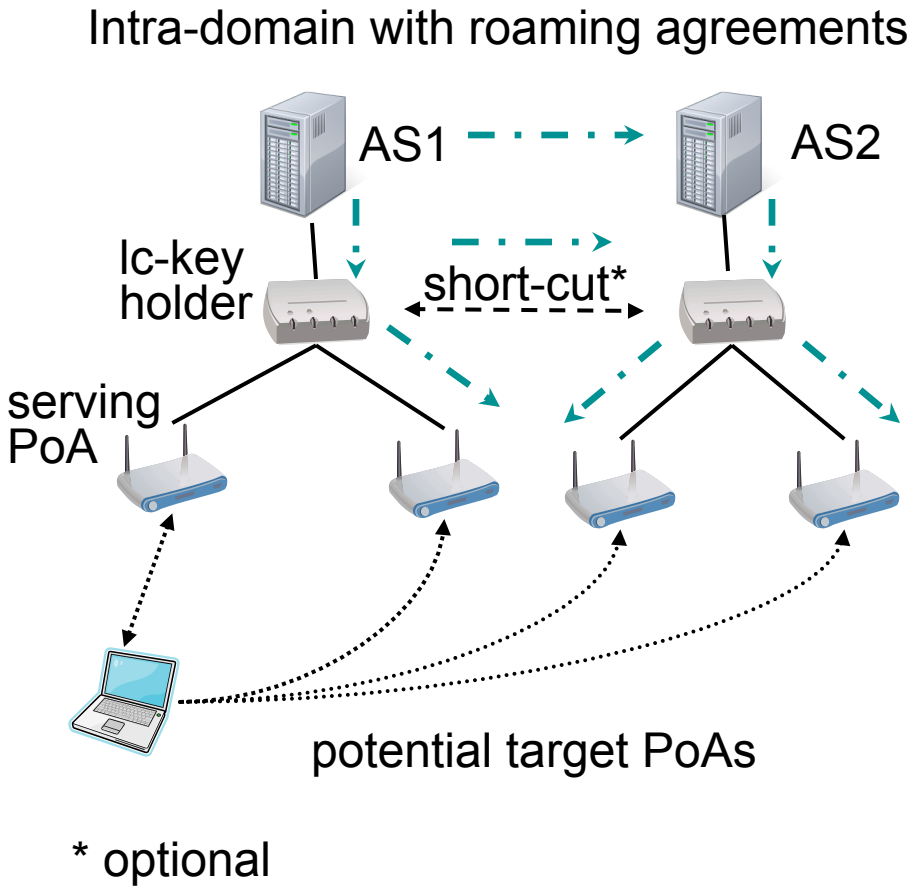
- What triggers the key distribution?
  - roaming or network information necessary for timely distribution
- Who distributes the keys?
  - key-distributor must receive trigger, derive keys and distribute them to target network
- How are keys distributed?
  - protocols must be efficient in terms of preparation & execution time as well as traffic & computation overhead

Triggers

	Roaming-specific	**Periodical distribution**	**Event-based**
What triggers key distribution?	signal strength, SNR, PoAs in range, etc..	every ΔT	e.g. after every successful node authentication
Who triggers key distribution?	mobile user, in special cases serving network	serving network	serving network
Who receives keys?	target PoA(s) (on-demand)	any potential PoA (pro-active)	any potential PoA (pro-active)

Key Distribution Approaches

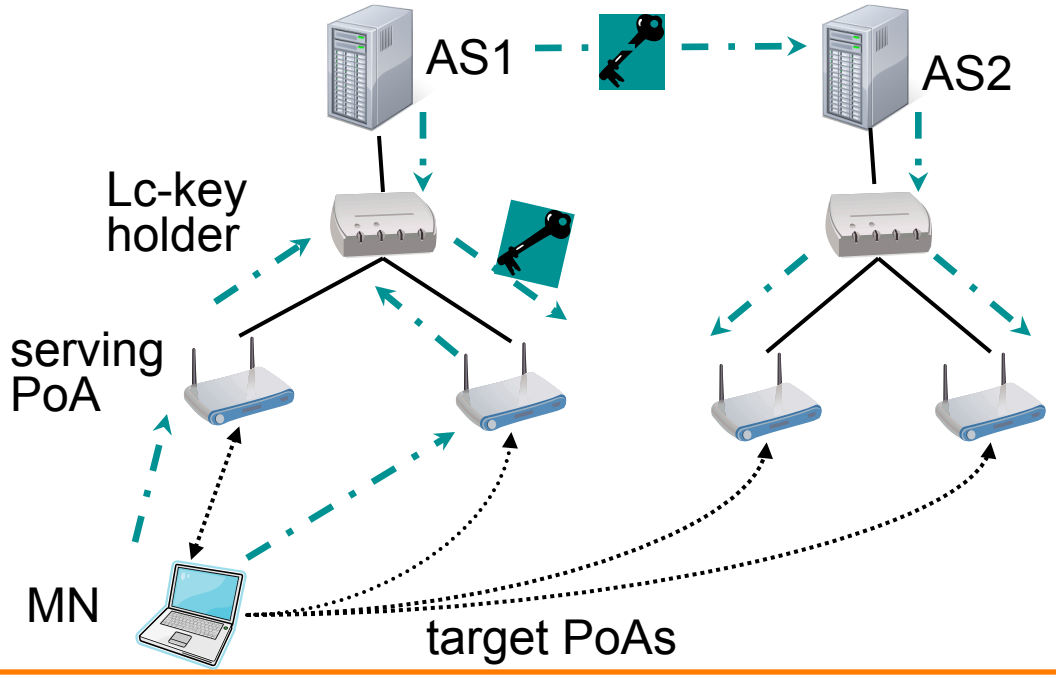
- Key distributors
  1. serving AS
  2. lowest common key holder (lc-key holder)
  3. lowest key holder with short cut to target network



⇒only AS can serve as key distributor in all HO scenarios

Key Distribution Protocols

- Pull protocol
  - on-demand distribution
  - triggered by node through
    a) serving link
    b) target link
- Push protocol
  - pro-active distribution by serving AS
  - triggered periodically or event



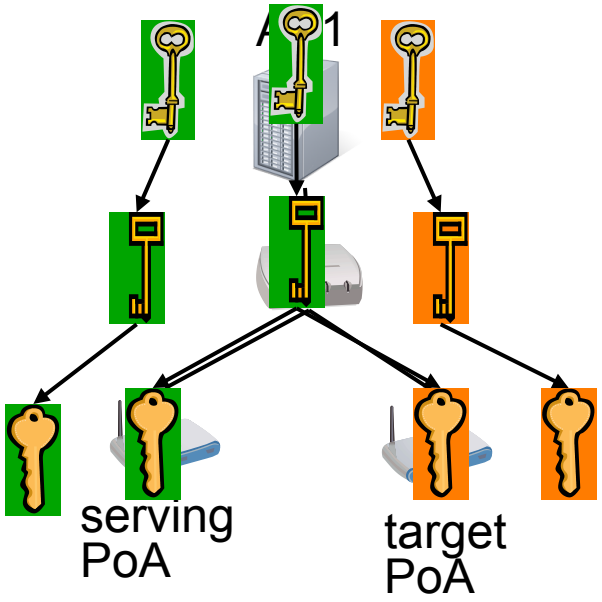
2. Secure Re-use of Keying Material

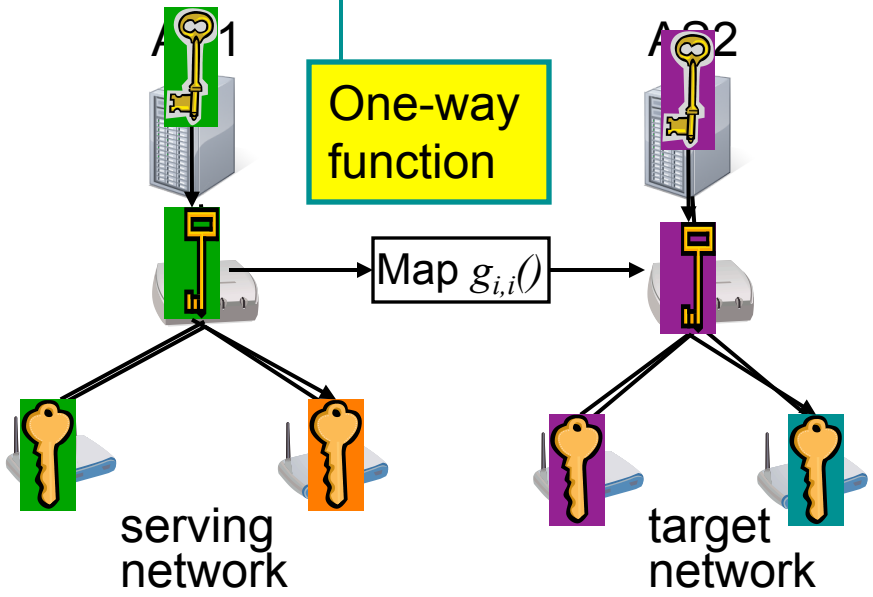
- Which keying material can be re-used?
  - set of key holders in inter domains disjoint
  - key hierarchies may differ in inter-technology HOs
    - # of keys, key holder roles, key entropy, key lifetime ...
- How are keys re-used to derive HO keys?
  - key derivation must be efficient, maintain security level and prevent replay attacks

Intra-technology HO

- Similarities in serving and target networks
  - # of key holder levels, roles and key properties the same
  - intra domain solution: merge hierarchies in lowest common key LcK
  - inter domain solution: apply mapping function
  - $=g_{i,i}($, $info)$

To prevent replay attacks

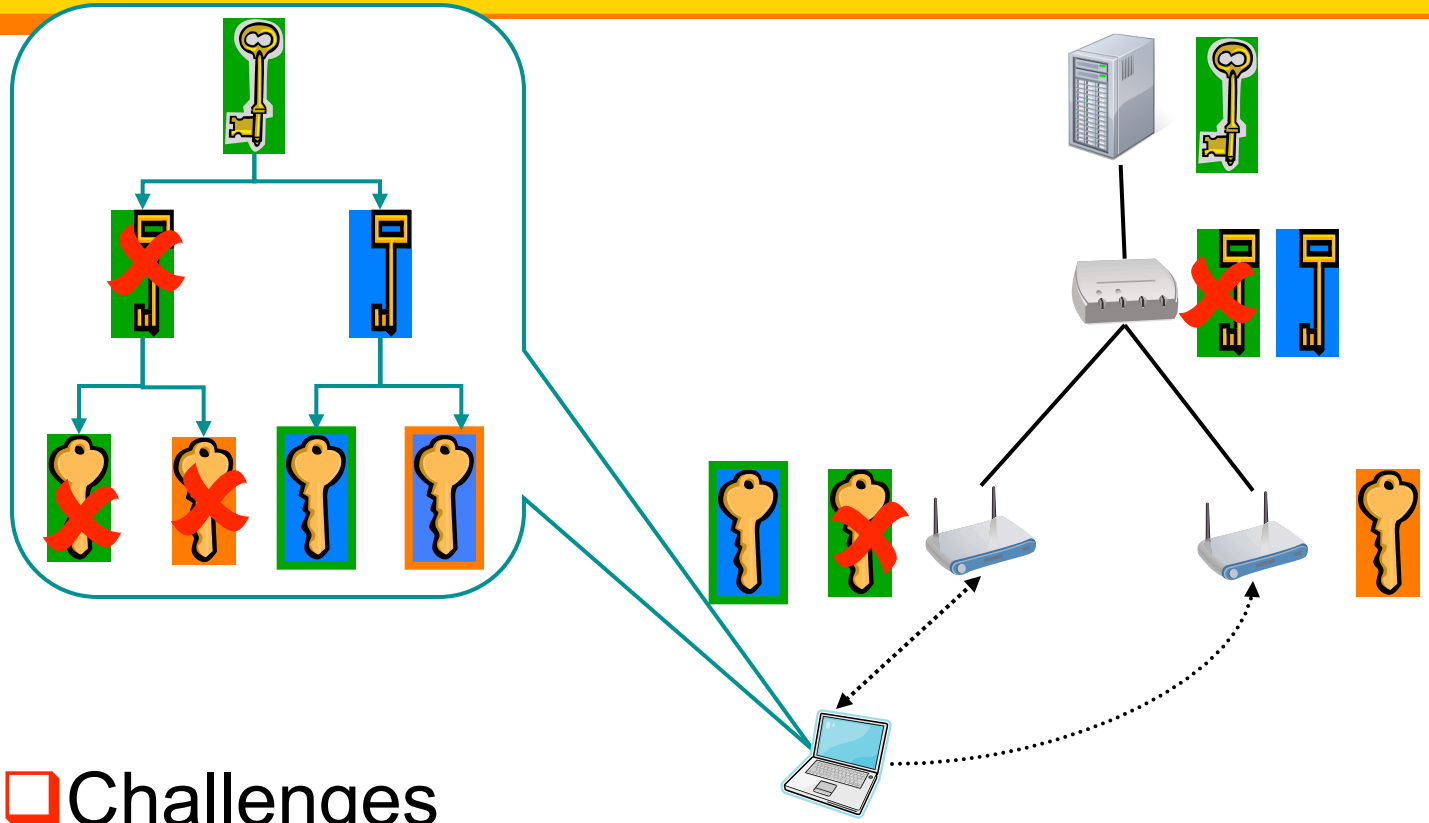




Inter-technology HO

- Technologies have common key in their hierarchies
  - use merging method
  - e.g. IEEE 802.11i and 802.16e both utilize EAP
- Technologies have no common key
  - use mapping method, where  $= g_{i,j}($  , $info_T)$ must satisfy
    - mapping function $g_{i,j}()$ is one-way
    - $info_T$ as defined in target wireless technology; also prevents replay attacks
    -  has at least security strength required by 
  - requires mapping function $g_{i,j}()$ for each technology pair and direction

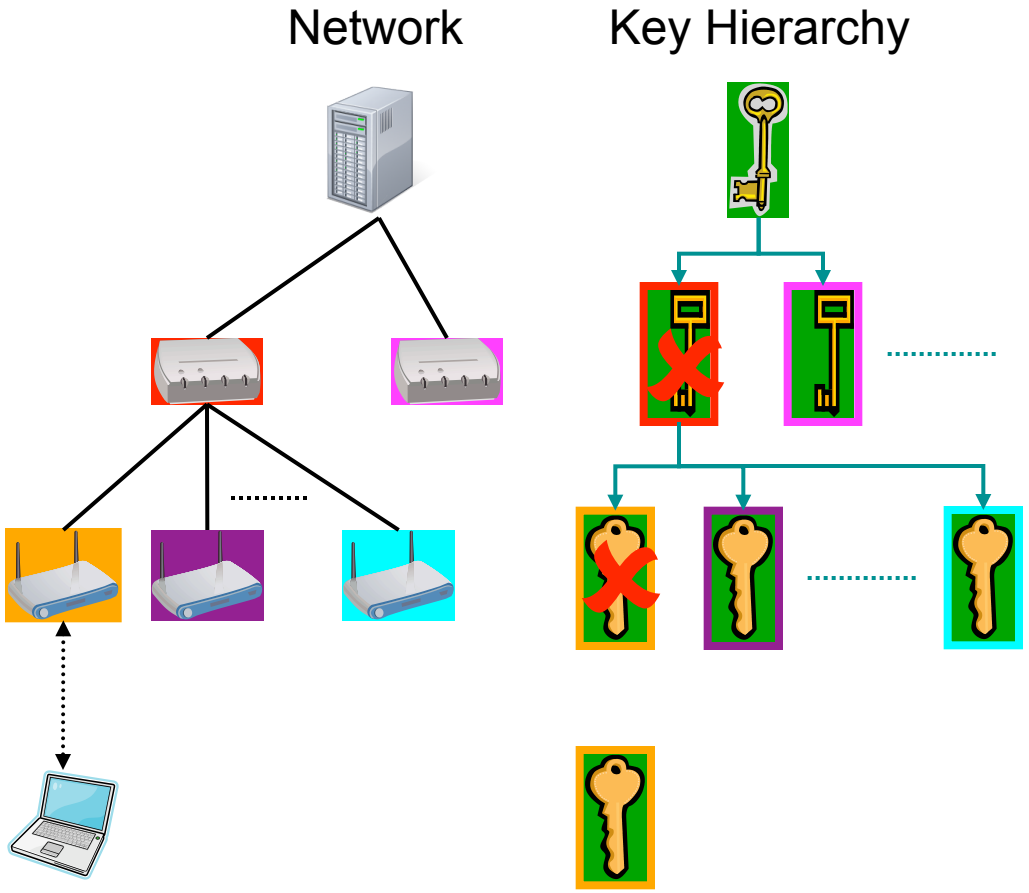
3. Key Update and Synchronization



- Challenges
  - how can key updates be synchronized across network(s) and mobile nodes?
  - who can execute key updates?

Key Update

- To ensure network-wide synchrony
  - the serving AS should update keys
  - in the special case that only transient keys (PTK) are compromised, the serving PoA may derive new transient keys



Key Update Computation

- Key updates must use a one-way function with the following inputs
  - an uncompromised key from a higher level
  - time-variant information for replay prevention, e.g.
    - sequence numbers (devices need to keep track)
    - timestamps (requires synchronization)
    - nonces (require 4-way handshake for exchange)

4. Trust Models & Server-Centric Trust

- Problem: no homogenous trust model across all non-cellular wireless access technologies
  - keys are not shared among PoAs
  - .11 AP not physically protected as .16 BS
  - trust comparison of key holders in different branches or networks difficult
  - often authentication server anchor of trust

Performance vs. Security

- Minimizing AS involvement reduces delays in HO
  - utilize LcK-holder or short-cut endpoints for efficient key distribution
- Only serving AS can enable certain security features
  - synchronized key distributions & updates in any HO
  - sequence number verifications
  - channel bindings to bind keys to identifiers of all intermediate key holders

Performance vs. Security (cont'd)

- Push protocols
  - large traffic overheads with redundant key distributions
  - easy key synchronization
  - only costs in preparation time, in subsequent HOs keys already in place
- Pull protocols
  - reduce overhead & redundancy, but executed for each HO
  - smallest overhead through target network, but requires MN to be connected to serving and target PoA
  - on-demand required to enable certain security properties
    - replay prevention, channel bindings, etc

Conclusions

- Analysis suggests maintaining certain security properties requires AS to act as key distributor using pull protocols
- More efficient solutions are feasible if some security properties can be compromised
- Wireless technologies deriving EAP keying material best candidates due to possible key hierarchy mergers

Thank you!

- Questions?
  - katrin.hoeper@nist.gov