Augmented SEND: Aligning Security, Privacy, and Usability

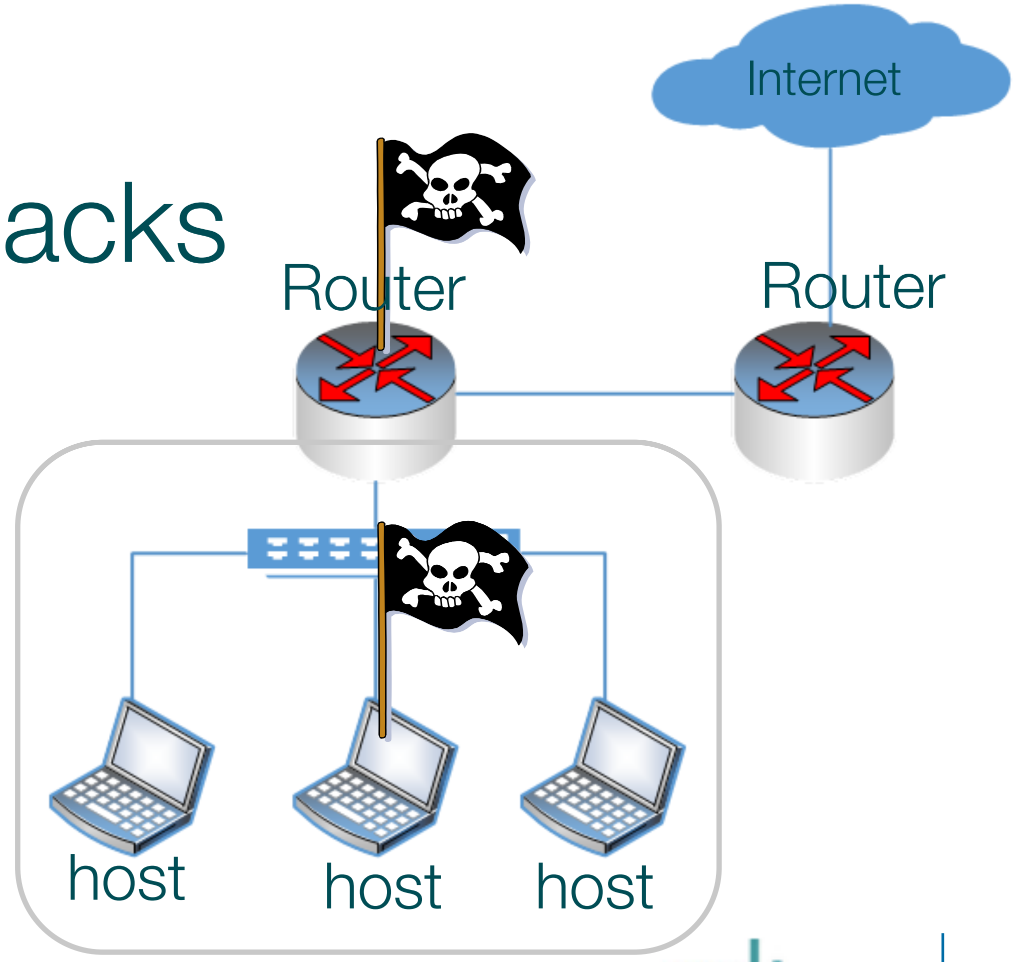
Dr. Ahmad Alsadeh
Birzeit University
Palestine

Neighbor Discovery Protocol (NDP)

- Fundamental protocol in IPv6 suite
  - Obtain configuration information
  - Determine when a neighbor is no longer reachable
  - Perform address resolution
- Local link protocol (subnet scope)
- Basic shield is not enough
  - NDP can suffer similar problems of ARP Spoofing
- IETF
  - RFC 4861 and RFC 4862 known as Neighbor Discovery Protocol (NDP)

Neighbor Discovery Protocol (NDP)

- NDP messages lack authentication
- Attacks might come from malicious
  - host
  - router
- NDP is vulnerable to many attacks
  - Spoofing
  - Replay
  - Rogue router



NDP Vulnerabilities (continue …)

- IETF efforts:
  - RFC 3756: IPv6 Neighbor Discovery (ND) Trust Models and Threats
  - RFC 3971: SEcure Neighbor Discovery (SEND)
  - RFC 3972: Cryptographically Generated Addresses (CGA)
- NDP Hacking Tools
  - Parasite6
  - Alive6
  - fake_router6
  - detect-new-ip6
  - dos-new-ip6
  - flood_router6
  - fake_advertiser6
  - …

The Hacker's Choice

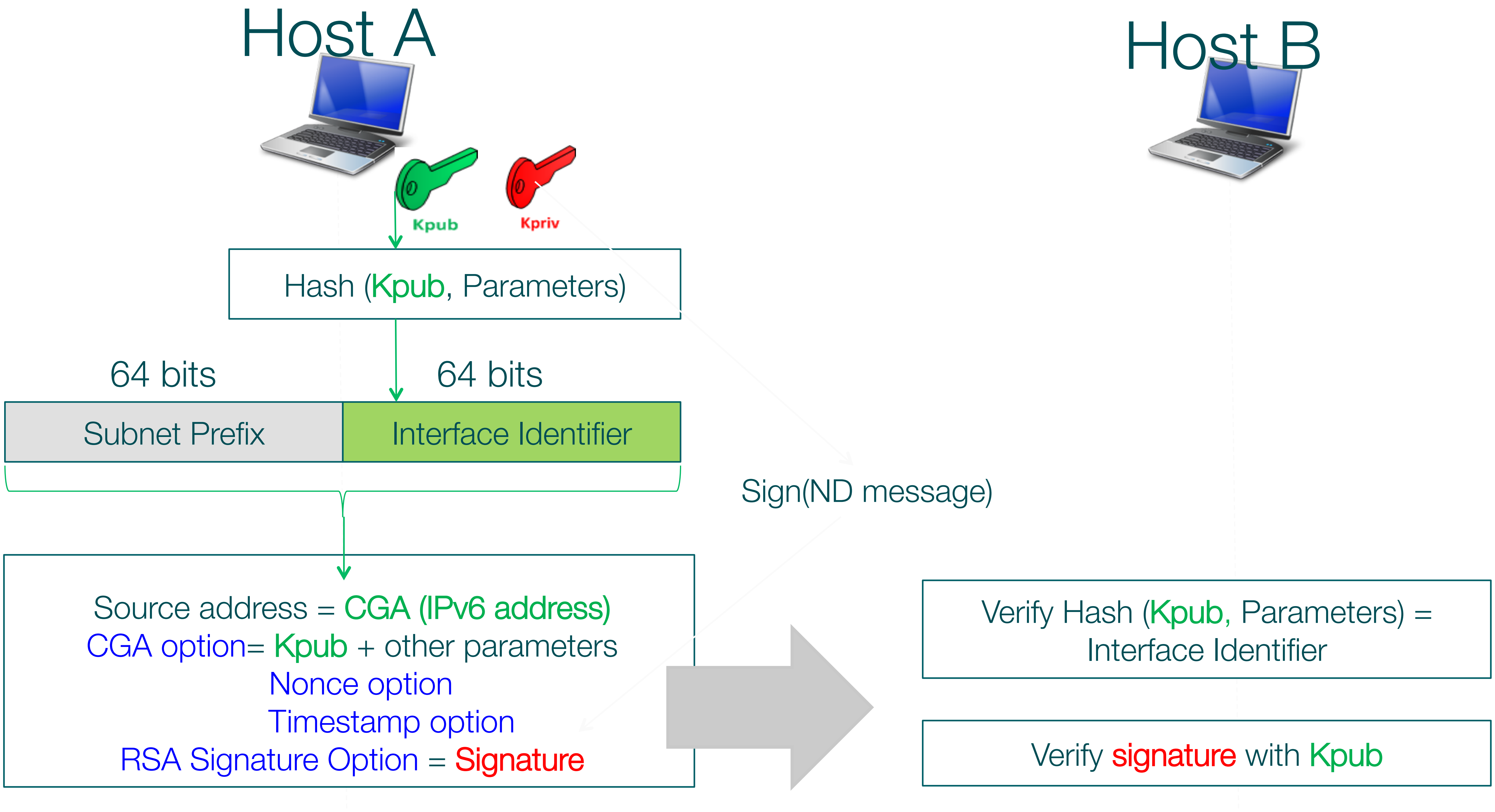
THC-IPV6 : Attack toolkit
http://www.thc.org/thc-ipv6/

RIPE

SEcure Neighbor Discovery (SEND)

- SEND is an integral part of NDP
- SEND offers three functionalities to NDP
  - Address Authentication (Address Ownership Proof)
  - Replay Protection
  - Authorization Delegation Discovery (ADD)

SEND (Simplified)



Hash (Kpub, Parameters)

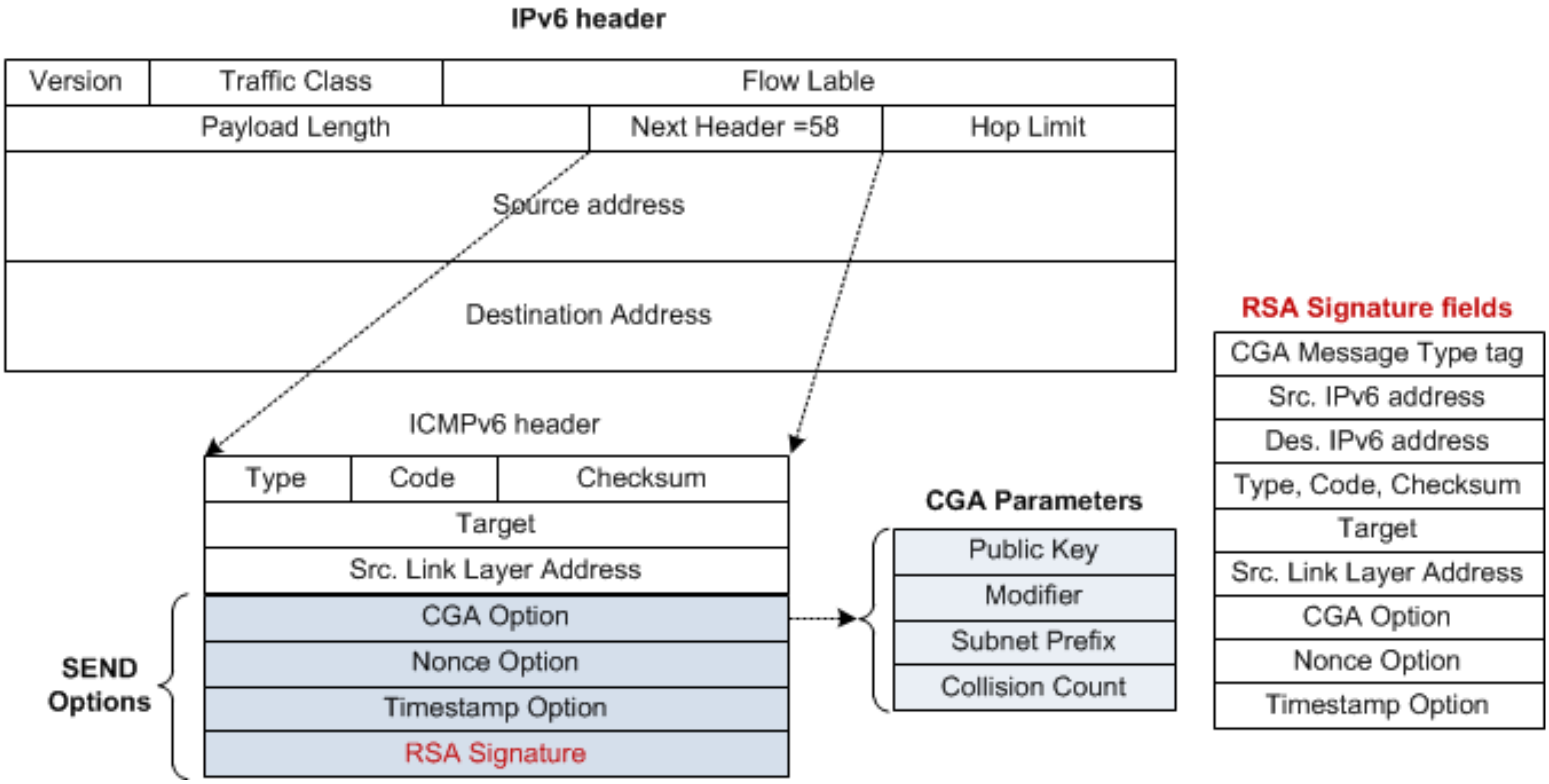
Source address = CGA (IPv6 address)
CGA option= Kpub + other parameters
Nonce option
Timestamp option
RSA Signature Option = Signature

Verify Hash (Kpub, Parameters) = Interface Identifier

Verify signature with Kpub

SEND options are sent with the NDP message

NDP Message Protected by SEND



IPv6 header

Version | Traffic Class | Flow Lable

Payload Length | Next Header =58 | Hop Limit

Source address

Destination Address

ICMPv6 header

Type | Code | Checksum

Target

Src. Link Layer Address

SEND Options

CGA Option

Nonce Option

Timestamp Option

RSA Signature

CGA Parameters

Public Key

Modifier

Subnet Prefix

Collision Count

RSA Signature fields

CGA Message Type tag

Src. IPv6 address

Des. IPv6 address

Type, Code, Checksum

Target

Src. Link Layer Address

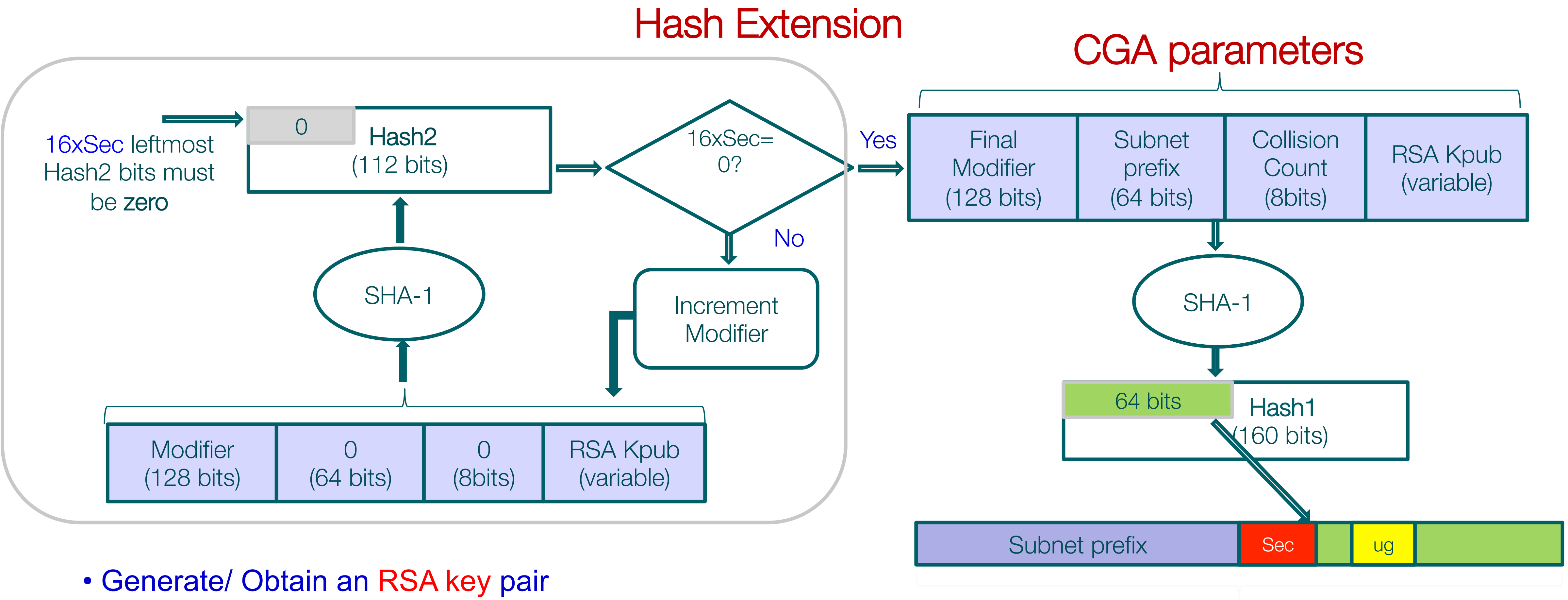
CGA Option

Nonce Option

Timestamp Option

RFC 3972: CGAs

- Address authentication (Address ownership proof)
- Sender’s public key is bounded to IPv6 address
- CGA generation algorithm



- Generate/ Obtain an RSA key pair
- Pick a random Modifier
- Select a Sec value
- Set Collision Count to 0

CGA

Check the uniqueness of IPv6 address (DAD)

Problem Statement

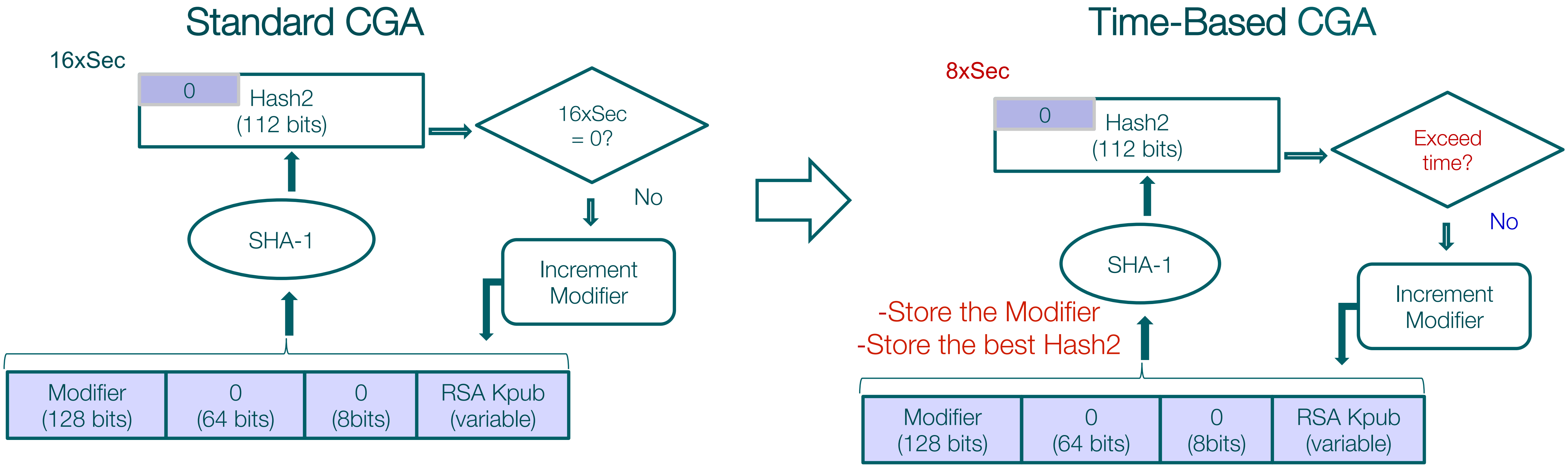
- There are several factors that limit SEND deployment
  - SEND is compute-intensive and bandwidth-consuming
  - SEND high time complexity may lead to privacy-related attacks
  - Router Authorization Delegation Discovery (ADD) mechanism is at initial stage
  - SEND has not mature implementation for end user operating systems
- Publication:
  - Ahmad AlSa'deh, Christoph Meinel, "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations," IEEE Security & Privacy, July-Aug. 2012.

WinSEND: Windows SEND

- It is the first SEND implementation for Windows
- Ahmad Alsadeh and Hosnieh Rafiee
  - Winners of the 1st place in the International IPv6 Application Contest 2011, German IPv6 Council, Germany

Time-Based CGA (TB-CGA)

- TB-CGA: Modifications to standard CGA
  - Select "time parameter" as an input
  - Keep track of the best found security level within determined time
  - Reduce the granularity of the security level from "16" to "8"



- Select a Sec

- Select a Time Parameter

Privacy Concerns

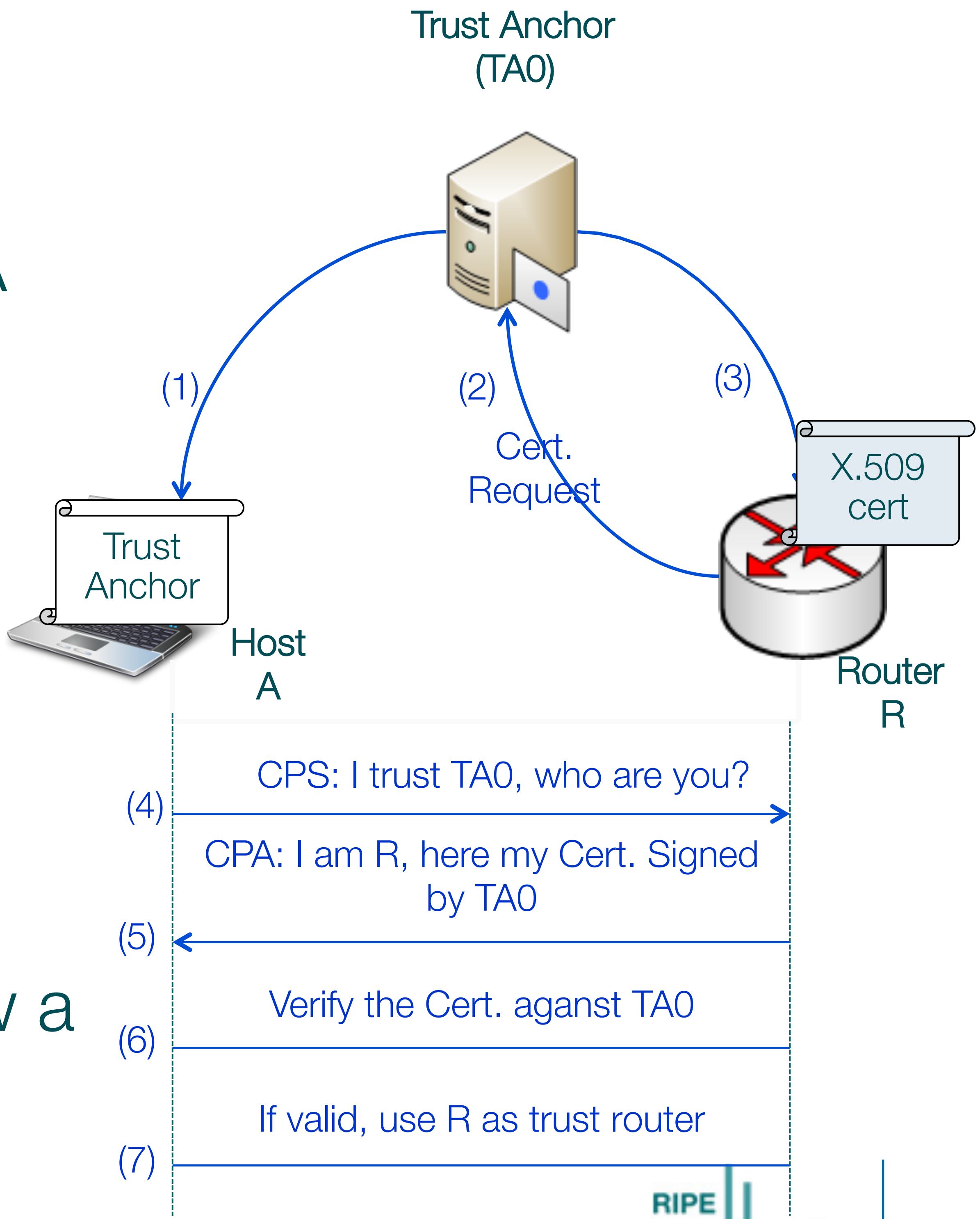
- High Sec value may cause unacceptable delay
- It is likely that once a host generates an acceptable CGA, it will continue to use
    - this same address
    - the same public key
- Hosts using CGAs could be susceptible to privacy related attacks

CGA Privacy Extensions

- Three main modifications
  - Setting a CGA Address lifetime
  - Reducing the granularity of CGA security levels
  - Automatic key pair generation

SEND Router Authorization (Simplified)

- Hosts provisioned with trust anchor(s) (TA)
- Router has certificates from a TA
- Two ICMPv6 messages
  - Certificate Path Solicitation (CPS)
  - Certificate Path Advertisement (CPA)
- Two ICMPv6 Options
  - Trust anchor Option
  - Certificate Option
- Hosts pick routers that can show a certificate chain to TA



Trust Anchor (TA0)

(1)

(2) Cert. Request

(3)

X.509 cert

Trust Anchor

Host A

Router R

(4) CPS: I trust TA0, who are you?

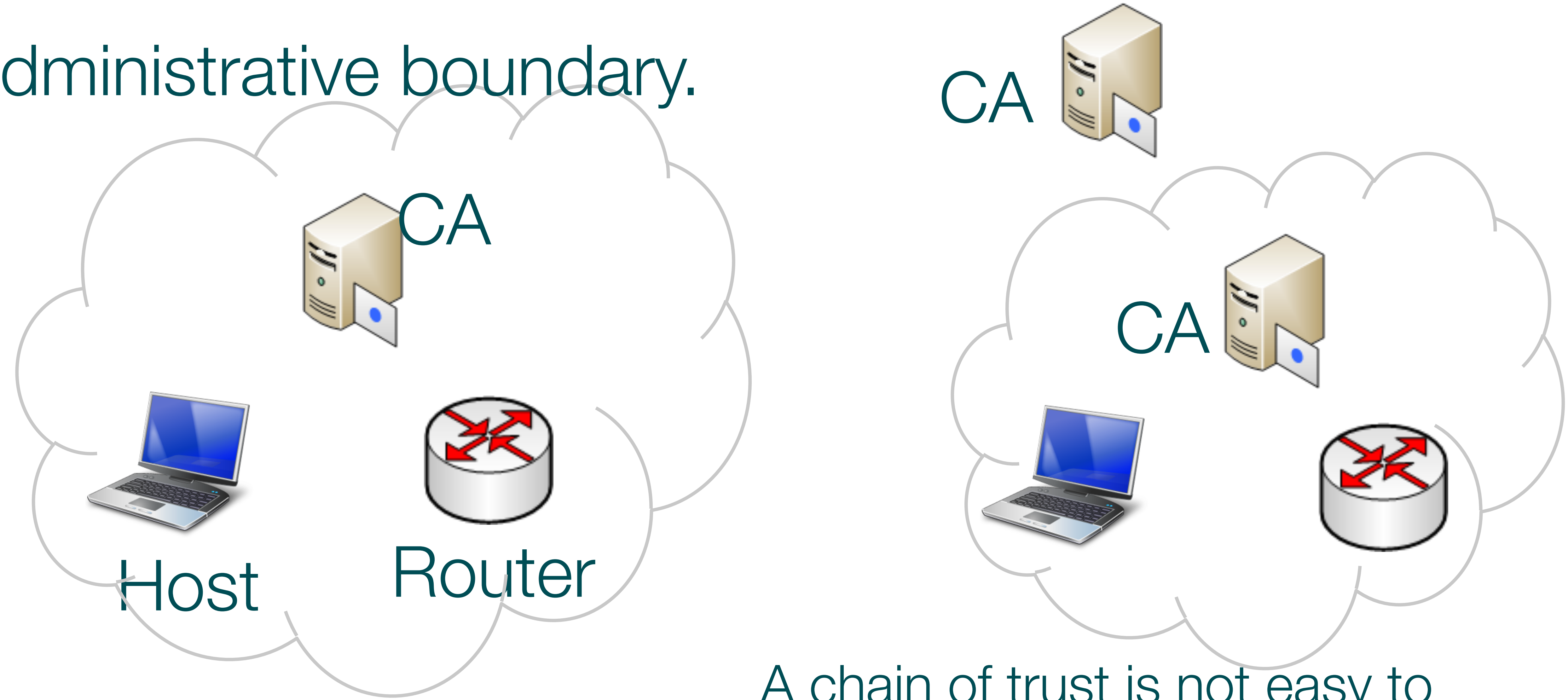
(5) CPA: I am R, here my Cert. Signed by TA0

(6) Verify the Cert. aganst TA0

(7) If valid, use R as trust router

Router Authorization Challenges

Administrative boundary.



A chain of trust is not easy to establish outside administrative boundaries

RPKI for SEND

- Certificate validation may be more complex
  - Long chain certificate authorization
  - It requires Public Key Infrastructure
  - No global root to authorized routers
  - Routers are required to perform a large number of operations

- Resource PKI (RPKI) can provide an attractive hierarchical infrastructure for SEND path discovery and validation
- Many ISPs do not support RPKI

Conclusion

- SEND is a promising technique to secure NDP
- SEND is still in trial stage
- Enhancing CGAs & SEND and make it simple and lightweight is very important. Otherwise, IPv6 network will be vulnerable to IP spoofing related attacks
- Among our contributions we hope to bring more usage and deployment of SEND and CGA in IPv6 networks

List of Publication

- Book Chapters
  - Ahmad AlSa'deh, Hosnieh Rafiee, and Christoph Meinel, SEcure Neighbor Discovery Review: a Cryptographic Solution for Securing IPv6 Local Link Operations. In CRYPSIS, pp. 178 -198, IGI Global, May 2013.
  - Tayo Arulogun, Ahmad AlSa'deh and Christoph Meinel. "Mobile IPv6: Mobility Management and Security Aspects." In Architectures and Protocols for Secure Information Technology Infrastructures, pp. 71-101, 2014.
- Journals & Magazines
  - Ahmad AlSa'deh, Christoph Meinel, "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations," IEEE Security & Privacy, vol. 10, no. 4, pp. 26-34, July-Aug. 2012
- Conferences
  - Ahmad AlSa'deh, Christoph Meinel, Florian Westphal, Marian Gawron, and Björn Groneberg. “CGA integration into IPsec/IKEv2 authentication”. SIN '13. ACM, pp. 326-330. 2013.
  - Ahmad AlSa'deh, Hosnieh Rafiee, and Christoph Meinel, "IPv6 stateless address autoconfiguration: Balancing between security, privacy and usability," Foundations and Practice of Security, vol. 7743 of Lecture Notes in Computer Science, pp.149--161. 2013.
  - Ahmad AlSa’deh, Hosnieh Rafiee, Christoph Meinel, "Cryptographically Generated Addresses (CGAs): Possible Attacks and Proposed Mitigation Approaches," cit, pp. 332-339, 2012 IEEE 12th International Conference on Computer and Information Technology, 2012.
  - Ahmad AlSa'deh, Hosnieh Rafiee, Christoph Meinel, "Stopping time condition for practical IPv6 Cryptographically Generated Addresses," icoin, pp.257-262, The International Conference on Information Network 2012, 2012.
  - Ahmad AlSa'deh, Feng Cheng, Christoph Meinel, "CS-CGA: Compact and more Secure CGA," icon, pp.299-304, 2011.
  - Ahmad AlSa’deh, Feng Cheng, Sebastian Roschke, and Christoph Meinel, “IPv4/IPv6 Handoff on Lock-Keeper for High Flexibility and Security,” in 4th IFIP International Conference onNew Technologies, Mobility and Security (NTMS), 2011, pp. 1–6.
  - Hosnieh Rafiee, Ahmad Alsa’deh, and Christoph Meinel, “WinSEND: Windows SEcure Neighbor Discovery,” SIN 2011, 2011, pp. 243–246.
  - Hosnieh Rafiee, Ahmad Alsa'deh, Christoph Meinel, "Multicore-based auto-scaling SEcure Neighbor Discovery for Windows operating systems," icoin, pp.269-274, 2012.
  - Tayo Arulogun, Ahmad AlSa’deh, and Christoph Meinel. "IPv6 Private Networks: security Consideration and Recommendations." In the Proceedings of the 4th International Conference on Mobile e-Services (ICOMeS) Oct. 16 – 17, 2012. Volume 4, ISBN: 978-2902-43-8.

Contact Information

Ahmad Alsadeh, PhD

Electrical and Computer Engineering Department

Faculty of Engineering and Technology

Birzeit University

P.O.Box 14-Birzeit, Palestine

Mobile: +972 59 786 8474

Phone: +972 2 298 2935

Fax: +972 2 298 2125

Email: asadeh@birzeit.edu

Questions?