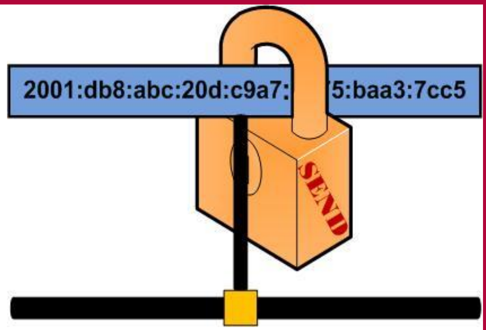



# Augmented SEND: Aligning Security, Privacy, and Usability


**Ahmad AlSadeh**

Supervisor: Prof. Dr. Christoph Meinel

Hasso-Plattner-Institut, University of Potsdam

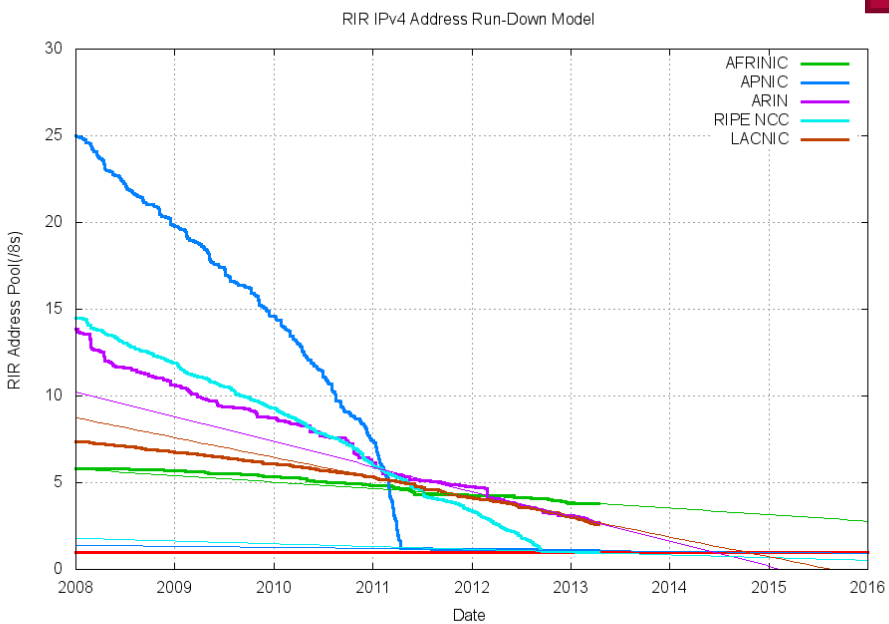

April 23, 2013

Hasso Plattner Institut

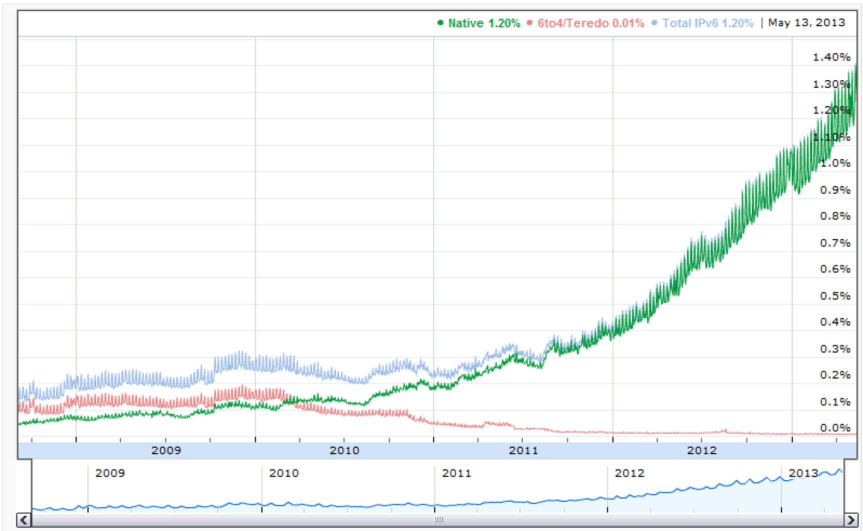
# IPv4 address exhaustion



- IANA unallocated address pool exhaustion: **03-Feb-2011**
- IPv6 deployment is happening
  - World IPv6 Launch Day: June 6, 2012




IPv4 Address Report
http://www.potaroo.net/tools/ipv4/



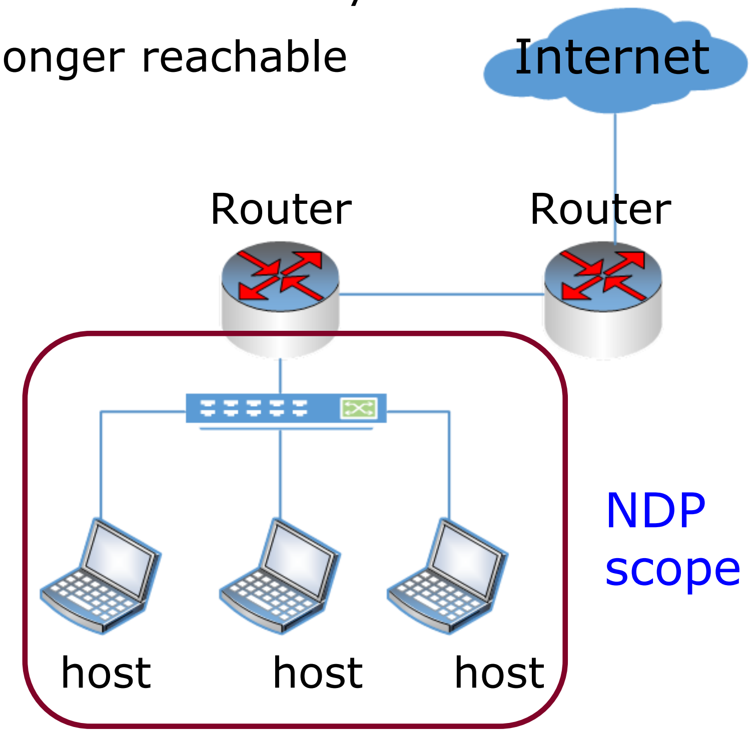

Google IPv6 Statistics
http://www.google.com/ipv6/index.html

# Comparison of IPv4 and IPv6

| | IPv4 | IPv6 |
|---|---|---|
| **Number of Addresses** | $2^{32}$ = 4,294,967,296 = **4 billion** addresses | $2^{128}$ = **340 trillion trillion trillion** addresses |
| **Address Format** | Decimal notation: 192.146.200.67 | Hexadecimal notation: 2001:5FEB:BEEF::CAFE |
| **Prefix Notation** | 192.146.0.0/24 | 2001:5FEB:BEEF::/64 |
| **Addresses configuration** | Manually or through DHCP | Stateless Address Autoconfiguration, assigned using DHCPv6, or manually configured |
| **IP<--> MAC Translation** | Address Resolution Protocol (ARP) | Neighbor Discovery Protocol (NDP) |

# Neighbor Discovery Protocol (NDP)

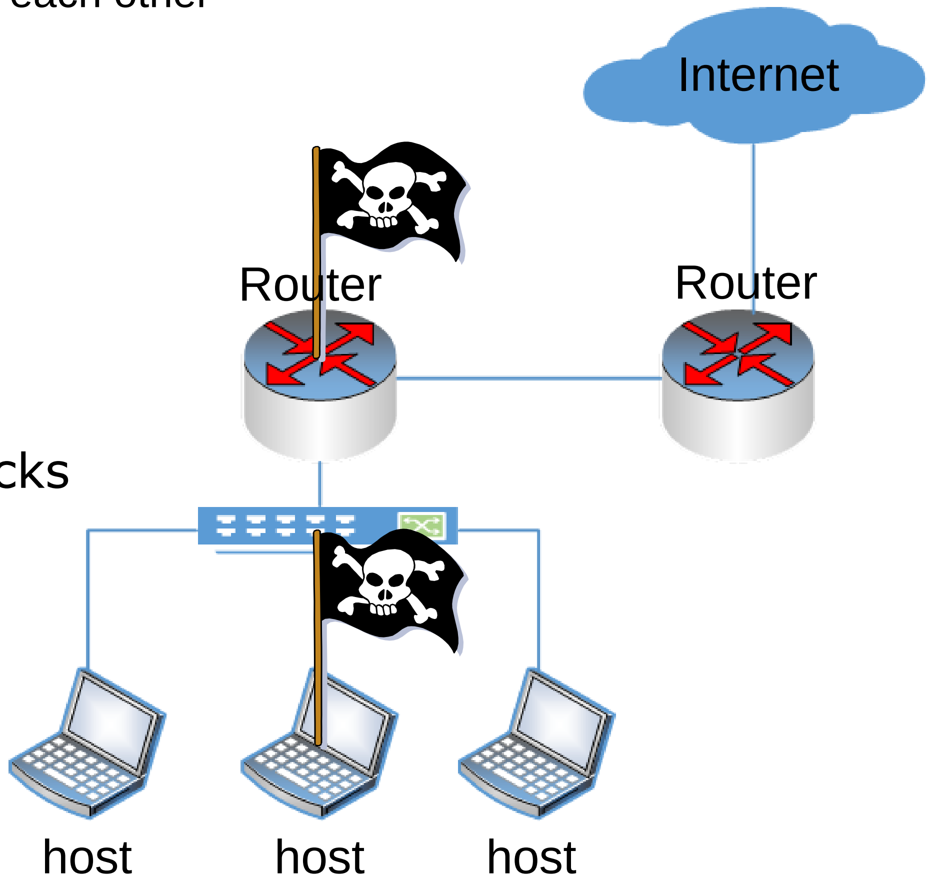
- NDP is a part of ICMPv6
- Fundamental protocol in IPv6 suite
  - Obtain configuration information including:
    - Router, subnet prefix, and parameter discovery
  - Determine when a neighbor is no longer reachable
  - Perform address resolution
  - …
- Local link protocol
  - Subnet scope



# NDP vulnerabilities



- NDP messages lack authentication
  - The assumption that all nodes trust each other
- Attacks come from malicious
  - host
  - router
- NDP is vulnerable to many attacks
  - Spoofing
  - Replay
  - Rogue router
  - …



# NDP vulnerabilities ( continue ...)



- Duplicate Address Detection (DAD) DoS attack
  - THC-IPv6 Attack Suite http://www.thc.org/thc-ipv6/
    - *dos-new-ip6*


- SEcure Neighbor Discovery (SEND) is the proposed solution

# Outline

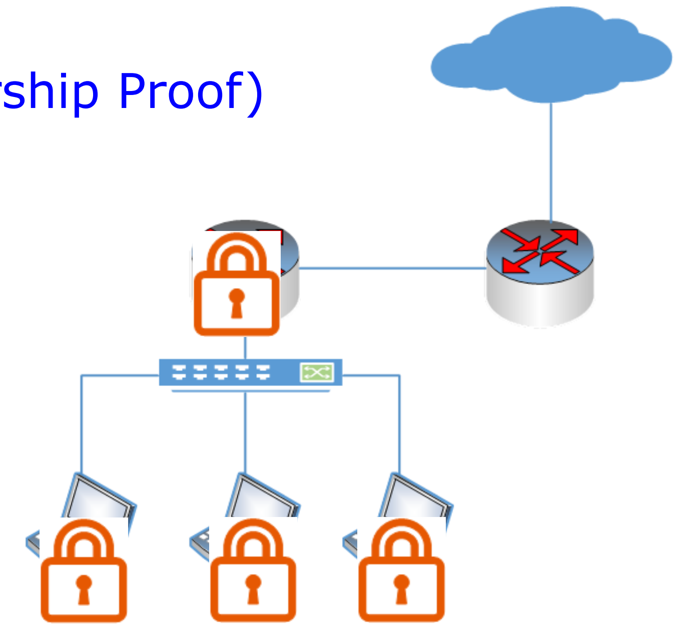


- SEcure Neighbor Discovery (SEND)
- Problem statement
- SEND users' preferences
  - Time–Based CGA
  - CGA privacy Extension
- WinSEND
- CGAs enhancements: security and performance
- SEND and IPsec
- Conclusion

# SEcure Neighbor Discovery (SEND)

HPI Hasso Plattner Institut

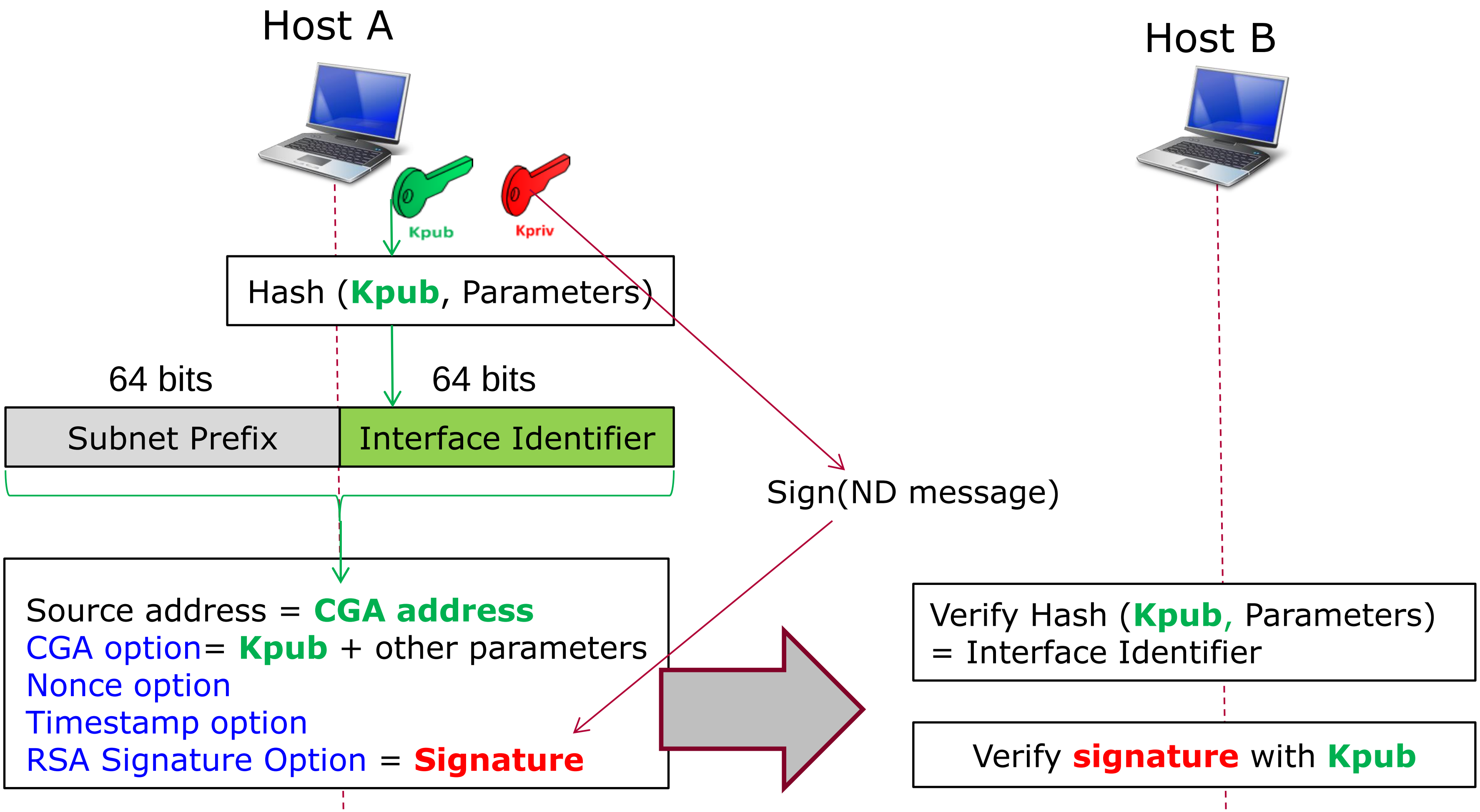
- SEND is an integral part of NDP
- Address Authentication (Address Ownership Proof)
  - CGA Option
  - RSA Signature Option
- Replay Protection
  - Nonce Option
  - Timestamp Option



- Authorization Delegation Discovery (ADD)
  - Certificate Path Solicitation (CPS), ICMPv6 message
  - Certificate Path advertisement (CPA), ICMPv6 message

# SEND (Simplified)

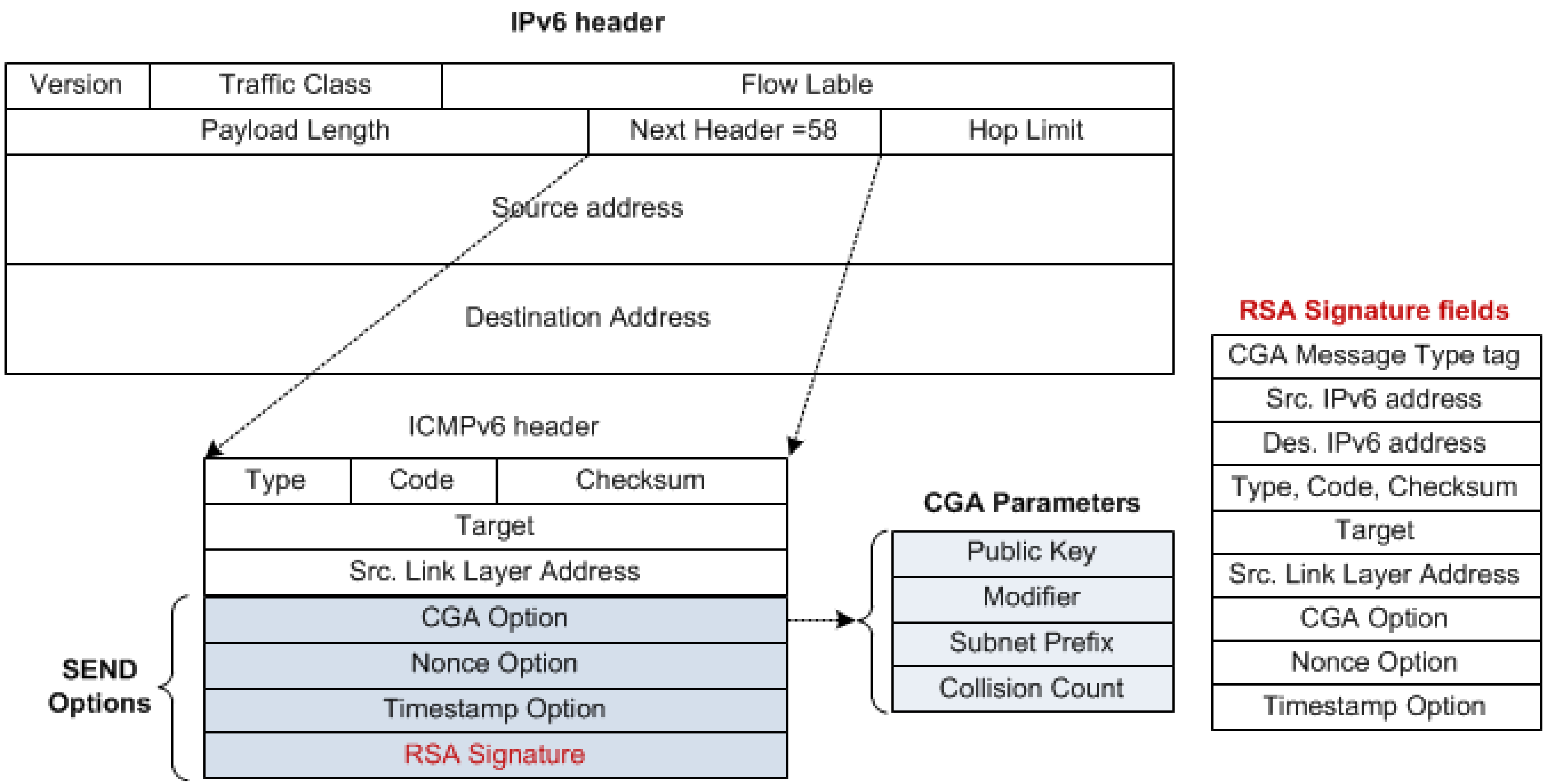





SEND options are sent with the NDP message

# NDP message protected by SEND

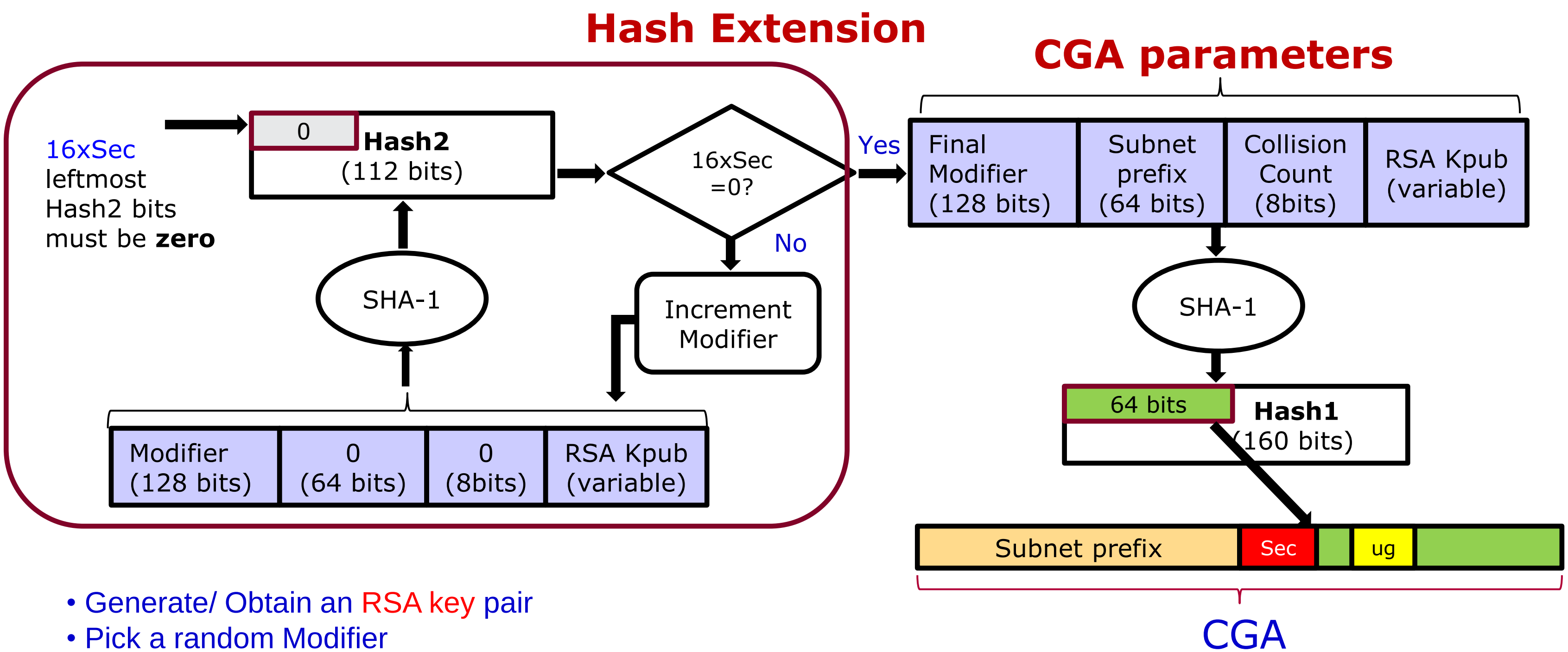




# Cryptographically Generated Addresses (CGAs)

Hasso Plattner Institut

- 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

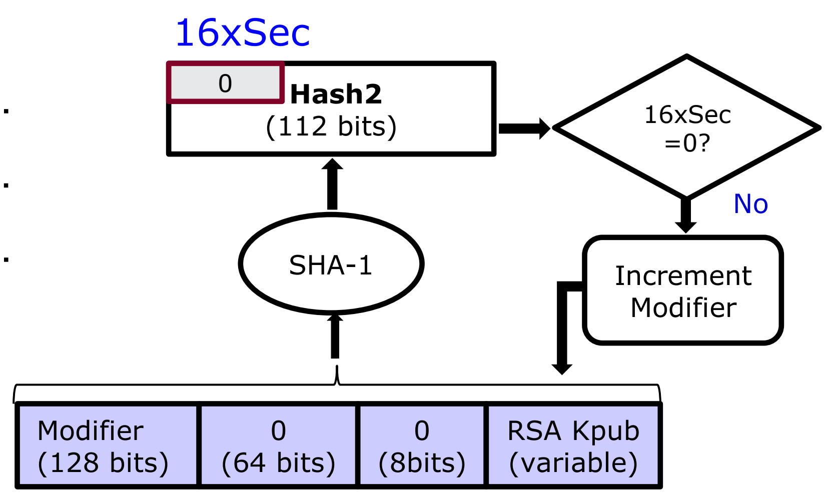
Check the uniqueness of IPv6 address (DAD)

# Sec value of the CGA



- In CGA, Sec (0 to 7), unsigned 3-bit integer, is scale factor which increases the cost (hash operation) for both
  - The attacker : $O(2^{59+16xSec})$
  - The address generator: $O(2^{16xSec})$

- For example
  - Sec=0, Hash2=0X123456789ABCD…
  - Sec=1, Hash2=0X000056789ABCD…
  - Sec=2, Hash2=0X000000009ABCD…
  - …



# 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
  - SEND has not mature implementation for end user operating systems
  - SEND is still vulnerable to DoS attacks
  - Router Authorization Delegation Discovery (ADD) mechanism is so far theoretical rather than practical

**Publication:**


- 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.

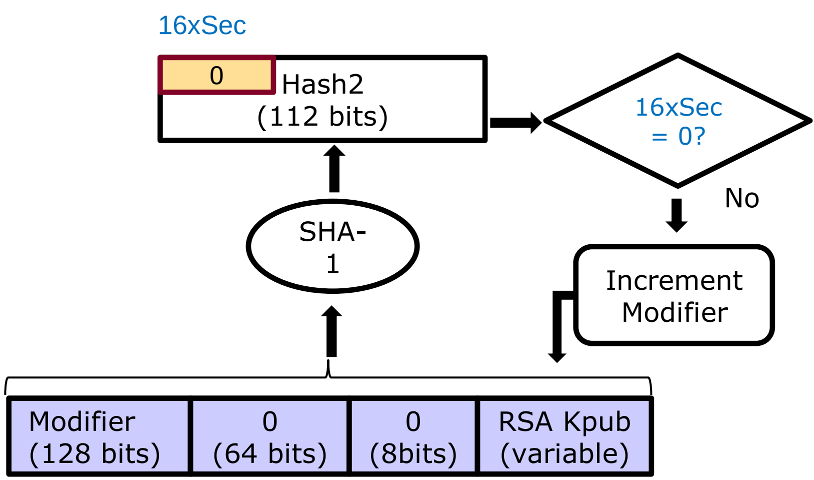
# Research questions

- How could we decrease the complexity of SEND calculations to make it usable without major changes to the SEND itself?
- How could we enhance CGA against the privacy-related attacks?
- What could we do to make SEND available for end users?
- How SEND and IPsec can work together for securing IPv6 networks?

# 1. SEND is compute-intensive

- Cryptography means a lot of computations
- The average time for CGA address generation

| Processor with 2.6 GHz | |
|---|---|
| **Sec** | **Average time** |
| 1 | ~ 0.5 seconds |
| 2 | ~ 2 hours |
| 3 | ~ 12 years |
| 4 | ~ 1.6. $10^6$ years |

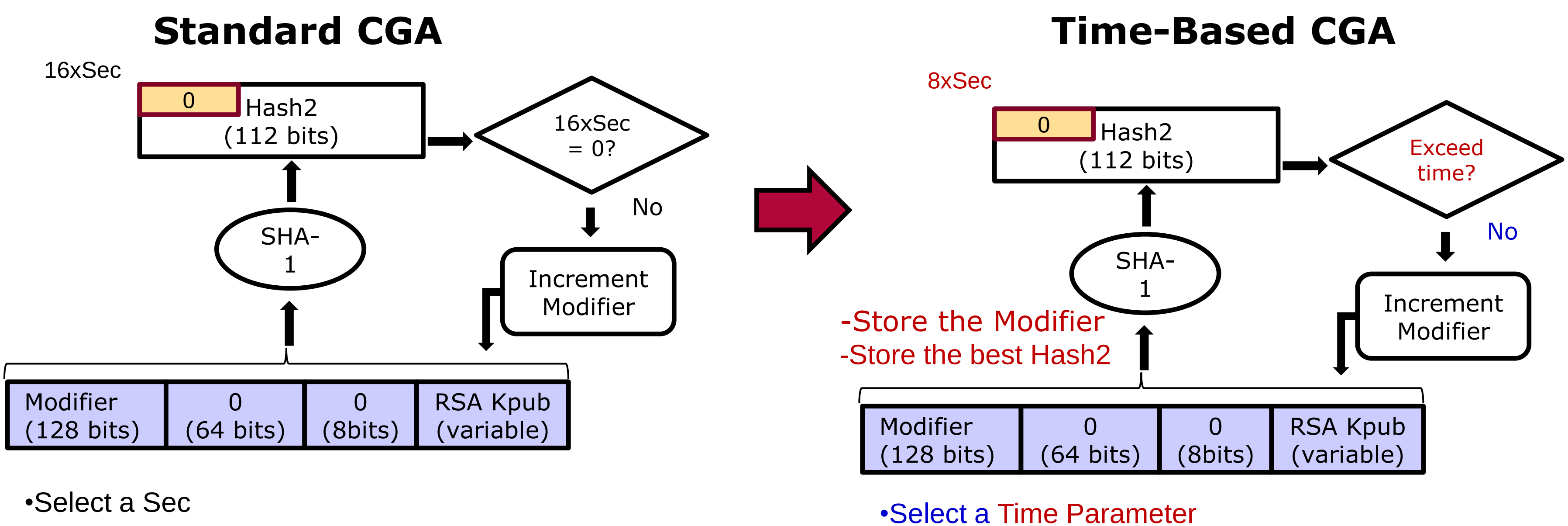



•Select a Sec

- Even for the same Sec value, predicting the convergence time is very difficult

# 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"



# Sec value measurements for different granularity

HPI Hasso Plattner Institut

- Granularity 16 (before)

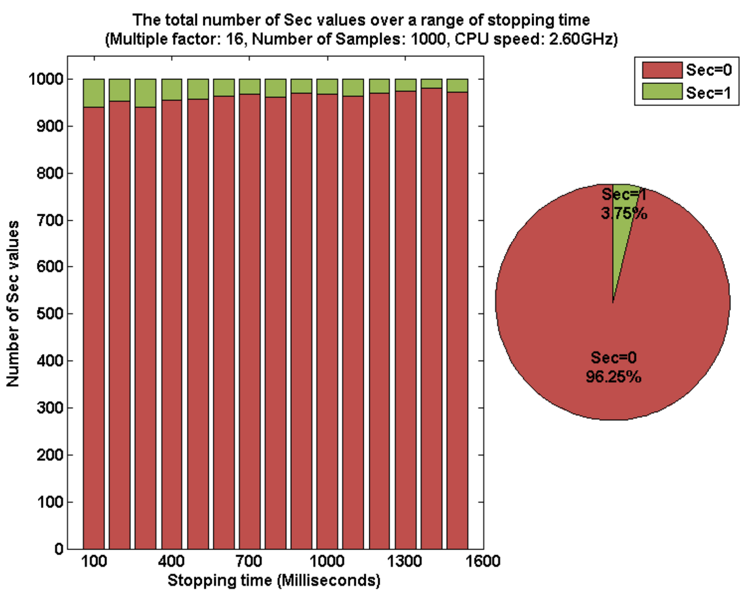
  For Sec=0: 96.25%

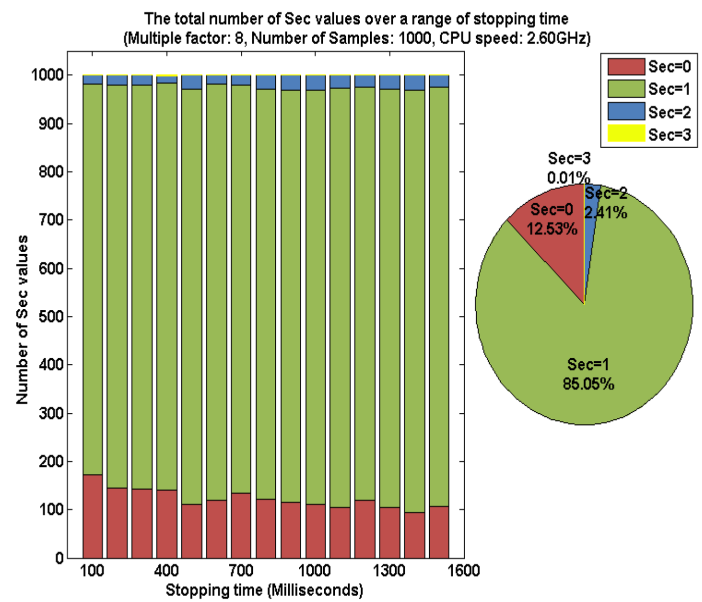
  For Sec=1: 3.75%

- Granularity 8 (after)

  Sec=0: 12.53%

  Sec=1: 80.05%




- 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.

## 2. Privacy concerns



- High Sec value may cause unacceptable delay

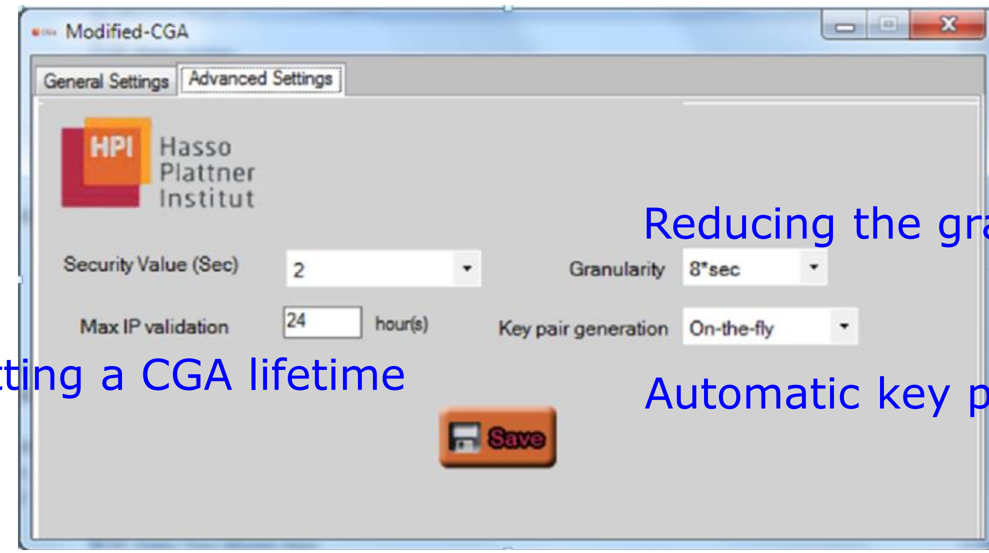
- It is likely that once a host generates an acceptable CGA, it will continue to use
  - this same address
  - the same public key

- hosts using CGAs could be susceptible to privacy related attacks

# CGA privacy extensions



- Three main modifications




Reducing the granularity of CGA

Setting a CGA lifetime

Automatic key pair generation

- Ahmad Alsa’deh, Hosnieh Rafiee, and Christoph Meinel, "IPv6 Stateless Address Autoconfiguration: Balancing Between Security, Privacy and Usability" in 5th International Symposium on Foundations and Practice of Security, FPS 2012, LNCS 7743, pp. 149–161, 2012.

# CGA privacy extensions - advantages



- Setting a lifetime for a CGA address  protect the user's privacy
  - Tracking users becomes more difficult

- We choose the granularity factor 8 for the following reasons:
  - It is unnecessary to select a high Sec when using a short lifetime
  - The multiplication factor of 8 increases the maximum length of the *Hash Extension* up to 56 bits which is sufficient  (59-115 bits total hash length)

# 3. Lack of mature implementations

- Some proof of concept implementations for Linux and FreeBSD
  - DoCoMo SEND
  - NDProtector
  - ...

- No implementation for Windows
  - *"Microsoft does not support SEND in any version of Windows" [Microsoft TechNet] http://technet.microsoft.com/en-us/library/bb726956.aspx*
  - Windows account more than 80% of usage compare to other OSs

# WinSEND



- We used WinSEND to demonstrate the feasibly of our extensions to SEND
- It is the first SEND implementation for Windows
- Ahmad Alsadeh and Hosnieh Rafiee
  - Winners of the 1st price in the International IPv6 Application Contest 2011, German IPv6 Council, Germany

# WinSEND (Continued ...)



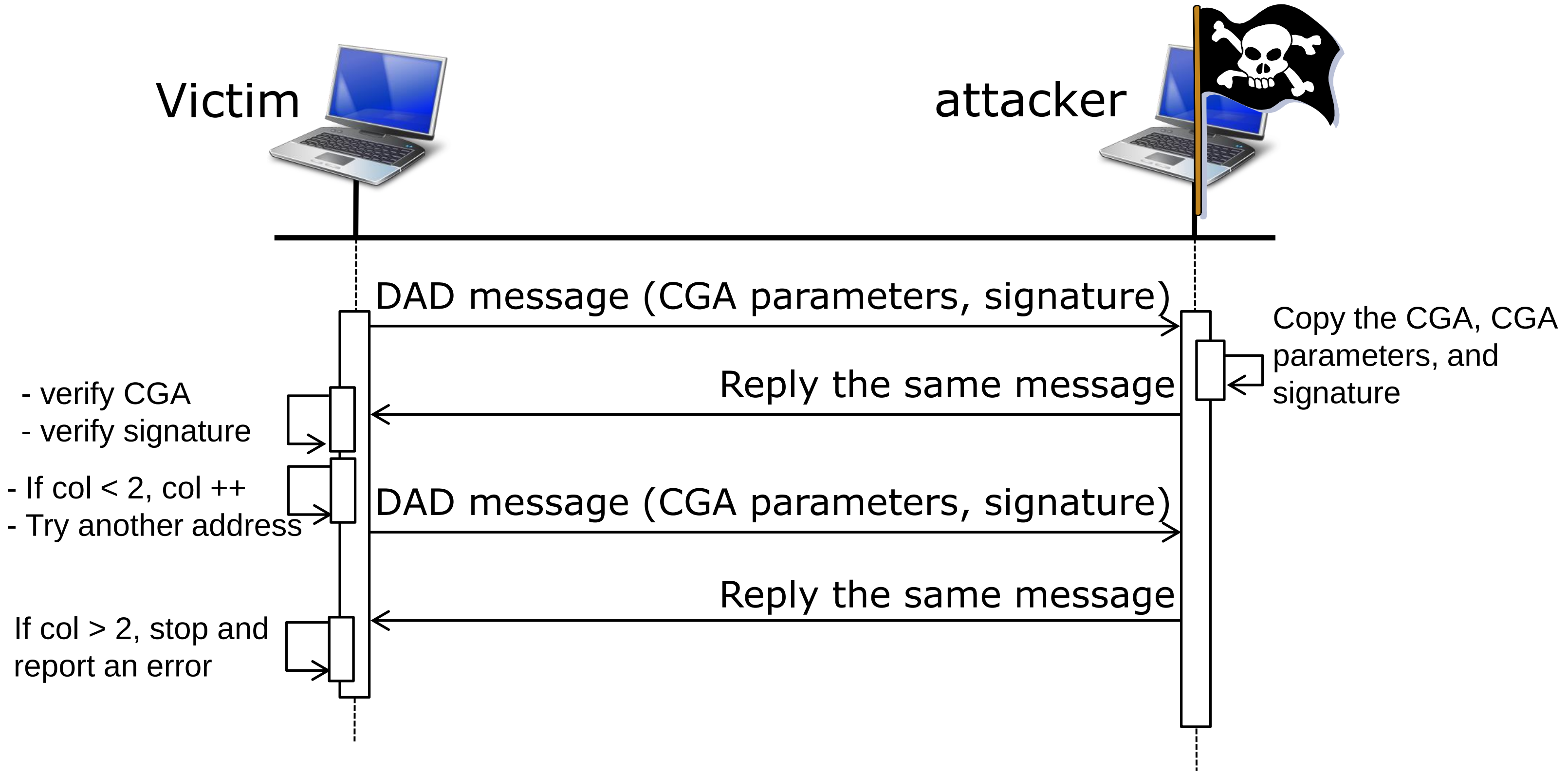
- Multicore-Based Auto-Scaling SEND
  - Parallelize Hash2 condition of CGA algorithm
  - Determine the number of tasks based on the number of cores

| CGA average generation time (Milliseconds) 1024-bit RSA key, Sec=1 | | | |
|---|---|---|---|
| **Number of cores** | **Parallel Mode** | **Sequential Mode** | **Percentage of Speedup** |
| 2 | 376.34 | 516.26 | 27.1% |
| 4 | 304.13 | 437.82 | 30.5% |
| 8 | 261.43 | 426.36 | 38.7% |

- Hosnieh Rafiee, Ahmad Alsa'deh, Christoph Meinel, "Multicore-based Auto-scaling SEcure Neighbor Discovery for Windows operating systems," icoin, pp.269-274, The International Conference on Information Network 2012, 2012

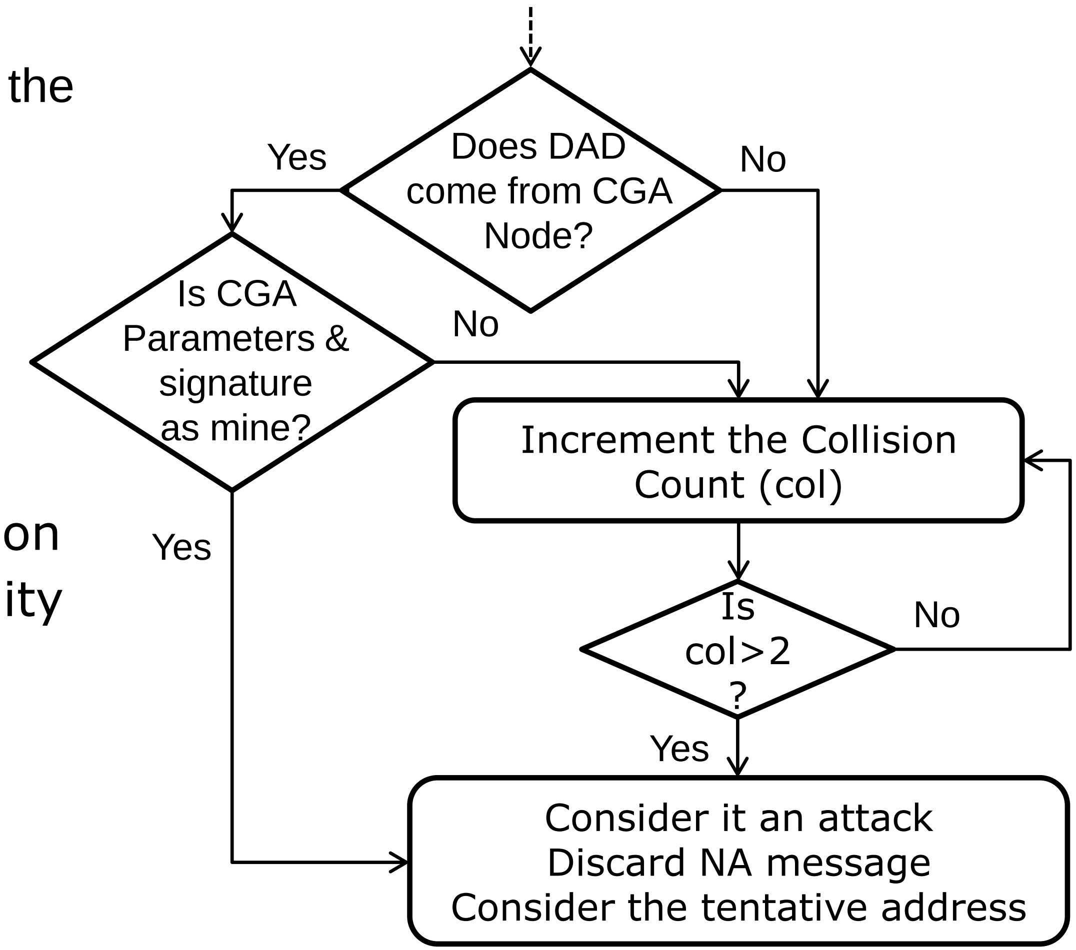
# 4. DoS attack against CGA

- SEND and CGA are mainly vulnerable to DoS attacks
  - DoS attack against CGA verification procedure is still possible



# DoS attacks mitigation

- We proposed an extension to the CGA DAD verification
- The probability that two nodes generate interface identifier is very low (Bagnulo, et al)
- If there is 100 000 nodes on the same link the probability of collision is $Pb \leq 1.7\ e^{-08}$




- Ahmad AlSa'deh, Hosnieh Rafiee, and Christoph Meinel. Cryptographically Generated Addresses (CGAs): Possible attacks and Proposed Mitigation Approaches. In *IEEE 12th International Conference on Computer and Information Technology* ,CIT'12, pp. 332--339, 2012.

# Compact and more Secure CGA (CS-CGA)

HPI Hasso Plattner Institut

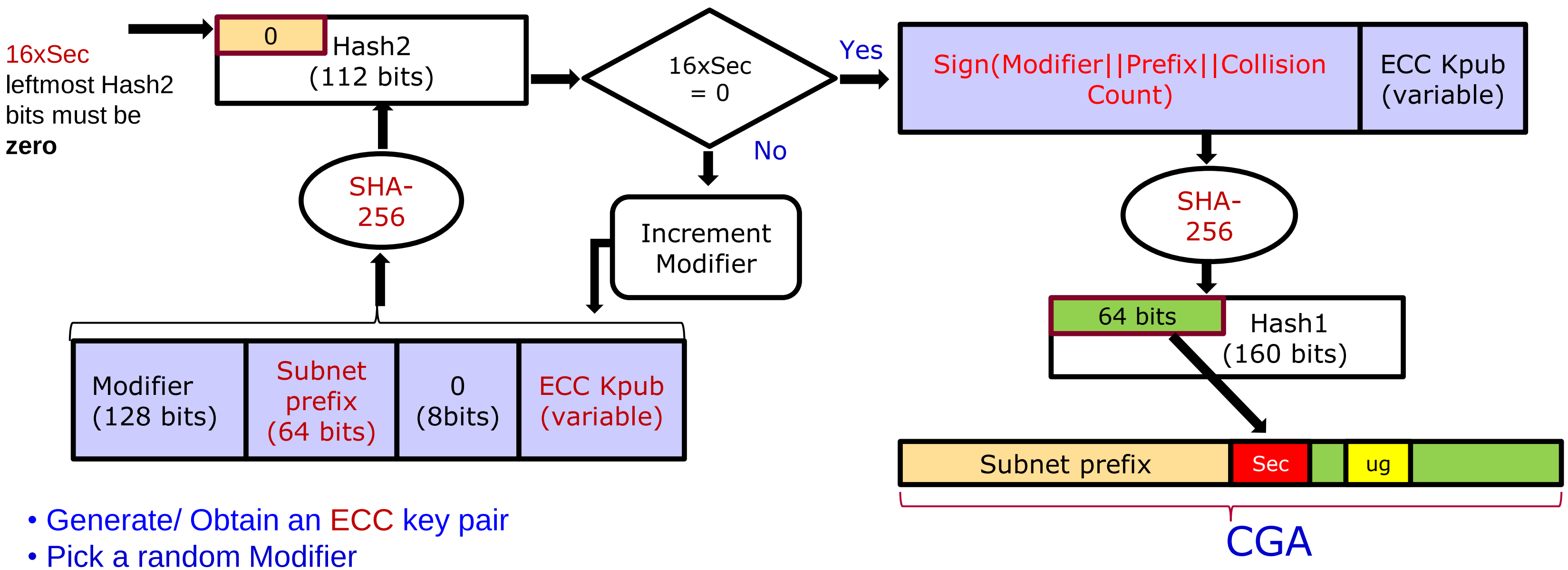


- CGA is vulnerable to Time-Memory Trade-Off (TMTO) attack
  - CGA ++: enhanced CGA vision against global TMTO attack
    - J. W. Bos, O. Özen, and J.-P. Hubaux, "Analysis and optimization of cryptographically generated addresses," in Proceedings of the 12th International Conference on Information Security, ser. ISC '09. Berlin, Heidelberg: Springer-Verlag, pp. 17–32,2009
  - CGA++ required more computation than standard CGA

- CS-CGA: Modifications
  - Use shorter keys (e.g., Elliptic Curve Cryptosystem (ECC) instead of RSA keys to reduce the SEND options size
  - CS-CGA is a modified CGA that incorporates ECC and CGA++

- Ahmad AlSa'deh, Feng Cheng, Christoph Meinel, "CS-CGA: Compact and more Secure CGA," ICON, pp.299-304, 2011 17th IEEE International Conference on Networks, 2011

# CS-CGA: generation algorithm




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

# CS-CGA performance evaluation-1



- NDP messages size comparison
- RSA (3072) and ECC (P-256) provide equivalent security [NIST ]

| **Security level (Sec = 1)** | | | |
|---|---|---|---|
| | CGA | CS-CGA | |
| **Cryptosystems** | **RSA (3072)** | **ECC (P-256)** | |
| **ND message type** | **NS** | **NS** | **Saved bytes** |
| ICMPv6 Message length (bytes) | 928 | 288 | 640 |
| CGA option length (bytes) | 456 | 120 | 336 |
| Signature option length (bytes) | 408 | 96 | 312 |

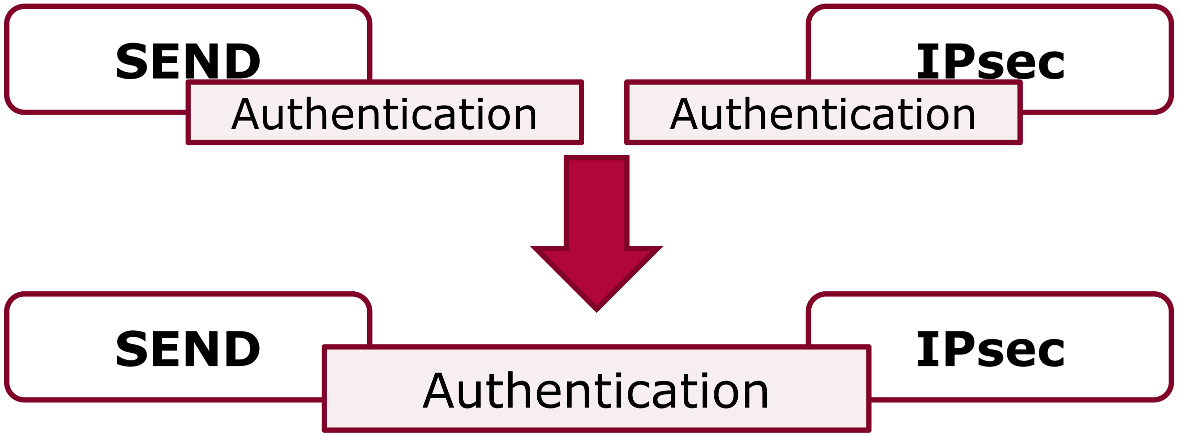
# CS-CGA performance evaluation-2

- Addresses generation and verification time

| Security level (Sec = 1) | | | | |
|---|---|---|---|---|
| **Number of Samples (1000 samples)** | | | | |
| **Algorithm** | **Cryposystems** | **Hash function** | **Address generation time(sec)** | **Address verification time(msec)** |
| CGA | RSA ( 3072) | SHA-1 | 2.183 | 0.695 |
| CS-CGA | ECC (P-256) | | 1.960 | 0.723 |
| CGA | RSA ( 3072) | SHA-256 | 2.637 | 0.702 |
| CS-CGA | ECC (P-256) | | 2.046 | 0.735 |

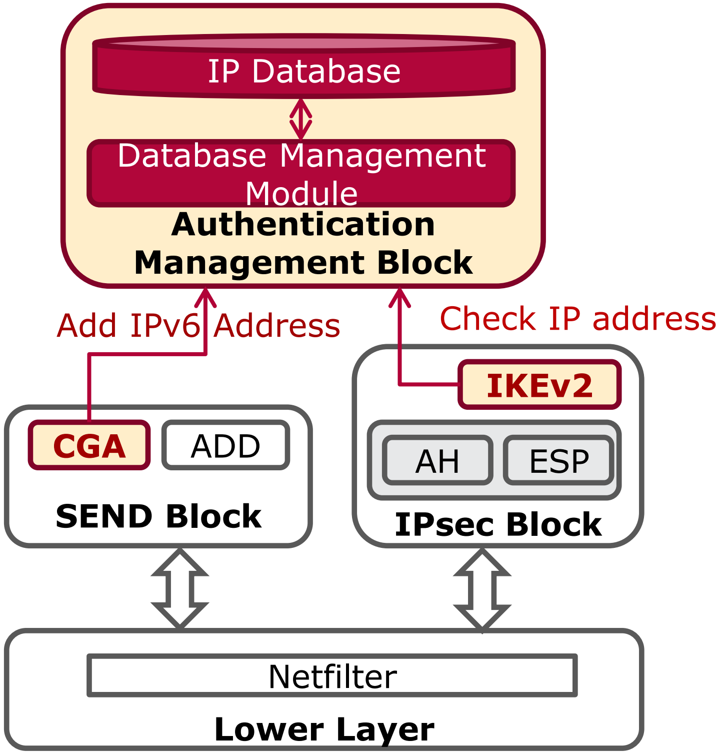
# SEND and IPsec: problem statement

- **Two** security mechanisms should be used at network-layer
  - SEcure Neighbor Discovery (SEND): authentication within the IP address
  - IP Security (IPsec): end-to-end authentication
- Although both provide authentication, neither subsumes the other
  - The duplicate authentication increases the processing cost
- The idea: let them work together (if possible) to reduce the overhead and decrease the hurdles of IPsec configuration



# SEND and IPsec combined authentication method

- SEND and IPsec work together under the mediation of an Authentication Management Block:
  - Store and manage the authentication information




- SEND does the CGA generation (IP address authentication) and stores the authenticated IP addresses in an IP Database

- IPsec uses the public-private keys obtained by SEND rather than negotiating its own

# IPsec authentication time

- The modified implementation performs ~ 50% faster than the original authentication
- Ahmad Alsadeh
  - Winner of the 3rd place of the International IPv6 Application Contest 2012: Applications & Implementations category.

# Conclusion

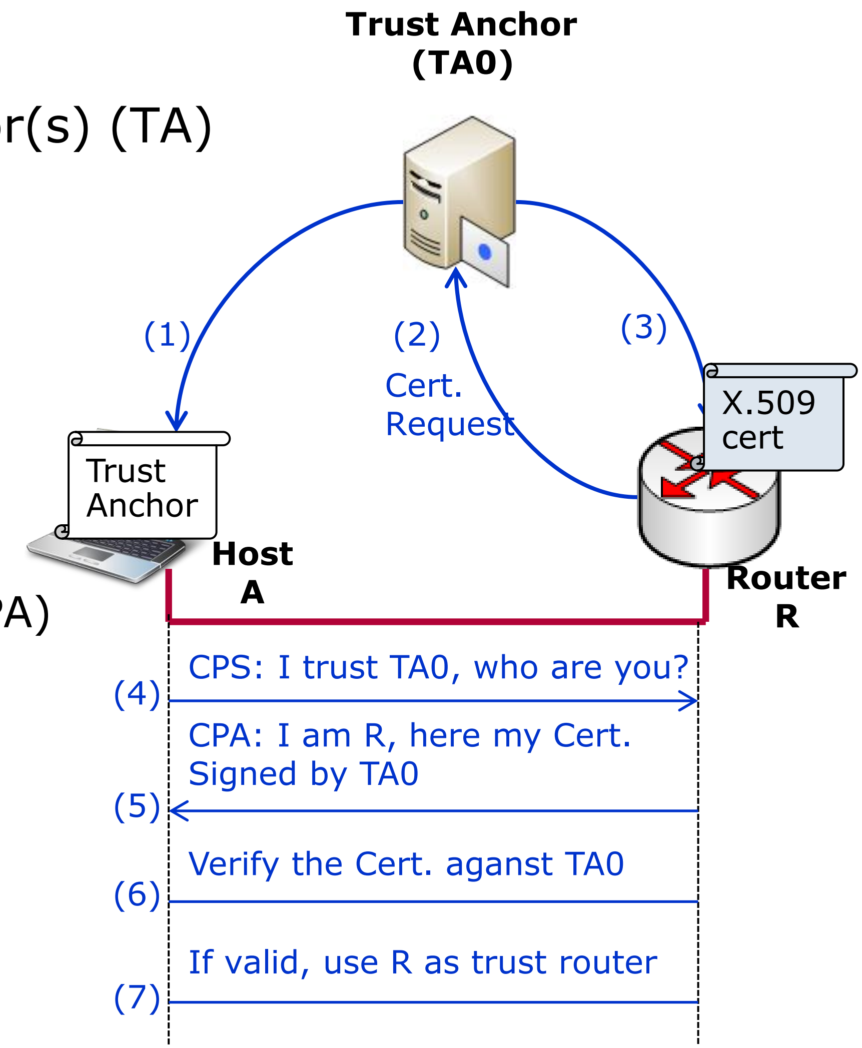


- SEND is a promising technique to secure NDP
- SEND is still in trial stage
- Enhancing CGAs & SEND and make it simple and lightweight is very important. Otherwise, IPv6 network will be vulnerable to IP spoofing related attacks
- Among our contributions we hope to bring more usage and deployment of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

# Thank you

# 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)
- Hosts pick routers that can show a certificate chain to TA



# 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

- DFN does not support RPKI

# NDP Messages

- NDP is a part of ICMPv6 messages “RFC 4443”
- ND specifies 5 ICMPv6 Type messages

| ICMPv6 Type | Message | Description |
|---|---|---|
| Type 133 | Router Solicitation (RS) | The host sends RS to ask for RA (at the boot time) |
| Type 134 | Router Advertisement (RA) | – Answer RS<br>– Periodic RA |
| Type 135 | Neighbor Solicitation (NS) | – Determine the link-layer of a neighbor<br>– Check the reachability<br>– Detect duplicate address |
| Type 136 | Neighbor Advertisement (NA) | – Answer NS<br>– Advertise the change of physical address |
| Type 137 | Redirect | Used by a router to inform a host of a better router to specific destination |

# StateLess Address AutoConfiguration (SLAAC)

HPI Hasso Plattner Institut



| Subnet Prefix | Interface Identifier |
|---|---|

**IPv6 Address**

**Prefix can be**

- Link-Local address (FE80::/64)
- Global Unicast address
  - Routers send periodic Router Advertisement (RA) which contains link **prefix**, lifetime, MTU, etc.
  - Host may also send router solicitation (RS) to get trigger RA

**The interface ID generated by**

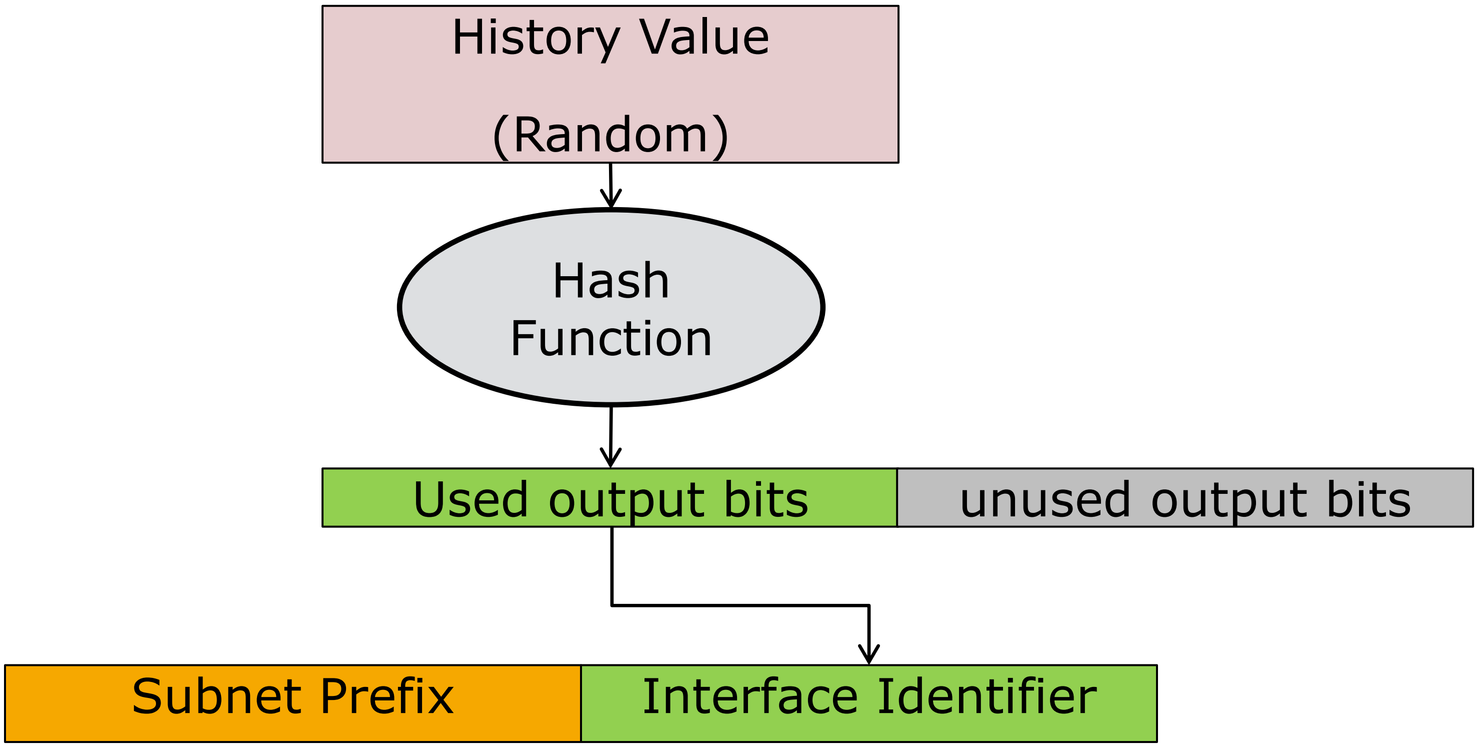
- EUI-64→ Formed from MAC Security and privacy →

- Privacy Extension→ Provides some level of privacy

- CGA → Provides some level of privacy and security→

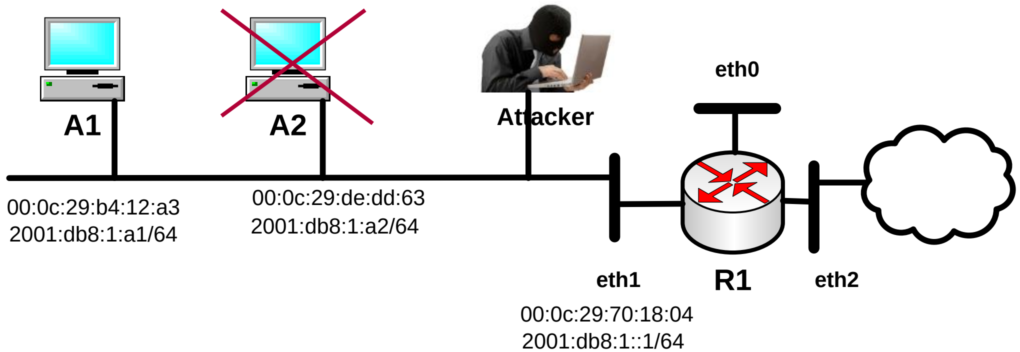
# Privacy Extension






**It solves the privacy issue but not the security issue**

# DoS Attack on DAD




The victim host **before** generating the DoS attack.

```
root@A2:~# ifconfig eth0 | grep inet6
        inet6 addr: fe80::020c:29ff:fede:dd63/64 Scope:Link
        inet6 addr: 2001:db8::a2/64 Scope:Global
root@A2:~# ifconfig eth0 down
root@A2:~# ifconfig eth0 up
```

Global IPv6 addr.

The attacker succeeds to spoof the address of new host joint to LAN as shown below:

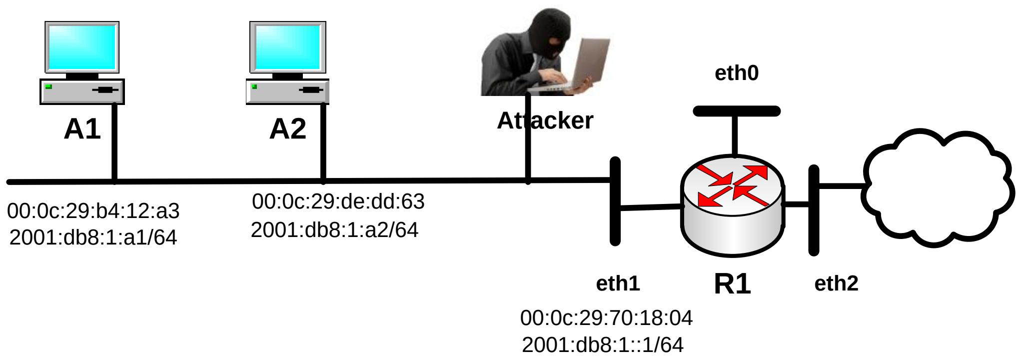
```
root@test-desktop:/home/test/Desktop/thc-ipv6-0.7#./dos-new-ip6 eth0
Started ICMP6 DAD Denial-of-Service (Press Control-C to end) ...
Spoofed packet for existing ip6 as fe80:0000:0000:0000:020c:29ff:fede:dd63
```

The victim (A2) machine **after** generating the attack:

```
root@A2:~# ifconfig eth0 | grep inet6
        inet6 addr: fe80::020c:29ff:fede:dd63/64 Scope:Link
```

Global IPv6 addr. Lost

# Fake RA Attack



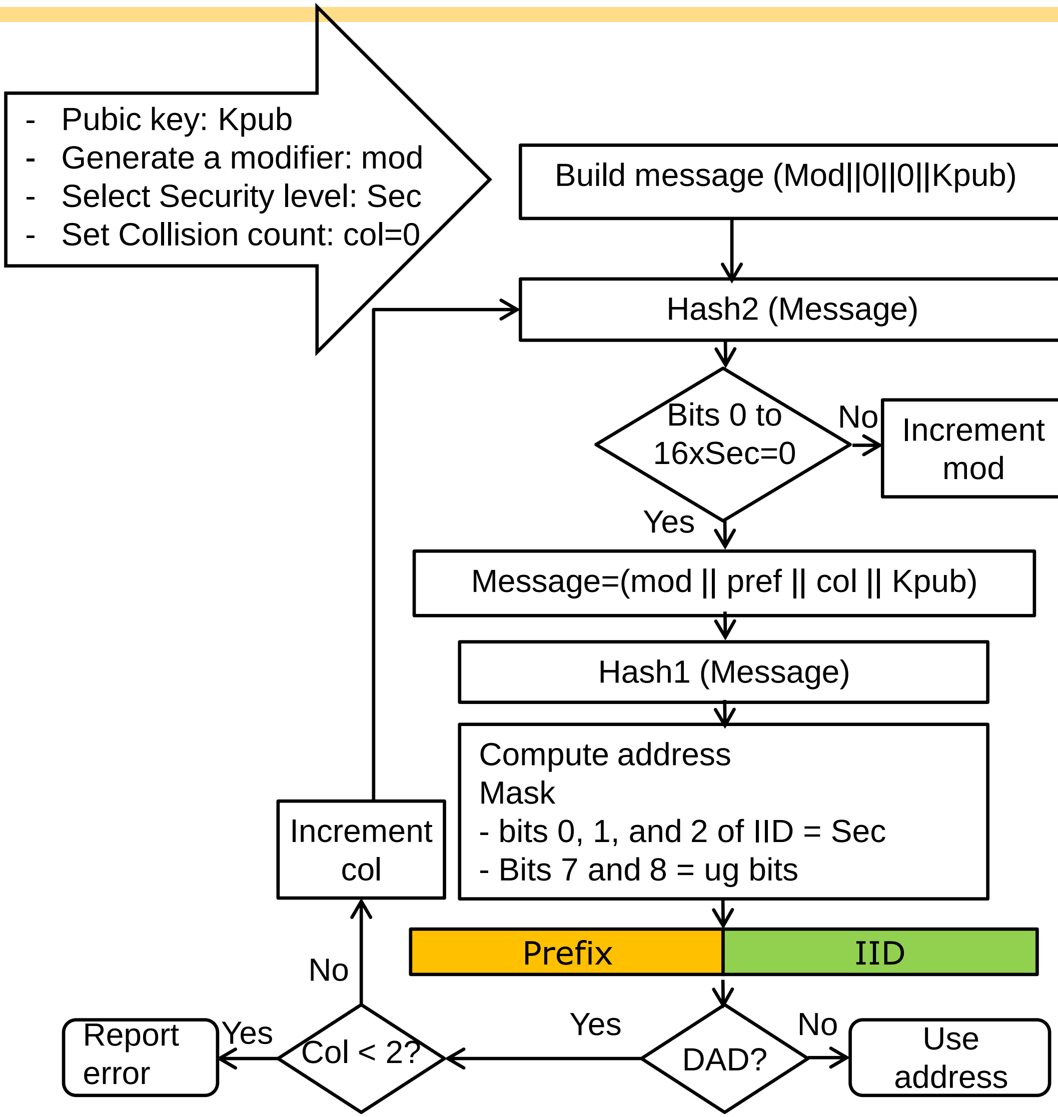

```
root@test-desktop:/home/test/Desktop/thc-ipv6-0.7# ./fake_router6 eth0
fe80::20c:29ff:fe92:280e 2001:bad:bad:bad::/64 1000
Starting to advertise router fe80::20c:29ff:fe92:280e (Press Control-C to end) ...
```

Attacker sends fake RA

```
root@A2:~# ifconfig eth0 | grep inet6
        inet6 addr: 2001:bad:bad:bad:20c:29ff:fede:dd63/64 Scope:Global
        inet6 addr: fe80::020c:29ff:fede:dd63/64 Scope:Link
        inet6 addr: 2001:db8::a2/64 Scope:Global
```

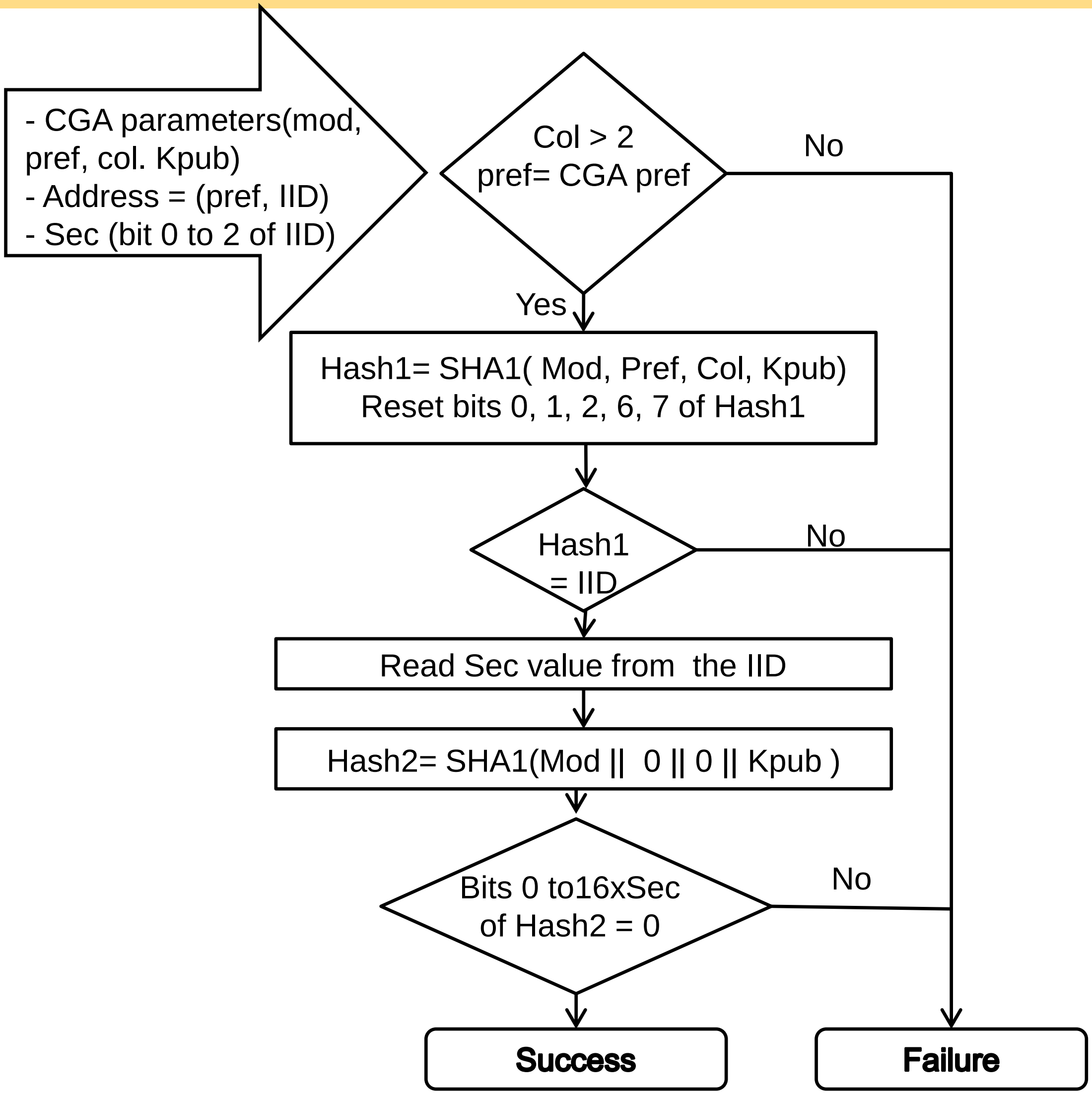
IPv6 address from the rogue router

# CGA – Generation




1. Set CGA initial values
2. Concatenate (mod, 0, 0, Kpub)
3. Execute SHA-1 algorithm
4. Compare if 16xSec = 0?
5. Concatenate (CGA parameters)
6. Execute SHA-1 algorithm
7. Form an interface ID
8. Concatenate ( Prefix, IID)
9. Check the uniqueness of IPv6 address

# CGA- verification




1. Check that Collision is 0, 1, 2 and the prefix = CGA prefix
2. Concatenate CGA parameters and execute SHA-1
3. Compare Hash1 with IID
4. Read Sec value from bit 0 to 2 of the IID
5. Concatenate (mod, 0, 0, Kpub) and execute SHA-1
6. Compare the 16xSec of Hash2 to 0

# CGA – Design Rationale

- Hash Extension
  - Interface ID is only 64-bit to accommodate the Hash result
  - Sec is scale factor→ determines the length of the Hash extension
    - The address owner : $O(2^{16xSec})$
    - The attacker (brute force attack) : $O(2^{59+16xSec})$

- Hash2
  - Modifier → Randomness
  - Subnet Prefix = **0** → Mobility (Hash extension too expensive for mobiles)
  - Collision Count = 0 → Efficient
  - Public Key→ Prevent Stealing Modifiers, assign the Modifier to the node

# The other SEND options



- Nonce Option
  - Used to make sure that a response to a solicited message is "fresh"
  - The reply advertisement must contain the same *nonce* in return

- Timestamp Option
  - Avoid replay attack for unsolicited advertisements (e.g., RA)

- RSA Option
  - Digital signature made by concatenating
    - Source address
    - Destination address
    - Some ICMPv6 fields
    - NDP message header
    - All NDP options before the signature

# Global Time-Memory Trade-Off Attack on CGA for IPv6



- Hash2 is independent of the subnet prefix to help mobility
  - avoid computing Hash2 over and over again
  - mobile nodes do not have much computation power
- This helps an attacker as well

**Time-Memory Trade-off Attack**

- Eliminate the effect of Hash Extension at the cost of storage
  - Is feasible at the cost of memory or database size
  - Database with valid Modifiers that satisfy Hash2 condition
  - Store valid address from each network
- Much easier for large networks
  - For network with $2^{20}$ nodes, 8 terabytes of storage is needed
- Impersonate a random node NOT a specific node

# Setting a lifetime for CGA

- The lifetime for a CGA address ($T_l$) depends on
  - $T_G$ : the average time needed for a node to generate a CGA address

    $$T_G = (2^{8 \times Sec} \times T_2) + T_1 \quad if\ 0 \leq Sec \leq 7$$

    - $T_1$: The time needed to compute Hash1
    - $T_2$: The time needed to compute Hash2
  - $T_A$ : the average time for an attacker to impersonate an address

    $$T_A = \begin{cases} 2^{59} \times T_1 & if\ Sec = 0, \\ (2^{59} \times T_1 + T_2) 2^{8 \times Sec} & if 1 \leq Sec \leq 7. \end{cases}$$

  - The user desired settings for security and privacy

- The lifetime for a CGA is described by the equation

$$mT_G \leq T_l \leq \frac{T_A}{n}$$

$m$ and $n$ are integers