SVO logic and applications

An analysis of the MIPv6 security protocols

Marco Costa

University of Pisa

Table of contents

Introduction

Goal of the presentation

1. Present the SVO logic and its constructs
2. A brief comparison between SVO and BAN logics
3. Introduce the MIPv6 standard for mobile communications and related security concerns
4. Evaluate the two MIPv6 security protocols using SVO logic

Historical overview

1989 BAN logic proposed by Burrows, Abadi and Needham became a standard for formalizing reasoning about authentication protocols

1990 Nessett criticizes the BAN logic and its limitations:

- the idealization step is “error-prone”
- can’t reason on some security protocols, in particular when ‘confidentiality’ is a threat

1990-93 GNY, VO and AT logic were proposed to overcome the BAN limitations

1994 Syverson and van Oorschot present the SVO logic which unifies the previous four protocols overcoming the BAN limitations trying to maintain its simplicity

The SVO logic

BAN logic limitations

1. no way to evaluate if the idealized form is valid (error-prone)
2. no method to check the validity of the initial assumptions (possible strange conclusions)
3. BAN syntax and inference rules cannot reason about some security protocols, in particular when ‘confidentiality’ is a threat

For example, BAN logic assumes that all the involved parties are honest. Thus, it doesn’t allow to find security flaws caused by malicious parties.

SVO logic:

- does not simply extends with a new notation and rules the BAN logic (potentially unsound)
- defines a new model of computation and a logic that is sound with respect to that model
- retains the expressiveness of the various BAN extensions (GNY, AT and VO) remaining a way simpler than them

Logic steps

While a BAN logic verification typically takes the following steps: (i) idealizing the original protocol, (ii) defining assumptions about the initial state (iii) applying inference rules repeatedly until getting the intended results, SVO divides it in 5 steps:

(i) defining assumptions about the initial state
(ii) annotating a target security protocol
(iii) asserting comprehension of the received messages
(iv) asserting interpretation of comprehended messages
(v) applying inference rules until getting the intended results

Note: the BAN idealization is split into steps (iii) and (iv) in order to solve the BAN idealization problems.

Notation

SVO extends and redefines the BAN notation as follows: (where P and Q are principals, X is a message and K is a key)

SVO [1/2]

- $\neg\varphi$: logic negation of a formula φ
- P believes X: P acts as if X is true
- P received X: P has received a message including X
- P said X: P sent X at one time
- P controls X: P has jurisdiction on X
- $fresh(X)$: X is fresh
- $P \overset{K}{\longleftrightarrow} Q$: K is a shared key between P and Q.
- $\{X\}_K$: X is encrypted with K

Notation

SVO [2/2]

- $PK(P, K)$: K is a public key of P. Also the following notation can be used
  - $PK_\sigma(P, K)$ K is a public signature key
  - $PK_\psi(P, K)$: K is a public ciphering key
- $\lfloor X \rfloor_K$: X is signed with K
- $SV(X, K, Y)$: given a signed message X, applying K to it verifies that X is the result of signing Y with the corresponding private key of K
- $\langle X \rangle_{*P}$: P does not know or recognize X but P will recognize $\langle X \rangle_{*P}$ if it will receive the message again.
- X from P: X was sent by P

Inference rules

While BAN logic has several inference rules SVO logic has only two: *Modus Ponens* (MP) and *Necessitation* (NE).

Modus Ponens

$$\frac{\varphi \quad \varphi \rightarrow \psi}{\psi}$$

Necessitation

$$\frac{\vdash \varphi}{\vdash P \text{ believes } \varphi}$$

'$\Gamma \vdash \psi$' means the formula ψ can be derived from the set of formulae Γ plus the axioms. '$\vdash \varphi$' means that φ is a theorem, derivable from axioms alone.

Axioms [1/2]

Belief Axioms (BA)

- **BA1**: $(P \text{ believes } \varphi \wedge P \text{ believes } (\varphi \to \psi)) \to P \text{ believes } \psi$
- **BA2**: $P \text{ believes } \varphi \to P \text{ believes } (P \text{ believes } \varphi)$

Source Association Axioms (SAA)

- **SAA1**: $(P \overset{K}{\longleftrightarrow} Q \wedge R \text{ received } \{X \text{ from } Q\}_K) \to (Q \text{ said } X \wedge Q \text{ has } X)$
- **SAA2**: $(PK_\sigma(Q, K) \wedge R \text{ received } X \wedge SV(X, K, Y)) \to Q \text{ said } Y$

Receiving Axioms (RA)

- **RA1**: $P \text{ received } (X_1, ..., X_n) \to P \text{ received } X_i, \text{ for } i = 1, ..., n$

Axioms [2/2]

Saying Axioms (SA)

- **SA1**: P said $(X_1, \ldots, X_n) \rightarrow (P$ said $X_i \wedge P$ has $X_i)$, for $i = 1, \ldots, n$
- **SA2**:
  P says $(X_1, \ldots, X_n) \rightarrow (P$ said $(X_1, \ldots, X_n) \wedge P$ says $X_i)$, for $i = 1, \ldots, n$

Freshness Axioms (FA)

- **FA1**: $\mathit{fresh}(X_i) \rightarrow \mathit{fresh}(X_1, \ldots, X_n)$, for $i = 1, \ldots, n$

Jurisdiction and Nonce-Verification Axioms

- **NVA**: $(\mathit{fresh}(X) \wedge P$ said $X) \rightarrow P$ says X
- **JA**: $(P$ controls $\varphi \wedge P$ says $\varphi) \rightarrow \varphi$

The MIPv6 standard

MIPv6

Mobile IP (MIP) are a set of protocols developed as a subset of Internet Protocol (IP) to support mobile connections, in particular to allow mobile device users to move from one network to another while maintaining a **permanent IP address**[1].

Mobile IPv6 (MIPv6), is the MIP implementation for the next generation of the Internet Protocol, IPv6. MIPv6 is defined in RFC 6275.

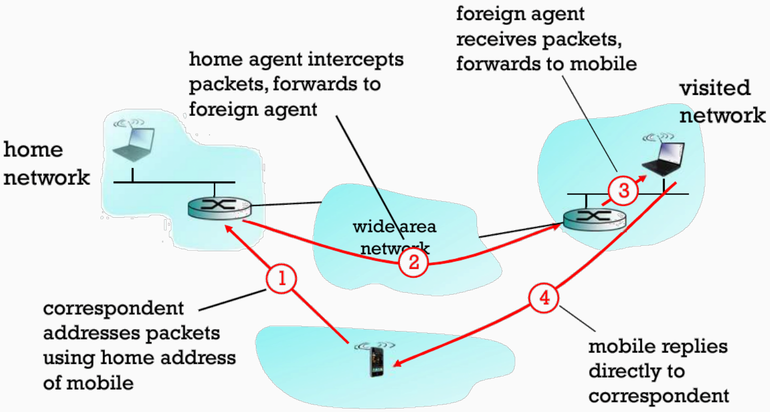
[1] Fundamental for mobility

Mobile communication

How to manage the network communication inside an "high-mobility" context, making it transparent to the user? Two possible solutions:

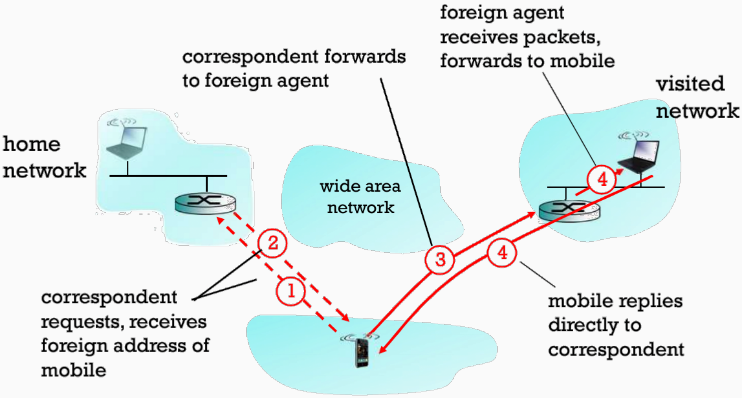
1. Indirect routing (or Bidirectional Tunneling)
2. Direct routing (or Route Optimization)

Indirect routing



- Inefficient due to triangle routing

Direct routing



- Solves the triangle routing inefficiency

Binding

Every mobile node has two addresses: the *Home Address* (*HoA*) and the *Care-of Address* (*CoA*). The *HoA* is a permanent address related to the Home Network of the node, while the *CoA* is a temporary address related to its current *visited network*[2]. The relation between the two addresses is called binding.

So, it's necessary for every mobile node to update its binding information whenever changing its location, this procedure is called binding update and is performed between the mobile node and the router of the visited network, i.e. the *Corresponding Node* (*CN*).

[2]Which makes it reachable inside the visited network

Security in MIPv6

Redirect attacks

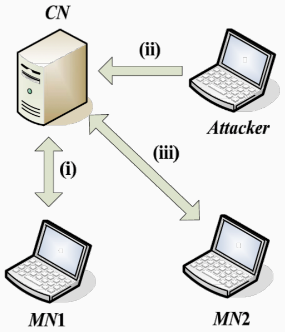
In MIPv6, when moving to a new network, every MN should inform both its HA and CNs of its new location, i.e., CoA, through the binding update message. If such a binding update procedure is not secured, MIPv6 is vulnerable to the redirect attacks. They can be classified into two categories:

- Session Hijacking (SSH)
- Malicious Mobile Node Flooding (MMF)

Furthermore, the binding update procedure has to be carefully designed not to be vulnerable to the Man-In-The-Middle (MiTM) and Denial of Service (DoS) attacks

Session Hijacking (SSH)

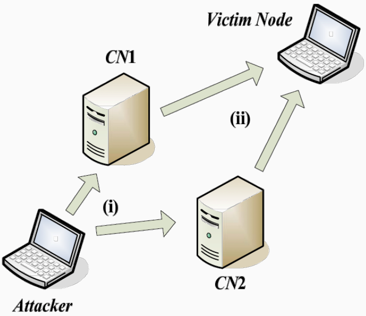
Aims to steal victims' session. The Attacker tries to launch this attack by sending the CN a forged *binding update* message or an old one, which claims that MN1 has moved to a new CoA owned by MN2. If successful, CN redirects MN1's traffic to MN2. Prevented authenticating the *MNs* and their binding update messages.



(i) *MN*1 communicates with *CN*
(ii) *Attacker* sends a forged binding update message to *CN*
(iii) *MN*2 steals the *MN*1's session while communicating *CN*

Malicious Mobile Node Flooding (MMF)

Aims to making victims flooded. The Attacker communicates with several CNs, i.e., CN1 and CN2 sending a binding update message arguing it has moved to the Victim Node's location. If the CNs approve the message, they redirect the MN's traffic to the Victim Node at the same time. Prevented checking if the *MN* exists at the claimed address (address test).



It is assumed that Attacker is a legitimate node.
(i) *Attacker* sends a forged binding update message to *CN*1 and *CN*2
(iii) *CN*1 and *CN*2 sends packets to *Victim Node*

GGA

Challenge: authenticate two previously unknown nodes without global CA or trusted third party. Solved with CGA (`RFC 3972`).

A Cryptographically Generated Address (CGA) is an Internet Protocol Version 6 (IPv6) address that has a host identifier computed from a cryptographic hash function. This procedure is a method for binding a public signature key to an IPv6 address.

- formed by replacing the least-significant 64 bits of the 128-bit IPv6 address with the cryptographic hash of the public key of the address owner (plus auxiliary parameters)
- the messages are signed with the corresponding private key

MIPv6 security protocols and verification

Extension of the SVO logic

There have been attempts to formally verify the MIPv6 security protocols through BAN logic, however BAN logic:

- doesn’t support the CGA method so reasoning about public key validity are not possible
- cannot show the target protocol is not vulnerable to the MMF attack

In order to precisely analyze the MIPv6 security protocols, an extension of the SVO logic with new notation and axioms is proposed.

New notation

The notation is extended as follows:

SVO notation extension

- $ADP(P, A, K)$: The CGA parameters P indicates that the key K is derived from the address A.
- $KA(Q, K, A)$: The principal Q, the key K and the address A are related to each other.
- $OWN(Q, A)$: The principal Q is the owner of the address A.
- $RR(X, Q, A)$: The value X has been sent to the address A to check if the principal Q exists at A.
- $EV(X, K, Q)$: The value X has been encrypted with the PK K and sent to the principal Q.
- $+\{X\}_K$: $(X, MAC(K, X))$, where K is a shared key, X is a message and $MAC(\cdot)$ is a MAC function.
- $Q@A$: Q exists at the address A

New axioms

Mobile Internet Protocol 1 (MIP1)

$$((R \text{ received } AP \text{ from } Q) \wedge ADP(AP, A, K))$$
$$\rightarrow KA(Q, K, A) \wedge PK(Q, K)$$
$$\text{where } PK(Q, K) \text{ can be } PK_\sigma(Q, K) \text{ or } PK_\psi(Q, K)$$

MIP1 formalizes the public key verification through CGA parameters. Note: this does not mean that Q is the owner of A but just that Q is related to K and A

Where P, Q are principals, A an address, K a key and AP are CGA address parameters.

New axioms

Mobile Internet Protocol 2 (MIP2)

$$(KA(Q,K,A) \wedge PK_\sigma(Q,K) \wedge (R \text{ received } X \text{ from } Q \wedge SV(X,K,Y)) \\ \rightarrow (OWN(Q,A) \wedge Q \text{ said } Y)$$

MIP2 verifies the address ownership using MIP1 and digital signature.

Mobile Internet Protocol 4 (MIP4)

$$(RR(X,Q,A) \wedge Q \text{ says } X) \\ \rightarrow Q@A$$

MIP4 formalizes the address test: in order to prevent the MMF attack it is checked that a principal exists at is argued address (i.e., *CoA*, *HoA*).

New axioms

Source Association Axiom 3 (SAA3)

$$((P \stackrel{K}{\leftrightarrow} Q) \wedge (R \text{ received } +\{X \text{ from } Q\}_K)) \\ \rightarrow ((Q \text{ said } X) \wedge (Q \text{ has } X))$$

Saying Axiom 3 (SA3)

$$((Q \text{ said } \{X\}_K \text{ to } P) \wedge (PK_\psi(P, K)) \\ \rightarrow Q \text{ said } X$$

Notation for MIPv6 security protocols

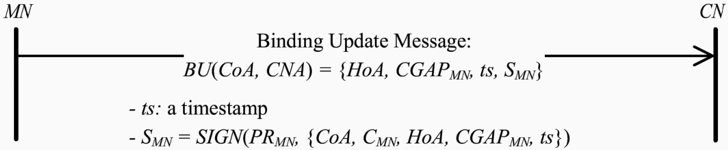
We use the following notation to efficiently express the protocols:

MIPv6 Notation

- $Msg(S, D)$: Msg is sent from S to D, where Msg is a message and S and D are IPv6 addresses.
- MN, HA and CN: a mobile node, an home agent and a corresponding node
- HoA, CoA and CNA: MN's home address and care-of-address, and a CN's address.
- $H(M)$: hash on message M.
- $SIGN(K, M)$: the digital signature on message M with private key K.
- $HMAC(K, M)$: the HMAC operation on message M with shared key K.
- PU_X and PR_X: X's public and private key.
- $CGAP_X$: X's CGA parameters including X's public key.

Analysis on two authentication protocols for MIPv6:

1. Child-proof Authentication for MIPv6 (CAM)
2. Enhanced Route Optimization (ERO) protocol



$$*C_{MN} \equiv CNA$$

Initial state assumptions

- **A11**: CN believes $ADP(CGAP_{MN}, HoA, PU_{MN})$
- **A12**: CN believes $SV(\lfloor BU \rfloor_{PU_{MN}^{-1}}, PU_{MN}, BU)$[3]
- **A13**: CN believes $fresh(ts)$

[3] BU will be defined in the Interpretation step

Security analysis of CAM

Annotation

- **A21**: CN received $(CoA, CNA, HoA, CGAP_{MN}, ts, S_{MN})$

Comprehension

- **A31**: CN believes CN received $(CoA, CNA, HoA, \langle CGAP_{MN}\rangle_{*CN}, ts, \langle S_{MN}\rangle_{*CN})$

Interpretation

- **A41**: CN believes CN received $(CoA, CNA, HoA, \langle CGAP_{MN}\rangle_{*CN}, ts, \langle S_{MN}\rangle_{*CN})$
  $\rightarrow$ CN believes CN received $(BU, \langle \lfloor BU \rfloor_{PU_{MN}^{-1}} \rangle_{*CN})$
  where $BU = (MN@CoA, CNA, MN@HoA, \langle CGAP_{MN}\rangle_{*CN}, ts)$

Security analysis of CAM

Derivation

(From A41)

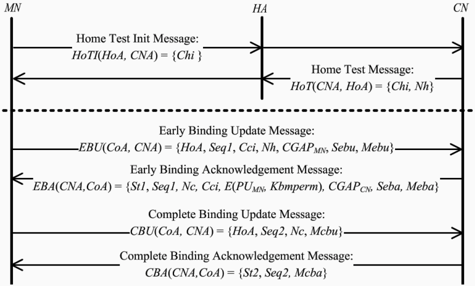
- **D1**: CN believes CN received $(BU, \langle \lfloor BU \rfloor_{PU_{MN}^{-1}} \rangle_{*CN})$
  By A31, A41 and BA1
- **D2**: CN believes CN received $(\langle CGAP_{MN} \rangle_{*CN}$ from $MN)$
  By D1, RA1 and BA1
- **D3**: CN believes $(KA(MN, PU_{MN}, HoA) \wedge PK_{\sigma}(MN, PU_{MN}))$
  By D2, A11, MIP1 and BA1
- **D4**: CN believes $(OWN(MN, HoA) \wedge MN$ said $BU)$
  By D1, RA1, D3, A12, MIP2 and BA1
- **D5**: CN believes MN says BU
  By D4, A13, FA1, NVA and BA1
- **D6**: CN believes MN says $(MN@HoA, MN@CoA)$
  By D5, SA2 and BA1 [47]

Security analysis of CAM

From the previous security proof we can conclude that:

- The CAM protocol is not vulnerable to session hijacking attack, because the MN and its public key are authenticated by the CN (D5)
- These beliefs cannot convince the CN that the MN indeed exists at *HoA* and *CoA* making the protocol vulnerable to the MMF
  - *CN* believes *MN* **says** (*MN*@*HoA*, *MN*@*CoA*)
  - A malicious but legitimate *MN* can trick its *CN* to redirect its traffic to a victim node
  - The ERO protocol solves this issue

Note: this protocol can be formally verified using BAN logic without reasoning about the validity of PU_{MN} (*CN* believes *MN* believes *BU*)



- *Chi*: home init cookie, *Cci*: care-of init cookie
- *Nh*: a home nonce randomly generated by the *CN*
- *Nc*: a care-of nonce randomly generated by the *CN*
- *SeqX*: The *X*th Sequence number of the binding update message
- *StX*: This value indicates the *X*th result of the binding update
- $K1 = H(Nh|Zero64)$, where *Zero64* is composed of 64 0 bits
- $ebuBody = (CoA, CNA, HoA, Seq1, Cci, CGAP_{MN})$
- $Sebu = SIGN(PR_{MN}, ebuBody)$, $Mebu = HMAC(K1, ebuBody|Sebu)$,
- $ebaBody = (CoA, CNA, St1, Seq1, Nc, Cci, E(PU_{MN}, Kbmperm), CGAP_{CN})$
- $Seba = SIGN(PR_{CN}, ebaBody)$, $Meba = HMAC(K1, ebaBody|Seba)$
- $K2 = H(Nc|Kbmperm)$
- $Mcbu = HMAC(K2, CoA|CNA|HoA|Nc|Seq2)$, $Mcba = HMAC(K2, CoA|CNA|St2|Seq2)$

- *HoTI*, *HoT* may be performed before the *MN* changes location
- *Kbmperm* is a longterm secret used to protect the subsequent binding update messages
- HMAC guarantees both the integrity and authenticity of a message
- *MN* shows its presence at *Hoa* and *CoA* proving the receipt of *Nh* and *Nc*
- Once completed *CBA*, *MN* can enter the movement phase

Security analysis of ERO

Initial state assumptions [1/2]

- **A11**: CN believes $ADP(CGAP_{MN}, HoA, PU_{MN})$
- **A12**: CN believes $SV(\lfloor ebuBody \rfloor_{PU_{MN}^{-1}}, PU_{MN}, ebuBody)$[4]
- **A13**: CN believes $fresh(Nh)$
- **A14**: CN believes $RR(Nh, MN, HoA)$
- **A15**: MN believes $ADP(CGAP_{CN}, CNA, PU_{CN})$
- **A16**: MN believes $SV(\lfloor ebaBody \rfloor_{PU_{CN}^{-1}}, PU_{CN}, ebaBody)$[5]
- **A17**: MN believes $fresh(Seq1)$
- **A18**: MN believes CN controls $St1$

[4] where *ebuBody* is defined in the Comprehension step
[5] where *ebaBody* is defined in the Comprehension step

Security analysis of ERO

Initial state assumptions [2/2]

- **A19**: MN believes $RR(Seq1, CN, CNA)$
- **A1a**: MN believes CN controls $fresh(MN \overset{K}{\longleftrightarrow} CN)$
- **A1b**: MN believes $PK_{\psi}(MN, PU_{MN})$
- **A1c**: MN believes CN controls $MN \overset{K}{\longleftrightarrow} CN$
- **A1d**: CN believes $MN \overset{K2}{\longleftrightarrow} CN$
- **A1e**: CN believes $fresh(K2)$
- **A1f**: CN believes $fresh(Nc)$
- **A1g**: CN believes $RR(Nc, MN, CoA)$
- **A1h**: MN believes $fresh(Seq2)$
- **A1i**: MN believes CN controls $fresh(St2)$

Security analysis of ERO

Annotation

- **A21**: CN received (Chi)
- **A22**: MN received (Chi, Nh)
- **A23**:
  CN received $(CoA, CNA, HoA, Seq1, Cci, Nh, CGAP_{MN}, Sebu, Mebu)$
- **A24**: MN received $(CoA, CNA, HoA, Seq1, Nc, Cci, \{Kbmperm\}_{PU_{MN}},$
  $CGAP_{CN}, Seba, Meba)$
- **A25**: CN received $(CoA, CNA, HoA, Seq2, Nc, Mcbu)$
- **A26**: MN received $(CoA, CNA, St2, Seq2, Mcba)$

Comprehension

- **A31**: CN believes CN received $(\langle Chi \rangle_{*CN})$
- **A32**: MN believes MN received $(Chi, \langle Nh \rangle_{*MN})$
- **A33**: CN believes CN received $(ebuBody, \langle Sebu \rangle_{*CN}, \langle Mebu \rangle_{*CN})$
  where
  $ebuBody = (CoA, CNA, HoA, Seq1, \langle Cci \rangle_{*CN}, Nh, \langle CGAP_{MN} \rangle_{*CN}$ from $MN)$
- **A34**: MN believes MN received $(ebaBody, \{\langle Kbmperm \rangle_{*MN}\}_{PU_{MN}},$
  $\langle Seba \rangle_{*MN}, \langle Meba \rangle_{*MN})$ where
  $ebaBody = (CoA, CNA, \langle St1 \rangle_{*MN}, Seq1, \langle Nc \rangle_{*MN}, Cci, \langle CGAP_{CN} \rangle_{*MN}$ from $CN)$
- **A35**: CN believes CN received $(CoA, CNA, HoA, Seq2, Nc, \langle Mcbu \rangle_{*CN})$
- **A36**: MN believes MN received $(CoA, CNA, \langle St2 \rangle_{*MN}, Seq2, \langle Mcba \rangle_{*MN})$

Security analysis of ERO

Interpretation

- **A41**: (A33): CN believes CN received $(ebuBody, \langle Sebu\rangle_{*CN}, \langle Mebu\rangle_{*CN})$
  $\rightarrow CN$ believes CN received $(ebuBody$ from $MN, \langle\lfloor ebuBody\rfloor_{PU_{MN}^{-1}}\rangle_{*CN})$
- **A42** (A34): MN believes MN received $(ebaBody, \{\langle Kbmperm\rangle_{*MN}\}_{PU_{MN}},$
  $\langle Seba\rangle_{*MN}, \langle Meba\rangle_{*MN})$
  $\rightarrow MN$ believes MN received $(\widehat{ebaBody}$ from $CN, \langle\lfloor\widehat{ebaBody}\rfloor_{PU_{CN}^{-1}}\rangle_{*MN})$
  where $\widehat{ebaBody} = (ebaBody, \{MN \xleftrightarrow{\langle K2\rangle_{*MN}} CN\}_{PU_{MN}}, fresh(\langle K2\rangle_{*MN}))$
- **A43** (A35):
  CN believes CN received $(CoA, CNA, HoA, Seq2, Nc, \langle Mcbu\rangle_{*CN})$
  $\rightarrow CN$ believes CN received $+\{(CoA, CNA, HoA, Seq2, Nc,$
  $MN \xleftrightarrow{K2} CN)$ from $MN\}_{K2}$
- **A44** (A36):
  MN believes MN received $(CoA, CNA, St2, Seq2, \langle Mcba\rangle_{*MN}) \rightarrow$
  MN believes MN received $+\{(CoA, CNA, \langle St2\rangle_{*MN}, Seq2)$ from $CN\}_{\langle K2\rangle_{*MN}}$

Security analysis of ERO

Derivation [1/4]

(From A41)

- **D1**: CN believes CN received $(ebuBody$ from $MN, \langle \lfloor ebuBody \rfloor_{PU_{MN}^{-1}} \rangle_{*CN})$
  By A33, A41 and BA1
- **D2**: CN believes CN received $(\langle CGAP_{MN} \rangle_{*CN}$ from $MN)$
  By D1, RA1 and BA1

... applying the same rules as the CAM Derivation on slide 30 we obtain:

- **D4**: CN believes $(OWN(MN, HoA) \wedge MN$ said $ebuBody)$
- **D5**: CN believes MN says $ebuBody$
- **D6**: CN believes MN says (HoA, CoA)
  By D5, SA2 and BA1
- **D7**: CN believes $MN@HoA$
  By D5, SA2, A14, MIP4 and BA1 [48]

that verifies the first part.

Derivation [2/4]

(From A42)

- **D8**: MN believes MN received $(\widehat{ebaBody}$ from $CN, \langle \lfloor \widehat{ebaBody} \rfloor_{PU_{CN}^{-1}} \rangle_{*MN})$
  By A34, A42 and BA1
- **D9**: MN believes MN received $(KA(CN, PU_{CN}, CNA) \wedge PK_{\sigma}(CN, PU_{CN}))$
  By D8, RA1, A15, MIP1 and BA1
- **D10**: MN believes $(MN$ received $OWN(CN, CNA) \wedge CN$ said $\widehat{ebaBody})$
  By D8, RA1, D9, A16, MIP2 and BA1
- **D11**: MN believes CN says $\widehat{ebaBody}$
  By D10, A17, FA1, NVA and BA1
- **D12**: MN believes $\langle St1 \rangle_{*MN}$
  By D11, SA2, A18, JA and BA1

Security analysis of ERO

Derivation [2/4]

...

- **D13**: MN believes $CN@CNA$

  By D11, SA2, A19, MIP4 and BA1
- **D14**: MN believes $fresh(\langle K2 \rangle_{*MN})$

  By D11, SA2, A1a, JA and BA1
- **D15**: MN believes $MN \xleftrightarrow{\langle K2 \rangle_{*CN}} CN$

  By D10, SA1, A1b, SA3, D14, NVA, A1c, JA and BA1 [49]

that verifies the second part.

Derivation [3/4]

(From A43)

- **D16**: CN believes CN received $+\{(CoA, CNA, HoA, Seq2, Nc, MN \xleftrightarrow{K2} CN)$ from $MN\}_{K2}$

  By A35, A43 and BA1
- **D17**: CN believes MN said $(CoA, CNA, HoA, Seq2, Nc, MN \xleftrightarrow{K2} CN)$

  By A1d, D16, SAA3 and BA1
- **D18**: CN believes MN says $(CoA, CNA, HoA, Seq2, Nc, MN \xleftrightarrow{K2} CN)$

  By A1f, D17, FA1, NVA and BA1
- **D19**: CN believes MN says $MN \xleftrightarrow{K2} CN$

  By D18, SA2 and BA1
- **D20**: CN believes $MN@CoA$

  By D18, SA2, A1g, MIP4 and BA1

that verifies the third part.

Security analysis of ERO

- D19 guarantees that the *CN* belief to successfully share *K*2 with the *MN*
- D20 shows that the *CN* trusts the *MN* exists at *CoA*. In other words, the ERO protocol is not vulnerable to the MMF attack anymore

Security analysis of ERO

Derivation [4/4]

(From A44)

- **D21**:
  MN believes MN received $+\{(CoA, CNA, \langle St2\rangle_{*MN}, Seq2)$ from $MN\}_{\langle K2\rangle_{*MN}}$
  By A36, A44 and BA1
- **D22**: MN believes CN said $(CoA, CNA, \langle St2\rangle_{*MN}, Seq2)$
  By D15, D21, SAA3 and BA1
- **D23**: MN believes CN says $(CoA, CNA, \langle St2\rangle_{*MN}, Seq2)$
  By A1h, D22, FA1, NVA and BA1
- **D24**: MN believes $\langle St2\rangle_{*MN}$
  By D23, A1i, JA and BA1

that ends the proof.

Security analysis of ERO

From the formal analysis we obtain the following results:

- The *CN* believes the *MN* owns *HoA* while being at *HoA* and *CoA*. So, the protocol can prevent the redirect attacks (D4, D7, D20)
- *K2* is a good key shared between the *CN* and the *MN* (D14, D15, D19, A1d, A1e)

Conclusions

Conclusions

- A brief introduction about the motivations behind the SVO logic was made. Subsequently, the notation and constructs of SVO were observed, showing that SVO is more than an extension of BAN logic
- We introduced the MIPv6 as the (not so) future standard for mobile communications, showing its architecture and security concerns
- Finally, we gave a formal verification of the MIPv6 security protocols using SVO logic, in particular proving that the CAM protocol is vulnerable to MMF attacks while the ERO protocol is not

Questions?

References

- Syverson, Paul F., and Paul C. Van Oorschot. ”On unifying some cryptographic protocol logics.” *Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy.* IEEE, 1994.
- Syverson, Paul, and Iliano Cervesato. ”The logic of authentication protocols.” *International School on Foundations of Security Analysis and Design.* Springer, Berlin, Heidelberg, 2000.
- Kuang, Shilei, Robert Elz, and Sinchai Kamolphiwong. ”Investigating enhanced route optimization for mobile IPv6.” 2008 *13th Asia-Pacific Computer Systems Architecture Conference.* IEEE, 2008.
- You, Ilsun, Yoshiaki Hori, and Kouichi Sakurai. ”Enhancing SVO Logic for Mobile IPv6 Security Protocols.” *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 2.3 (2011): 26-52.
- Stefano Chessa’s notes for the Mobile and CyberPhysical Systems course.
- Kurose, James F., and Keith W. Ross. ”Computer Networking: A Top-Down Approach . 6th.” Harlow, UK: Pearson Education Ltd (2012).

D4: CN believes $(OWN(MN, HoA) \wedge MN$ said $BU)$

$\implies$ (A13) CN believes $(MN$ said $BU \wedge fresh(ts))$

$\implies$ (FA1) CN believes $(MN$ said $BU \wedge fresh(BU))$

$\implies$ (NVA) $(MN$ said $BU \wedge fresh(BU)) \rightarrow MN$ says BU

D5: CN believes MN says BU

By D4, A13, FA1, NVA and BA1

[30]

$$
\begin{aligned}
& \textbf{D5}:\ CN \text{ believes } MN \text{ says } ebuBody \\
\Longrightarrow\ & \text{(SA2) } CN \text{ believes } MN \text{ says } Nh \\
\Longrightarrow\ & \text{(A14) } CN \text{ believes } (MN \text{ says } Nh \wedge RR(Nh, MN, HoA)) \\
\Longrightarrow\ & \text{(MIP4) } (MN \text{ says } Nh \wedge RR(Nh, MN, HoA)) \rightarrow MN@HoA \\
& \textbf{D7}:\ CN \text{ believes } MN@HoA
\end{aligned}
$$

By D5, SA2, A14, MIP4 and BA1

[38]

D10: MN believes (MN received $OWN(CN, CNA) \wedge CN$ said $\widehat{ebaBody}$)

$\Longrightarrow$ (SA1) MN believes CN said $\{MN \xleftrightarrow{\langle K2 \rangle *MN} CN\}_{PU_{MN}}$

$\Longrightarrow$ (A1b) MN believes (CN said $\{MN \xleftrightarrow{\langle K2 \rangle *MN} CN\}_{PU_{MN}} \wedge PK_{\psi}(MN, PU_{MN})$)

$\Longrightarrow$ (SA3) ((CN said $\{MN \xleftrightarrow{\langle K2 \rangle *MN} CN\}_{PU_{MN}}) \wedge (PK_{\psi}(MN, PU_{MN}))$
$\rightarrow$ (CN said $MN \xleftrightarrow{\langle K2 \rangle *MN} CN$)

$\Longrightarrow$ (D14) MN believes ($fresh(\langle K2 \rangle_{*MN}) \wedge$ (CN said $MN \xleftrightarrow{\langle K2 \rangle *MN} CN$))

$\Longrightarrow$ (NVA) ($fresh(\langle K2 \rangle_{*MN}) \wedge$ (CN said $MN \xleftrightarrow{\langle K2 \rangle *MN} CN$))
$\rightarrow$ (CN says $MN \xleftrightarrow{\langle K2 \rangle *MN} CN$)

$\Longrightarrow$ (A1c) MN believes ((CN controls $MN \xleftrightarrow{K} CN) \wedge$ (CN says $MN \xleftrightarrow{\langle K2 \rangle *MN} CN$))

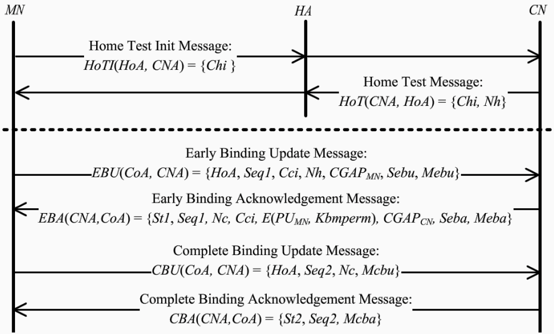
$\Longrightarrow$ (JA) ((CN controls $MN \xleftrightarrow{K} CN) \wedge$ (CN says $MN \xleftrightarrow{\langle K2 \rangle *MN} CN$))
$\rightarrow$ ($MN \xleftrightarrow{\langle K2 \rangle *CN} CN$)

D15: MN believes $MN \xleftrightarrow{\langle K2 \rangle *CN} CN$

By D10, SA1, A1b, SA3, D14, NVA, A1c, JA and BA1

[40]

ERO protocol



- *Chi*: home init cookie, *Cci*: care-of init cookie
- *Nh*: a home nonce randomly generated by the *CN*
- *Nc*: a care-of nonce randomly generated by the *CN*
- *SeqX*: The *X*th Sequence number of the binding update message
- *StX*: This value indicates the *X*th result of the binding update
- $K1 = H(Nh|Zero64)$, where *Zero64* is composed of 64 0 bits
- $ebuBody = (CoA, CNA, HoA, Seq1, Cci, CGAP_{MN})$
- $Sebu = SIGN(PR_{MN}, ebuBody)$, $Mebu = HMAC(K1, ebuBody|Sebu)$,
- $ebaBody = (CoA, CNA, St1, Seq1, Nc, Cci, E(PU_{MN}, Kbmperm), CGAP_{CN})$
- $Seba = SIGN(PR_{CN}, ebaBody)$, $Meba = HMAC(K1, ebaBody|Seba)$
- $K2 = H(Nc|Kbmperm)$
- $Mcbu = HMAC(K2, CoA|CNA|HoA|Nc|Seq2)$, $Mcba = HMAC(K2, CoA|CNA|St2|Seq2)$