Security Problems in Internet Routing Protocols

Tao Wan, Evangelos Kranakis, Paul Van Oorschot

Digital Security Group
School of Computer Science
Carleton University

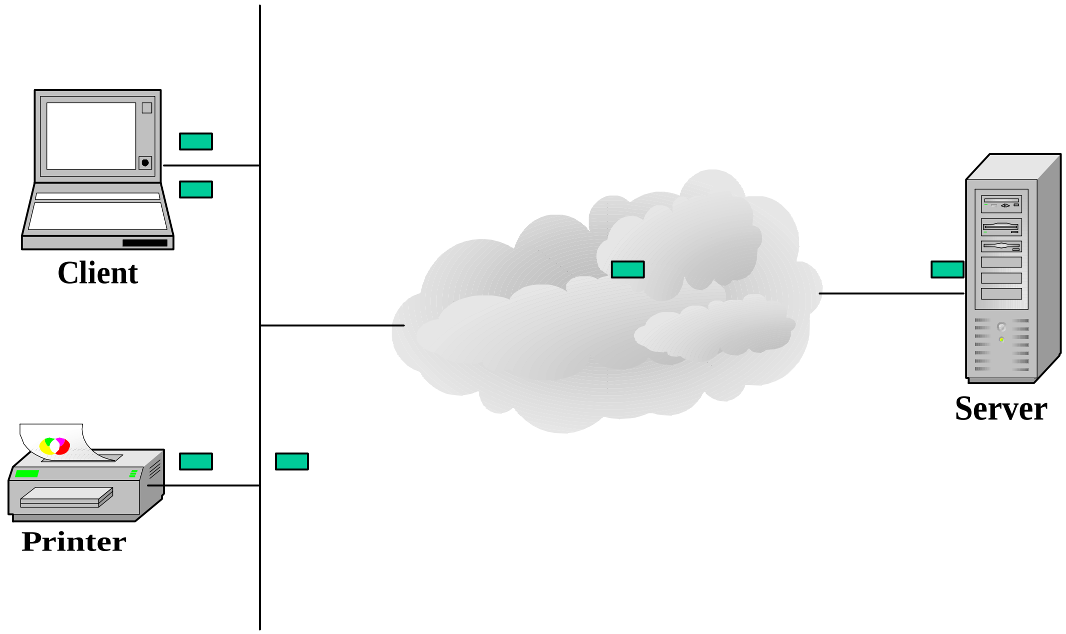
Oct 20, 2003

Outline

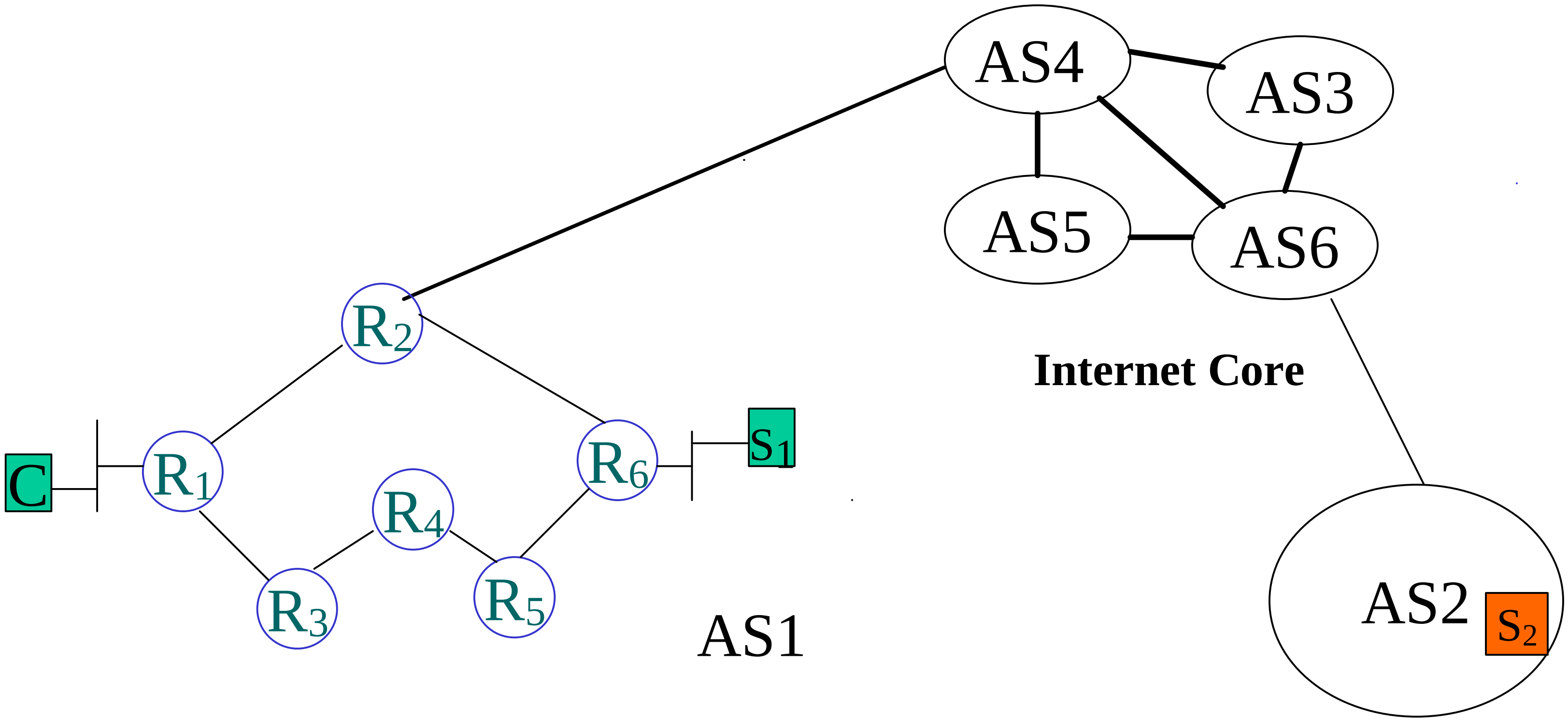
- Introduction
- Routing Protocols & Vulnerability Analysis
- Countermeasures
- Our Approach
- Concluding Remarks

Introduction

An Example of Client/Server Communication

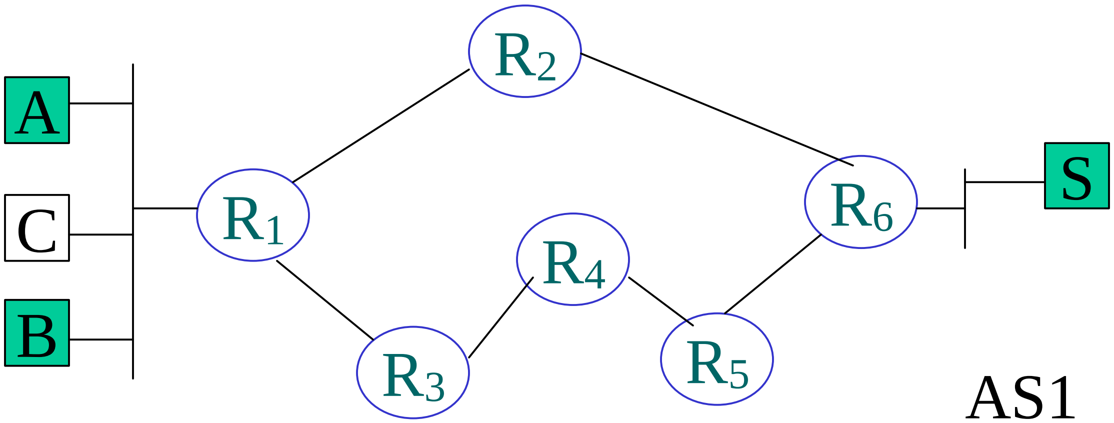


Internet Routing Infrastructures



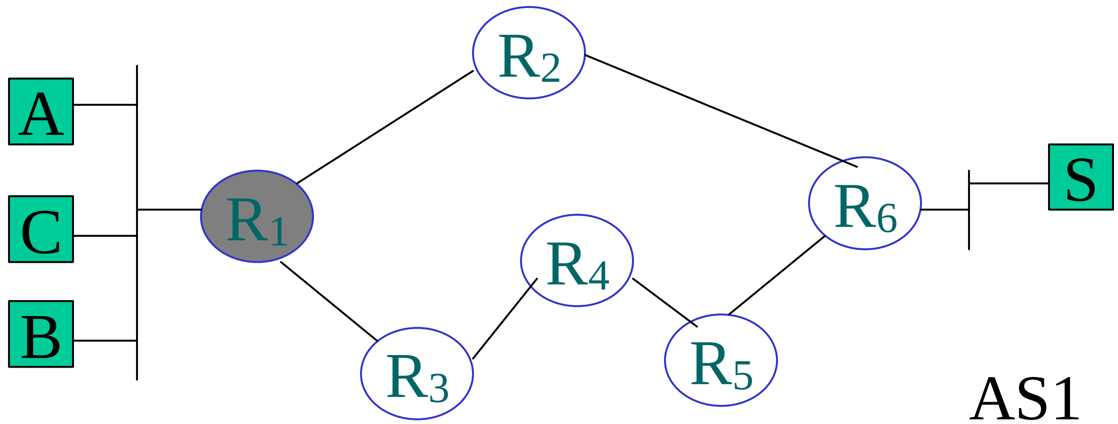
AS: Autonomous System.

Compromise an end-user Computer (C)



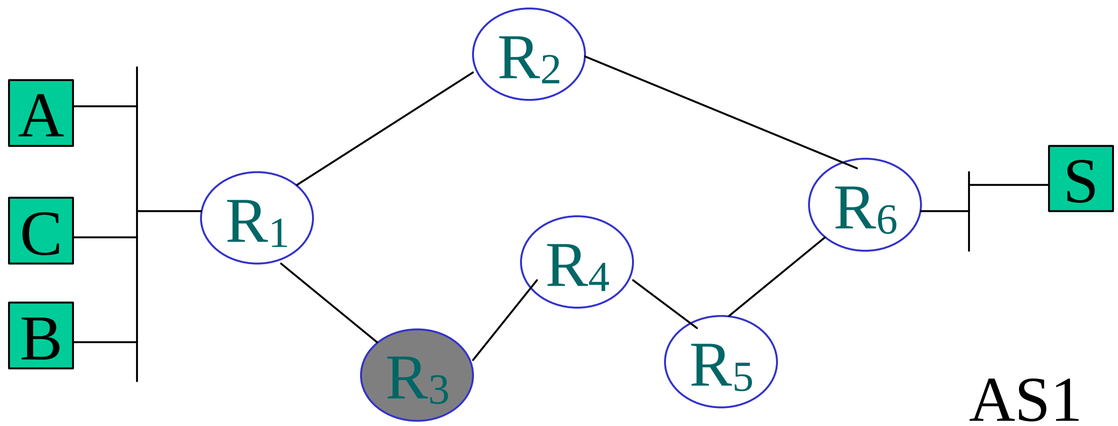
- Eavesdropping (C to/from S, maybe A and B)
- Session Hijacking (C to/from S, but not A or B)
- Denial of Services (C)

Compromise a Router (R_1)



- Eavesdropping (A, B and C to/from S)
- Session Hijacking (A, B and C to/from S)
- Denial of Services

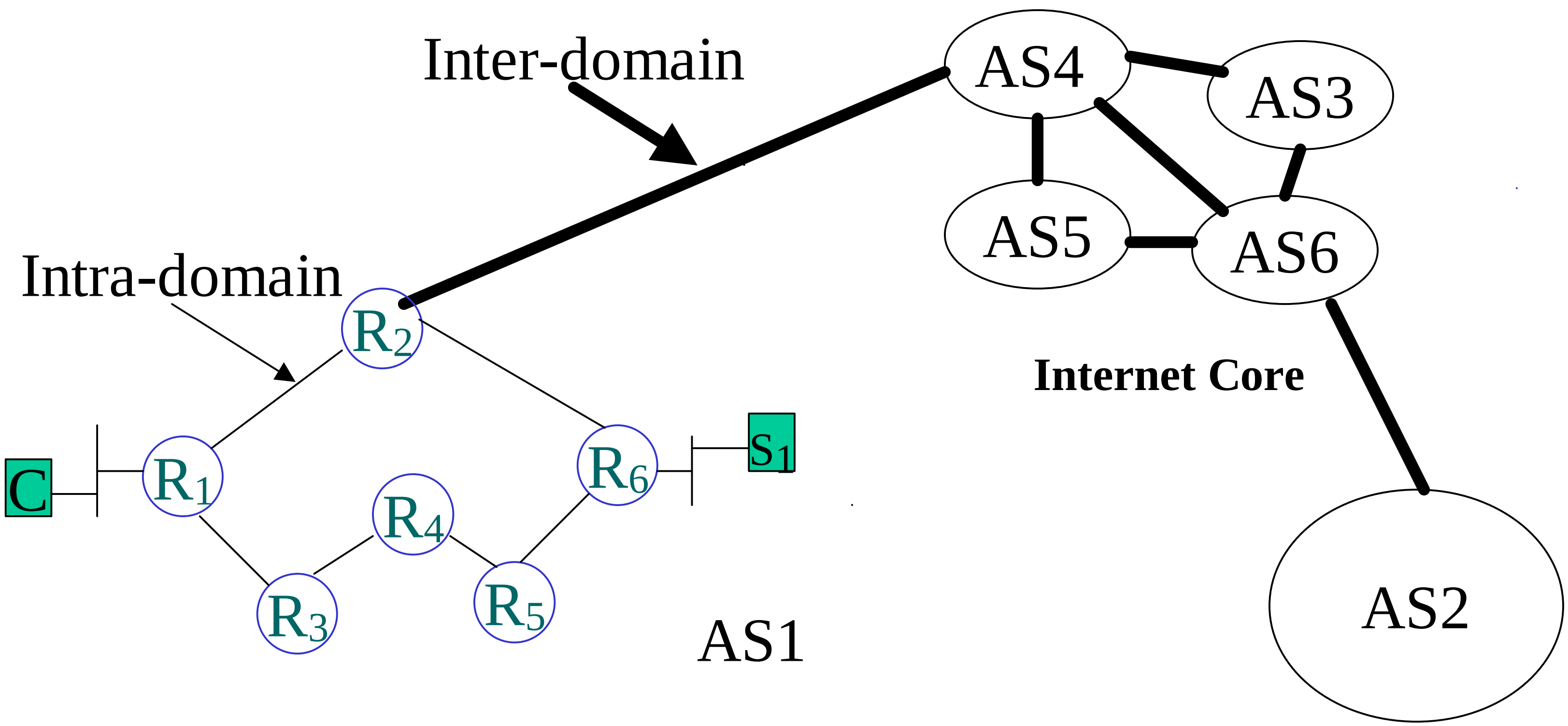
Compromise a Router (R_3)



- Eavesdropping (A, B and C to/from S)
- Session Hijacking (A, B and C to/from S)
- Denial of Services

Internet Routing Protocols & Vulnerability Analysis

Internet Routing Protocols



AS: Autonomous System.

Internet Routing Protocols

- Inter-domain Routing Protocol
  - Border Gateway Protocol (BGP)
- Intra-domain Routing Protocol
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)

Routing Information Protocol (RIP)

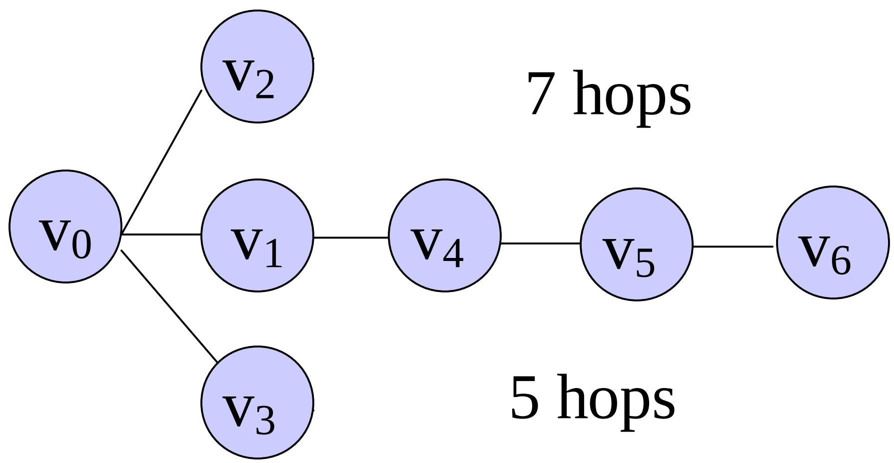
- $G=(V, E)$
- Distance vector routing protocol (v_i)
  - [v_0, dist(v_i, v_0), nextHop(v_i, v_0)]
  - [v_1, dist(v_i, v_1), nextHop(v_i, v_1)]
  - ….
  - [v_n, dist(v_i, v_n), nextHop(v_i, v_n)]
- Distributed Bellman-Ford algorithm
  - $\text{dist}(v_i, v_j)=0$ if $i=j$
  - $\text{dist}(v_i, v_j)=\min\{\text{dist}(v_i, v_k)+ \text{dist}(v_k, v_j)\}$ v_k ? $\text{nb}(v_i)$
- Over UDP

An Example

$V_{2:}$ [v_6, 7, *]
$V_{1:}$ [v_6, 3, v_4]
$V_{3:}$ [v_6, 5, *]

?

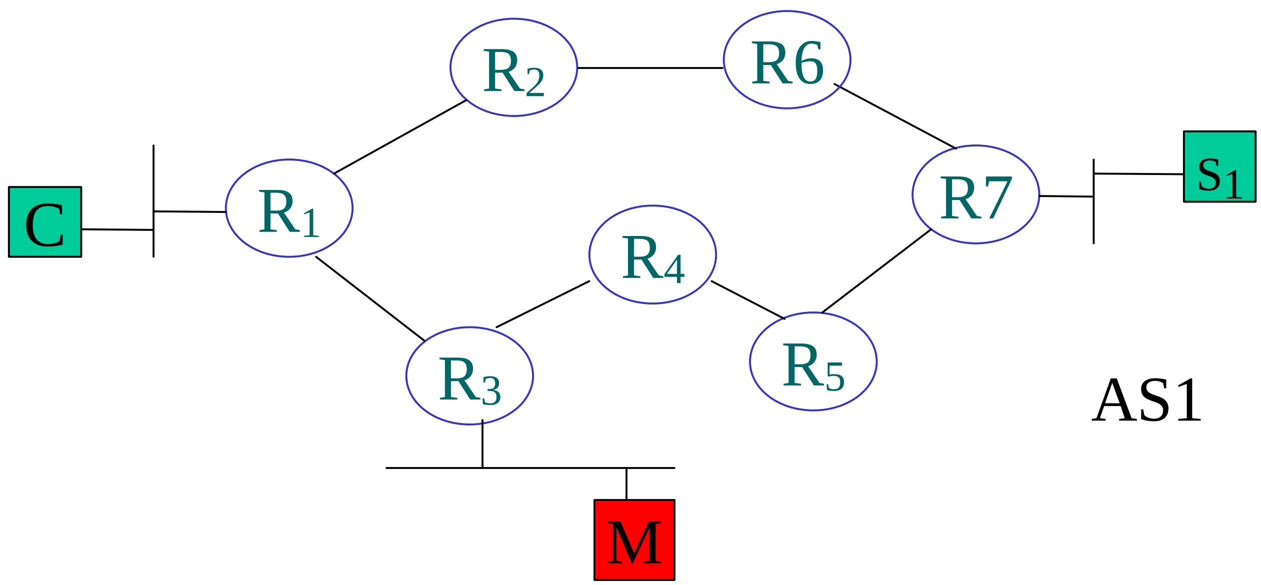
$V_{0:}$ [v_6, 4, v_1]



RIP Vulnerabilities

- Null/weak authentication
  - RIPv1 (*everybody can participate*)
  - RIPv2 (*system-wide password in plain text*)
  - RIPv2 with MD5 (*system-wide shared keys*)
- Manipulating routing advertisements
  - make a distance shorter (*attract traffic*)
  - make a distance longer (*avoid traffic*)
  - Create loops

Joining a RIP domain without authorization



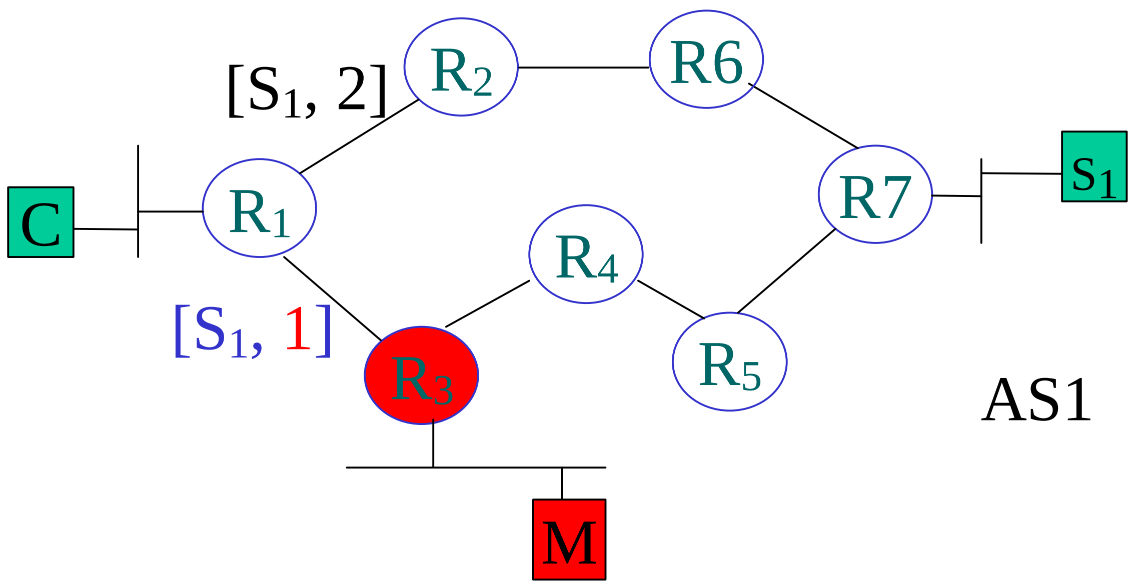
- A malicious node (M) may become a RIP peer by expoiting RIP vulnerabilities.

Shorter Distance Fraud

$R_{2:}$ [S_1, 2]
$R_{3:}$ [S_1, 1]

?

$R_{1:}$ [S_1, 2, R_3]

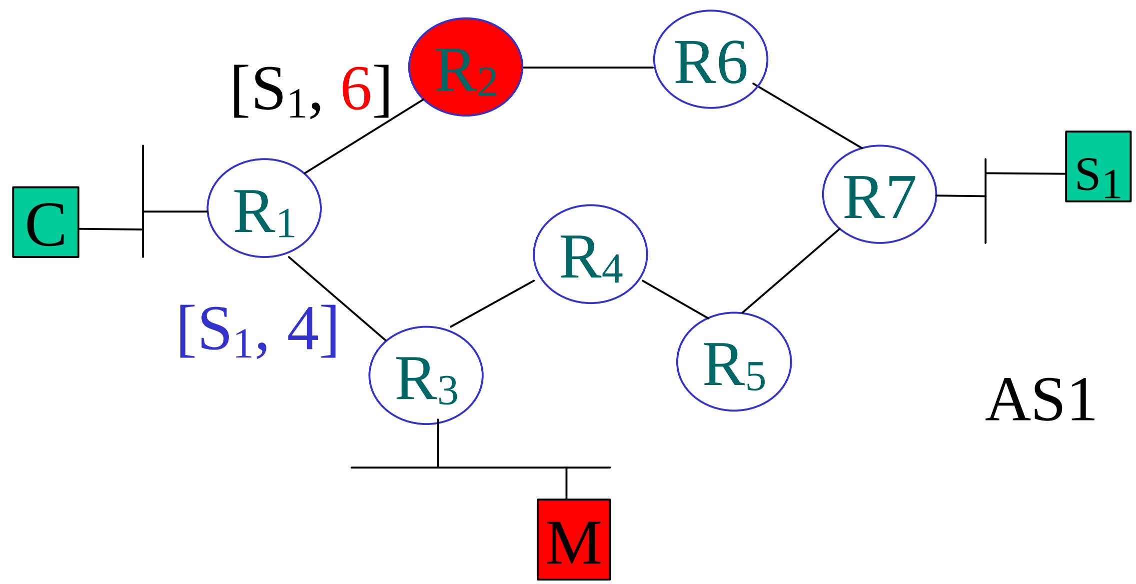


Longer Distance Fraud

R_2: [S_1, 6]
R_3: [S_1, 4]

?

R_1: [S_1, 5, R_3]



Summary of Routing Vulnerabilities

- Routing Protocol Vulnerabilities
  - Lack of security services
    - *entity authentication*
    - *message authentication or integrity*
  - Weak Assumptions
    - *nodes are trustworthy*
    - *Node are cooperative*
- System Vulnerabilities
  - Software flaws
  - Other vulnerable protocols (*SNMP, Telnet, HTTP, etc*)
  - Misconfigurations

Countermeasures

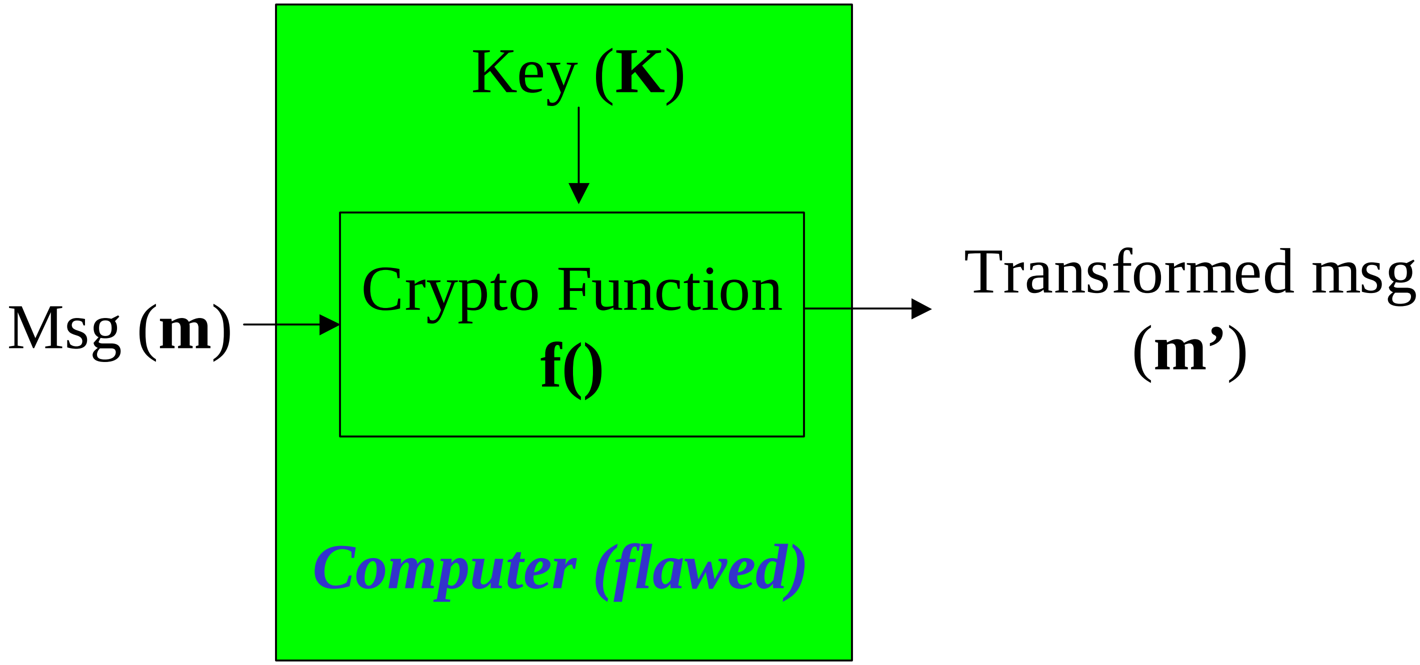
Countermeasures

- Symmetric key mechanisms
  - System-wide shared keys
    - advantage: simple and efficient
    - disadvantage: no entity authentication, compromise one = compromise all
  - Pair-wised shared keys
    - advantage: entity authentication, efficient
    - disadvantage: key management is complex
- Digital Signatures
  - advantage: applicable to cross-domain
  - disadvantage: require public key infrastructures

What does crypto provide us

- Entity Authentication
  - What do you know (e.g., password, PIN, secret key)
  - What do you have (e.g., secure token)
  - what do you inherit (e.g., fingerprint)
- Data Integrity
- Confidentiality, etc

Weak Assumption by Crypto



- Compromising a computer **=** compromising K
- K can be read from disk or memory

What is the Problem

- A correctly signed message may contain false information
- A router with credentials may spread fradulent routing updates
- How to validate the ***factual correctness*** of routing updates ?

Our Approach

- Node Reputations
- Consistency Checks
- Accumulated Confidence
- Sized Window

Node Reputation

- $r_i(j, t_m)$: Node i’s rating of node j’s reputation at time t_m

$$r_i(j, t_m) \; ? \; \mathop{?}\limits_{t?1}^{t_m} [c_i(j,t) \; ? \; w(t)]$$

  - $c_i(j,t)$: a value calculated based on i’s determination of the correctness of j’s information at time t;
  - $w(t)$: a time weighting factor

$$c_i(j,t) \; ? \; \begin{array}{l} ?0.5 \quad \text{if j provides consistent information at time t} \\ ? \\ ?0 \quad \text{otherwise} \end{array}$$

$$w(t) \; ? \; \frac{1}{2^{tm ? t ? 1}}$$

Node Reputation

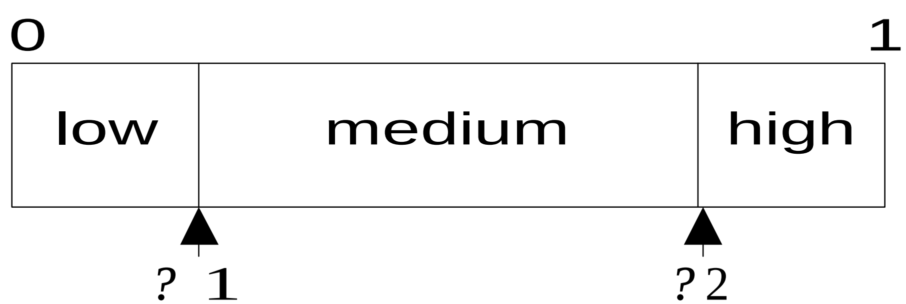
- A new reputation can be computed from a previous one.

$$r_i(j,t ? 1) ? \frac{r_i(j,t)}{2} ? c_i(j,t ? 1) \qquad 0 ? r_i(j) ? 1$$

- Examples:
  - Let r_i(j,1)=0.5; after providing an incorrect routing update, r_i(j,2) =0.25; r_i(j,3) =0.125
  - Let r_i(k,1)=0.5; after providing a correct routing update r_i(k,2)=0.75; r_i(k,3)=0.875

Node Reputation

- Two thresholds (✍$_1$,✍$_2$) divide reputation domain into three ranges, *low*, *medium*, and *high*.

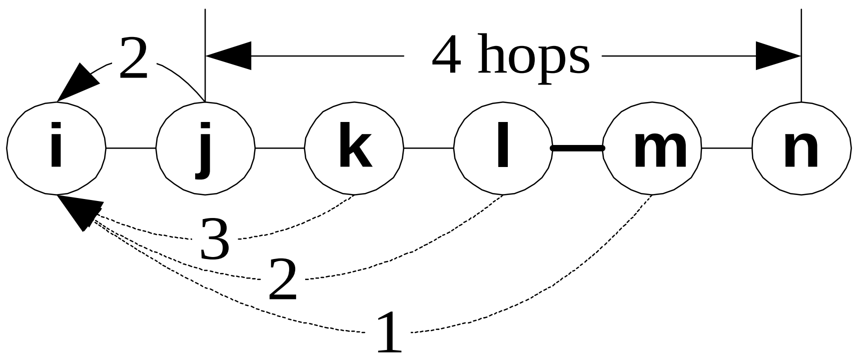


Rules

- Rule 1 (*Low Reputation*): If $0 \le r_i(j) < \theta_1$, node i will *ignore* a routing advertisement received from j without validating it. (*distrusted*)
- Rule 2 (*Medium Reputation*): If $\theta_1 \le r_i(j) < \theta_2$, node i will validate a routing advertisement received from j. (*on probation*)
- Rule 3 (*High Reputation*): If $\theta_2 < r_i(j) \le 1$, node i will accept a routing advertisement received from j without validating it. (*trusted*)
- Rule 4: Node reputation is periodically re-initialized with a value in the medium range.

Consistency Checks

- Use consistency to approximate correctness
- Check the consistency of an advertise route with those nodes that are informed of that route.



Consistency Checks in Other Contexts

- Paper Reviewing
- Reference Letters
- Intrusion detection by anomaly analysis
- Correlate sensor outputs in a distributed sensor network

Accumulated Confidence

- If nodes v_1, v_2, …, v_n agree with each other on an advertised route, node i calculate its accumulated confidence in that route as :

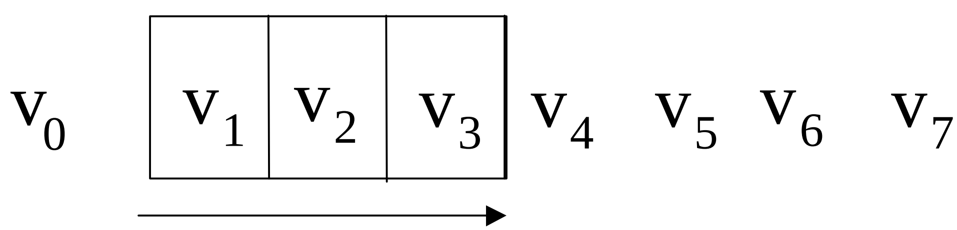
$$r_i(v_{[1..n]}) \; ? \; \begin{cases} r_i(v_1) & if\ n\ ?\ 1 \\ r_i(v_1)\ ?\ [1\ ?\ r_i(v_1)]\ ?\ r_i(v_2) & if\ n\ ?\ 2 \\ r_i(v_{[1..n\ ?\ 1]})\ ?\ [1\ ?\ r_i(v_{[1..n\ ?\ 1]})]\ ?\ r_i(v_n) & if\ n\ ?\ 2 \end{cases}$$

Properties

- An entity with a reputation of 0 does not contribute to an accumulated confidence.
- An entity with a reputation of 1 increases an accumulated confidence to 1.
- The order by which entities to be consulted is of no significance.
- Consistent with Dempster-Shafer Theory of Evidence Reasoning

Sized Window

- A sized window starts with only one node, which is the originator of the advertised route to be validated.
- The window size keeps growing until:
  - the accumulated confidence in the corroborating group is greater than ✍$_2$; or
  - all the informed nodes have been involved; or
  - disagreement arises



An Example - Secure RIP (SRIP)

- Prevent fraudulent routing updates from spreading
- Incremental Deployable
- Incremental Security
- Simulated in Network Simulator NS-2

Concluding Remarks

- "*Abuse of the routing mechanisms and protocols is probably the simplest protocol-based attack available*." Steven Bellovin, 1989.
- Securing routing infrastructures is a hard problem.
- Future work - Study Border Gateway Protocol (BGP)

Acknowledgements

- MITACS
- OCIPEP
- Alcatel Canada

Thanks!