BARTER: Profile Model Exchange for Behavior-based Access Control in MANETs

IBM Security and Privacy Day, Nov '06

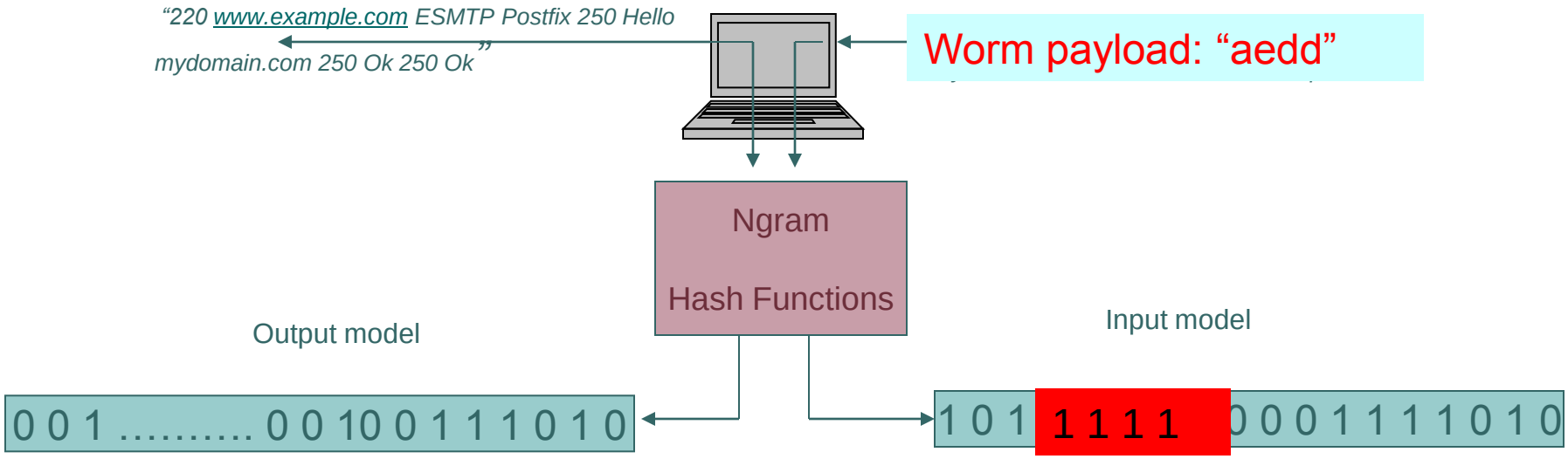
Vanessa Frías-Martínez
Salvatore J. Stolfo
Columbia University

What is Barter and why do we need it?

- ***Idea***
  - We present a new behavior-based access control method for Mobile Ad-hoc Networks (MANETs) based on the profiles of devices.
  - Membership Acceptance and Update -- Devices are accepted/rejected/expelled to/from the MANET depending on their behavior
- ***Motivation***
  - Current approaches try to port “wired” solutions to MANETs.
  - Distributed cryptographic techniques based on keys.
  - Security at a routing level
  - We propose a comprehensive technique based in profiles for both access control and update membership to enhance, not substitute, previous approaches.

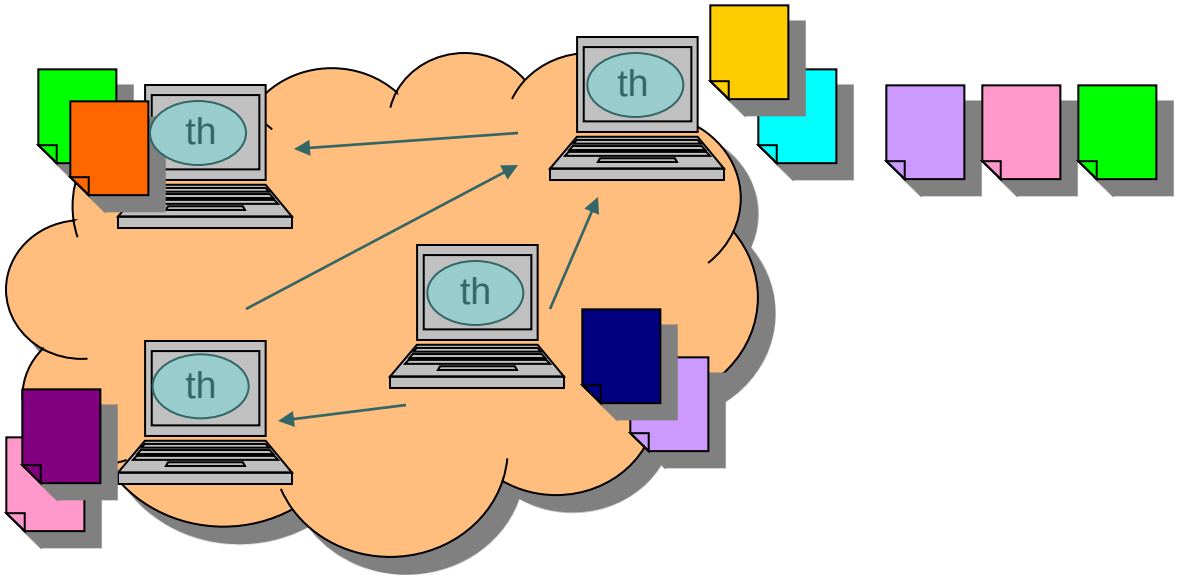
Modeling the behavior

- Behavior = traffic generated and received by a certain application at the host (content modeling)
- Behavior is saved as a BloomFilter (BF) to keep privacy exchanged
- “Good” BloomFilters are obtained by hashing normal, clean traffic to the BF
- “Bad BloomFilters are BF that contain malicious payload of one or more worms hashed into them



Training the system

- Definition of “normal model” for each device in the MANET is captured
  - “Normal”, clean traffic is used to train multiple BFs.
  - The collection of BFs will define a “normalcy threshold”

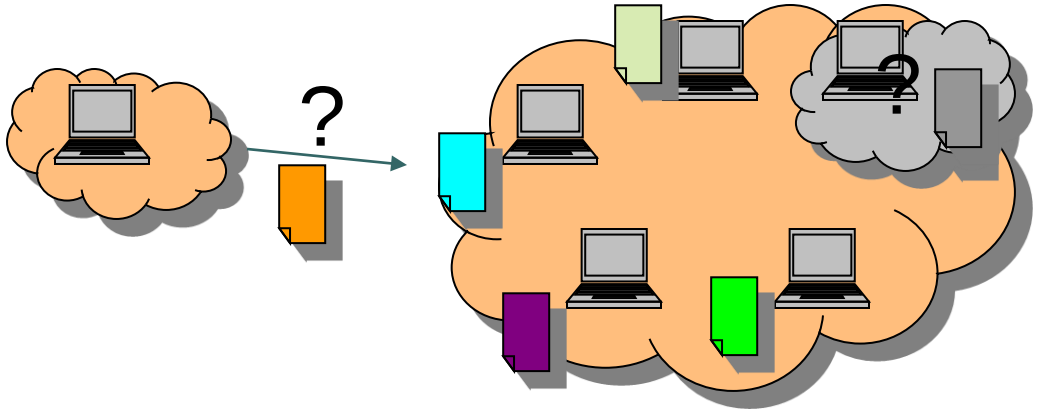


@node 1: d1 = Dist(m_in_1,m_out_2)
d2 = Dist(m_in_1,m_out_3)
d3 = Dist(m_in_1,m_out_4)

th_1 = Max (d1,d2, d3)

Testing the system

- Membership acceptance and update testing:
  - Membership Acceptance and Update -- Devices are accepted to/expelled from the MANET when their models don't differ much from the MANETs' models.
  - Voting System – a distributed voting system among all members decides whether a certain model is similar enough or far too different from the normal model defined in the MANET.



@node i: Dist(m_in_i,m_out_j) < Th_i?
i=1,..i-1,i+1,…n

➔ vote?

TestBed: ORBIT

- Real MANET with real traffic from a MANET application (wireless P2P applications) – avoid network simulators or traffic simulators
- 400-node grid with Debian images located at Rutgers University
- Each node represents a device in a MANET. The nodes are connected via Ethernet or via AODV.
- MANET application: a number of *x* users will exchange emails among them.
- In order to make it realistic, the devices will exchange real email from the ENRON dataset (chat application was also considered but we don't have big chat datasets)
- Once all devices are started, traffic is captured at
  - an SMTP level, to model content exchange
  - at an IP level (with AODV routing, not Ethernet), to model routing information, RREQ, RREP packets, frequency of requests
- Content and Routing is modeled as BloomFilters, and compared versus learnt normal models

BARTER: Profile Model Exchange for Behavior-based Access Control for MANETs

IBM Security and Privacy Day, Nov ’06
Thank You!!

Vanessa Frias-Martinez
Prof. Salvatore J. Stolfo
Columbia University