Strong Security for Active Networks

S. Murphy, E. Lewis, R. Puga, R. Watson and R. Yee

Presenter: Jianhong Xia

10/08/2002

How Strong Security Is

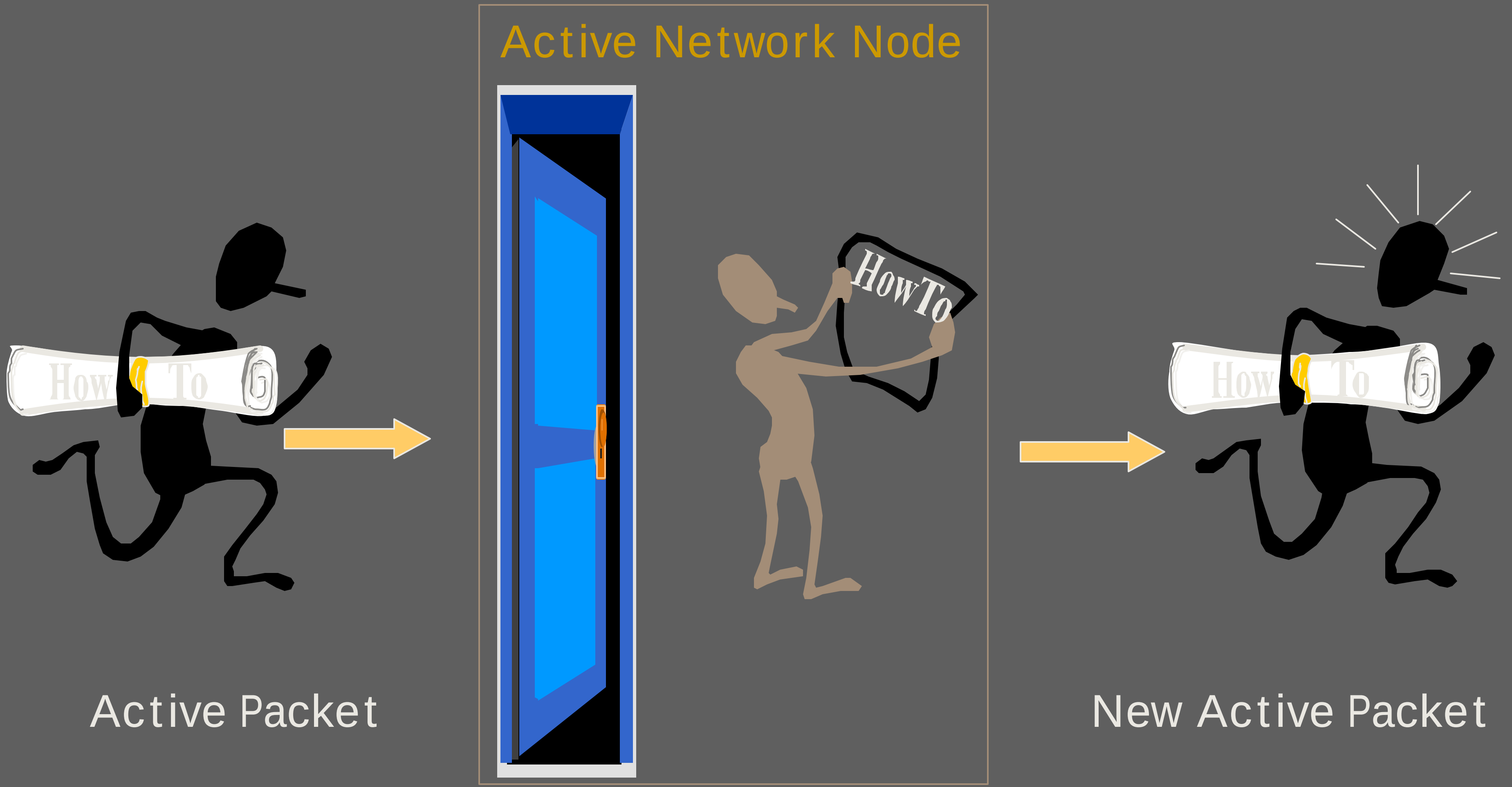
- End-End authentication and integrity protection
- Authorization information carried by active packet itself.
  - Enforcement of each node’s authorization policy
  - End user controls over access of its own state
  - Node policy takes precedence over active code policy

Outline

- Background
- Security Requirements
- Trust Model/Challenges
- SANTS
  - Components
  - Authentication
  - Authorization
- Security Architecture
- Conclusion

Active Networks Security

--- from S. Murphy's slides

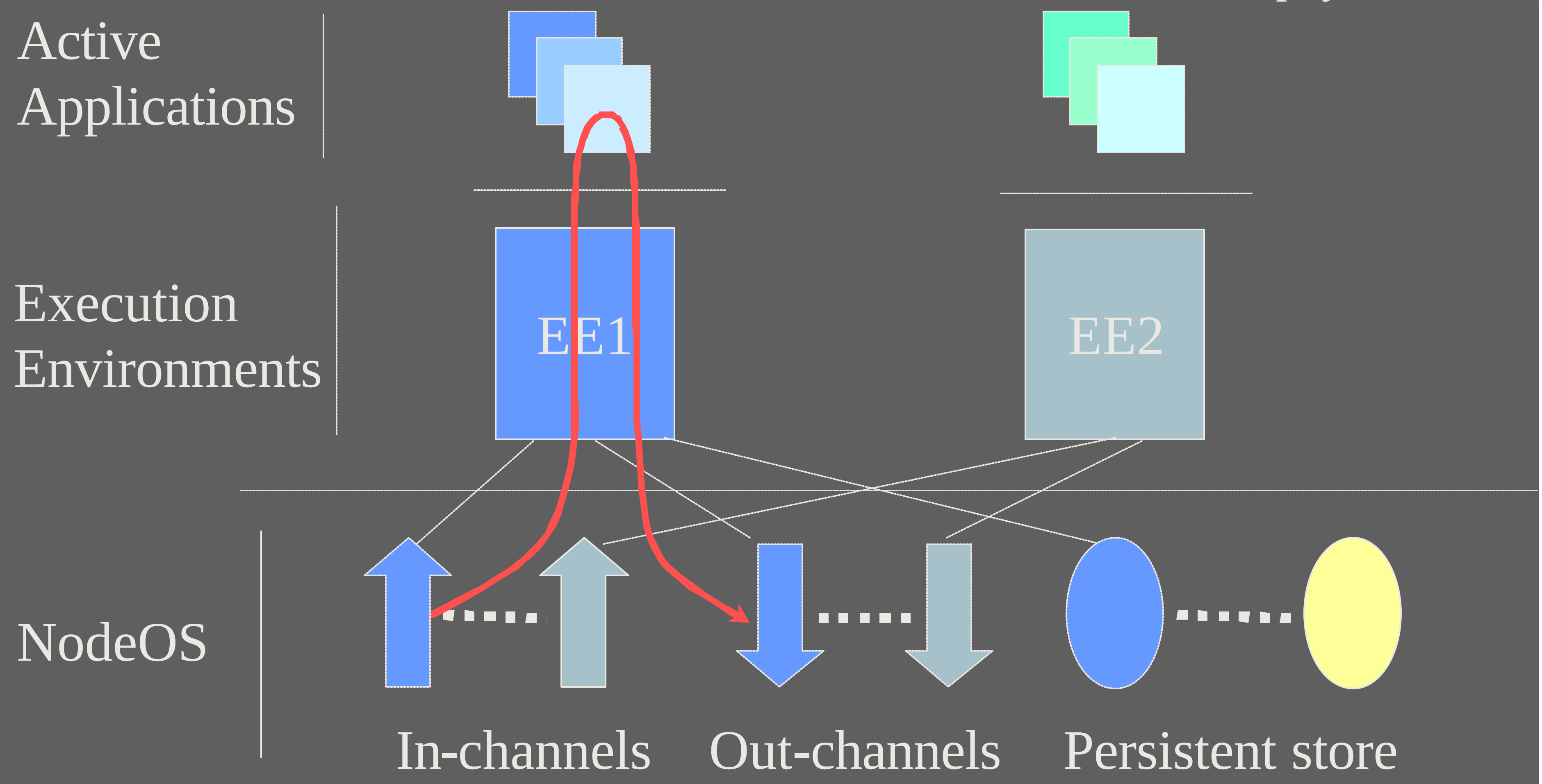


Background

- Features of Active Network
  - Rapid deployment of new network services
  - Complex computations to be performed on packets
- But, Security Concerns
  - Network operators
  - End users

Active Networks Node Architecture

--- from S. Murphy's slides



Security Requirements

- Need to protect
  - End users, Active Node, EE, Active Code/Domain
- End User's security concerns
  - authenticity, integrity and confidentiality
- Active Node/EE's security concerns
  - authorization of use of its services and resources
  - integrity and confidentiality of its own state
- Active Code's security concerns
  - access to its services and sharable persistent states

Trust Model --- End User Viewpoint

- Would rather not trust active nodes, EEs and other active codes
- So, End-End Cryptographic protections
  - Protect its own data from active node and EE
  - But limit the network services in active node
- Expected Features
  - Enable end users to choose trusted nodes/EEs
  - Avoid transmitting the packet to untrusted nodes/EEs

Trust Model --- Node Viewpoint

- Would rather not trust EEs, active codes, arriving packets
- Control over the allocation of resources and privileges to an EE's domain
- Balance the trust it holds in an EE
- Control the threat from active code
- countering clogging attacks from arriving packets is another research area.

Trust Model --- EE Viewpoint

- Would rather not trust active codes and arriving packets
- Control the threat from active codes
- Rely on the node to enforce the EE's policy governing acceptance of arriving packets

Trust Model --- Active Code Viewpoint

- Would rather not trust Active node, EEs and other active codes
- Active code must trust the nodes and EE's on/in which it executes
- Avoid those it does not trust
- Enforce its policy to avoid potential attacks from other active codes

Protection Techniques

- Two Approaches
  - Language based
    - Limit the possible actions of programs
    - Low cost technique with a large payoff
  - Authorization based
    - Associate a principal with each request for an action
    - Enforce a policy that states which principals are permitted to perform which actions

Authentication Challenges

- Identification of the principal itself in active networks
  - Multiple and varying principal identities or attributes
- Choice of an authentication mechanism
  - Hop-Hop protections
  - Symmetric/Asymmetric techniques

SANTS

- Security ANTS
- Prototype a secure active network
  - Authorization enforcement
    - nodes, EE's and active code
  - Integrity protection
    - packets
  - Distributed authentication mechanism
    - Retrieval of identities and attributes
    - Dynamic assignment of attributes

Components

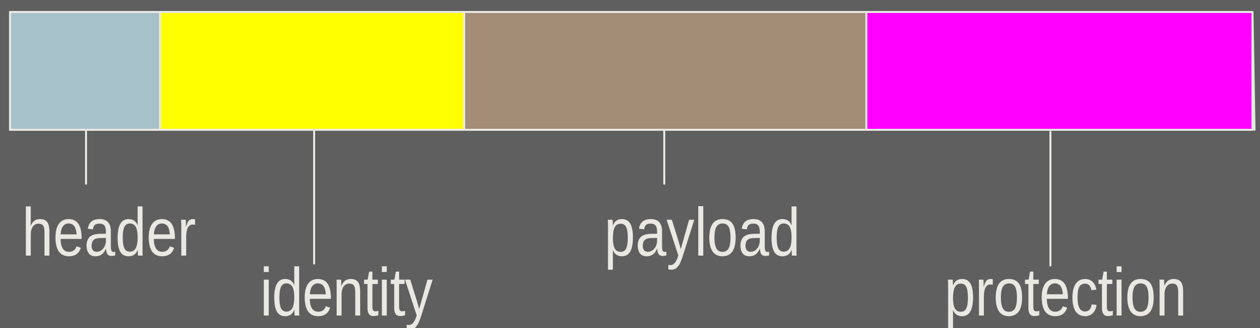
- Authentication
  - X.509v3 certificates
  - DNSSEC
  - Java Crypto API
  - KeyNote policy system
- Authorization
  - Java 2 security features, class loader
  - A separation between EE and Node Classes
  - A shared data capability, Bulletin Board

Authentication

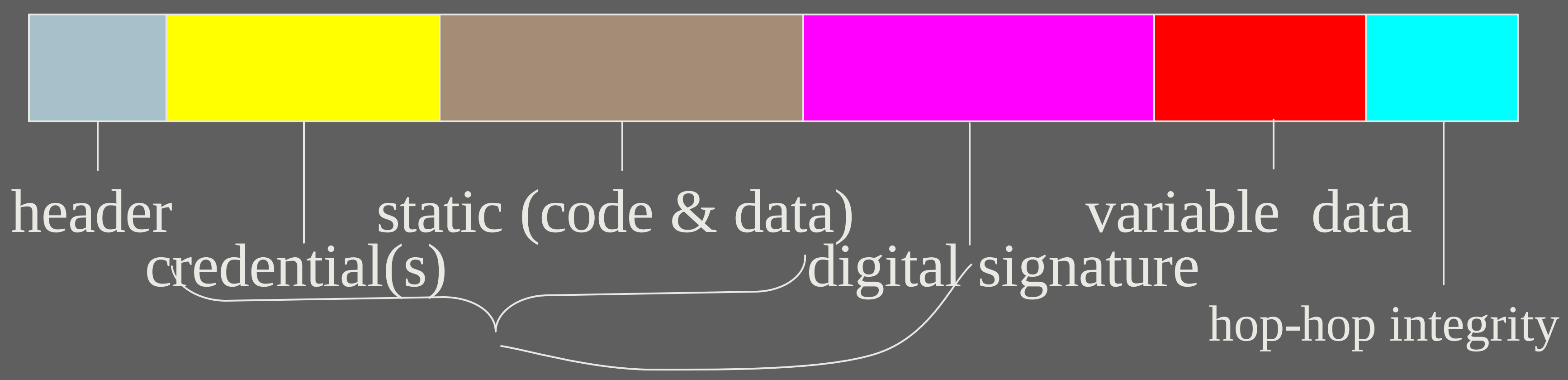
- Hop-Hop
  - HMAC-SHA1 integrity protection
- End-End
  - Digital signature for authentication and integrity protection

Authentication Issues

General Crypto Protected Packet



SANTS Protected Packet



SANTS Authentication

- Strong End-End Authentication
  - Digital Signatures
  - Protection applies to static areas only
- Hop-Hop Integrity
  - HMAC-SHA1
  - Protection Applies to entire packet
- Distributed Security Infrastructure
  - X.509 Certificates stored in DNS CERT records
  - Access uses DNSSEC

SANTS Authorization

- Authorization Control at the NodeOS Level
  - Policy Manager in the NodeOS
  - Policy manager exposed
    - To EE
    - To Active Packet
- Authorization Based on Security Attributes
  - Carried in X.509 Certificates

Bulletin Board

- Active packet travel through the network encountering different administration with their own policies.
- EE provides a Bulletin Board shared data service to incoming active code.

Security Architecture

- Includes:
  - Naming
  - Packet Format
  - Policy Language
  - Security Support System
  - Enforcement Architecture

Security Architecture

- Components should be placed in NodeOS
- Domain creation NodeOS call must include an authentication policy and an access control policy.

Security Processing in NodeOS

- Receive packet
- Verify hop-hop integrity
- Assign packet to existing domain
- Extract credential list
- Check credentials authenticity according to authentication policy for the domain
- Check credentials against access control policy for domain
- Deliver entire packet to the domain, including the credentials, authentication protection fields, etc

Security processing in the EE

- Receive a packet including credentials
- Create a sub-domain, providing
  - security context parameters
  - access control and authentication policies
- Modify
  - access control policy,
  - authentication policy
  - security context
- Add or remove cryptographic protections to user data

Conclusion

- SANTS does provide strong security
  - Fine Grained Authorization
  - Strong End-End Authentication
  - Dynamic Policies
- Too Complicated, is it worthy to apply?