Mobile Agent Security

Quote of the day

"In Ireland the inevitable never happens and the unexpected constantly occurs."
-Sir John Pentland Mahaffy

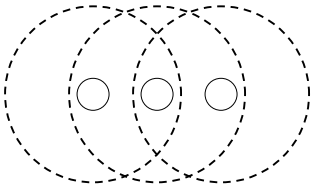
"Everyone is entitled to be stupid, but some abuse the privilege."
-Unknown

Topics of Discussion

- MANETs
- Mobile agents & their applications
- Protecting agents

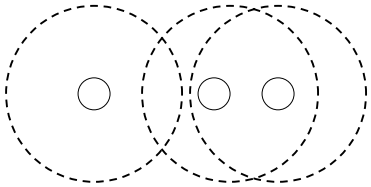
Mobile Ad Hoc NETworks

- MANET – “infrastructure-less”
- Transmission range
- Group coordination – routing



Problem

- Recall, nodes are mobile
- What happens if…



Tactical MANETs

- Joint mission
- Group communication

Issues

- Group connectivity
- Routing
- Secure communication

Possible Solution

Mobile Agents (MAs)

- autonomous
- work on someone's behalf
- well-defined mission
- self-propagating

Mobile Agent Concerns

- Trade-offs with security
- Protect hosts
- Protect agents

Other MA Applications

- Stock-watcher
- Travel agent
- Network manager – respond to changes in network behavior
- PDAs – off-line operation

Protecting Agent

"Towards Mobile Cryptography"
T. Sander & C.F. Tschudin (1998)
Proceedings of the IEEE Symposium on Security & Privacy: 215-224

Requirements for Agent Security

1. Code & execution integrity
2. Computing with secrets in public
3. Code privacy

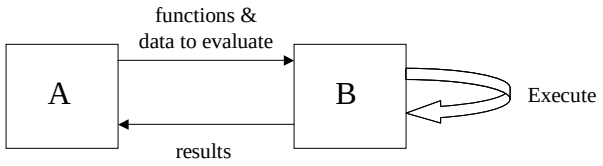
Necessity for MA Security

Move away from cleartext code & data

"In the same sense that you can communicate some ciphermessage to another party without understanding it, we would like a computer to execute a cipherprogram without understanding it."

-Authors

Ideal System



Goals:

1. Non-interactive evaluation
2. Minimal information leakage

Authors' Solution: Signatures

Execute $m = f(x)$

Compute the signature $z = s(m)$

Output the pair (m, z)

Vulnerability!!

Authors' Solution: Corrected

Composition of functions

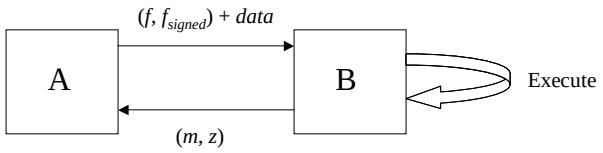
$$f_{signed} := s \circ f$$

Execute $m = f(x)$

Compute the signature $z = f_{signed}(x)$

Output the pair (m, z)

Solution



Goals:

Achieves non-interactive evaluation

Amount of information leakage (security) up to debate

Result of Server Execution

The pair (f, f_{signed}) enables the MA to create signatures on a server without revealing the signature function s

Notice

On input x,

$$f(x) = m \text{ and } f_{signed}(x) = s(f(x)) = s(m).$$

Thus, (m, z) called an *undetachable* signature.

Authors' "Solution"

- More a model
- Kipnis & Shamir showed attack against some authors' assumptions*
- Implementation left open

* "Cryptanalysis of the Oil & Vinegar Signature Scheme." *CRYPTO 1998*: 257-266.

An Implementation

"Secure Transactions with Mobile Agents in Hostile Environments"

P. Kotzanikolaou, M. Burmester & V. Chrissikopoulos
2000 LNCS 1841: 289-297

The Idea

Uses RSA scheme & a hash function (e.g., MD5)

Customer-Server model (transaction analogy)

- Customer creates MA
- Server executes what MA tells it to

Variables

C – customer identifier

req_C – customer requirements

$h = hash(C, req_C)$

S – server identifier

bid_S – server bid

Public Knowledge

Using public key cryptography, therefore (n,e) represents public-key pair of Customer C.

So, (n,e) known by all Servers S.

Composition of MA

As code,

$f(.) := h^{(.)} \bmod n$ **and** $f_{signed}(.) := k^{(.)} \bmod n$

where $k := h^d \bmod n$ is C's signature of h.

Notice,

$f_{signed}(.) = s(f(.)) = s(h^{(.)}) = (h^{(.)})^d = (h^d)^{(.)} = k^{(.)}$.

Composition of MA

As data,

$$(C, req_C).$$

Migrate MA to various servers.

MA execution

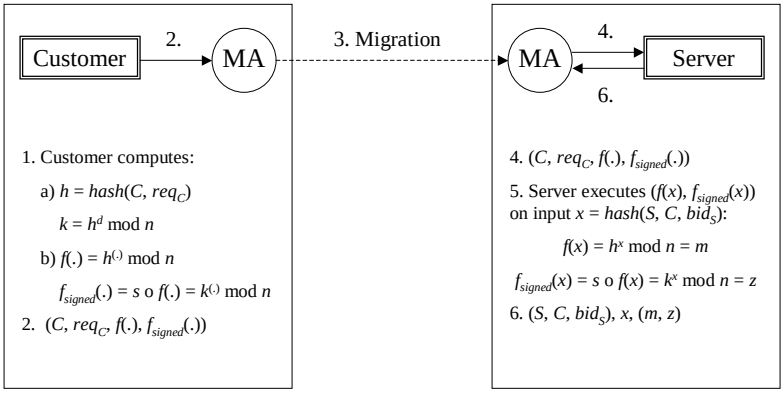
Server inputs $x = hash(S, C, bid_S)$ to f & f_{signed} to obtain (m, z) where

$$m = f(x) = h^x \bmod n$$

and

$$z = f_{signed}(x) = k^x \bmod n = (h^d)^x \bmod n$$
$$= (h^x)^d \bmod n = m^d \bmod n = s(m).$$

Protocol



Signature Validation

- Both customer & servers can validate

Does $z^e \bmod n = m$?

$$z^e = (f_{signed}(x))^e = (k^x)^e \bmod n = ((h^d)^x)^e \bmod n$$
$$= (h^x)^{de} \bmod n = h^x \bmod n = m$$

Issues for Tactical MANETs

- Cleartext messages
- Requirements
- Bids
- Asymmetry

Message Privacy

- Assuming PKI
- Customer encrypts code & data under public key of Server
- Server encrypts result under Customer's public key

Requirements

- What are good fields to include in req_C?
- Recall goals of group connectivity, routing & secure communication (slide 7).

Bids

- What are good fields to include in bid_S?
- Dependent on req_C.

Asymmetry

- Customer is committed to its req_C by a valid signature z.
- Server is not committed to its bid_S.
- To alleviate, Customer requests for the Server to sign its bid.

Review

- MA protection model
- MA protection implementation
  (Burmester et al.)
- Application to Tactical MANETs