Security Issues in Mobile Code Systems

David M. Chess
High Integrity Computing Lab,
IBM T.J. Watson Research Center
Hawthorne, NY, USA

"Mobile code systems are becoming popular and ubiquitous,and while… the security issues that these systems raise must now be dealt with more thoroughly."

Presented by Ruobing Pan

Outline

- Introduction
- Common Assumptions & Their Negations
- New Security Issues
- Conclusion

Introduction

- What is mobile code system?
  - “In mobile code systems, programs or processes travel from host to host in order to accomplish their goals.”
- Two examples of mobile code attacks
  - CHRISTMA EXEC
  - Internet worms
- The advice of the general security community
  - “do not allow programs to execute on arrival, and do not make it too easy for users to execute programs [which are] received across the network.”
- As mobile code systems are becoming popular, it is no longer possible for the security community to say simply “Do not allow...”

Common Assumptions & Their Negations

- Identifying Programs with Persons

1. “Whenever a program attempts some action, we can easily identify a person to whom that action can be attributed, and it is safe to assume that that person intends the action to be taken.”

   Negation for mobile code systems:

   “When a program attempts some action, we may be unable to identify a person to whom that action can be attributed, and it is not safe to assume that any particular person intends the action to be taken.”

2. “When a program attempts some action, we can determine whether or not the action should be permitted by consulting the details of the action, and the rights that have been granted to the user running the program.”

   Negation for mobile code systems:

   “When a program attempts some action,we cannot determine whether or not the action should be permitted by simply consulting (the details of the action, and) the rights that have been granted to the user running the program, since the program may well not reflect the intent of that user.”

Common Assumptions & Their Negations(cont.)

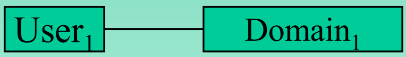
- Identifying Programs with Persons

3. "Only persons that are known to the system can execute programs on the system."

Negation for mobile code systems:

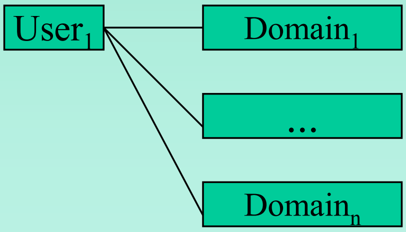
Some person not known to the system may be the most able to determine whether it is appropriate to execute programs on the system.

4. "There is one security domain corresponding to each user; all actions within that domain can be treated the same way. "



Negation for mobile code systems:

"There are potentially many security domains corresponding to each user; different actions initiated by the same user may need to be treated differently."



5. "Single-user systems require no security."

Negation for mobile code systems:

"Even single-user systems require security."

Common Assumptions & Their Negations(cont.)

- Trojan Horses are Rare

1. " Essentially all programs are obtained from easily-identifiable and generally trusted sources."

Trusted sources
Systems

Negation for mobile code systems:

" In mobile code systems,many programs may be obtained from unknown or untrusted sources."

Untrusted sources
Systems

2. "The users of a given piece of software are restrained by law and custom from various actions against the manufacturer's interests."

Negation for mobile code systems:

"The users of a given piece of software may be completely unknown to the owner of the software,and may not restrained by law and custom from various actions against the manufacturer's interests."

Common Assumptions & Their Negations(cont.)

- The Origin of Attacks

1. "Significant security threats come from attackers running programs with the intent of accomplishing unauthorized results."

Negation for mobile code systems:

"Significant security threats come from authorized users running programs which take advantage of the users' rights in order to accomplish undesirable results."

- Programs Stay Put

1. " Programs cross administrative boundaries only rarely, and only when people intentionally transmit them."

Negation for mobile code systems:

"Programs cross administrative boundaries often, and can arrange for their own transmission and reproduction."

Common Assumptions & Their Negations(cont.)

- Programs Stay Put

2. "A given instance of a program runs entirely on one machine; processes do not cross administrative boundaries at all."

Negation for mobile code systems:

"A given instance of a program may cross multiple machines; processes can cross administrative boundaries."

3. "A given program runs on only one particular operating system."

Negation for mobile code systems:

"A mobile program may run on many different operating systems."

4. "Computer security is provided by the operating system."

Negation for mobile code systems:

" Computer security may not be provided by the operating system; program receivers,language interpreters and runtime libraries must also be security-aware."

New security issues

- Authentication in Mobile Code Systems
- Reputation and Trust
- Secure Languages
- Preventing Floods
- The Problem of Malicious Hosts

Conclusion

- This article presents a comprehensive overview of the security issues involved in mobile code systems.
- It makes a good foundation for anyone interested in design and implementation of mobile code systems.

Question:Have you ever met any of these security issues?
Do you know the solution ?