Malevolent host masquerading as oppnet member

Vrishal K Dinar
Kavita P Tipnis
Akshitha Guduru

Department of Computer Science
Western Michigan University

Instructor: Prof. Leszek T. Lilien
15-minute project introduction presented on 9/28/2006
Definition:

Oppnets:
- Set of nodes which are deployed to form a larger network by extending invitations and thereby offering and/or receiving help.

Masquerading:
- Gaining unauthorized access to resources to disseminate (distribute) (mis)information.\textsuperscript{[11]}
Kinds of masquerading

- **Spoofing**: accessing a system as an unauthorized user.\[1\]
  - **Smurf attack** overwhelming a victim with ‘pong’ responses.
- **Phishing**: unauthorized entity attempting to gain sensitive data from gullible user(s). \[1\]
- **Man in The Middle**: attacker tampers data between two parties without their knowledge. \[1\]
Host masquerading

- A malicious entity takes over an oppnet node and looks for potential victims.
- Helpers are ‘ordered’ to release sensitive data under guise of ‘helping the network’.
- For example:
  - A trojan might be released into the network which attempts to gain sensitive data.
  - It might also attempt to do DoS attack on network resources.
Helper node masquerading

- Oppnet inviting a malicious helper to join.
- It might want to acquire resources of other helpers and/or obtain sensitive information.
- It might also try to bring the network down.
Examples of helper masquerading

- In case of a Military base, for example:
  - A traitor or a malicious intruder may pose as a control node and obtain sensitive data.
  - The malicious entity may trade secret information out of the military base camp which could cause potential harm.
Possible solutions

- The oppnet node should have strong authentication mechanisms.
  - for example
    - limiting number of login attempts
    - function generators, etc.
- Digital signatures to verify authenticity.
- 2-FA, SRP
Two-factor authentication (2-F A) is any authentication protocol that requires two independent ways to establish identity and privileges.

This contrasts with traditional password authentication, which requires only one factor (knowledge of a password) in order to gain access to a system.
Extensible Authentication Protocol (RFC 3748)[12]

- EAP is an extensive authentication framework that can be used in wireless networks and P2P connections.
- Several authentication methods/schemes included in EAP are EAP-MD 5, EAP-OTP, EAP TLS.
Secure Remote Password Protocol\cite{8}

- SRP is password authenticated key agreement protocol which allows a user to authenticate himself to a server.
- SRP is resistant to dictionary attacks mounted by an eavesdropper and does not require a trusted third party.
- Only one password can be guessed per attempt.
SRP (2)

- The SRP protocol creates a large private key shared between the two parties in a manner similar to Diffie-Hellman, then verifies to both parties that the two keys are identical and that both sides have the user's password.
- Only one password can be guessed at per attempt in revision 6 of the protocol.
CASE STUDY

- Analogy between Bluetooth and OppNets

Bluetooth: A short-range radio technology for communications among Internet devices and between devices and the Internet.
Special Interest Group

- Ericsson
- Toshiba
- Nokia
- Intel
- IBM
Bluetooth Was Originally a Cable-Replacement Technology [³]

Images copyright bluetooth.org©
Bluetooth’s role in Oppnets\(^4\)

Images copyright Nokia© Corporation.
Establishing a network connection

- Inquire
- Page- synchronizing devices
- Establish a link
- Discover services
- Authenticate
- Login
- Send and receive data
Advantages

- Devices start conversing without user input except where authentication is required.
- Handles both data and voice
- The helper nodes can be identified without much difficulty.
- Bluetooth uses frequency hopping. Its spread spectrum approach greatly reduces the risk that communications will be intercepted.
References

8. All images are copyright of their respective organizations. Appropriate reference to the source is given wherever applicable.