CYGNACOM SOLUTIONS

High Assurance Evaluations
Challenges in Formal Security Policy Modeling & Covert Channel Analysis

Sai Pulugurtha

September 24, 2008

Overview

- Introduction and Goals
- SPM and CCA Requirements in Common Criteria
- SPM and CCA Existing Literature
- Operating Systems vs. Network Information Flow Control Products (e.g. Firewall) comparison
- SPM Challenges– Level of Abstraction in the Model
- CCA Challenges
- Observations
- Future Directions

Introduction

- Based on our experience in developing Formal SPM and CCA evidence (ADV_SPM.3, AVA_CCA.2)
- For an Information Flow Control product (e.g. a Firewall)
- Presentation is based on CC v2.x requirements

Goals

- Point out the challenges faced and observations noted during the development of formal SPM
- Point out the challenges faced and observations noted during the development of CCA evidence
- Point our areas where guidance could be provided in CC v3.x/v4.x based on our observations
- High Assurance Product Developers – What they could do to mitigate some of the channels for a Firewall kind of product

SPM and CCA Requirements in Common Criteria

- Formal SPM Requirements (ADV_SPM.3)
  - Formal representation of information flow control policy of the system
  - Consistent and complete with respect to all policies of the TSP that can be modeled.
  - FSP and SPM correspondence (Semi Formal or Formal)

- CCA Requirements (AVA_CCA.2)
  - Identify covert channels through a systematic search
  - Consider the worst case exploitation scenario for each identified covert channel for estimating channel capacity
  - Estimate channel capacity

SPM Resources Used

- SPM Resources for development of Formal Security Policy Model
  - Formal model is expressed in Z (formally pronounced Zed) notation.
  - Z notation is based on set theory and mathematical logic.
  - Formal representation was produced using ProofPower
  - ProofPower is a suite of tools supporting specification and proof in Higher Order Logic (HOL) and in the Z notation.
  - HOL provides the proof rules that support logical reasoning.

CCA Resources Used

- CCA TCSEC and Other References
  - ~20 years old
- Methods Considered
  - Noninterference analysis
  - Syntactic information-flow analysis
  - Shared Resource Matrix Method
  - Cover Flow Trees (Relatively New)
- Method actually used
  - Shared Resource Matrix Method

Challenges with Formal Modelling

- **Selection of Languages and tools**
- **For an operating system product**
  - **Subjects**
    - Active entities (processes, servers, trusted processes)
    - Often dynamic (e.g. multiple subjects created & destroyed)
  - **Objects** – Passive entities (information containers)

- **For a network Information flow Control Product Subjects**
    - Passive entities(e.g. Network entities sending/receiving information, Network Interface)
    - Sometimes Static (e.g. Network interface accepting information, Rejecting information)
  - **Information –** could be active entities (datagrams,traffic, connections)

Challenges with Formal Modelling (Cont.)

- Model was built from scratch
- If the model is built from Scratch to model the product behaviour
  - Decisions regarding level of abstraction required while modelling have to be made for
    - IP Packets
    - Filter Rules
    - Connections (describing packet processing operations, sessions etc.)
    - Configuration (Set of policies, Rules)
    - Secure State
    - Operations
  - Model should accurately describe the TSF behaviour

Covert Channel Definitions from Various Sources

- Covert Channel (CC) – Illicit information flow (undefined in CC)
- Covert Channel (NCSC) – Given a nondiscretionary (e.g. mandatory) security policy model M and its interpretation I(M) in an operating system, any potential communication between two subjects $I(S_h)$ and $I(S_i)$ of I(M) is a covert if and only if any communication between the corresponding subjects S_h and S_i of the model M is illegal in M.
- Covert Channel (TCSEC) – a communication channel that allows a process to transfer information in a manner that violates the system's security policy.
- Covert Channel (Fisk, NCSC) – a channel that is neither designed nor intended to transfer information at all
- Subliminal channel (Fisk) – a channel where hidden data piggybacks on an innocuous-looking legitimate communication
- Covert Channel [Lampson73] - A communication channel is covert if it is neither designed nor intended to transfer information at all.
- Covert Channel [Kemmerer 83] Covert channels are those that "use entities not normally viewed as data objects to transfer information from one subject to another."

Lampson's definition of covert channel defines covert channel in the broadest terms and may better apply to Network Covert Channels

Implications for Operating Systems, Firewalls and other relevant product types

- Typical Covert Channels for Operating Systems
  - TCSEC guidance geared more towards Operating Systems
  - Guidance is still applicable and apt to find Covert Channels in OS centered products.
- Covert Channels in Networking Products
  - Differ from Typical OS Centric Products
  - Packet information could be used for Covert Communications
  - Covert Channel Vs Steganography
- Did the nature of Covert Channels change in the past 20 years ?

Selection of a method for CCA

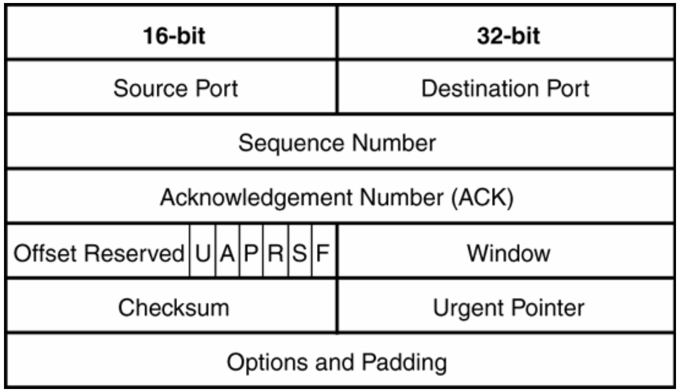
- Challenges in selecting a method
  - Identification of covert channels must be systematic.
  - The analysis need to be extended systematically while developing the product and as more and more information becomes available
    - For e.g. ST, FSP, HLD, LLD, IMP etc.
  - English like (Semi-Formal and Informal as mentioned in say EAL 6 assurance requirements) specifications should be usable while applying the methodology
  - Easily be reviewable by those persons (including the evaluator) participating in the design and implementation at different phases of product development

Kemmerer's Method (Shared Resource Matrix Methodology) – A method for CCA

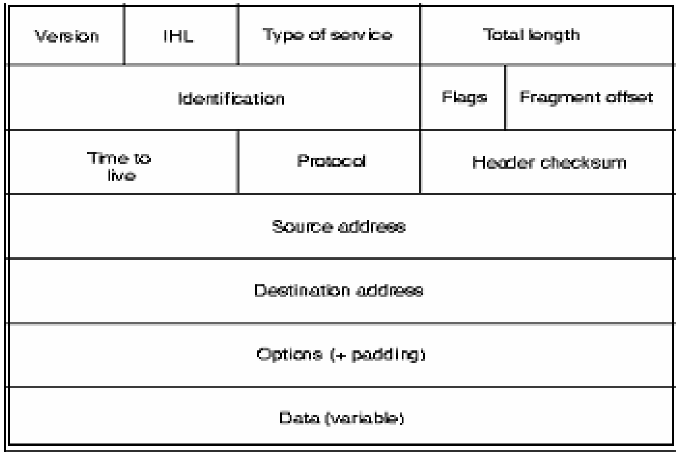
- Kemmerer's Original Method
  - Identify shared resources and primitive operations
    - Includes storage and time resources
  - Record type of access in shared resource matrix
  - Transitive closure on the entries of the shared resource matrix
  - Analyze SRM for potential covert channels
  - Analyze identified potential covert channels
- Recent Publication
  - [Kemmerer2] points out that the Shared Resource Matrix methodology was successfully applied to several systems and application of the methodology revealed a number of storage and timing channels

Covert Channel Analysis for an Information Flow Control Product – Shared Resources identified based on SRM Method

- Used Definition from Lampson
- TCP header used as a covert channel
- IP header field used as a covert channel
- Other protocol specifications (UDP and ICMP etc.)
- Connection/State table data
- Audit Records generated by the product based on information flows



16-bit	32-bit
Source Port	Destination Port
Sequence Number	
Acknowledgement Number (ACK)	
Offset Reserved U A P R S F	Window
Checksum	Urgent Pointer
Options and Padding	



<table>
<tr><td>Version</td><td>IHL</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Options (+ padding)</td></tr>
<tr><td colspan="5">Data (variable)</td></tr>
</table>

Examples of Covert Channels (shared resources) in Protocol headers

- Based on existing research on various protocols
- Based on tests on the product
- TCP,UDP,IP and ICMP header fields used as a covert channels
  - Initial Sequence Number IP Field [Rowland]
  - Manipulation of the IP Identification Field [Rowland]
  - TCP source ports
  - TCP header urgent pointer IP field when URG is set to 0
  - TCP data field when the flag is set to 0
  - Use checksum field of protocol headers
  - Data Field of ICMP Echo Request and Echo Reply messages
  - Similarly use unused bits of any protocol header where applicable as covert channel

- Similarly other headers were considered

Bandwidth Calculation Methods

- what do you do after identifying the channel ?
  - Calculate the bandwidth
  - Consider worst case analysis scenario to estimate the channel capacity
    - Covert Channels are noiseless
    - No Processes other than the sender and receiver are present in the system during channel operation and
    - The synchronization time is negligible

Bandwidth Calculation Methods

- [NCSC] is our main reference for Bandwidth Calculation methods
  - Information-Theory-Based Method for Channel-Bandwidth Estimation
  - Informal Method for Estimating Covert Channel Bandwidth
- However [NCSC] methods are not relevant to potential channels identified here
  - Storage elements are used differently in Channels today
  - The time necessary to set and read a storage element is significant in the types of channels in [NCSC].
  - [NCSC] must account for context switches between the sending process and the receiving process
- Hence, calculating bandwidth required different per channel basis formulae.

Our Observations

- SPM and CCA - Complement each other
  - SPM and CCA complement each other with SPM modeling the correct behavior of the system and CCA identifying ways to exploit the model.
- We found that the SRM method was appropriate during the course of analysis
- Bandwidth calculation methods mentioned in [NCSC] could not be applied to our analysis.
- However, the assumptions in [NCSC] regarding worst case scenario analysis are still appropriate

Future Directions

- CC Community - CEM improvement
  - V 3.x/4.x could provide some guidance on these topics
    - Level of abstraction in the SPM
    - Methods to be used based on product types
    - Bandwidth calculation methods based on product types
- Vendors making high Assurance products for network information flow control (e.g. Firewall)
  - Example of TCP wardens [Fisk]
    E.g.
    - IP padding bits – Zeroize the bits
    - IP Use unnecessary fields (ToS, options, DF if a fragment, etc) - Zero these fields
    - TCP data field when RST = 1 is set – Zeroize the data
    - UDP Checksum field – Recalculate the correct checksum or anomaly detection
    - Other similar protocol wrappers for Network stacks
  - Use existing technologies (e.g. NAT, Rate based control etc.)

Questions

Thank You

Sai Pulugurtha

spulugurtha@cygnacom.com

SPM References

- Z
  - Woodcock, Jim and Jim Davies, *Using Z: Specification, refinement, and proof*, http://www.usingz.com/, 1996
- ProofPower http://www.lemma-one.com/ProofPower/index/index.html
  - *ProofPower Document preparation (Lemma 1 Ltd.: Reading, UK) 2000*
  - *ProofPower Z tutorial* (Lemma 1 Ltd.: Reading, UK) 2000
  - *ProofPower HOL reference manual* (Lemma 1 Ltd.: Reading, UK) 2000
  - *ProofPower Z reference manual* (Lemma 1 Ltd.: Reading, UK) 2000

CCA References

NCSC	A Guide to understanding Covert Channel Analysis of Trusted Systems, NCSC-TG-030 Version 1, National Computer Security Center, 1993
Kemmerer	Richard A. Kemmerer, Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels, 1983
Kemmerer2	A Practical Approach to Identifying Storage and Timing Channels: Twenty Years Later
Fisk	Gina Fisk, Mike Fisk, Christos Papadopoulos, Josh Neil, Eliminating Steganography in Internet Traffic with Active Wardens, Lecture Notes In Computer Science; Vol. 2578 , Springer-Verlag, London, UK, p. 18-35, 2002
Murdoch	Murdoch and Stephen Lewis, Embedding Covert Channels into TCP/IP, 7th Information Hiding Workshop Barcelona, 2005
Lampson	B. W. Lampson, "A Note on the Confinement Problem," Communications of the ACM, 16:10, pp. 613-615, October 1973
Haigh	J. T. Haigh, R. A. Kemmerer, J. McHugh, and W. D. Young, "An Experience Using Two Covert Channel Analysis Techniques on a Real System Design," *IEEE Transactions on Software Engineering*, 13:2, pp. 157-168, February 1987.
Shannon and Weaver	C. E. Shannon and W. Weaver, *The Mathematical Theory of Communication*, The University of Illinois Press, Urbana, Illinois, 1964.
Ahsan	Ahsan, K., Kundur, D.: Practical data hiding in TCP/IP. In: ACM Workshop on Multimedia and Security. (2002)
Rowland	http://www.firstmonday.org/issues/issue2_5/rowland/È
Loki	http://www.phrack.org/show.php?p=49&a=6
Gasser	Morrie Gasser, "Building a secure computer system", 1998
Comer	Comer, Douglas E., *Internetworking with TCP/IP, Volume 1: Principles, protocols, and architecture* (Prentice-Hall, Upper Saddle River, New Jersey) 1995

CC References

- Common Criteria for Information Technology Security Evaluation
  - Part 1,2 and 3 of Version 2.x, Version 3.0
- CCEVS Guidance Documents- Methodology for Methodology Guidance for the CC Components at EAL5 and above (http://niap.bahialab.com/cc-scheme/policy/ccevs/methodology_above_eal4.pdf)