SAND2017-7569C

The Center for Cyber Defenders

Expanding computer security knowledge

Cyber Zone Defense

A Zoning Algorithm for Dynamic Cyber Zone Defense

Marci McBride, New Mexico Institute of Mining and Technology, Computer Science

Project Mentor: Dr. Robert Mitchell, Org. 9312

Problem Statement:

Attacks on cyber systems continue to plague public and private sector enterprises. Cyber Zone Defense (CZD) is an appealing strategy to prevent, disrupt, and tolerate these attacks; however, existing approaches assign hosts to zones based on their function or place in the architecture. This leaves the large number of human-operated commodity workstations within an enterprise unaddressed.

We propose a dynamic zoning algorithm which periodically, or asynchronously, assigns hosts to zones based on peer requests made by their human operators.

Introduction:

CZD uses Isolation Zone architecture to create self-organizing, dynamic, filtered virtual networks that restrict the attacker's visibility, access, lateral movement, exfiltration, and reach-back; this should effectively render malware inert.

Dynamic zoning connects the concept of CZD to the realm of Moving Target Defense (MTD). In particular, a dynamic CZD is a network-based MTD.

Our threat model assumes the adversary can implant malware in a host within the subject network, thus creating an insider threat. We assume the primary goals of an attacker are data exfiltration and lateral movement. We also assume command and control is an intermediate objective.

```
Algorithm Settings:
  The Maximum number of zones allowed         : 5
  The Maximum number of zones per host allowed: 5
  The Maximum number of hosts per zone allowed: 4
  The Maximum number of distuptions allowed   : 4
```

```
{   1: [['Robert', "2017-06-13-00-00-00"], ['Paul', "2016-01-11-00-00-00"]],
    2: [['Marci', "2017-06-10-00-00-00"], ['Beth', "2017-05-10-00-00-00"]],
    3: [['Stephen',"2016-01-01-24-01-01"], ['Dawn',"2016-01-01-24-30-20"],
        ['Doug',"2016-01-01-24-30-60"], ['Stan', "2016-01-01-24-30-55"],
        ['Alex', "2016-02-01-24-01-10"], ['David',"2016-01-01-23-30-20"]],
    4: []}
Requests made by users:
[ ('Marci', 'Marci'), ('Paul', 'Alex'), ('Robert', 'Paul')]
```

Method:

We obtained a list of host names for all network devices for an enterprise. We then used an information technology management database and a human resources database to add human and department fields to this host name list. The resulting list of <host name, human name, department name> tuples was the raw data set.

Metrics of Interest:

The metrics used to gauge the quality of our solution are the following:

1) Average number of hosts assigned to a zone
2) Average number of zones a host is assigned to
3) Number of disruptions

```
Welcome, this algorithm will determine the optimal zone membership
 for the lab's n devices in k zones.

>> Parsing Data ...
 ... Parsing Complete

>> Fulfilling Requests ...
 ... Requests Fulfilled

>> Placing hosts into zones ...
 ... Zoning Complete

Success! The Zoning Algorithm ran successfully.
```

```
New Zone Assignment =
{   1: [['Robert', '2017-06-13-00-00-00'], ['Paul', '2016-01-11-00-00-00'],
        ['David', '0000-00-00-00-00-00']],
    2: [['Marci', '2017-06-10-00-00-00'], ['Beth', '2017-05-10-00-00-00'],
        ['Stephen', '0000-00-00-00-00-00']],
    3: [['Doug', '2016-01-01-24-30-60'], ['Stan', '2016-01-01-24-30-55'],
        ['Alex', '2016-02-01-24-01-10']],
    4: [['Robert', '2017-07-05-15-48-57'], ['Paul', '2017-07-05-15-48-57'],
        ['Dawn', '0000-00-00-00-00-00']],
    5: [['Paul', '2017-07-05-15-48-57'], ['Alex', '2017-07-05-15-48-57']]}

Total disruptions = 3
```

Resulting Dynamic Algorithm:

The algorithm consists of three parts:

- **Part one** consists of importing data, calling the appropriate functions, and exporting the data.
- **Part two** consists of fulfilling peer requests. If a new host is added to a zone, the current date is added as the host's timecard data. This prevent the new host's removal during part three of the algorithm. Part two also verifies that the host pair added aren't High Value Targets (HVT) by making sure these hosts aren't in too many zones.
- **Part three** is the dynamic part of the algorithm. Hosts are moved to ensure zones do not become HVT. This process causes disruptions every time it removes a host from a zone. Previously, hosts were removed on a first-in, first-out basis; now, hosts are associated with timecard data and will be removed from a zone if it is the most inactive host in the zone. When a host is removed from a zone it is simply deleted from that zone. When a host is placed in a new zone during this part of the algorithm, the corresponding timecard data is reset to "0000-00-00-00-00-00". The host must use the new zone to receive a non-zero timecard, or the host risks being one of the most inactive hosts in the zone and may be moved.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration