Credit-based Network Management

2009-01-06
Outline

- The problem of Network Management
- The Idea of Credit-based Network Management
- An Implementation in Campus Network
- Conclusions
Network management headaches

- Widespread security problems
  - DDoS attacks
  - Address spoofing, misconfiguration
  - Unwanted traffic
- Poor QoS
- Problems brought up by new technologies
  - P2P, Wireless, mobility, IPv6
Physical vs behavioral problems

Abnormal events in a campus network in 2007

- Network Failure: 63%
- System Failure: 19%
- Connection Failure: 13%
- Abnormal User Behavior: 2%
- Other: 3%

Behavioral problems

- Very few real malicious guys
- A few youngsters try to be hackers
- Most problems caused by carelessness, exploited by other hackers
- Let’s consider a couple of common examples
DHCP Spoofing

- In many networks, users get IP addresses from a DHCP service
- An invalid DHCP server will cause problems to an entire LAN
- E.g. some WLAN router enables DHCP service, which causes problem to the LAN it is connected to
DHCP Request
10.1.1.1
aa-aa-aa-aa-aa-aa

Invalid DHCP Reply
10.1.1.3
cc-cc-cc-cc-cc-cc

DHCP Server
10.1.1.2
bb-bb-bb-bb-bb-bb

DHCP Reply

Invalid DHCP Reply

10.1.1.1
aa-aa-aa-aa-aa-aa

DHCP Request

dd-dd-dd-dd-dd-dd
ARP Spoofing

- In an IP/Ethernet network, both hosts and routers use ARP protocol to map IP to physical addresses.
- It is easy for someone to spoof ARP replies, causing problems to some hosts or the entire LAN.
A
IP: 10.0.0.1
MAC: aa-aa-aa-aa-aa-aa-aa

B
IP: 10.0.0.2
MAC: bb-bb-bb-bb-bb-bb

Hacker
IP: 10.0.0.3
MAC: cc-cc-cc-cc-cc-cc-cc

switch

Spoofed ARP reply
IP: 10.0.0.2
MAC: cc-cc-cc-cc-cc-cc-cc

Spoofed ARP reply
IP: 10.0.0.2
MAC: cc-cc-cc-cc-cc-cc-cc

ARP cache

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2</td>
<td>bb-bb-bb-bb-bb-bb</td>
</tr>
</tbody>
</table>

ARP cache

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>aa-aa-aa-aa-aa-aa</td>
</tr>
</tbody>
</table>
A's cache is poisoned
A
IP: 10.0.0.1
MAC: aa-aa-aa-aa-aa-aa

B
IP: 10.0.0.2
MAC: bb-bb-bb-bb-bb-bb

Hacker
IP: 10.0.0.3
MAC: cc-cc-cc-cc-cc-cc

The switch will then think that aa-aa-aa-aa-aa-aa is connected at this port.

To: cc-cc-cc-cc-cc-cc
Spoofed ARP reply
IP: 1.2.3.4
MAC: aa-aa-aa-aa-aa-aa

Spoofed ARP reply
IP: 1.2.3.4
MAC: aa-aa-aa-aa-aa-aa

The switch will then think that aa-aa-aa-aa-aa-aa is connected at this port.
Rooted in network architecture

- Open access
  - Favoring easy application development
  - Allow/support anonymous access (privacy)
  - Best-effort service
- Decentralized management for extensibility
  - Managed by many ISPs
  - Cooperate on “connectivity”
  - Lack of cooperation on management
Current management practice

- Focus is on infrastructure management
  - Setting up routers, access points, name service, email, web servers, routing policies
  - Monitoring network resources for reliability
  - Setting up local security (e.g. user accounts) to protect usage of local resources
  - Responding to security problems
Behavioral management

- Internet is another human society
- Behavioral problems can be dealt with using law enforcement
  - Too heavy-weight for many scenarios
- Current practice is mostly passive
  - Filters, firewalls...
- Is there a middle ground – a light-weight approach to behavioral management?
What kind of mechanisms?

- Should be simple to implement
- Should have positive influence on user behavior, and effects should be cumulative
- Should not negatively impact normal operation
- Should benefit both the ISPs as well as users

⇒ Apply credit ratings to users and ISPs
Concrete examples

- Managing a campus network:
  - Allocate management resources according to user classification
  - Assign credit rating to users, and adjust service levels according to credit ratings

- Managing peering relationships
  - Monitor unwanted traffic
  - Monitor QoS
Access network scenario
ISP peering scenario

Optimized Routes

Peer
Gain/lost evaluation
Peer

Unwanted Traffic
General case – cascading effect

Diagram showing interactions between SP, Backbone, Access Net, User, Third party, and Peer with behavior assessment and service assessment.
Framework

Credit-based service differentiation
- Services
- Priority
- Speed limit
- Charge

Credit assessment and management
- Recording
- Computing
- Analysis
- Reporting

Network behavioral measurement
- SPAM
- Virus
- Hijacking
- DoS
Methodology

- Credit rating methods in financial scenarios
- User classification methodologies based on machine learning
  - Need to consider structural/physical grouping, for ease of incentive application
- Reputation and incentive mechanisms in social networks
Other considerations

- Reward good behavior
- Punish bad behavior, but allow recovering
- Manual control (VIPs, over-rides)?
- Global cooperation, e.g.
  - Sharing of credit information
  - Standardized credit ratings
Case study – a campus network

- Behavioral problems increasing
- 2006 and 2007 data on campus

2006年度处理案例分析图

<table>
<thead>
<tr>
<th>Category</th>
<th>2006 Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Failure</td>
<td>55%</td>
</tr>
<tr>
<td>Connection Failure</td>
<td>4%</td>
</tr>
<tr>
<td>System Failure</td>
<td>20%</td>
</tr>
<tr>
<td>User Problem</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

2007年度处理案例分析图

<table>
<thead>
<tr>
<th>Category</th>
<th>2007 Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Failure</td>
<td>63%</td>
</tr>
<tr>
<td>Connection Failure</td>
<td>3%</td>
</tr>
<tr>
<td>System Failure</td>
<td>19%</td>
</tr>
<tr>
<td>User Problem</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>
Management difficulties

- Large user base (>50K), mobility
- Limited manpower for network admin
- New types of problems requirement more time and man power
- Cost for behavioral management is much higher than that of physical devices
Concentrated nature

Most problems tend to originate from a few classes of users
User classification

- After classification using selected attributes:
  - Male undergraduates (especially 1\textsuperscript{st} yr, or 4\textsuperscript{th} yr)
  - Specific departments
- Focused monitoring saves management resources
Physical attributes

- Physical grouping
  - Students can be grouped by dorm building
  - They belong to same subnets
  - Significant concentration with such grouping

- Ease of management based on physical grouping
  - Update equipment to prevent ARP spoofing first applied to more “dangerous” networks
Personal credit rating

- Repeat problematic users
  - 7.1% of problematic users are repeat users
  - They cause 14.3% of problems
  - The distribution of such users is random
- Need targeted treatment
Experimental credit rating system

- Credit rating values
  - Minimum is 0; maximum is 100; >50 acceptable

- Initialization of credit rating
  - Generously initialize (almost) all to 60

- Rating adjustments
  - First offense: deduct $10w$
  - Deduction for more offense = $\text{past} \times 0.5 + 10w$
  - Increment credit rating by 1 each month
Experimental results

Over span of 1.5 years, the fluctuation of problem users and credit adjustments:
Conclusion

- An important aspect of network management is user behavioral management.
- Credit-based management:
  - Focus management on problem users
  - Apply incentive system to influence behavior
- Cascading effect (conjecture)
  - Help improve entire Internet