Wireless Network Security
Spring 2016

Patrick Tague
Class #17 - Statistical Attack Detection
Reminders

• HW#4 is due Thursday, Mar 24

• No class, Mar 29

• Progress presentations Thursday, Mar 31

• Exam Tuesday, Apr 5
Progress Presentation

• Important updates since SoW presentation
  – Any changes to project scope, planned deliverables, schedule of deliverables, etc.

  – Brief overview of what has been done so far

  – Preliminary results, possibly a quick demo

  – Every team member should present

  – MAX 12 minutes
Class #17

• Challenges in attack/intrusion detection

• Trade-offs between detection, security, privacy, performance, etc.
Attack/Intrusion Detection

- Most work on network attack/intrusion detection has focused on the Internet

Table 2: Application category

<table>
<thead>
<tr>
<th>Category</th>
<th>Application/protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>web</td>
<td>http, https</td>
</tr>
<tr>
<td>p2p</td>
<td>FastTrack, eDonkey, BitTorrent, AresGnutella, WinMX, OpenNap, MP2PSoulSeek, Direct Connect, GoBoogySoribada, PeerEnablerftp</td>
</tr>
<tr>
<td>ftp</td>
<td>smtp, pop, imap, identd, nntp</td>
</tr>
<tr>
<td>dns</td>
<td>mms(wmp), real, quicktime, shoutcastvbricks streaming, logitech Videom IMnetbios, smb, snmp, ntp, spamassassinGoToMyPcssh, ssl</td>
</tr>
<tr>
<td>mail/news</td>
<td>chrome, gmail, outlook, exchange</td>
</tr>
<tr>
<td>streaming</td>
<td>network operation</td>
</tr>
<tr>
<td>encryption</td>
<td>games</td>
</tr>
<tr>
<td>games</td>
<td>chat</td>
</tr>
<tr>
<td>chat</td>
<td>attack</td>
</tr>
<tr>
<td>attack</td>
<td>unknown</td>
</tr>
</tbody>
</table>

From [Kim et al., CoNEXT 2008]
Defense

From [Douligeris & Mitrokotsa, Computer Networks 2004]
Challenges

- Many Internet-type models and defenses don't translate to wireless networks, even those that are part of the Internet
  - Attacks on WiFi APs don't look like attacks on an Internet router or wired gateway
  - Attacks launched from mobile devices over LTE may look similar once traffic is on the Internet, but look different in the LTE network itself
Challenges

• Mobility breaks many of the assumptions of traditional detection/defense systems
  – Paths change much more quickly, preventing network-layer fingerprinting of sessions and complicating traffic analysis
  – However, mobility may provide additional information, if the detector is smart enough to look for it
    • Ex: if the detector is in the LTE core, it doesn't know much about device mobility, while if little detectors are in the base stations, mobility info may be available
Challenges

• Where are the detectors?
  – In many of the traditional Internet-based detection / defense models, networks are nicely partitioned using gateways, firewalls, etc. with a domain-based detector behind each one
  – What about a MANET / WSN?
    • Where should the detector go? How much visibility does it need?
    • What should it monitor?
Challenges

• Security measures at various layers may actually prevent or interfere with attack detection
  – Goals of data secrecy, network privacy, anonymity, etc. are in direct conflict with certain attack detection techniques

  – Ex: many corporations are struggling with wide adoption of TLS/SSL/HTTPS because it breaks their packet inspection-based models for attack detection

  – Ex: if anti-traffic-analysis techniques make all traffic look the same, how to differentiate normal and attack traffic?
Common Approaches

- Attack detection must be context-appropriate
  - Ex: in a sensor network, there's much less variance expected in network traffic, so anomaly detection may be easier, possibly making tradeoffs more reasonable

- Attack detection may require collaboration
  - Dependencies between layers mean detection is not a layered activity, may need monitoring across various layers of the protocol stack and various locations in the network
Open Questions

• Due to wide variety of network types and need for context-appropriate detection mechanisms, this is a hard problem.
  – What specific detection mechanisms are needed for specific network / application scenarios?
  – How much can detection mechanisms be generalized?
  – Can detection schema be learned / trained in situ?
  – ...

©2016 Patrick Tague
Let's look at an example as an exercise
Example

- Consider a large-scale Wi-Fi network with dense deployment of monitors (watchdogs)

- **Attack:** [each malicious client, while moving around randomly]
  1) spoof a valid identity
  2) connect to a nearby AP
  3) flood SYN packets targeting a particular web server for a random duration
  4) stop flooding, disconnect, wait small random duration, go to 1).

- What useful statistics can the monitors collect?
- What useful analytics can be computed?
Mar 24: Location Service Security