Securing Static Nodes in Mobile-Enabled Systems using a Network-Layer Moving Target Defense

Stephen Groat, Reese Moore, Randy Marchany and Joe Tront
{ sgroat, ram, marchany, jgtront }@vt.edu
Virginia Tech, USA

May 25, 2013

Overview

- Introduction
- Overview

- The Need for Security in Mobile-Enabled Systems
- Moving Target Defenses
- Heterogeneous Moving Target Networks
- Moving Target IPv6 Defense (MT6D)
- Homogeneous Moving Target Networks

- Conclusions
- Engineering Principles

Security in Mobile-Enabled Systems

Mobile devices are becoming more prolific, for end users and for mission critical systems. Securing these systems is vital.

- Mobile users need information from the network
- Users need information from the mobile network
- Sensor networks gather and report potentially sensitive data

The organization of the network has a direct effect on what is considered "critical".

- A central server is more "valuable" than an end node

Moving Target Defenses (MTD)

Moving Target is a mechanism where a node maintains a constantly changing attack surface.

- Force the adversary to expend time/energy/resources to repeatedly "acquire the target".
- Minimizes the window of opportunity to attack the system.
- Moving Target can be applied offensively or defensively.
- Can be applied in many ways:
  - Address Space Layout Randomization (ASLR)
  - Fast Flux DNS
  - Network Layer MTD (e.g. MT6D)

Heterogeneous Moving Networks

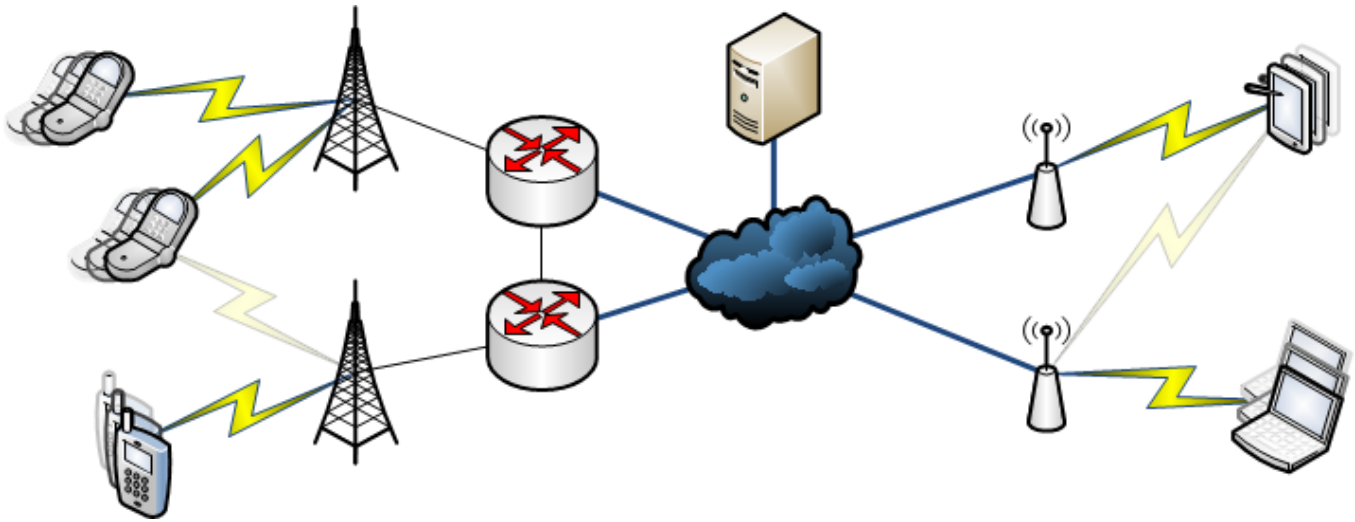

Figure : An example mobile network with a static server

An adversary can begin to infer information about the network and its participants through simple traffic analysis.

Moving Target IPv6 Defense (MT6D)

MT6D is a Network-Layer Moving Target Defense solution developed at Virginia Tech.

- Utilizes the immense (and sparse) IPv6 network address space
- Nodes rapidly change their network address in a deterministic but unpredictable fashion while maintaining communication
- Does rely on key distribution

"Analogous to frequency hopping in the IP space"

Homogeneous Moving Networks

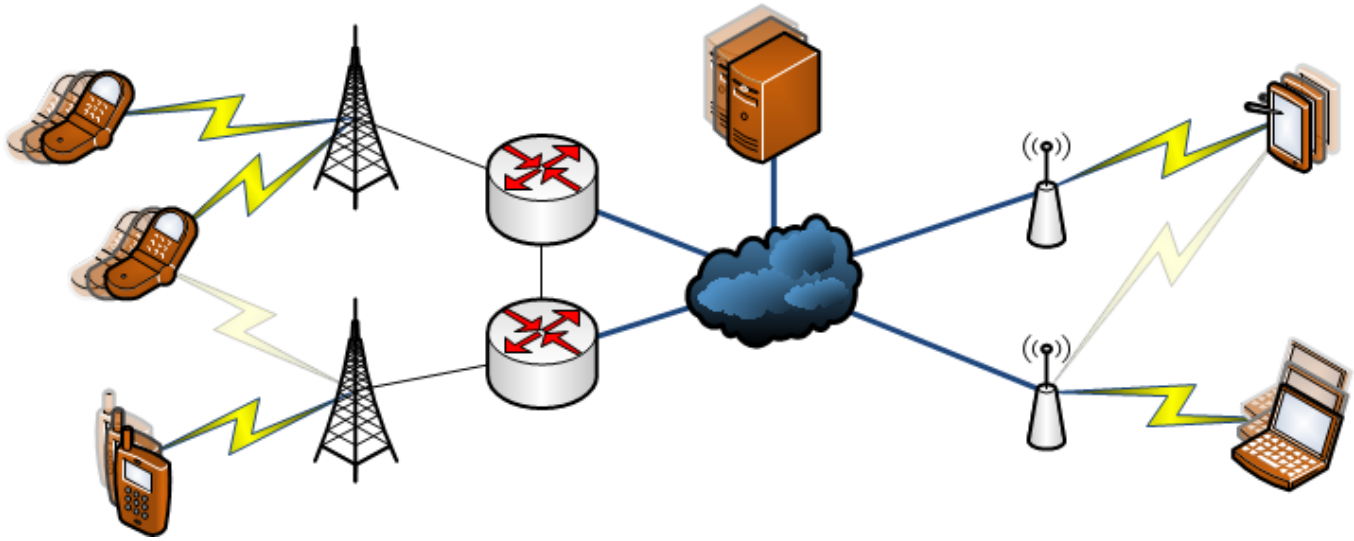

Figure : An example network with a network-layer MTD applied

After applying a network-layer MTD (such as MT6D) to the network, it becomes much more difficult for an adversary to infer information through network relationships.

Conclusions

- The security of mobile-enabled systems is important, especially into the future.
- Mobile enabled networks can have many of the properties of a network MTD.
- An adversary can utilize this to examine nodes that do not exhibit those properties and focus efforts there
- By applying a network layer MTD (such as MT6D) to the system, a homogeneous moving network is visible

Break-out Thoughts

Security as part of the process, not an afterthought

- "Adding security" should *not* be a step
- Anything added to the system can be used against it
- "How would I attack this component?"

IPv6 is the future, embrace it

- If the system uses the Internet, IPv6 will be a future concern
- More than just a different address format
- Allows for many things not feasible in IPv4

Questions?