TSA Cybersecurity – An Outsider's Perspective

Avi Kak

kak@purdue.edu

October 17, 2017

A Presentation Given at the "Advanced Development for Security Applications (ADSA)" Workshop, Boston, MA

Robot Vision Lab,
Purdue University

TSA and Its Networked Operations for Airport Security

- It is inevitable that the security ops at the airports will be networked in the near future for the following two reasons:

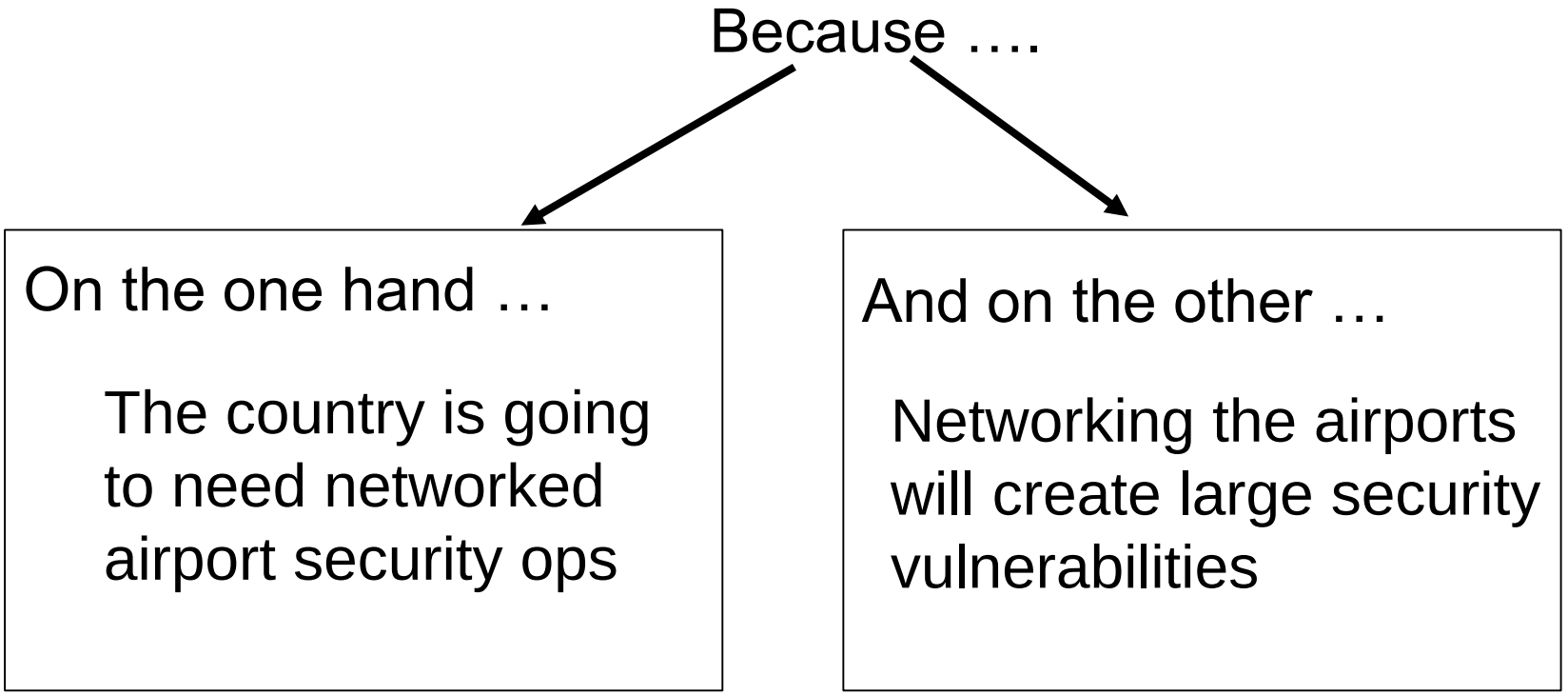
  1. Centralized patch management for software updates

  2. Synchronized changes to the decision thresholds used for controlling POD and FA rates.

- However, networking will create vulnerabilities to all sorts of attacks.

TSA's Cybersecurity Dilemma

But why are we talking about dilemmas?



This presentation reviews the types of attacks TSA should expect and the strategies for their mitigation.

Recent Breaches of Security Raise the Following Question:

- If organizations like NSA are failing repeatedly in protecting their systems, what is the probability that TSA of the future with its networked airport security would be able to do any better?

Today's Reality (Five Truths)

1. **Every organization must assume that sooner or later its security will be breached.**

2. If any organization claims that it cannot be broken into, it is an indication of the organization's lack of understanding of how the internet enterprise really works.

3. **Hiring the best engineers and programmers is only a small part of the overall strategy for ensuring computer security.**

Today's Reality (Five Truths)

4. In any organization there must not exist a single security credential whose loss can expose all of the information all at once.

5. A potential solution to this problem is that it must become exponentially more difficult for an adversary to extract exponentially larger chunks of information from an organization.

The rest of this talk touches on the following three points:

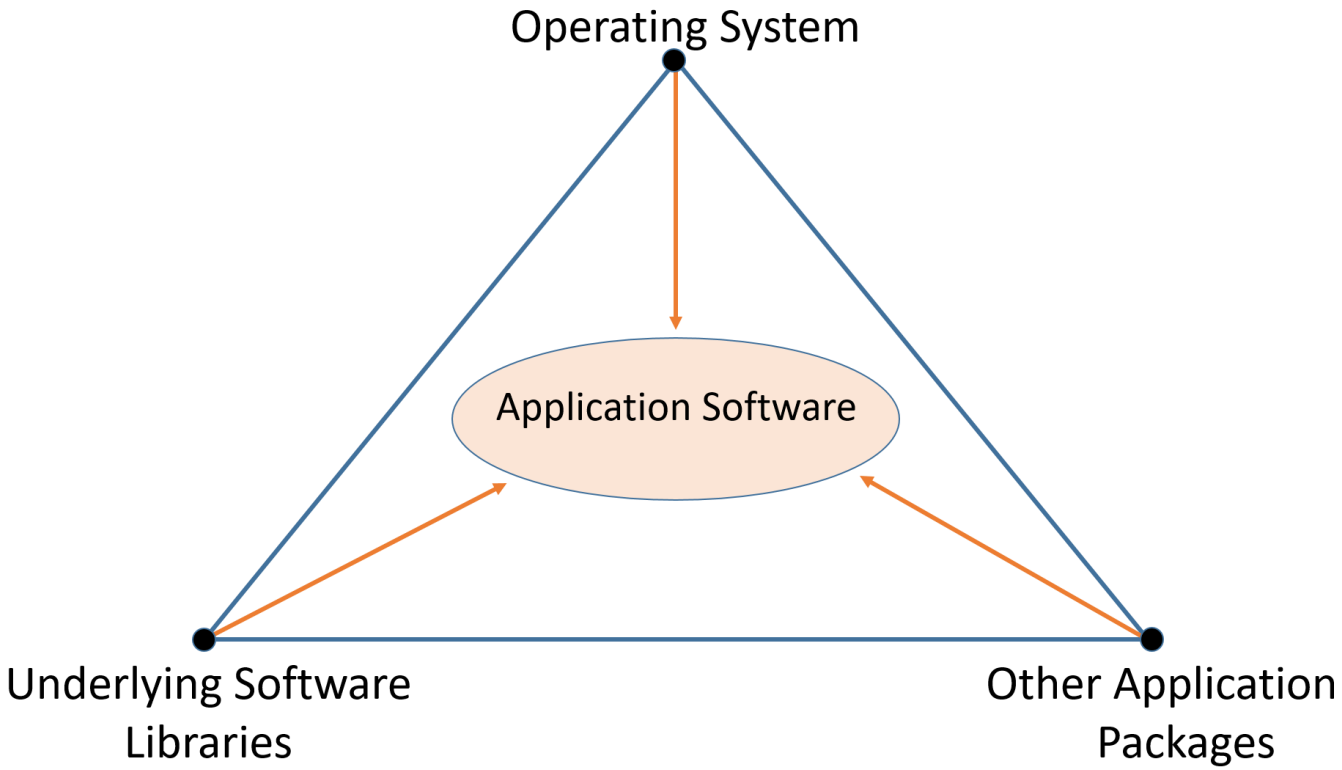
1. **Why does software need to be updated continuously?** (Fast and synchronized software updating is an important reason for networking our nation's airports.)

2. **Possible attacks on TSA's security services**

3. **Is using private leased lines a solution for TSA?**

1. Why does software need to be updated continuously?

All Software is in a Constant State of Flux



Modern software is best thought of as a living organism that is constantly evolving in a computer-communication ecosystem that must constantly adapt to the inexorable march of technology.

2. Possible Attacks on a TSA's Security Services

- **IP Scanning Attacks**

  Every IP address block in a geographic region is scanned for all known vulnerabilities in order to discover the servers that can be exploited.

- **Spear Phishing Attacks**

  These are particularly deadly when botnets are used for the attacks.

- **Dictionary Attacks**

  These attacks are specific to breaking into ports that are used for secure logins using plausible login names and passwords.

- **DoS and DDoS Attacks**

  Such attacks constitute extremely potent cyber weapons that could potentially shut down TSA central serves. Ex: Just a few months ago, the IoT based Mirai botnet was used to launch a 1 Terra bits/second DDoS Attack on the OVH web hosting service in France.

3. Is Using Private Leased Lines a Solution for TSA?

- One could argue that the most secure way for TSA servers to communicate with the software system at the airports would be using dedicated (private) fiber-optic circuits leased directly from the organizations that provide services for the internet backbone.

- Although such leased circuits would create a complete isolation between the TSA Network and the rest of the internet, that would constitute **only a partial solution to TSA's cybersecurity dilemma.** **Think the Stuxnet "worm" that destroyed Iran's nuclear centrifuges.**

THANK YOU

Background Slides

Some Recent Breaches of Computer Security

- **NSA --** Theft of highly classified tools for breaking into foreign networks for intelligence collection (Oct 2017)

- **NSA --** Theft of hacking tools from the NSA computers (June 2017)

  Some of these cyberweapons were subsequently used to attack hospitals, businesses, etc., in the form of ransomware.

- **NSA –** A theft similar to the one in the first item above (mid-2015)

- **Equifax –** Exposed 143 million social security numbers (Sept 2017)

And Some Not So Recent Breaches of Computer Security

- **Yahoo** – Now says that its massive data breach of 2013 affected all of its **3 billion** user accounts.
- **Target** -- Theft of account info on **70 million** customers in 2014
- **MySpace (now owned by Time)** – Lost names and passwords for **360 million** accounts (2013)
- **LinkedIn** – Exposed membership info on **100 million** members (2012)

How Can TSA Defend itself Against IP Scanning Attacks?

- The best defense here is to keep all the software systems constantly patched up.
- For obvious reasons, using private leased lines from the providers of the internet backbone infrastructure eliminates such attacks entirely.
- **Note that using private leased lines is NOT the same thing as using a VPN.** Even if you were to conduct all of your business through a VPN, your computer would still be vulnerable to all typical network based attacks.

How Can TSA Defend Itself Against Spear Phishing Attacks?

- Since these are "social engineering" based attacks, **there are no surefire defenses against them.**
- When bots are used to mount such attacks, it is difficult for intrusion detection system to thwart them.
- **The best strategy is to assume that sooner or later such an attack will be successful and to put security protocols in place that limit the damage from such an attack.**

How Can TSA Defend itself Against Dictionary Attacks?

- Although there now exist well-known methods that detect such attacks by analyzing the repetitiveness of the source addresses in the incoming packets, **a determined adversary can fool such methods by randomizing the outgoing packets or by using a botnet to launch such attacks.**

- The best defense against such attacks is the use of strong passwords, two-factor authentication, and variants thereof.

How Can TSA Defend Itself Against DoS and DDoS Attacks?

TSA could employ a number of methods to protect its central servers from such attacks:

- Multi-layer switching
- Packet filtering at the routers
- Placing the servers inside what are known as “Content Delivery Networks”

The Reasons for Why Network Isolation May Not be the Best Solution

- Prime exhibit for why network isolation may not work:

The Stuxnet worm that destroyed the centrifuges in Iran's nuclear program earlier this decade.

The computer system used for operating the centrifuges was isolated from the internet.

- Network isolation can create a false sense of security.