escrypt

SECURITY. TRUST. SUCCESS.

A Generic Framework for Security Risk Assessment for Intelligent Transportation Systems

Paul Bottinelli, Pino Porciello

ITS America 2018

Outline

- Introduction
- Classification of ITS Components
- Methodology and Examples
  - The Acting Component
  - The Reporting Component
  - The Reacting Component
  - Risk Rating
- Conclusion

5.7 Gap 7: Lack of advanced risk assessment tools

Risk assessment methodologies that can deal with multiple networked stakeholders working in collaboration need to be developed. This requires a different mind-set for existing risk management approaches, which often begin by scoping a system (i.e. defining its borders) prior to a risk assessment based on the individual elements. However, in interconnected systems this clear border does not exist. To address this gap we need to redesign risk management systems/approaches so that they operate from a stakeholder perspective rather than border perspective.

Source: European Union Agency for Network and Information Security (ENISA). (2016). *Cyber Security and Resilience of Intelligent Public Transport - Good practices and recommendations*, Online: https://www.enisa.europa.eu/publications/good-practices-recommendations/at_download/fullReport.

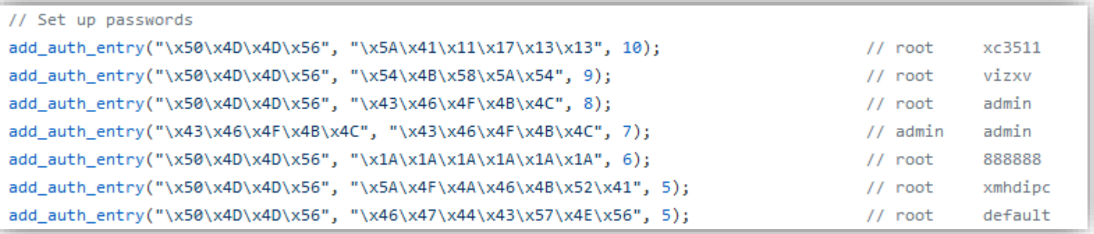
Introduction

Lack of a holistic approach for SRAs

→ *Existing ones are difficult to apply to ITS*

Goals:

- Improve security from design to development
- Take the stakeholder's perspective
- Make a difference before wide deployment of ITS



```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);          // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);               // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);               // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);           // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);           // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);       // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);       // root     default
```

Source: Mirai botnet source code at mirai/bot/scanner.c

Methodology

Goals

Develop a holistic SRA Framework for ITS

Drive a best practices approach from design to development

Raise security awareness

Dialogue instead of final binary outcome

Result

A lightweight framework

Can be used at multiple stages of development

Series of simple targeted questions

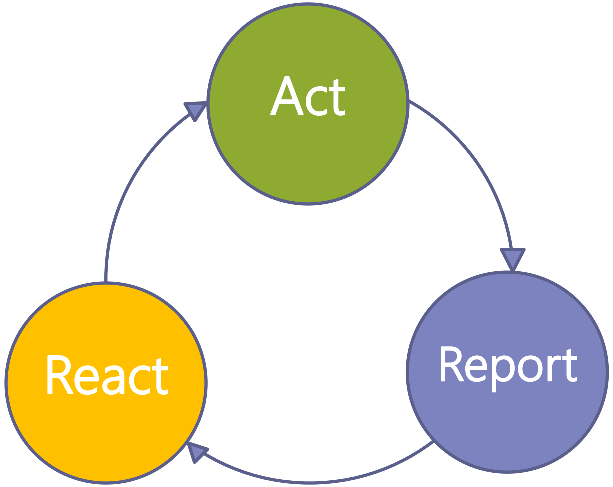
Broken down by components

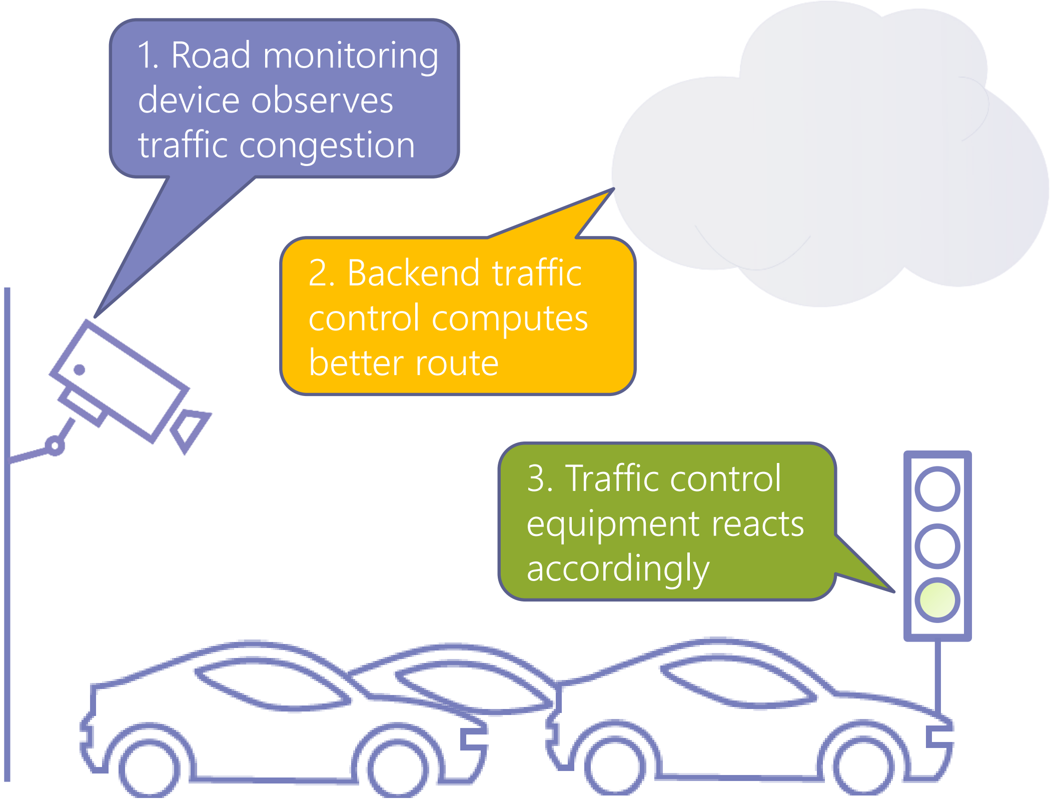
Based on OWASP's IoT Framework Security Considerations

Classification of ITS Components

Classify ITS participants in terms of the actions they perform.

→ *Some components may perform more than one.*




1. Road monitoring device observes traffic congestion

2. Backend traffic control computes better route

3. Traffic control equipment reacts accordingly

Acting Component

Channel security

Is the data sent over a secure channel (i.e., authenticated and encrypted)? If yes, using what protocol and underlying algorithms?

How are the keys/credentials generated?

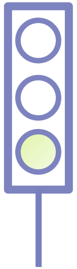
Are the entities mutually authenticated?

Application security and encryption

Is the data authenticated/encrypted before being sent?

How are the keys and credentials generated? Are the keys individual to ITS participants or are they shared?

Does the key distribution follow a process?



Automatic updates, update verification and up-to-date 3rd party components

Hardware Security

Secure offline capabilities

Etc.

Reporting Component

Channel and end-to-end security

Data trustworthiness and secure storage

Can the data be trusted?

How is the quality of the data assessed?

Does the component store any kind of data? If yes, is the data stored securely?

Attack mitigation and anomaly detection

Can the component detect and resist a large number of requests?

Can the component detect and resist malicious repeating requests?

Does the component have the ability to detect anomalies?

Logging, reporting and alerting

Automatic updates

Etc.

Reporting Component

Channel and end-to-end security

Secure storage

Security monitoring, defensive capabilities and strong logging

Is there a security event monitoring system in place?

Can the system detect and react to attacks? Does the system possess an Intrusion Detection and Prevention System (IDPS)?

Is there a firewall in place?

Audit capabilities and accountability

Does the component provide mechanisms to ensure delivery of specific messages? Does the component logs reception of specific messages?

Does the component log any additional events?

Does the system provide any audit capability?

Etc.

Risk Evaluation

Final point to reduce complexity of existing Risk Assessment methods

→ Simplify the risk rating

		Impact			
		Low	Medium	High	Critical
Probability	Low	Low	Low	Moderate	High
	Medium	Low	Moderate	High	Extreme
	High	Moderate	High	High	Extreme
	Very High	High	High	Extreme	Extreme

Risk ~ Impact x Probability

Methodology

2.1.9 **Default credentials**

2.1.9.1 No default credentials to access the device ○ ○ ○ ○

2.1.9.2 No shared credentials ○ ○ ○ ○

2.1.10 **Fail-safe defaults principle**

2.1.10.1 Interfaces are disabled by default ○ ○ ○ ○

Methodology

2.1.9 **Default credentials**

2.1.9.1 No default credentials to access the device ○ ◉ ○ ○

High Default (root, default) credentials for SSH

High Default (root, default) credentials for web interface

2.1.9.2 No shared credentials ○ ◉ ○ ○

High Same credentials for SSH and web interface

2.1.10 **Fail-safe defaults principle**

2.1.10.1 Interfaces are disabled by default ○ ◉ ○ ○

Med Telnet port open for no reason

Conclusion

We developed a Lightweight Security Risk Assessment framework for ITS

Set of targeted questions, driving security best practices and security awareness

Simple and flexible to use during whole product lifecycle

We've been successfully applying it to initiate dialogue that led to long-term relationships with customers.

ESCRYPT
419 Phillip Street, Unit B
Waterloo, Ontario
Canada

Phone: +1 (519) 749-3378

info@escrypt.com
www.escrypt.com