An exploration of real world network security

A set of principles and case studies

Rayhaan Jaufeerally <rayhaan@rayhaan.ch>

2020-10-29

AS 210036, Networking Enthusiast

Disclaimer: views not necessarily those of the author's employer.

Presenter is presenting in a personal capacity.

Table of contents

Intro

Objectives

Things to take away from this hour:

- Understand what a network is, defining threat models, reason about security properties,
- Have insights into some current network security protocols in the internet,
- Be able to apply the security mindset to real-world protocols and deployments beyond the regular internet,

Non-objectives

This is a meta-class, about how to think about security in the context of networked systems.

Not a checklist for an exam,

Not a step-by-step guide for securing a system.

Threat models

It's hard to defend against somthing you know nothing about.

Learn about your system and how it works.

Define what you want to protect.

Come up with ways that the system can break and prevent those (security mindset).

Very abstract, we'll apply these to concrete examples.

Security mindset

A way of thinking that applies to many things in eveyday life as well as systems analysis,

Think in terms of “what would an attacker do?”

Security Mindset – example

Trivial example but worth mentioning:

Website that shows sensitive personal information with a URL like:

`https://example.com/personal_info?user_id2345`

Security mindset thoughts:

- Why is the user_id specifiable by the user (even if not in GET params, it's a fundamental problem),
- Even if it's hidden somewhere in the javascript, or a cookie it's not safe,
- Encrypting or signing the field when it's under client control is the way to go,

What is a network?

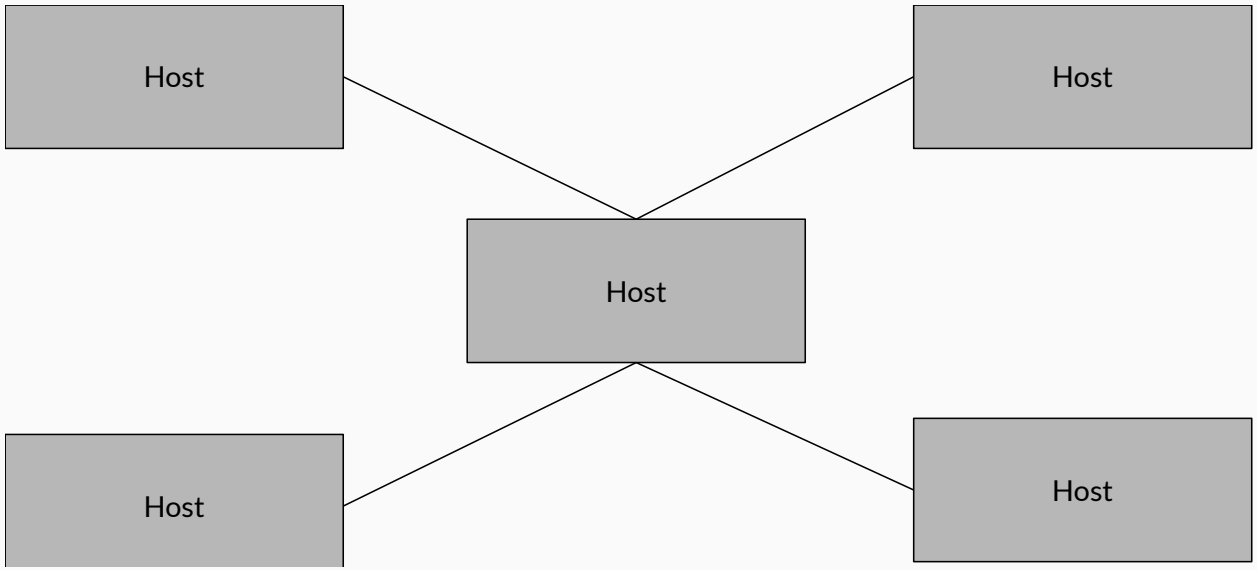
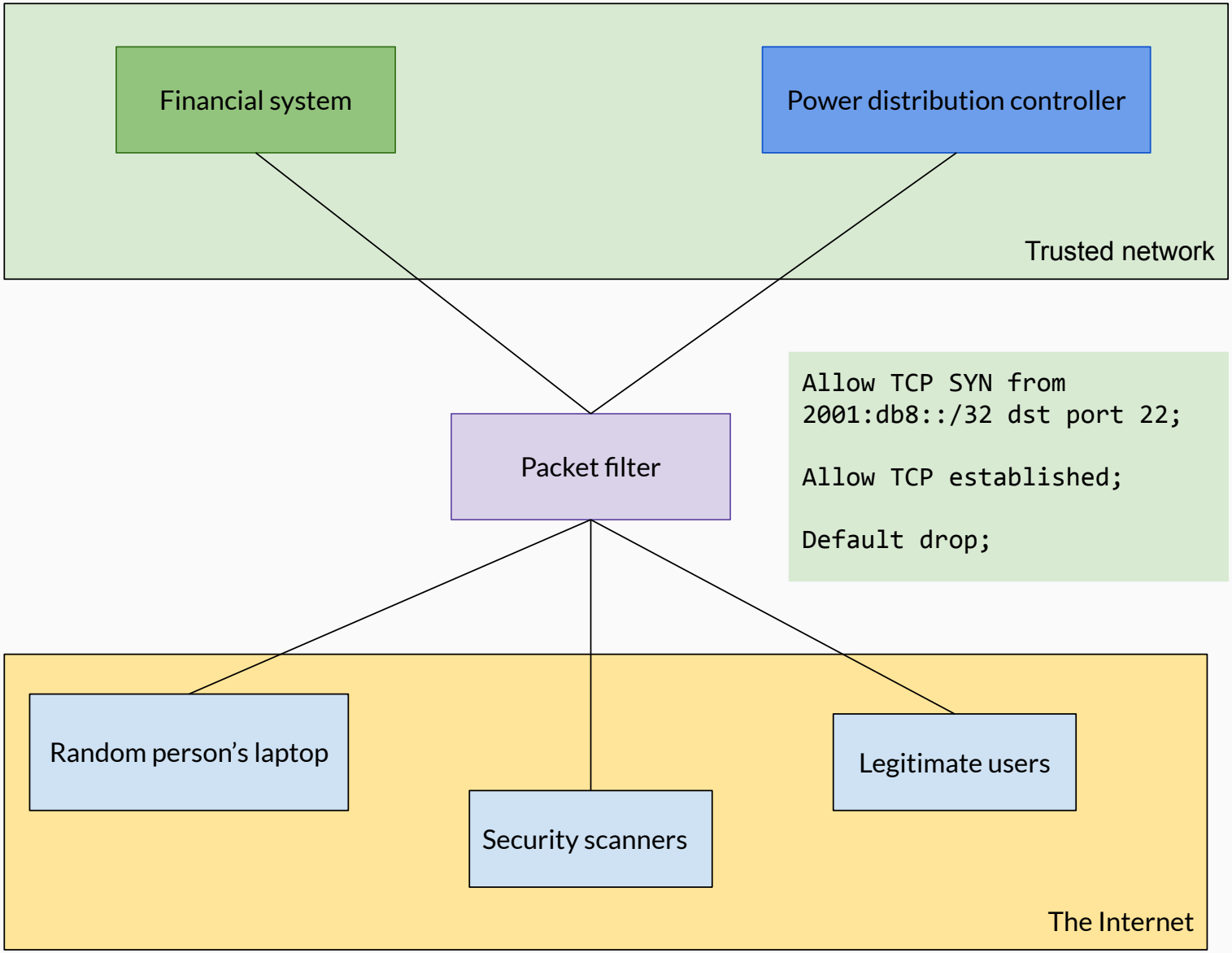


Figure 1: Example network with 5 hosts

Traditional approach to network security



Traditional approach to network security

Why is this broken?

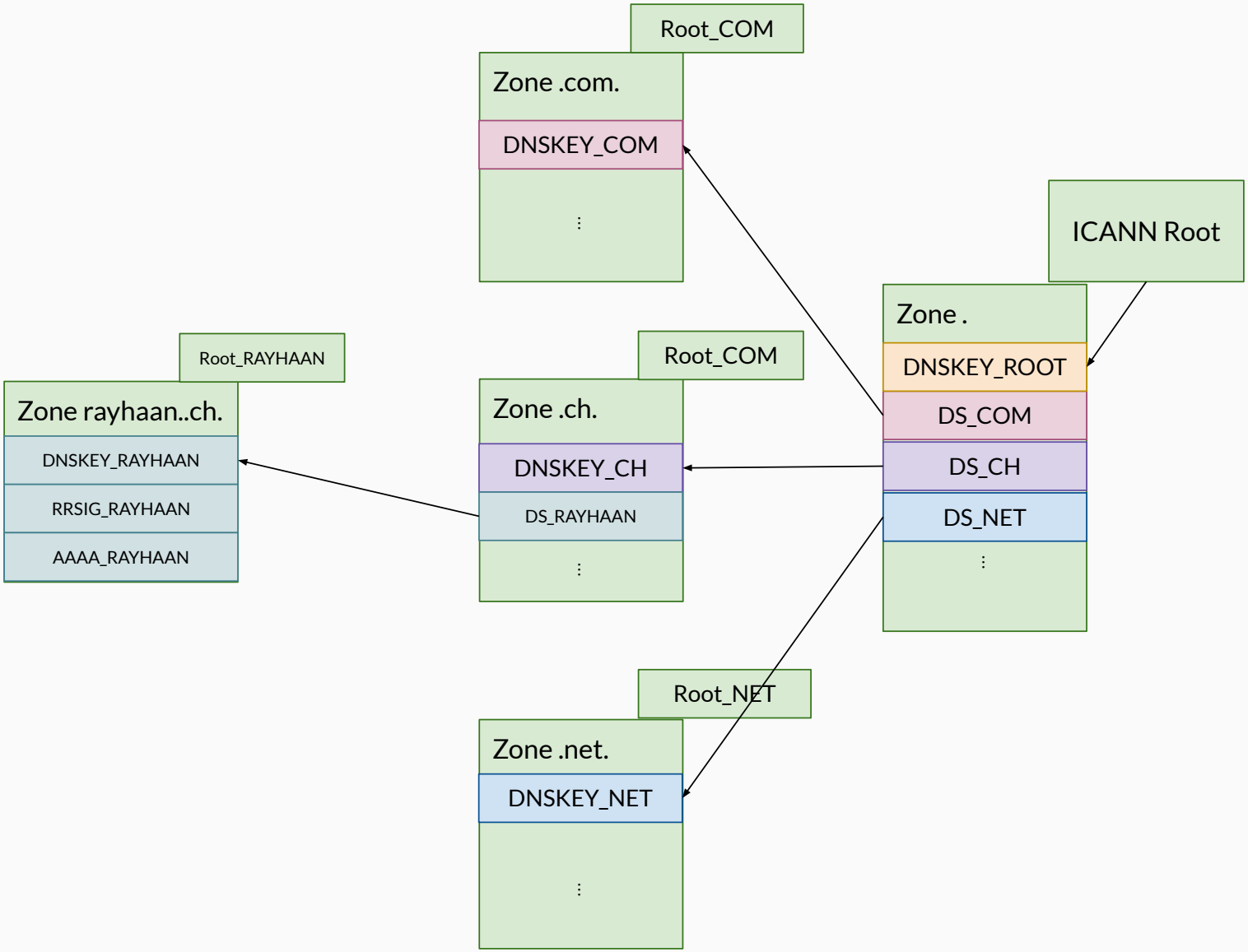
Implicit trust in the network does not match the physical reality.

Anyone can walk in to an office and plug in a malicious device.

What about attacks that violate the assumptions about source address, BGP hijack, etc.

Real world protocols

High level design of DNSSSEC



Threat model of DNSSEC

Attacker changing DNS responses to point to a malicious website,

Changing other data in DNS such as special site verification TXT records,

Does not cover privacy of DNS queries, that's what DNS over HTTPS / TLS does,

Problem: Does not specify how the end user is meant to know a site is DNSSEC protected.

It’s ok because we have TLS?

LetsEncrypt uses DNS challenges, where to prove domain ownership, a token is inserted into DNS

Then this is used to issue a certificate for the domain from a trusted CA,

Controlling DNS can lead to redirecting traffic, and undermining the PKI in one go,

RPKI

Already discussed RPKI and BGPSec in the previous lecture:

- RPKI provides protection against mistakes
- BGPSec secures end-to-end path but has operational concerns

Won't go over the details again here,

Opinions on RPKI / BGPSec

RPKI gets people to run software alongside their BGP routers (e.g. `https://nlnetlabs.nl/projects/rpki/routinator/`,

Typically on standard x86 machines, with a control plane path to the router for programming in rules,

This can be leveraged to run BGPSec validation completely on the high performance machine rather than on the router itself,

Introduction to phone systems

- Safety critical system,
- Legacy systems,
- Needs integration with other providers,

Sounds familiar? Interdomain routing? Service provider interconnections? Could it be BGP all over again?

Signaling System 7

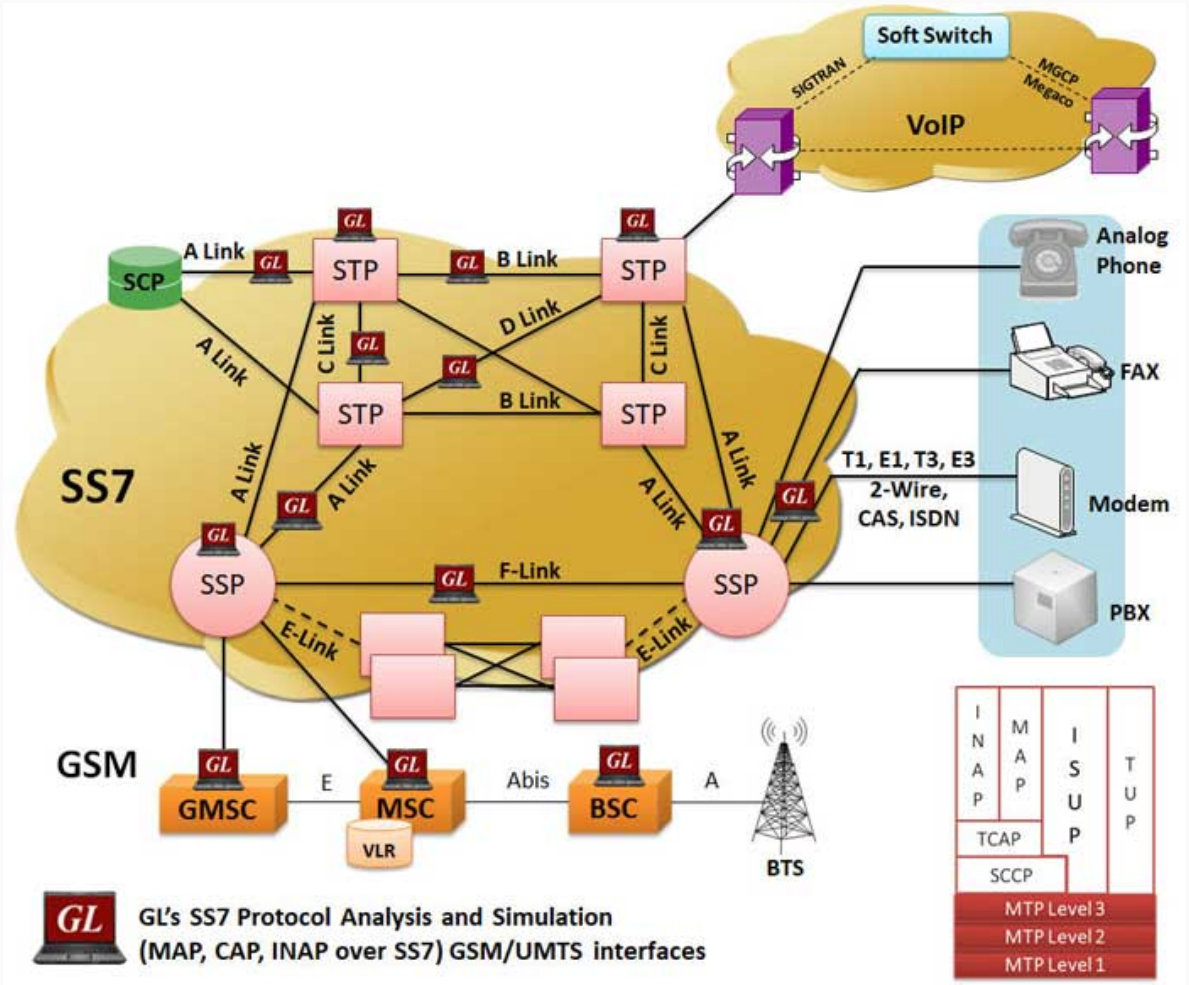


Figure 2: Image Source: https://www.gl.com/ss7-protocol-analyzer.html

Threat model of SS7

All parties connecting to each other in SS7 are trusted PSTN operators, *why would they hijack other phone numbers*?

All the equipment they run is properly secured *presumably*,

Traditionally gaining access to SS7 meant that an attacker can reroute phone calls and intercept SMS,

Due to some high profile attacks, carriers have implemented mitigations to this, but it depends on the carrier,

When is the last time you checked the SS7 implementation of your phone provider?

Real world attacks on SS7

Interception of SMS One Time Passcodes (OTP) used to secure bank accounts etc,

Attacks on bank OTPs:

- `https://www.theregister.com/2017/05/03/hackers_fire_up_ss7_flaw/`
- `https://www.fintechfutures.com/2019/02/uks-metro-bank-hit-by-ss7-attack/`

Possible because of other entrypoints to the SS7 network which were unexpected,

- Femtocells that providers give to customers, contianing IPSec or other means of connecting back,
- Find open SS7 servers on the Internet,

ACARS

Aircraft **C**ommunications **A**ddressing and **R**eporting **S**ystem

Used to send messages to and from aircraft,

Historically unauthenticated and unencrypted,

Some effort to authenticate and encrypt:
Honeywell ACARS Message Security

Passive observer of ACARS

Can read messages from ground to aircraft and aircraft to ground,

E.g. Routine planning of flight path, medical emergencies of passengers on board, emergency on the ground, etc...

Active transmitter of ACARS

Can inject messages to further the aims of an attacker,

In the complex geopolitical landscape, aircraft being led astray or going to the wrong destination is quite undesirable,

Satellite systems

Used in Aircraft, ships, oil rigs, offshore wind farms, lots of important stuff,

Typically connecting specialist equipment (embedded, hard to update devices),

On land side is typically corporate offices contianing control systems / databases,

Expensive to use, so ratio of valuable traffic : random browsing is high,

Faster reply attack

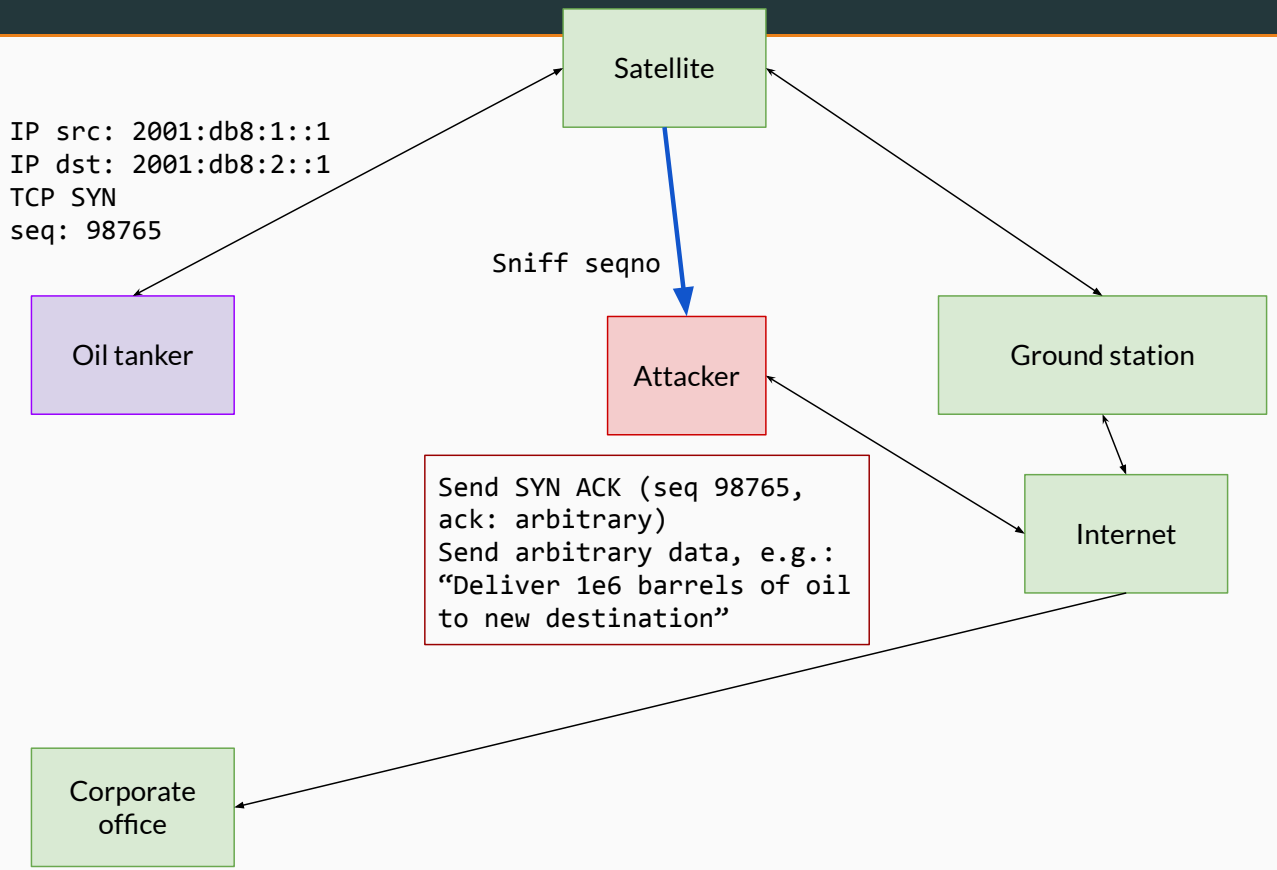


Figure 3: Attack Credit to James Pavur, Blackhat 2020[1]

[1] https://i.blackhat.com/USA-20/Wednesday/us-20-Pavur-Whispers-Among-The-Stars-Perpetrating-And-Preventing-Satellite-Eavesdropping-Attacks.pdf

Further pointers

IEC 61850

`https://en.wikipedia.org/wiki/IEC_61850`

A standard for protocols to control electrical substations

Makes the management and maintainance of these safety critical systems easier / automated,

Interesting for security researchers, see e.g.

M. T. A. Rashid, S. Yussof, Y. Yusoff and R. Ismail, "A review of security attacks on IEC61850 substation automation system network," Proceedings of the 6th International Conference on Information Technology and Multimedia, Putrajaya, 2014, pp. 5-10, doi: 10.1109/ICIMU.2014.7066594.

Boarding passes

PNR + Last name sufficient to “log in” as passenger.

Who would post photos of their boarding pass online?

Simple attack: Log in to airline website and claim air miles to central account

Advanced attack: Leverage access to travel booking APIs e.g. SABRE, Amadeus for rebooking, refund, etc.

Financial networks

Banks too are interconnected!

Send messages to each other about financial transactions,

Use networks / platforms such as SWIFT (`https://www.swift.com/`) to do the data exchange,

Typically have good security measures due to currency being involved,

Still vulnerable to the weakest link in the chain, see: `https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery`

Recap

- Zero trust, root in sound cryptography,
- Solve end-to-end problems, securing one component in isolation moves attacks elsewhere,
- Learn from mistakes already made,