Impact of Tampering and manipulation of ICT identifiers to network resources and operations (signaling and protocol prospective)

Latifa.S.Elhakim
UMST

Introduction

- Standards bodies have a unique ability and responsibility to address the affect of ICT identifiers toward connectivity in protocols
- There are immediate and relatively simple actions standards bodies can take to improve the vulnerabilities of all protocols currently being standardized.
- For that and In order to make a standardized protocol to all ICT community the Transport Layer Security (TLS) protocol was introduced. TLS was the basis of Wireless Transport Layer Security (**WTLS**) which is security level for Wireless Application Protocol (WAP). WTLS was introduced to reliability and privacy for wireless application.

Abstract

- Most organizations and companies as well users prefer using wired devices to keep their network information secured, data protected despite the distance limitations and costs. Although Wireless devices capacity and performance has increased exponentially and allow users to access the network remotely within the specified range they have many security threats. Securing wireless devices is necessary with the increase considerations about a secure access to your network using private wireless devices such as personal digital assistant (PDA), Smartphone and IP phone, since it became a critical issue. Smart phones and other handheld devices like PDAs are growing rapidly with their easy to access the Internet by using WIFI, LIFI or mobile data
- In order to get this happened and to avoid that problems we conduct a scientific research concerning the impact of Tampering and manipulation of ICT identifiers to network resources and operations (signaling and protocol prospective)

The work

- Therefore, in our testing laboratory in Sudan, we try to manipulate in the network resource elements by adding and scripting in the connectivity between client and server machines to conclude some results one these results was the affecting of Tampering and manipulation of ICT identifiers to network resources and operations (signaling and protocol prospective) bear in mind that testing procedure done for example according to ITU-T G.722 recommendation

Why?

- The hardware identifiers of common wireless protocols, e.g. an 802.11 MAC or GSM IMEI, are globally unique and do not change over the lifetime of a device, thereby permitting both tracking and physical device association As such, these identifiers can be exploited by Mobile theft or counterfeited industry for a range of attacks ranging from mobile privacy to targeted denial-of-service.
- For example illustrates a GSM air interface attack where the attacker must first know the IMEI of the intended victim.
- An attacker correlating hardware identifiers, can use details gleaned from protocol A to identify and exploit security vulnerabilities inherent to protocol B , increasing the available attack vectors.

What?
Is a Vulnerability in protocol ?

- a vulnerability is a weakness which can be exploited by a Threat Actor, **such** as an attacker, to perform **unauthorized** actions within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness.

(*mostly, the flaw of design in ICT device back to story that system had been manly manipulated with or tampered*)

Vulnerability in protocol alone is not consider a risk !

(*to be a real-time risk for system should be combined with a security risk*)

Protocol Vulnerability Types

- **Design and specification** (*tampering and manipulating*)
  - Tampering or manipulating in design make the protocol inherently vulnerable.

- Network packets pass by entrusted hosts.
  - Eavesdropping, packet sniffing
  - Especially easy when attacker controls a machine close to victim
- Denial of Service.

How?

"WTLS" Wireless Transport Layer Security protocol (case !)

- Here I shed some light on how tampering and manipulating the ICT Identifier could affect the network operation and resources as well:
  - WTLS protocols support among others, MACs, the MAC work by padding the message with 0s, dividing it to 5-byte blocks, the specification state that MAC only intended for device with limited CPU resources , The specification also tell us that the MAC may not provide as strong message integrity protection, In fact it is easy to see that the MAC does not provide any message integrity protection if stream ciphers are being used, regardless of the key length. If one inverts a bit position *n* in the cipher text, the MAC can be made to match by inverting the bit (*n* mod 40) in The MAC , This can be repeated arbitrary number of times.
  - Well, from that prospective its clear to see that there is huge impact toward network resource and operation when we dealing with tampering and manipulation with regard to Protocol and hardware ICT identifiers .

1- Impact of tampered and manipulated ICT identifiers to Protocol Vulnerabilities

- serious weakness in the protocol allows attackers within range of vulnerable device or access point to intercept passwords, e-mails, and other data presumed to be encrypted, and in some cases, to inject ransomware or other malicious content into a website a client is visiting.
- Threats change, but security vulnerabilities exist throughout the life of a protocol.

2- Impact of tampered and manipulated ICT identifiers to Protocol Vulnerabilities

- **Rapid7** conducted its own research into UPnP protocol vulnerabilities by scanning devices over the UPnP protocols for five-and-a-half months. The experiment found that nearly 17 million systems and UPnP protocols were exposed to external networks. The Rapid7 research also uncovered the following facts:
  - More than 6,900 products had discoverable flaws.
  - More than 23 million systems had a vulnerability to a single remote code execution flaw.
  - Twenty percent of 81 million systems displayed SOAP API vulnerabilities. This significant security flaw could allow cyber attacks that hack devices behind a firewall.

Recommendation

- Within the ICT industry, mobile phones are clearly the largest focus for counterfeiters, but chips and other ICT components are now found in other industries. E-commerce is a boon to counterfeiters — criminals are adept at cross borders and moving around to avoid restrictions and tax. Regulation applied to redress the problem does not work alone — a preventative approach is needed to tackle this problem at its source.
- An inclusive approach is needed involving regulators, governments, consumers, civil society and the industry.
- Preventative approaches are needed to reduce incentives throughout the supply chain; a better and more efficient use of existing technical solutions, such as international standards
- analyze and disseminate more data about the nature and impact of counterfeit and substandard products, and the role of ICTs in combating them.

References

- ITU-T G.722
- Institute of Research Engineers and Doctors