HARDWARE SECURITY

Hardware is a collection of physical elements that constitutes a computer system. Hardware is used by everyone even if they are not aware of it. Hardware in this context might be:

a. **Computer Hardware**: Some computer hardware are Processors, firmware, memory etc.

i. Processors: is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output (I/O) operations specified by the instructions

ii. Firmware: is the combination of a hardware device, e.g. an integrated circuit, and computer instructions and data that reside as read only software on that device

iii. Memory: Memory refers to the device used to store information for use in a computer.

b. **Mobile Hardware**: Sim Card, RFID/Smart Card, Chip and Pin

i. Sim Card: is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).

ii. RFID: is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. For example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line.

iii. Smart Card: is any pocket-sized card with embedded integrated circuits. Smart cards are made of plastic, and can provide strong security authentication for single sign-on (SSO) with large organizations.

Iv Chip & Pin: "Chip" refers to a computer chip embedded in the smartcard, and "PIN" refers to a personal identification number that the customer must supply. "Chip and PIN" is also used in a generic sense to mean any EMV smart card technology that relies on an embedded chip and a PIN.

c. Future Hardware: PUFs (Physically Unclonable Functions) PUFs have a unique fingerprint in a physical object that means if you have an object with one fingerprint, another object with the same fingerprint cannot be created. It uses challenge/response for it's operations. The challenge/response explains that if a message is sent to a physical object and the physical object is changed to another physical object, and same message is sent to the second physical object, the two physical objects react differently because of their unique fingerprint.

ATTACKS ON HARDWARE

1. Physical Attacks: The main thing that differentiates hardware attacks from software attacks is the physicality of the attack done with hardware tools. This raises the bar for hardware attacks because any attacker that wants to performed an attack on the hardware needs to have extensive knowledge of the hardware, unlike the software attacks that can be done by just downloading a vulnerability tool on the internet to perform attacks.

2. Generally, the hardware wants to protect a secret so the secret is embedded in a physical object. For example, the bank card wants to protect your pin, the pin is encoded in the card and if the attacker can probe the chip of the card and read the pin then the card is useless. The secret in the hardware should not be writable even though it provides the information on the card when placed on a terminal. If we consider STRIDE, we have to consider two main points : the Information Disclosure (Confidentiality) which means something is hidden, and Tampering (Integrity) which means it is not writable.

3. Attack Vectors: The hardware that would be used to protect the secret would be fabricated by someone in a factory. The factory will either program the secret onto the hardware or send the hardware to the company with memory for read access in one component and write access in another component so that the company can program the hardware and destroy the write component to avoid rewriting. This approach can't be used for all hardware. For example, subway cards need to be rewritten to every month so in that case, the terminals have write access to the card but the user doesn't have write access so it can't be overwritten by the user.

To fabricate the hardware, the laboratory/factory needs to be trusted. And to prove they are trustworthy, the laboratory gets certified. The certification body sends people in, to audit them,

check out the employees and their procedures and conclude whether the laboratory is trusted or not.

4. Supply Chain: After the hardware has been made, it will be shipped to stores that will sell it or it is shipped to the consumers from the store. During shipping it could be intercepted by the attackers and tampered with, then re-packaged without the knowledge of the store or the consumers. Also, some attacks can be performed on point of sale terminals when some insider (employees) have access to the terminals and tampered with it in the warehouse

5. Accidents: there are a lot of memory based devices (e.g. USB Keys, Digital picture frames) which may contain malware in them accidentally, which could affect the system of the user. The company that created this hardware may not be aware of the malware on the device. Examples of companies that had this kind of accidents are IBM, Dell, Samsung, HP, Apple, etc.

All the attacks stated above are the main reasons for why the user might get a bad hardware.

ATTACK CIRCUITS

RFID, Smart Card, Micro- Controller, ASICS, FPGAs

RFID is passive, a signal can be sent to it and it responds. It can't be programmed, it can't performs any computations based on the signal sent to it. **Smart card**, on the other hand, performs computations based on what was sent to it.

Micro-controller is like an ID with no chip,

ASCIS are fabricated circuits that are custom made to do implementations so all your processors and memory are on ASICS. ASICS are expensive because they are custom made, and before the design is committed to ASICS, a lot of testing will be done with FPGAs to make sure that circuit actually works.

FPGAs are programmable chips. When the chip is bought, its blank and it can be programmed with software to do whatever you want. They are not as fast as ASCIS because they are general purpose. FPGAs are faster than software but slower than ASCIS.

Why are we attacking Circuits?

The main reason for attacking circuits is to recover a secret that had been encoded on a piece of hardware or for the attacker to program a certain value to the circuit. The secret could be the actual algorithm itself. Some attackers reverse engineer the algorithm of the RFID or Smart Card to find flaws in the algorithm itself. This is because some developer wants to keep the algorithm used to protect the circuit a secret due to the fact that the developers are not using a standard algorithm. The algorithm used should be a standard algorithm so as to know how to better protect it.

The Circuit attacks are:

1. **Black Box Testing**: To perform this attack, the attacker sends an input to the circuit and receives an output. Based on the input and output behavior, the attacker will decide what kind of algorithm to used. An example is Speed Gas RFID which are proprietary stream cipher. The attackers found the documentation and modified it to discover the cipher used and break the circuit. This type of attack is non-invasive, meaning that the card/chip will not be destroyed when probed so it can be used another time. Another method that can be used in black boxing is fuzzing in software security which allows large random inputs to the circuit and get strange responses like undocumented features, factory testing, etc.

2. **Physical Probing**: To perform this attack the attacker sticks a probe unto the chip itself and reads data off the chip. Within a circuit, there is a wire that connects components to each other called the bus and the bus is where the information would be read as the data is moving around in the bus. The data can also be read off the memory location in the circuit. The probe can have a submission precision and it's an invasive method. A lot of circuits are driven by a clock, and if the attacker can slow down the clock it gives a lot of time to the attacker to read the voltage of the circuit.

3. **Reverse Engineering**: To perform this attacker, the attacker must acquire the smart card and physically expose the circuit. The smart card is manufactured with different layers and each layer is removed until the physical circuit is exposed. The attacker then takes a high resolution

photographs of the circuit and uploads it to a computer and uses a code and machine learning application to figure out what the actual circuit does. Once the circuit is figured out, then the algorithm used in the smart card also is exposed and the algorithm can be broken. An example of a smart card where the reverse engineering attack was performed on is the Mifare (Subway card).

4. **Fault Generation**: Some technologies fail. E.g. A TV providers sends a message to the client asking if the clients wants to renew the subscription. If TV providers doesn't receive a message NO from the clients, they don't disconnect, so the clients are granted access. So some clients can just cut the power at the right time to prevent the response to the TV providers, since they won't disconnect with no response. This is a non-invasive attack. Other things that can be done are modifying the memory contents (non-invasive), glitch (rapid change) the power or clock (non-invasive), heating up components e.g. with a user (semi- invasive), modify chip e.g. cutting wires (invasive) etc.

5. **Side Channel Analysis**: To perform this attack, the attackers makes use of the hardware normally but makes sensitive measure of certain things and based on the measurements done, the attacker can infer secrets. An example of things to measure is power (the amount of voltage in an ATM), timing analysis in cryptography (software effect), electromagnetic emission, acoustic sounds (performed on RSA). These are called side channel because they are outside the normal channels. They are non-invasive. It is slower than the normal attacks.

COUNTER MEASURES

1. Obfuscate data (Scramble, encrypt) on buses
2. Obfuscate the ASICS layout, 3D stacking
3. Metal mesh on top of the circuit (if the circuit is probed, it causes a short and the memory resets)
4. Side Channel: physical shields, asynchronous circuits. Also, a decrease in the signals from the circuits of the hardware like the noise or add artificial noise or low the circuit's power

METHODOLOGIES

There is no good methodology for hardware (that means no static analysis or dynamic analysis of hardware). It is an open question that needs to be researched on. Most of it haa to do with domain specific knowledge and it is advisable to follow the requirement engineering process. Common criteria/NIST have protection profiles which provides the properties not how to achieve them.

EXAMPLE ATTACK

The example attack is on a CHIP & PIN. The attack is CICA 2000 and it was performed in the United Kingdom. It's actually a protocol attack, but in order to perform it, you need customized hardware. The basic hardware used is the bank card. The bank card might have been stolen and the attacker didn't know the pin to the card, but wants to buys somethings with the card without the pin. This attack can't be performed on an ATM because it uses a different protocol, it can only be performed on a handout terminals at a store.

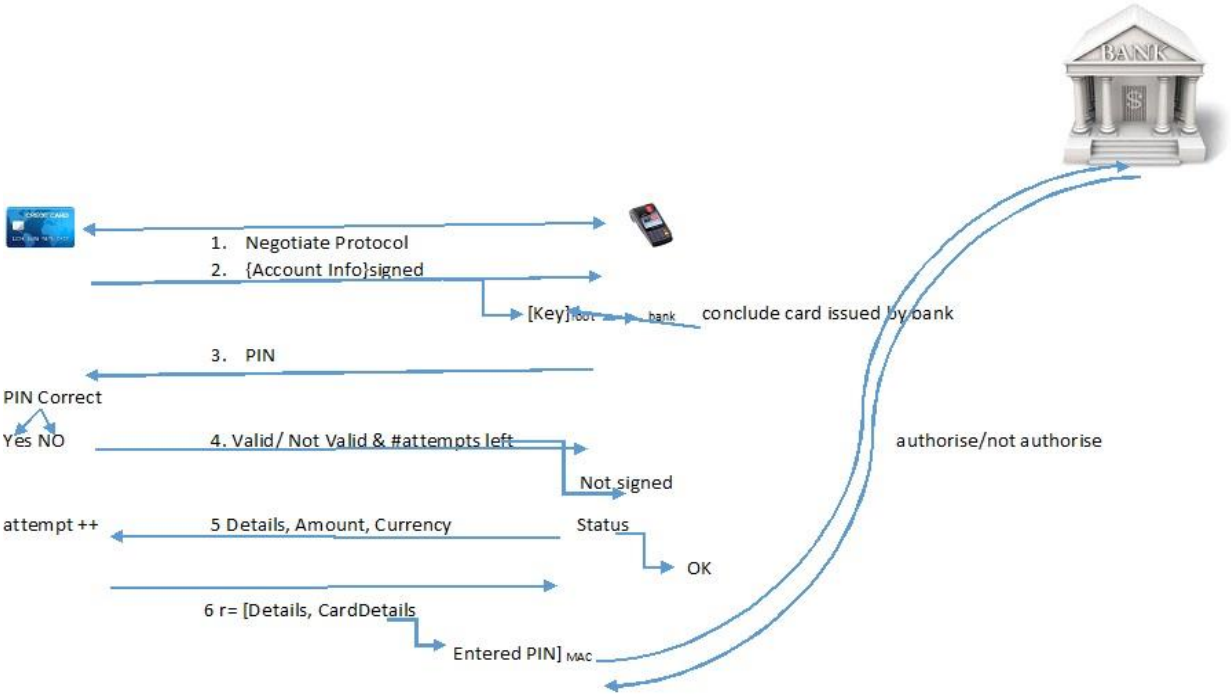

Figure 1: Simplified diagram of Protocol used

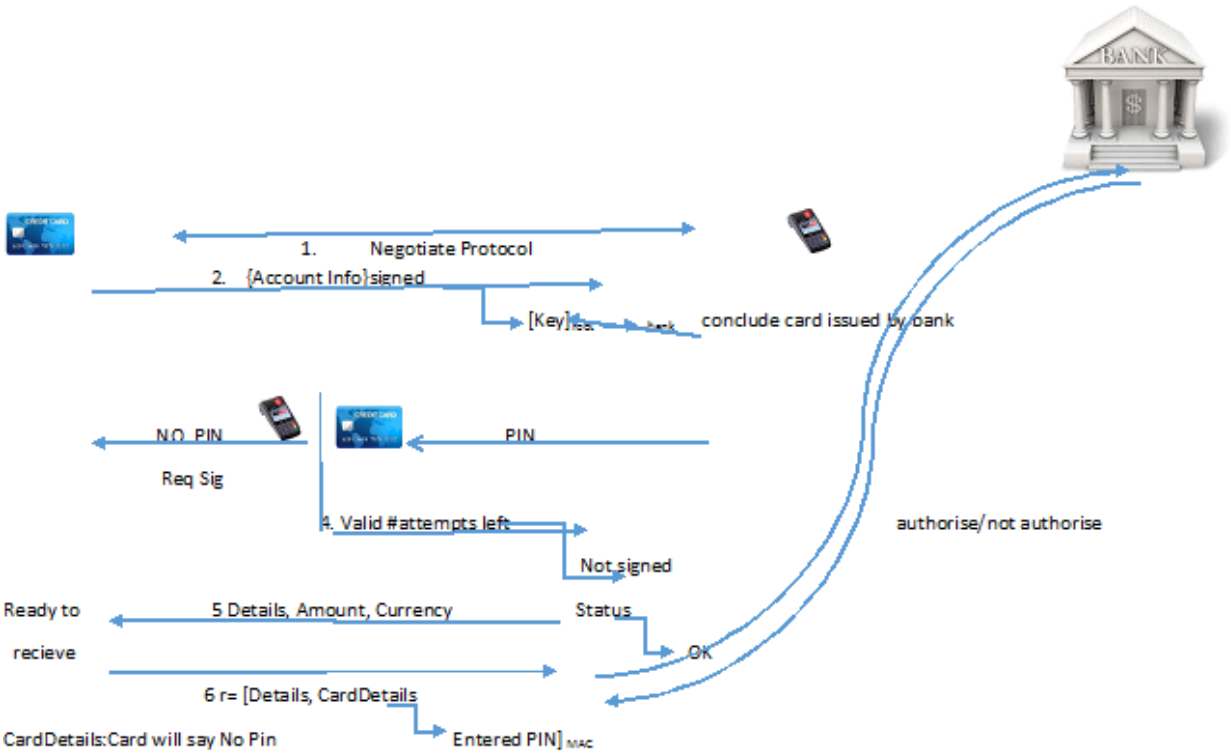

Figure 2: The attack

Issues of this attack

1. The Pin (Invalid not signed)
2. Details used in the protocol is not enough
3. CardDetail : Terminal can't parse only bank can

REAL LIFE IMPLEMENTATION.

The attacker would need the stolen card, a card reader, a laptop, a circuit (FPGA), wire and a fake card.

.

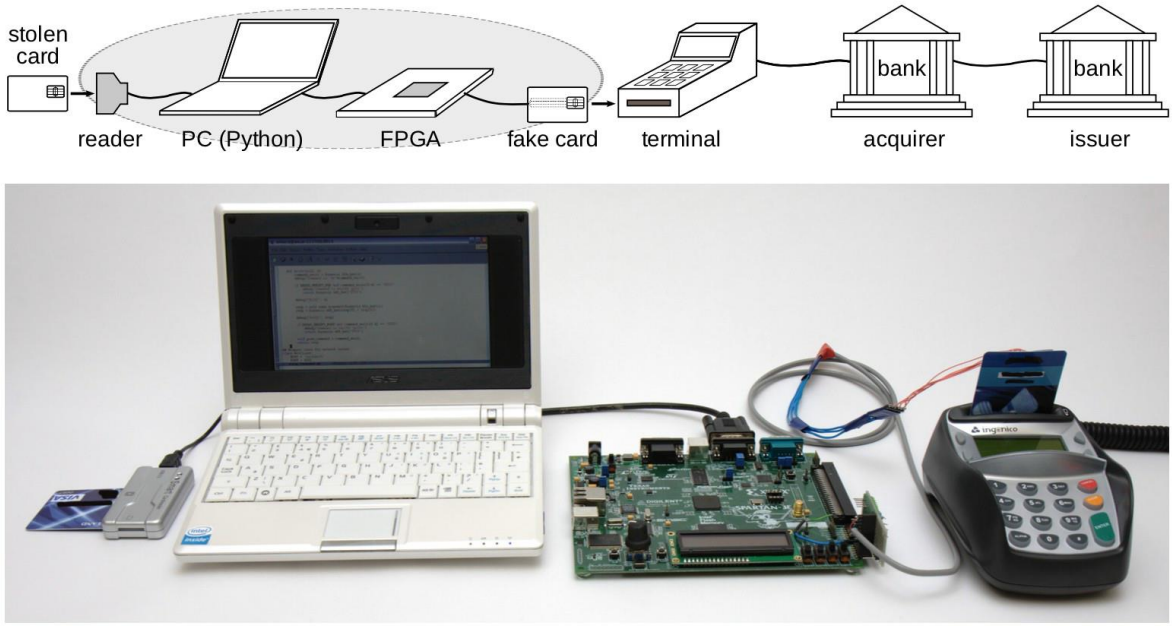

Figure 3: Real life implementation of Chin & Pin attack

In the diagram above, the attacker would stick the card in a card reader and the card reader is placed in a computer, the computer is connected to a circuit like an FPGA. The attacker then have a wire that runs to a fake bank card that is in the terminal. The wire is attached to the circuit which was attached to the computer that the card reader which contains the real card is inserted. This is the Man-in-the-middle device, the stolen card would transfer all the information on the card to the fake card in the terminal. To perform this attack in real life, all the equipment would be placed in a bag pack and the wire would be passed inside the cloth and since by law the cashier is not supposed to touch the card, the fake card is inserted with the wire on the circuit and the attack is performed. This attacked happened in the UK but this kind of attack cannot happen in Canada.