Secure Embedding Communication Channels: An Exploration of the Use of Simulated Quantum Electro Dynamic Systems

Najib SAYLANI

Abstract--**This paper proposes a novel approach that would complements traditional encryption based methods used to secure the flow of sensitive and confidential information traveling the different channels that exist in embedded systems. The paper outlines the use of techniques adopted from the field of Quantum Electro Dynamic used to simulate weak perturbations through wave scattering. New and logical communication paths are simulated through the process of particles scattering phenomena. Information is encoded as waves packets transmitted through the same generated channels.**

Keywords-- **Quantum Electro Dynamic (QED), Security, Wave scattering.**

I. INTRODUCTION

Common embedded systems in use today to support various critical IT infrastructures implemented for both government and industries require, in addition to encrypting information, a more robust environment for the dissemination of critical and confidential information. Unsecure internal communication channels in a given system represent a so often ignored danger of compromising any system. We outline in the next section an approach from Quantum Electro Dynamic that is actually part of a large security system we are working on for the past six years. Paper referenced in [7] outlines the overall system. This is a tiny subset of such system that target securing communication paths taken by information within an embedded system. The idea is to make these paths invisible to hacking by mapping the whole process to the simulated process of waves' propagation through scattering process. We claim that this process, while is not a form of encryption, is a way to increase challenges for any potential hackers and to thwart attacks that have as a purpose the interception of embedded communication channels and the compromise of information within the system itself. The approach is to create chaotic but controlled phenomena that are extremely hard to determine by attackers.

II. BACKGROUND AND THE PROPOSED APPROACH

Quantum Electro Dynamic (QED) is the quantum field theory of electrons, positrons and photons. The techniques adopted for the proposed systems are limited to the case of weak perturbations when wave scattering occurs. The discussion related to QED is completely adopted from [5].

The scattering simulates a multi-treaded environment where information between CPU, BUS, RAM, and various ports on the system is already encrypted. We believe that this technique will efficiently complement techniques surveyed in the paper by Elbaz et Al [3]. The referenced paper is selected because it outlines traditional techniques based on encryption and it is one of several research paper s that inspired us to work on this area. We also claim that low overhead through using the proposed approach in systems where information is not encrypted at all.

We are aware of the fact that processors, bus, and main memory architecture and the associated ports used in internal communications are not secret. This same knowledge may make this environment a source of security compromises.
The following is a summary of the main points of such system:
-Information to be secured is encoded as a wave packet and propagated from source to destination within a given system.

N. SAYLANI, Hosftra University, USA

-The process of encoding and propagation is randomly generated and mapped to a certain number of threads managed through Inter Process Communication (IPC) schema.
-In this case, a single known channel of communication is mapped to multiple 'virtual' or 'logical' channels maintained through simulated oscillations kept alive through simulated local potentials (energy).
-The propagation/scattering process is assumed to happen in real or simulated real time through the introduction of artificial delays. The process is represented by the following $Schr\ddot{o}dinger$ wave equation [4]:

$$i\eta\frac{\partial(x,t)}{\partial t}=-\frac{\eta^2}{2m}\nabla^2\Psi(x,t)+V(x,t)\Psi(x,t)$$

The equation describes the interaction of a particle of mass *m* with a potential constant in space. (In our case the potential is not fixed-which would cause it to have different equations for different generated paths, with different potentials at various given times).

The question is how the information is retrieved later at destination? The answer is that, in QED, it is well established that:

If Ψ is known at position x, and at time t then Ψ is also know at t_0 <t and t'>t.

In the proposed model generated paths (i.e. channels) is achieved through a true simulation of a comparable physical system exhibiting identical phenomena. QED supports real world physical systems where past and future behavior of the scattering can be determined. In QED analyzing the behavior of the scattered waves across different paths (generated logical channels) is helped by the use of the *Green's Function*.
Green's Function describes the probability amplitude associated with the scattering process.
In our model, defining a specific path of scattering will help determine the solution to all $Schr\ddot{o}dinger$ equations involved. Across all generated paths the solutions to a specific $Schr\ddot{o}dinger$ equation would be linearly superposed on the *Green's Function*. In order to analyze the process of scattering we need to introduce the Huygens Principle:

$\Psi(x,t)$ at time t' position x' is known if $\Psi(x,t)$ is known at source x at time *t.*

$$\left[\Psi(x',t')=i\int d^3xG(x',t';x,t)\Psi(x,t)t'>t\right. \quad (1)$$

The intensity of Ψ at (x',t') is proportional to Ψ at $\Psi(x,t)$

Here $iG(x',t';x,t)$ is the constant of proportionality in (1)
$G(n',t';x,t)$ is the *Green's Function* of the *Hamiltonian* $\hat{H}$ or *Hamiltonian operator*

$$\hat{H}=-\frac{\eta^2}{2m}\nabla^2+V(x,t)$$

Backward and Forward propagations are considered. This assumes that within our model if the path is defined then one can proceed by assuming either a forward or backward propagation.
For that case there are two types of *Green's Function*:

- *Forward or retarded Green's Function*

$$G^+(x',t';x,t)=\begin{cases}G(x',t';x,t) & t'>t\\ 0 & t'<t\end{cases}$$

That is a causal backward or evolution of $\Psi(x,t)$ from $\Psi(x',t')$

- *Backward or advanced Green's Function*

$$G^-(x',t';x,t)=\begin{cases}G(x',t';x,t) & t'<t\\ 0 & t'>t\end{cases}$$

This is a causal backward or evolution of $\Psi(x,t)$ from $\Psi(x',t')$
Determination of a resulting wave packet backward or forward necessitates the introduction of step-function θ.

$$\theta(\tau)=\begin{cases}1\ for\ \tau>0\\ 0\ for\ \tau<0\end{cases}$$

The causal evolution of $\Psi(x',t')$ from $\Psi(x,t)$ where $t'>t$ can be represented by $\theta(t-t')\Psi(x',t')=-i\int d^3xG^-(x',t';x,t)\Psi(x,t)$
It is noted that the *Green's Function* is considered only when a potential V of a scattering position x and at time t is not zero. $(V(x,t)\neq 0)$. If $V(x,t)=0$ we speak of a *free Green's Function* noted G_0.

As stated before, when a scattering path is chosen in our model at time t_1 and at position x_1 (a node x, of a given path) the corresponding scattered wave can be found by solving the following *Schrödinger* equation:

$$i\eta\frac{\partial}{\partial t_1}\Psi(x_1,t_1)+\frac{n^2}{2m}\nabla^2\Psi(x_1,t_1)=V(x_1,t_1)\Psi(x_1,t_1)$$

And if $V(x_1,t_1)$ is on during a fraction time Δt_1:

$$\Psi(x_1,t_1)=\phi(x_1,t_1)+\Delta\Psi(x_1,t_{1)}$$

ϕ: free wave

$\Delta\Psi$: scattered wave

if $\mathrm{V}(\mathrm{x}_1,t_1)$ is off after Δt_1:

$$\Delta\Psi(x_2,t_2)=i\int d^3x,\nabla G0(x_2,t_2;x,t,)\Delta\Psi(x_1,t_1)$$

Other computations lead to:

$$\Delta\Psi(x_1,t_1)=\frac{1}{\eta}V(x_1,t_1)0(x_1,t_1)\Delta t_1$$

The *Green's Function* and *Huygen's Principle* will enable us to compute a wave function at a given position at a given time when the wave is known at a former position and time (in the same scattering process).

The choice of scattering' paths within the system are critical in reconstructing the waves and, by the same process, retrieve the encoded information. There are different equations to solve across different paths. The idea is to compute or construct the wave $\Psi(x,t)$ at a position x along a given path at time t during a potential V. We note that by $V(x,t)$

Assume $\phi(x,t)$ is the initial wave associated with the incoming particle; it is established that $\phi(x,t)$ is a solution of the *Schrodinger* equation for a free particle.

Therefore, if no interaction affected $\phi(x,t)$ then it is stated that $\Psi(x,t)=\phi(x,t)$. In the future at position x' and time t' we have the following result:

$$\Psi^{(+)}(x',t')=\phi(x')+\int d^4x_1G_0^+(x';x_1)V(x_1)\Psi^{(+)}(x_1)\quad(2)$$

$(+)$: future scattering

Here $\Psi(x_1)$ is the original wave packet. The second term of (2) is the scattered wave.

Following specific rules of waves' superposition, coherence and given local oscillations maintained by a local energy, the techniques outlined here makes it easier to trace back along any path the whole wave (information/pattern) by only using partial or chunks of waves at any time at the level of any point or group of points along a given generated path.

The simulation is to be conducted using mathematical and programming tools presented in [1][4][6].

The following is a summary of steps to be taken in this process:

-Determine source and destination of information within the system (embedded system).

-Determine all devices partners in such communication.

-Encrypted or not information set is determined.

-Encode information by using initial states of original waves at the source.

-Randomly generate a set of virtual/logical channels between source and destination through the creation of multiple processes residing in randomly selected and available areas in system memory.

-Start simulation the propagation of original waves through these virtual/logical channels.

-The simulated scattering of waves cannot be predicted ahead of its occurrence. The selected set of paths is determined through multiple random processes that mimic the scattering process of a real world physical system.

-Determine and compute all related equations at destination to assemble original waves through processing partial states of each to regenerate the original information back at destination.

-Repeat for each transmission by resetting the simulation each time.

Because the process of scattering is a 'pseudo non-deterministic' set of events, it represents a kind of black boxes whose contents (processes, information, paths) cannot be determined.

III. CONCLUSION

We should acknowledge the fact that this approach adds an extra layer of protection to existing traditional layers (i.e. encryption). Another inspiring research article is referenced in [3] and we feel our approach may complement such work. Theoretical analyses of such system through the already proven techniques in QED fully support the claim that the new environment is robust and extremely challenging to the would-be hackers/attackers. This environment adds a very large number of unknown to a specific

physical topology (known communication channels) through the creation of simulated logical topology (simulated and claimed to be invisible channels of communication). A much more in depth study of the effect of such approach on the over-all performance of the system must be undertaken. Some of the challenges depicted in [8], although not directly related to the challenges faced by our system, should be considered especially at the hardware design level. For now, we are limited to simulating a system using existing architecture. And, as with any security system, a paradox does exist; how to secure the simulation process itself? A paradox similar to the one related to the storage of passwords and other similar concerns. In the case of the proposed system, a hacker/attacker can only disturb the system without gaining access to the information being transmitted. The hacker/attacker cannot determine what channel to intercept.

REFERENCES

[1] Brandt, S., Dahmen, H. D., Quantum Mechanics on the Personal Computer Third Edition, SpringerVerlag, New York, (1994).

[2] Coburn J., et Al, SECA: security-enhanced communication architecture, Proceedings of the international conference on Compilers, architectures and synthesis for embedded systems, 2005

[3] Elbaz, R. et Al, Hardware Engines for Bus Encryption: a Survey of Existing Techniques, Proceedings of the conference on Design, Automation and Test in Europe - Volume 3, 2005

[4] Feagin, J. M., Quantum Methods with Mathematica, Springer-Verlag, New York, (1994).

[5] Greiner, Reinhardt, Quantum Electrodynamics, Springer-Verlag, New York, (1994).

[6] Hockney, R. W., Eastwood, J. W., Computer Simulation Using Particles, Mc Graw-Hill, New York, (1989).

[7] Najib Saylani, "A Proposal for an Automated Approach to Real Time Profiling of IT Security Compromises", The 2004 International Multi-conference in Computer Science & Computer Engineering (June 2004)

[8] Remond, F., Physical design challenges for multi-million gate SoC's: an STMicroelectronics perspective, Proceedings of the international symposium on Physical design, 2006