Proposta de Trabalho - MAC0499 Trabalho Supervisionado de Formatura

Aluno: Gabriel Capella
Supervisor: Alfredo Goldman vel Lejbman

23 de Abril de 2018

1 Tema

O tema principal desse trabalho é verificação remota, em inglês *Remote Attestation*).

Atualmente o temas como internet das coisas e cidades inteligentes estão sendo amplamente estudados. Esses temas envolvem a utilização de hardware específico para a realização de certas tarefas, esse hardware também é conhecido como sistemas embarcados. Hardwares desse tipo já estão sendo utilizados na indústria a um longo tempo para aplicações específicas. No entanto, por causas dos temas citados, atualmente eles estão sendo conectados a internet para receber e enviar dados.

Muito se fala sobre a segurança desses dispositivos. Infelizmente, investir em segurança e prevenir falhas é algo custoso e não é aplicado em muitos projetos. Ou até mesmo, existem cenários que essas medidas são levadas em consideração, mas o dispositivos continuam sendo alvo de ataques. Prevenir ataques a esses dispositivos pode ser difícil ou até mesmo impossível, no entanto é possível realizar contra medidas, ou seja, identificar se o dispositivo foi atacado para possível substituição, desativação ou reparo do mesmo.

Uma das contra medidas mais utilizada para esse tipo de ocorrência é a verificação remota. Nela, comumente pela internet, os dispositivos são interrogados e devem satisfazer uma série de critérios que visam afirmar que ele continua com o seu software integro e igual ao que foi programado. Esse campo é relativamente novo e existem algumas soluções propostas.

A primeira dela é relativa a verificação remota por software. Nela toda a parte responsável por atestar a integridade do dispositivo é feita por software. No entanto diversas propostas desses tipo tem se mostrado falhas e ineficientes, um exemplo dessas dificuldades pode ser vista no artigo "*On the difficulty of software-based attestation of embedded devices*"[1].

O segundo tipo de verificação remota é a realizada por hardware. Já existem propostas e projetos bem elaborados nessa área, principalmente para computadores [2], que incluem módulos anexados ao processador ou até mesmo dentro

dele. No entanto para dispositivos embarcados de baixo custo soluções ótimas estão sendo exploradas.

Uma dessas soluções é sugerida no artigo SMART[3]. Nesse artigo, os pesquisadores tentam criar uma estrutura mínima necessária para implementação da verificação remota em dispositivos embarcados. No entanto, eles apenas fazem sugestões e dizem como a implementação deve funcionar. Ou seja, não foi realizado nenhum teste ou implementação desse algoritmo.

Durante o trabalho formatura pretendo refazer os passos sugeridos nesse artigo e verificar a solução proposta. No entanto a solução envolve a confecção de hardware específico. Montar esse hardware é custoso e inviabilizaria o projeto. Mas, devido a uma tecnologia conhecida como FPGA (*Field-programmable gate array*), é possível descrever em uma linguagem de programação o hardware e testá-lo. Pretendo utilizar essa tectonologia para averiguar o funcionamento do algorítimo e hardware proposto no artigo.

2 Justificativa

O estudo desse tópico envolve tanto a parte de hardware como a de software para resolver uma questão de segurança. Durante a confecção do trabalho, serão realizados estudos em diversas áreas, sempre visando a segurança do dispositivo. Ou seja, não estamos querendo desenvolver algo novo, mas sim, repensar em uma solução convencional (no caso um microcontrolador) visando sempre a segurança da mesma.

Ultimamente várias soluções tem sido propostas utilizando caminhos mistos como esse. Por isso, é interessante seguir em soluções mistas que envolvem hardware e software.

3 Objetivos

O principal objetivo desse trabalho e verificar se a sugestão de verificação remota sugerida no artigo é válida.

Além desse objetivo, haverá a tentativa de propor melhorias para o algoritmo de verificação remota por hardware.

Queremos chegar em uma solução que consiga verificar remotamente a integridade de um dispositivo.

4 Metodologia

Segue abaixo as tarefas que serão executadas durante a elaboração do trabalho. Note que não existe uma tarefa específica de escrita do texto final, pois o mesmo será desenvolvido ao longo do trabalho.

1. Levantamento bibliográfico e estudo do mesmo.
2. Aprendizado de linguagem descritiva de hardware.

3. Simulações e testes em um FPGA - inclui definir o modelo correto para prosseguir o experimento.

4. Teste e implementação de algum microcontrolador dentro do FPGA.

5. Implementação da arquitetura de verificação remota.

6. Testes e sugestões de melhoria.

5 Cronograma

Parte do tarefa 1 já foi realizada.

Mês/Tarefa	1	2	3	4	5	6
Março	X					
Abril	X					
Maio	X	X				
Junho		X	X			
Julho		X	X			
Agosto				X		
Setembro					X	
Outubro					X	X
Novembro						X
Dezembro						

Referências

[1] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente. *On the difficulty of software-based attestation of embedded devices*. ACM CCS, 2009.

[2] Trusted Computing Group. TPM Main Specification Level 2 Version 1.2, 2011. https://trustedcomputinggroup.org/tpm-main-specification/

[3] K. Eldefrawy, A. Francillon, D. Perito and G. Tsudik, *SMART: Secure and Minimal Architecture for (Establishing Dynamic) Root of Trust*, ISOC Symposium on Network and Distributed System Security (NDSS), 2012.