OS RISCOS DE SEGURANÇA INERENTES AO USO DOS MODERNOS EQUIPAMENTOS MÉDICOS INFORMATIZADOS

Claudio André da Silva Junior, UNIFAL, claudioandre.br@gmail.com

Palavras-chave: informática médica; dispositivos de suporte à vida; software malicioso.

Introdução

Os equipamentos e dispositivos médicos são uma realidade no mundo moderno (KRAMER et al., 2012). Sejam esses dispositivos implantados no paciente para monitorar e corrigir sua atividade cardíaca ou controlar sua taxa de glicose. Sejam os grandes aparelhos de tomografias ou ressonâncias, ou mesmo aqueles equipamentos encontrados em uma unidade de terapia intensiva (UTI); todos facilitam o controle e o diagnóstico das doenças.

Contudo, todos esses aparelhos, apesar de seu maior ou menor grau de especialização são, em essência, computadores, sujeitos, portanto, a erros de projeto ou de implementação e a falhas de segurança. Por consequência, susceptíveis aos problemas recorrentes dos equipamentos de informática. Todavia, as consequências de uma falha em um desses equipamentos vão muito além do dano material ou financeiro.

Isto posto, este trabalho analisará o risco e a viabilidade de se encontrar e explorar uma eventual falha em um contexto de medicina auxiliada por computador.

Justificativa

Os avanços na eletrônica, informática e telecomunicações têm ampliado o alcance e efetividade da medicina moderna. Essas máquinas, porém, são vulneráveis (KRAMER et al., 2012; ROBERTSON, 2012; ICS-CERT, 2013). Os danos resultantes do mal funcionamento de qualquer desses aparelhos podem ser o acesso ou divulgação de dados sensíveis de algum paciente, ou pior, acarretar algum dano físico. Ou seja, os efeitos de uma falha em um dispositivo médico incluem prejuízos à saúde, inclusive o óbito.

Por esta razão uma análise apurada dos desafios que este florescente campo tecnológico enfrenta é necessária, de sorte a mitigar os riscos de segurança inerentes ao seu uso, e a permitir que a evolução nos processos de monitoramento e automação do trabalho médico possam seguir adiante.

Fundamentação Teórica

Referências a falhas presentes em dispositivos médicos, apesar de recentes, não são algo novo (ROBERTSON, 2012). Entretanto, de maior interesse são os eventos relacionados a implantes autônomos tais como monitores/desfibriladores cardíacos e bombas injetoras de insulina. Infelizmente, mesmo nesse campo, o alerta do ICS-CERT (2013) destaca que há problemas: há uma porta alternativa para acesso a alguns desses dispositivos, uma senha padrão presente no código fonte do programa. Embora este seja um erro básico no projeto de segurança desses aparelhos, nota-se que o mesmo afeta aproximadamente 300 dispositivos médicos de cerca de 40 fabricantes. Desta forma, basta ao atacante descobrir uma dessas senhas coringa para conseguir acessar e controlar uma miríade de dispositivos.

Não bastasse isto, é simples comprovar com uma simples amostra empírica que a qualidade das senhas usadas pelos usuários da maioria dos sistemas informáticos não é adequada. Na realidade, mesmo os caros e complexos equipamentos médicos não são protegidos com senhas fortes (ROBERTSON, 2012). Portanto, apesar da agência reguladora americana FDA já estabelecer normas e diretrizes sobre os requisitos de segurança de tais aparelhos (KRAMER et al., 2012), ainda não se disseminou um conjunto de boas práticas e padrões a serem perseguidos pela indústria ou pelos usuários de tais aparelhos. De fato, mesmo no estabelecido mercado de produtos de rede, é possível se encontrar erros

perturbadores. O software CISCO de infraestrutura de rede e serviços empresarias possui uma brecha de segurança que permite que as senhas usadas no sistema sejam facilmente descobertas (CISCO SECURITY RESPONSE, 2013), como se verá adiante neste estudo.

Assim, mesmo que incipiente, os fatos levantados pela comunidade científica em torno da segurança da informação do aparato médico é um chamamento para que o debate seja ampliado e aprofundado.

Objetivos

Este trabalho mostrará que os equipamentos médicos são susceptíveis a ataques que buscam explorar falhas de segurança e que a realização de um ataque desse tipo é viável. Por fim, apresentará um estudo de caso que comprovará a existência de uma brecha de segurança em uma tecnologia de mercado.

Metodologia

O método empregado consiste de uma revisão da literatura, da seleção de fatos relevantes obtidos na consulta a bases de dados ligadas à segurança e no desenvolvimento de um estudo de caso que corrobore a tese em foco.

Resultados

No estudo de caso realizado neste trabalho ficou provado que a técnica de *hash Type 4* desenvolvida pela fabricante de equipamentos CISCO foi inadequadamente implementada (SILVA JUNIOR, 2013). Ou seja, a CISCO definiu que o tal mecanismo usaria *salt* e seria iterado, com uma quantidade de *rounds* de alguns milhares. Verificou-se, porém que não é este o caso. Para tal, este trabalho criou uma implementação paralela em OpenCL do citado algoritmo. No processo comprovou que as regras de alto nível definidas não foram, de fato, implementadas. Pelo contrário, o algoritmo que está no *software* e *firmware* comercializados pela CISCO são muito mais fáceis de burlar do que deveriam (se os programadores que desenvolveram os produtos tivessem seguido à risca o projeto).

Por fim, é imperativo ressaltar que o desempenho do algoritmo desenvolvido neste trabalho é da ordem de 10^5 vezes superior ao esperado do projeto original da CISCO. Ou seja, um atacante utilizando o famoso *software* de auditoria de senhas John the Ripper acoplado ao algoritmo criado consegue quebrar qualquer senha de até 10 caracteres se dispuser de recursos adequados (por exemplo, placas de vídeo de valor inferior a R$ 5.000,00). Logo, a segurança oferecida por um produto de uma das marcas líderes não é adequada, tampouco, suficiente, para resistir a tentativas de invasão.

Conclusão

A literatura e os resultados obtidos neste trabalho comprovam que equipamentos médicos são susceptíveis a ataques informáticos. O estudo de caso apresentado demonstra que erros crassos são encontrados mesmo nos produtos de grandes fabricantes. E embora a tecnologia atacada não seja empregada em dispositivos médicos autônomos implantados, um ataque bem-sucedido a um produto CISCO pode comprometer a integridade ou o sigilo de algum banco de dados médico, ou resultar em dano à infraestrutura, aliás, como já ocorreu no caso extremo em que os pacientes precisaram ser transferidos para outro hospital porque havia um vírus em um equipamento do laboratório de cateterismo (KRAMER et al., 2012).

Para finalizar, vale destacar que a contribuição deste trabalho está em demonstrar a existência de uma falha em um recurso de segurança de um produto de mercado. Este fato comprova que falhas existem em artefatos usados nos hospitais, que tais falhas podem ser exploradas e que, portanto, danos podem decorrer da exploração dessas falhas.

Referências

CISCO SECURITY RESPONSE. **Cisco IOS and Cisco IOS XE Type 4 Passwords Issue**. Março. 2013. Disponível em: <http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4/>. Acesso em 15/03/2014.

ICS-CERT. **Medical Devices Hard-Coded Passwords**. Department of Homeland Security. Junho. 2013. Disponível em: <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01/>. Acesso em 15/03/2014.

KRAMER, D. B. et al. Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. **PLoS ONE**. v. 7. n. 7. p. 1-7, julho. 2012

ROBERTSON, J. **Many Doctors Don't Secure Medical Devices From Hackers**. Bloomblerg. Dezembro. 2012. Disponível em: <http://go.bloomberg.com/tech-blog/2012-12-06-many-doctors-dont-secure-medical-devices-from-hackers-study-finds/>. Acesso em 15/03/2014.

SILVA JUNIOR, C. A. **OpenCL RAWSHA-256**. GitHub. 2013. Disponível em: <https://github.com/magnumripper/JohnTheRipper/blob/bleeding-jumbo/src/opencl/sha256_kernel.cl>. Acesso em 15/03/2014.