Posted by Comunicação NAPSoL on Tue, 05/05/2015 - 16:12

Pesquisa busca criar mecanismos para detectar antecipadamente ameaças de segurança em redes de computadores [1]

Pesquisa busca criar mecanismos para detectar antecipadamente ameaças de segurança em redes de computadores [1]

Os Sistemas de Alerta Antecipado (em inglês, Early Warning Systems) são muito utilizados para mitigar as consequências de desastres naturais. Um tsunami, por exemplo, se detectado com antecedência, pode ter um impacto consideravelmente menor no número de mortes e nas perdas materiais da região atingida.

Entretanto, tais sistemas também podem ser extremamente úteis em outras áreas. O foco da pesquisa de Rodrigo Campiolo, doutorando do Departamento de Ciência da Computação do IME-USP, é o emprego de Sistemas de Alerta Antecipado em redes de computadores.

Na qualificação de sua tese, intitulada *Detecção antecipada de ameaças à segurança usando fontes de dados não estruturados* e orientada pelo Prof. Dr. Daniel Macêdo Batista, Campiolo argumenta que ?a sofisticação de ataques, ameaças dia zero e o volume de dados em redes de computadores impõem desafios para os mecanismos tradicionais de segurança?.

Segundo o autor, mesmo quando um ataque é detectado, a cooperação limitada entre administradores de sistemas muitas vezes não evita que outros potenciais alvos sejam atacados. Justamente por isso, um bom EWS não apenas detecta ou prevê ameaças, mas propaga os alertas de forma eficiente, alcançando o maior número possível de interessados.

A pesquisa de Campiolo está voltada principalmente para a análise de fontes de dados abertos, como redes sociais, fóruns e blogs. A ideia é propor um mecanismo para monitorar e detectar antecipadamente eventos e incidentes de segurança através da correlação dos dados disponíveis nessas fontes, e uma ferramenta que possibilite a troca de informações entre colaboradores.

Uma das motivações para seu tema de doutorado é a demora que alguns desenvolvedores levam para publicar comunicados oficiais sobre a existência de falhas de segurança em seus softwares. A existência do vírus Conflicker, por exemplo, só foi confirmada pela Microsoft aproximadamente três meses após o surgimento das primeiras evidências ? um Sistema de Alerta Antecipado eficaz que coletasse informações de redes sociais e fóruns poderia ter

diminuído o número de computadores infectados.

Mão na massa

Antes mesmo de ter sua tese defendida, Campiolo já vem colocando em prática a teoria que embasa o seu doutorado. Ele é integrante de um grupo de trabalho formado por pesquisadores de três universidades ? USP, UTFPR e UFBA ? que está desenvolvendo mecanismos que viabilizem um Sistema de Alerta Antecipado capaz de emitir alertas sobre possíveis ameaças e ataques a sistemas informatizados a partir do cruzamento de dados abertos.

Todo o desenvolvimento do EWS, ainda em versão alfa, está sendo realizado com ferramentas livres (API da Apache, API do Twitter, Python e Java) e provavelmente o produto final terá seu código disponibilizado para que qualquer um possa estudá-lo, copiá-lo e modificá-lo de acordo com os seus interesses. No site [2] do grupo é possível saber mais sobre o projeto e também baixar os binários da interface do EWS para três sistemas operacionais: GNU/Linux, Windows e OS X.

Nos dias 18 e 19 de maio, o status atual do EWS, que emprega parte da pesquisa desenvolvida pelo Rodrigo Campiolo, será demonstrado no Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos em Vitória-ES.

Por André Solnik da Assessori de Comunicação do CCSL-IME

Syndicate