DARPA plans hack resistant hardware to protect military systems from cyber attacks under their System Security Integrated Through Hardware and firmware (SSITH) program

An internal report produced by the J-2 intelligence directorate stated that cyber security officials are concerned that Lenovo computers and handheld devices could introduce compromised hardware into the Defense Department supply chain, posing cyber espionage risks, said officials familiar with the report. The chairman of the House Judiciary Committee wrote to the FBI warning that secrets stored on former secretary of state Hillary Clinton's private email server may have been compromised by a Clinton aide's use of a Lenovo computer. Rep. Bob Goodlatte (R., Va.) stated in a letter to FBI Director James Comey that Heather Samuelson, former White House liaison to the State Department, used two Lenovo laptops to sort some of the thousands of classified emails from Clinton's server, as reported by Bill Gertz.

The report warned that use of Lenovo products could facilitate cyber intelligence-gathering against both classified and unclassified–but still sensitive–U.S. military networks. One official said Lenovo equipment in the past was detected "beaconing"–covertly communicating with remote users in the course of cyber intelligence-gathering.

About 27 percent of Lenovo Group Ltd. is owned by the Chinese Academy of Science, a government research institute. In April, a Chinese Academy of Sciences space imagery expert, Zhou

Zhixin, was named to a senior post in the Chinese military's new Strategic Support Force, a unit in charge of space, cyber, and electronic warfare.

A National Security Agency document made public by renegade contractor Edward Snowden revealed that China has stolen sensitive military technology through cyber attacks, including radar designs, engine schematics, and other data through a program code-named Byzantine Hades. The program caused "serious damage to DoD interests," according to a briefing slide.

"China remains one of the main threats to U.S. government and corporate information systems," Larry Wortzel, a former military intelligence official and member of the congressional U.S.-China Economic and Security Review Commission said. "One way to keep those systems safe is to ensure you are not getting system updates that may have a back door that can be opened by a Chinese intelligence service."

Electronic system security has become an increasingly critical area of concern for the DoD and the broader U.S. population. Current efforts to provide electronic security largely rely on robust software development and integration. Software security development environments, methodologies, and verification have been extensively analyzed and documented; however, current security measures remain inadequate.

Present responses to hardware vulnerability attacks typically consist of developing and deploying patches to the software firewall without addressing the underlying hardware vulnerability. As a result, while a specific attack or vulnerability instance is defeated, creative programmers can develop new methods to exploit software access to the remaining hardware vulnerability and a continuous cycle of exploitation, patching, and subsequent exploitations ensues. A new approach is necessary to break this cycle of hardware vulnerability exploitation.

The goal of the DARPA's SSITH program is to develop hardware design tools that provide security against hardware vulnerabilities that are exploited through software in DoD and commercial electronic systems. SSITH seeks to leverage current research in hardware design and software security to propel new research in the area of hardware security at the microarchitecture level. Security approaches will limit the permitted hardware to states that are assured to be secure while maintaining the performance and power required for system operation.

The strategic challenge for participants in the SSITH program will be to develop new integrated circuit (IC) architectures that lack the current software-accessible points of illicit entry, yet retain the computational functions and high-performance the ICs were designed to deliver. Another goal of the program is the development of design tools that would become widely available so that hardware-anchored security would eventually become a standard feature of ICs in both Defense Department and commercial electronic systems.

"Security for electronic systems has been left up to software until now, but the overall confidence in this approach is summed up in the sardonic description of this standard practice as 'patch and pray,'" said SSITH program manager Linton Salmon of the Agency's Microsystems Technology Office. "This race against ever more clever cyberintruders is never going to end if we keep designing our systems around gullible hardware that can be fooled in countless ways by software.

System Security Integrated Through Hardware and firmware (SSITH) program

The System Security Integrated Through Hardware and firmware (SSITH) program addresses the use of hardware security architectures to help protect systems against classes of hardware vulnerabilities, rather than focusing on single

instances of software weaknesses that exploit those vulnerabilities.

There are seven known classes of hardware vulnerabilities listed in the Common Weakness Enumeration (CWE) list 1 : permissions and privileges, buffer errors, resource management, information leakage, numeric errors, crypto errors, and code injection. Changes to the integrated circuit architecture could provide hardware protection against vulnerability instances by addressing the vulnerability classes at their source, the hardware.

Researchers have documented some 2800 software breaches that have taken advantage of one or more of these hardware vulnerabilities, all seven of which are variously present to in the integrated microcircuitry of electronic systems around the world. Remove those hardware weaknesses, Salmon said, and you would effectively close down more than 40 percent of the software doors intruders now have available to them.

DARPA scientists are interested in security approaches that will limit computer hardware to states that are secure while maintaining the system performance and power.

The security architecture may incorporate concepts like cryptography, metadata tagging, formal verification, verified state matching, anomalous state detection, secure multi-party computing, semi-homomorphic computing, and security through compartmentalization.

Security architectures will be instantiated in custom hardware to demonstrate the security of the resulting systems as well as to evaluate the impact of securitization on the performance, power, area, software compatibility, and security (PPAS) of resulting systems.

In addition to the PPAS impact, SSITH will also evaluate the scalability, flexibility, and adaptability of the security architectures developed in the program. Scalability will be

needed to apply across a broad range of applications from small, ultra-low power systems to large, high performance systems. Flexibility will be needed to ensure responsiveness of hardware security to evolving system threats. Adaptability will allow hardware systems to respond to detected attacks.

Architectures and design tools developed through this program will provide and flexible solutions applicable to DOD and commercial electronic systems, DARPA officials say.

Technical Areas

This SSITH BAA is soliciting proposals in two technical areas:

Technical Area 1 (TA-1) will develop scalable, flexible, and adaptable integrated circuit security architectures that can be easily implemented in DoD and commercial SoCs.

The key elements are to develop and demonstrate one or more security architectures that can be used to protect electronics systems from software assisted attacks, develop design tools required to implement the chosen security architectures in arbitrary circuit designs and evaluate the impact of the security architecture implementation on key circuit metrics.

Technical Area 2 (TA-2) will establish a methodology for evaluating the security provided by the architectures developed in TA-1.

The focus of TA-2 is to develop a methodology and metrics by which to measure secure electronic systems. Specifically, TA-2 teams are intended to develop quantitative metrics required to evaluate trade-offs in security, performance, power, area and other standard circuit metrics. In addition, TA-2 teams are intended to establish a framework that enables representation of hardware/firmware security properties to overall system designers.

Out of Scope Technical Areas

The SSITH BAA will not focus on attacks that are not mediated through software access to the hardware. Although other areas of security are important, SSITH will focus on hardware vulnerabilities that are exploited through software to define achievable goals in a limited, but critical, part of the overall cybersecurity enterprise.

Examples of out of scope topics are:

1. Development of physical elements of hardware security such as Physically Unclonable Functions (PUF) and Random Number Generators (RNG). Physical elements can be used as a part of a SSITH proposal, but SSITH will not fund their development.

2. Protection against hardware-only vulnerabilities such as EM side-channel attacks or insertion of hardware Trojans during design and/or fabrication.

3. Vulnerabilities that occur exclusively in the software domain, such as insecure interaction between software components or cross-site request forgeries.

References and Resources also include:

http://www.homelandsecuritynewswire.com/dr20170411-hackresistant-hardware

https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-SN-17-31%20/listing.html