June 8, 2015 6.25am BST

# US hack shows data is the new frontier in cyber security conflict

**AUTHOR**

**Bill Buchanan**

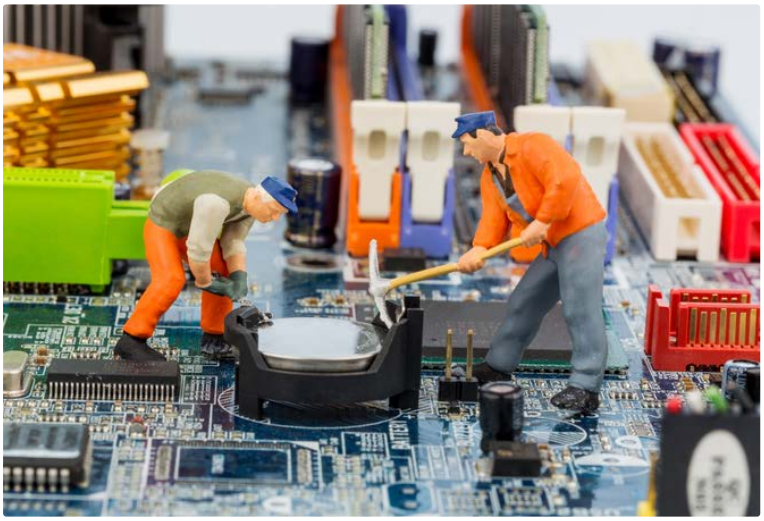
Head, Centre for Distributed Computing, Networks and Security at Edinburgh Napier University

**DISCLOSURE STATEMENT**

Bill Buchanan does not work for, consult to, own shares in or receive funding from any company or organisation that would benefit from this article, and has no relevant affiliations.

Edinburgh Napier UNIVERSITY

Provides funding as a Member of The Conversation UK.
napier.ac.uk/Pages/home.aspx



Data mining. Shutterstock

More than four million personal records of US government workers are thought to have been **hacked and stolen**, it has been. With US investigators **blaming the Chinese** government (although the Chinese deny involvement), this incident shows how data could be the new frontier for those in cyberspace with a political agenda.

In April 2015, the US Office of Personnel Management (OPM) Ð the body that provides the human resources function for the federal government and is responsible for background checks for security clearances Ð realised its records had been hacked.

Along with the direct personnel details, there are a whole range of references and contacts contained in the OPM records. The sensitive data could be used to identify people with security clearances, and could be used for the impersonation or blackmail of federal employees. Someone with security clearance could be exposed to

Festival of Education 2015: Celebrating Diversity in Bristol and Beyond Ñ Bristol

MORE EVENTS

identity fraud, where an intruder could gain access to sensitive information using the stolen identifies.

The data could also be used to hack into other government sites. For example, intruders recently **attempted to breach** the Inland Revenue ServiceÕs systems (this time it was blamed on Russia) using personal information taken from tax returns stolen during other commercial breaches.

Such attacks create a certain amount of national humiliation. The hacking of confidential data from Sony **highlighted how embarrassing** it can be for information to leak. The contents of its sensitive emails are now searchable **on Wikileaks**, and we have probably only seen the tip of the iceberg in terms of the data that was taken.

## How did the hackers beat the system?

Aware of the threat of attack, the OPM said it has Ò**undertaken an aggressive effort**Ó to improve its cybersecurity over the last year. So why, many might ask, did it take the government so long to detect the security breach?

Many large companies now use advanced intrusion detection systems (IDS) that raise alerts of possible security breaches that are then collected, logged and analysed. At the OPM, the system that detected the breach was called EINSTEIN. It was developed by a division of the Department of Homeland Security to monitor the exit points of US government by examining the packets carried around a network for possible signs of intrusion.

The growing threat of attacks has led to the use of tools that gather all the event logs from IDS agents on a network. Human analysts then have to make sense of the events coming in, in order to spot possible signs of an intrusion. To do this advanced computer systems filter down the event logs and present only the most important ones to the analysts.

Facebook 3

LinkedIn 2

0 Comments

Print

TAGS

Cyber security, Cyber ethics

ARTICLES BY THIS AUTHOR

June 1, 2015
Oracle vs Google case threatens foundations of software design

May 19, 2015
Apple and Starbucks could have avoided being hacked if theyÕd taken this simple step

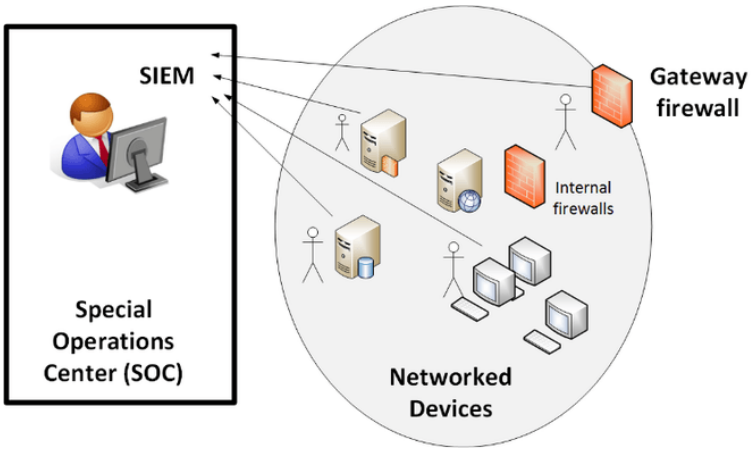
May 14, 2015
When amateurs do the job of a professional, the result is smart grids secured by dumb crypto

February 24, 2015
LenovoÕs security debacle reveals blurred boundary between adware and malware

January 22, 2015
If Obama is talking about securing the net, it should be on everyone elseÕs lips too

RELATED ARTICLES

Home Depot hack shows online card fraud still as easy as shooting fish in a barrel




Special Operations Centres (SOC) and SIEM (Security Information and Event Management)

Unfortunately some of the tell-tale signs of an intrusion could be lost. In the case of EINSTEIN, the system has to monitor the gateways devices coming from each of the partner government agencies, where it might be difficult to detect an intruder who has remote access to the inside of one the networks.

It is common for an IDS to detect where there are high rates of data loss (which large amounts of data are filtered off the network). So if this data loss is fairly slow, the IDS will often not detect it. The system must be tuned to show standard signs of intrusions so it does not trigger too many alerts and swamp its human administrators. Cyber attackers, however, often understand these standard detection methods and will use ways to slowing down the intrusion and avoid being noticed.

Many networks use a firewall to separate servers that can be accessed from untrusted networks from the protected main network infrastructure is then protected on another network. In many large networks, IDS agents exist across the whole network and listen for possible intrusions. The problem is that an intruder can often get over the firewall, and then remotely access the protected systems. Many organisations also allow employees to access their computer remotely through a secure network connection. With stolen access details, an intruder can use this remote access path in the same way.

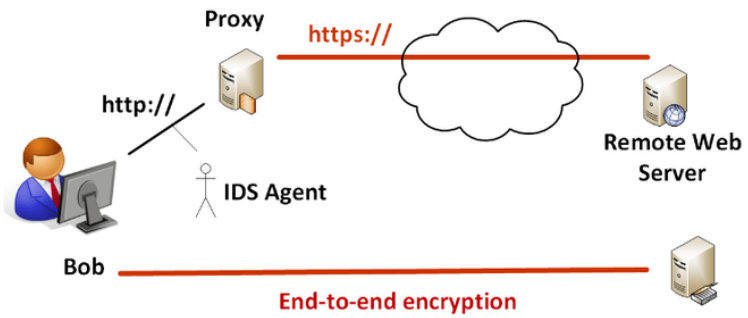
The other major weakness of many IDSs is that they cannot examine the contents of encrypted data packets, such as where users visit secured websites starting with Òhttps://Ó. To overcome this, many systems ban direct secure connections and route the data via a proxy, where they can examine the packets between the userÕs computer and the secure connection to the internet. Unfortunately, intruders can set up connections using what is known as an end-to-end encryption tunnel that bypass this provision and in which data loss

why data-breach reporting should be mandatory

JPMorgan hack signals banks and retailers can do more to keep our data safe

Hacking the secrets of Australia's Joint Strike Fighter

cannot be detected by the proxy or IDS.




Secure tunnels with proxy and end-to-end

While it has not been proven that the most recent attack was driven by a political agenda, the information once leaked from a site can then be sold on for the purposes of compromising nation states. Governments still need to understand the risks around their documents and make sure there are effective safeguards in place to restrict access to sensitive information. They often have a lot to learn from high-risk companies, such as in the **finance sector**, where there is often large-scale detection of intrusions and monitoring for data loss.

The US agencies are saying that all those affected by the hack of the OPM will be insured against any loss they might experience as a result. But data is the life blood of most organisations and probably one of its important assets, so the need for improved security increases by the day.

Republishing guidelines
Research and Expert Database
Events
Our feeds
Our charter
Our team
Our blog
Partners and funders
Contributing institutions
Contact us