Centre for Cyber Security, Audit, Forensics and Education

School of Computing & Mathematical Sciences
UNIVERSITY of GREENWICH

Visit: http://cms1.gre.ac.uk/research/csafe

July 31, 2012 issue #2

This issue:

CSAFE News

Ryan Heartfield and George Loukas have produced a security paper from the CSAFE based on social engineering techniques that can be used to exploit Cloud Storage services:

"On the Feasibility of Semantic Attacks in the Cloud"

For those interested in reading this paper please email:

hr811.secure@gmail.com

CSAFE Short Courses

- Computer Forensic Evidence and the Law (Legal Aspects)
- Computer Forensics for Lawyers
- EnCase Computer Forensics 1 and 2 Certification (EnCE©)
- Introduction to Computer Forensics
- Introduction to Computer Forensics
- Penetration Testing and Vulnerability Assessment

Does the Evolution and advantages of mobile phone technology compromise our private and sensitive information?

By Jane Teh, CSAFE contributing writer

It is hard to imagine that the internet has only been around in its current form since the mid-1990s, since then it has touched almost every facet of our lives.

Even the smallest of companies now have a global reach, we can video conference and message each other on the move, house hold appliances can update themselves, we can shop and buy from a global market place and even organise protest movements and plot the downfall of governments!

Coincidentally the first massed produced user friendly mobile phones hit the market around the same time, mid 1990s. They were quite clunky and were mainly used for text messaging and phone calls. The first consumer internet enabled phones were released in 1996, from which time mobile companies have been merging computers, phones, cameras, GPS systems, media centres into a single device.

Never has so much personal, sensitive and confidential information been carried around or transferred over invisible wireless networks and with the development of mass remote storage, anything we save to any device can potentially be accessed from our mobile phones.

How secure is the data we store and access from our phones, and what measures can we take to protect it?

There have been some well publicised phone hacking scandals involving the British press, who accessed voice mails through default pin numbers that users did not change when setting up their voicemail. Other documented cases involve methods such as spoofing & changing a phone caller's ID number to that of a hacking victim, when a call to the number is made, the network assumes it is the legitimate caller & routes to voicemail, allowing the caller to listen to messages & change voicemail settings. Mobile phone companies have implemented more robust security measures but by simply setting a voicemail pin number; a user can make it much more difficult for unauthorised users to access their voicemail.

Password Protection

All phones can be set to auto-lock themselves after a pre-defined time of inactivity; users can set a login password which must be correctly entered to start using the phone again. Some phones can be set to permanently locked, if too many incorrect attempts are made to unlock them, requiring a call to the phones network operator to reset the SIM password.

Wireless data connection

Hackers can gain access to mobile phones through: wireless connections or Bluetooth; users should disable wireless connections when they are not being used to prevent data theft.

AutoFill

Web browsers often have an option to remember passwords, usernames and commonly used fields such as address details. AutoFill should be disabled to prevent unauthorised access to personal data.

Cookies and Cache

Cookies and cache store elements of visited web pages to provide a faster browsing experience, some of this stored information can relate to shopping, browsing habits, cookies automatically send information to websites, which then send targeted advertising relating to past shopping/browsing habits. This information can also be accessed by other users, either remotely or if they have physical access to the device. Users can turn off cookies and should regularly empty their internet cache.

Encryption

There are third party applications which can encrypt some data types and even remotely wipe a phones memory if it is stolen.

Malware

Malware can be added to applications (apps) or message attachments, to collect personal information such as credit card/password details and email them to a remote user, users can install anti malware software and avoid installing applications from unofficial sources.

GPS Tracking

A number of phone manufacturers allow the setting up of tracking via GPS displaying the location of a stolen phone in real time; a user can send a message, wipe the phone or alert the authorities to the phone's location.

Forensic detection has been used by Law enforcement for over 100 years to identify victims, investigate crime scenes, and prove guilt/innocence of the accused.

It was widely recognised that mobile phones were being used for criminal activity but it wasn't until the development of smart phones around the early 2000s that mobile forensics branched out from general computer forensics to form its own specialised branch of forensic investigation.

This was needed as mobile phones use unique interfaces, file systems, and language for each device type, at first methods were quite clumsy and the phones were examined by accessing and examining the device itself. Since then software has been developed to extract a phone's memory where it can be analysed by a forensic examiner using specialist software.

Originally forensic officers would examine messages, phone logs and address book information but with the development of smart phones and the sophisticated software used, forensic tools and techniques have been adapted to include investigation of: GPS and location data, images, sound files, videos, internet cache and logs, hidden messages/information, retrieving deleted information, examination of header files showing when applications were accessed and email logs.

SOFTWARE

Monthly Pick

8 iOS Security Apps for Jailbroken Devices!! Must read...

It is still a hot discussion whether jailbreaking your iDevice actually exposes your phone to hackers or as some put , opening the front door & inviting them to invade the privacy of your phones content or if it actually provides users with more security options? It is debatable, but one thing is for certain the battle between apple and the Jailbreak community seems likely to continue as new versions of the iPhone are released.

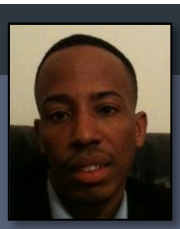
Click the icon below to find out more.

Q: What is jailbreaking and what does it do?

A: Jailbreak essentially means you release you're iDevice (iPhone, iPad, iTouch) from constraints orlimitations imposed by your vendor (Apple, Vodafone), e.g. modifying the existing vendor file system on the iDevice, so you have the freedom to do whatever you want on your phone. Jailbreaking your phone has been declared legal but arguments persist from manufacturers and jailbreaking can affect your device warranty.

Jailbreaking an iPhone allows users to install pirated software and access apps not available in the appstore, for example Apple does not allow developers to access certain system functions. The Jailbreak community claim that jailbreaking some system structure of the phone.

Interview with a Security Expert – Ron Nurse



Q: Hi Ron, please tell us a little about your information security profile experience in the field of information security

A: I've worked in IT for over 15 years and for 5 years have been specialising in information security. I've had the fortunate opportunity to work with very large companies and see different environments, work with different people, technologies and see processes put in place and how such changes have benefited the security posture of various organisations.

I currently work as a consultant for a well-known communications company, and the majority of the work I'm involved in is based heavily on compliance with industry and HMG standards.

Q: As an experienced security professional, what advice would you give people interested in starting a career in information security?

A: Know the basics – network security, operating systems, security vendors and solutions. Understand the field you want to get into – is it Risk Management, Incident Response, Governance, BCP or DR.

Consider what experience and qualifications you need to have, and go get it. Consult forums, view webinars, talk to people in the field.

Read, read, read and then read some more.

Q. With various high profile attacks such as Stuxnet, Duqu and Hacktivism dominating the information security domain in recent years- it seems the good guys are continuously playing catch-up what are your thoughts on this?

Unfortunately this is true. However for example, you never know if an intruder is coming to your house for your personal belongings, but you can prepare for it.

You identify weakness or gaps and fix them whether it is installing an alarm, adding more bolts to doors etc. Similarly with information security adopting the defence in depth model is particularly important. By thoroughly analysing the infrastructure the correct controls can be put in place whether it is:

Implementing tighter controls around the perimeter by restricting network traffic, varying firewall vendors…
Restricting the movement and accessing of data via file level permissions, data loss prevention…
Better code writing – adhering to standards, OWASP, MS SDL…
Provide security awareness training for colleagues and affiliated business groups and third parties.

Q. What are your expectations for the information security field for the rest of 2012?

I see cloud computing and BYOD as being interesting arenas for info sec. Issues such as how companies deal with PID (Personal Identifiable Data) and of course malware continuing to raise its ugly head.

Last year was the year of hacktivism, will we see as much, I don't know.

About the Author

This week's author:

Jane Teh

Jane Teh is a current postgraduate student pursuing her MSc in Computer Forensics & System Security at the University of Greenwich.

Her Master's project is based on developing a prototype that provides central investigative functions that enhances mobile phone forensic investigation.

Email: Janehlt84@hotmail.com

CSAFE Collaborations

Turkish fraudsters just having fun, luck for us... this time!

By First Cyber Security

So Turkish fraudsters have poisoned a master DNS lookup and diverted traffic to another domain.

This time it would appear other than some slight embarrassment no harm was done but the result could have been very different, and Vodafone, Betfair, UPS, The Telegraph and other major organisations could have been looking at major reputational damage and huge loss of confidence in their online presence. Not to mention loss of revenue and increased costs directly due to such attacks.

We often hear from consumers that they trust websites of major organisations as they know what they look like. However just going to identical looking fake sites if redirected by a poisoned DNS could mean consumers lose data. So no matter how big you are you are not immune from such attacks, in fact as in this case the bigger the better.

FCS previously warned about the issue of DNS poisoning almost 3 years ago, it hasn't gone away. It can be incredibly difficult to 'know' whether you are on an authentic site or a fake one, just because it looks right doesn't mean it is. Phishing attacks depend on 'look-a-like' sites and phishing is still on the increase.

So what's the answer? Perhaps to use a technology that not only warns the consumer but also alerts the website owner in real-time of the presence of an attack, and automatically redirects consumers to a safe haven.

The solution is out there. But companies seem to have to get impregnated before they take precautions. In other life choices it's the other way around.

In fact if this available British patent pending technology had been deployed this wouldn't have even been a news story. When did you last see a headline "Bank foils thieves by locking front door"? The analogy is real, we have the technology.

First Cyber Security are manufacturers of cyber protection.

See www.firstcybersecurity.com to find out more about FCS services, security solutions and media coverage.

Fig.1 Typical DNS poisoning scenario