Social Engineering Award 2015 – Cloud Attack!

predict
prioritise
prevent
TRESPASS

Report of the Jury

Challenge Description

The challenge “Security Nightmare 2015 – Cloud Attack!” introduced a concrete scenario involving a company called International Traders Ltd. (ITL) that stores an important *fileX* containing details of its clients and business transactions in the self-administered cloud on company’s premises. The scenario introduced some technical details on the company’s network and cloud architecture, as well as seven employees of the company, from high and middle management to the technical and cleaning personnel, with different access rights to the ITL’s physical and virtual infrastructure. The challenge consisted in providing an attack scenario that exploits human factors in a novel way to get access to *fileX*.

Evaluation Procedure

We received five submissions. Firstly, all members of the jury independently evaluated all submissions on the scale from 1 to 5 (lowest to best) according to the following main criteria:

- Creativity
- Feasibility
- Deceivability (defined as the ability of the suggested attack steps to deceive the target)
- Quality of explanation
- Quality of suggested countermeasures

The following secondary criteria were used to break any possible ties:

- Quality of research proposal / experimental design
- Cost-benefit trade-off of the attack

Secondly, the submissions were ordered according to their scores and discussed in several online meetings in order to resolve some details that appeared unclear or ambiguous to the jury. The final order of the submissions remained unchanged at the end of this process.

The Threat Landscape

The jury was greatly impressed by the creative and multifaceted attack scenarios presented by the participants. We firstly briefly describe the presented ideas in the order of submission, and then discuss the three entries that scored the highest in more detail.

Submission 1 presents a clever email- and telephone-based scam where the ITL's fraud investigator gets a faked request from the ITL's CEO to forward *fileX* to a law firm in order to comply with a (non-existent) court request. Submission 2 introduces a very disturbing threat of the corrupt cloud provider and presents imaginative ideas on how to coerce or persuade ITL to use the corresponding cloud service instead of its own cloud by combining a Denial of Service (DoS) attack on the cloud with a timely and low-priced business proposal. Submission 3 develops a Hollywood-like scenario that involves several phone calls to the CEO from various non-existing persons, a DoS attack on the ITL's cloud and on the system administrator, that cumulatively result in the CEO divulging his access credentials to a sympathetic and "helpful" stranger. Submission 4 describes an elaborate multi-step scenario involving a lot of people and technical means that results in persuading the system administrator to shut down a part of the cloud architecture as to transfer *fileX* to a less secure virtual machine. Finally, Submission 5 imaginatively combines some well-known social engineering techniques such as spear phishing to get access credentials, and impersonation of the cleaning personnel to get the physical access to ITL's premises.

The Third Place: Peter Carmichael

Peter Carmichael (Newcastle University, UK) has developed a very ingenious attack scenario. The aim of the attack is to pressure the actors at ITL so much that they will rearrange the structure of the system which ensures that all VM's (Virtual Machines) are transferred to one server (Server 2). Then, the attacker will physically access the laptop of Finn, the financial manager who has the access to Server 2, but not to Server 1, where *fileX* is supposed to reside under the usual circumstances. That will make it possible to access the desired information - *fileX*, for example by means of privileges elevation. Peter's attack consists of six steps: 1) Get *Cleo's - the cleaner* - working hours, through social engineering. 2) Get *Grey's - external to ITL* - email address, by arguing that a friend is interested in is job and would like to ask him for advice. 3) Get *Finn's - the financial manager* - email address by impersonating Grey. 4) Spear-phish *Finn:* craft an email to Finn spoofing Grey; the aim is to get Finn's credentials and to install a Trojan on Server 2. The purpose of the Trojan is to generate "suspicious" encrypted traffic originating from Server 2. 5) Convince ITL to copy *fileX* from Server 2 to Server 1, to which Finn has got access. To this end, the attacker impersonates the official authorities and claims that suspicious activities originating from Server 2 at ITL were found during a cybercrime investigation. 6) Acquire *fileX* by physically entering the office of ITL and accessing *File X* on Server 1 through Finn's account.

Peter's scenario is audacious and original. Several times there is personal contact between the attackers and someone from (or related to) ITL. Also, entering the office can be a risky endeavour. This makes Peter's attack particularly dangerous for the attacker. Also, at each step the danger is that someone will not behave as expected and the attack could end right there. Peter discusses the pros and cons of each step, showing insight in psychology as well as in IT security. We found the scenario dangerous, but also convincing and adequate.

The Runner-up: Uwe Schmalfeld

The attack scenario presented by Uwe Schmalfeld (City of Nuremberg's IT department, Germany) tells a compelling tale of social interactions, worthy of a Hollywood thriller. The main idea is to exploit the trust relationship between the CEO and the system administrator.

The attacker first finds out how the communication between the CEO and the sysadmin is usually conducted in case of emergencies. This is done by pretending to the sysadmin to conduct an "anonymous" telephone survey on work-life-balance of the IT personnel, asking among other things the crucial question about the contact possibilities in emergency situations. The attacker subsequently creates an emergency situation for the CEO during bank holidays (for example, Christmas) by simulating a call from a client company about a just discovered case of financial fraud where one of ITL's employees seems to be involved, prompting the CEO to check some information in *fileX*.

At the same time, the access to the ITL's cloud is disrupted by a technical DoS attack. Also, the CEO's access to the system administrator is disrupted by running a DoS attack on the emergency communication channel, in this case the sysadmin's mobile phone number, by posting it at several porn, real estate and classifieds websites as offering very good deals. Thus, the CEO does not have any possibilities to access *fileX* in order to get a better insight in the situation.

Posing as a friend of the sysadmin, the attacker contacts the CEO with the news that the sysadmin is in the hospital and should not be disturbed, vaguely hinting at a suicide attempt. The "friend" pretends to be a sysadmin as well, sympathizing with the CEO about the issues arising out of the unavailability of the ITL's sysadmin. This conversation results in the CEO asking advice on how to get access to *fileX*. "Helping" the CEO, the attacker executes a man-in-the-middle attack between the CEO's computer and the ITL's network, thus getting the access credentials to *fileX*.

The author provides sound psychological motivation for all attack steps. For example, one of the fundamental social engineering principles is *distraction* (the sysadmin answers a survey that is seemingly disconnected from any possible attacks, the CEO is simultaneously hit by the news of the sysadmin's illness and by a fraud emergency), another one is *transfer of trust* (sysadmin's "friend" is trusted because the sysadmin is trusted). Also targeting the CEO as a likely person to disobey security policies is a well-known phenomenon. Overall, this attack scenario has a reasonable probability of success. At the same time it requires very astute social engineering skills and some good luck for the attacker.

The Winner: David Kelm

The scenario developed by David Kelm (IT-Seal, Darmstadt, Germany) starts with clarifying assumptions about the environment, namely that access to *fileX* on virtual machine VM1 is only accessible from the laptop in the internal room and requires access credentials from either the CEO, the sysadmin or the owner of the file, Ethan. Correspondingly, his attack consists of two parts: getting login credentials for the laptop as well as getting physical access to the laptop.

David lists several alternatives for gathering login credentials, focusing on the CEO as he might be the most customer-oriented and possibly less technically savvy. The different alternatives try to learn more about the CEO, for example by inviting him to a fake conference to get further information, a CV, possibly to allow access to his social media accounts. Spoofing ITL's web login together with a spear-phishing attack might give login credential to ITL's internal webpage. Lastly, posing as a competitively priced surveillance company could possibly trick ITL to install cameras in the internal space allowing 'shoulder surfing'. Multiple of these alternatives could be tried, as they do not appear to be 'attacks'.

For physical access, David proposes a man-in-the-middle attack between the CEO and the cleaning company, cleverly allowing to bring somebody external to the internal rooms of ITL, thereby giving access to the laptop when no-one else from ITL is around.

In combination, these steps could give access to the goal to access *fileX*. As this scenario focuses on social engineering techniques, less on technical attacks, not so much technical knowledge is required and this kind of attack, though not easy, is hard to prevent.

David's proposal also offers a comprehensive combination of technical and non-technical means for countermeasures, such as using stronger authentication methods (2-factor), logging and video surveillance (by a trusted partner), systematic phone call verification, better background checking of the personnel, education and awareness training, but also physical security measures like guards outside office hours.

Conclusion

The participants provided many creative and dangerous attack ideas. Apart from the well-known social engineering principles such as authority, scarcity and liking, the authors extensively use DoS as a means of creating an emergency situation while disrupting the business communications flow, which leads the actors into non-rational decision making. This emphasizes the importance of *availability* as security goal. We encourage all participants and all readers of this document to further deepen the insight of the IT security community into the social engineering threats by developing creative and practical suggestions for the scientifically sound and ethical feasibility tests of the suggested attack ideas, and by designing the corresponding countermeasures.

Dr. rer. nat. Zinaida Benenson
University of Erlangen-Nuremberg: leader, Human Factors in Security and Privacy Group
Prof. Dr. Thomas Gross
University of Newcastle upon Tyne: director, Centre for Cybercrime and Computer Security
Prof. Dr. Marianne Junger
University of Twente: chair, Cyber Security and Business
Drs. ing. Roeland van Zeijst
INTERPOL Singapore: digital crime officer; Dutch National Police: senior strategy expert