

## Analyzing a Computer Crime

Norwich University MSIA Program  
Week 2 Essay

Perry Carpenter

The computer crime that I've chosen to analyze for this week's essay is the Paris Hilton T-Mobile cell phone hack. I chose this incident because it illustrates several issues, technical and human, related to Information Assurance failures. This incident demonstrates many of the weaknesses/flaws inherent in customer facing services.

### Background:

The Paris Hilton T-Mobile cell phone hack became big news in early 2005.<sup>1</sup> The incident involves the compromise of hotel heiress Paris Hilton's<sup>2</sup> account services associated with her T-Mobile cell phone. The services offered as part of her *Sidekick II* phone included email, notes, contact lists, and an online photo album which stored photos taken via the phone's integrated camera.<sup>3</sup> After compromising the services associated with Ms. Hilton's account, the perpetrator(s) posted copies of the content to several publicly available web-sites.

The information posted on the internet included the personal contact information of over 500 of Hilton's acquaintances, including several high-profile celebrities. In addition to the celebrity contact information, some very personal photos and diary entries became widely distributed. The case, investigated by the US Secret Service<sup>4</sup>, Department of Justice, and other agencies, resulted in the capture and conviction of an unnamed teen.<sup>5</sup>

### Analysis:

In analyzing this case, my intention is to outline the events supported by the majority of reports available. By utilizing Howard and Meunier's "Common Language" and taxonomy<sup>6</sup>, I intend to present a clear outline of events and associated security implications.

---

<sup>1</sup> Slowplay.com, the Drudge Report, and other "gossip" outlets kept a running story as events unfolded. See: <http://www.slowplay.com/archives/2005/02/20/paris-hilton-hack-update.php>.

<sup>2</sup> Paris Hilton is, as her last name implies, the heir to the Hilton Hotel franchise. See: [http://en.wikipedia.org/wiki/Paris\\_hilton](http://en.wikipedia.org/wiki/Paris_hilton).

<sup>3</sup> The Sidekick II phone is a T-Mobile exclusive. Product features and specifications are available for review at <http://www.t-mobile.com/shop/Phones/Detail.aspx?device=154e9bca-a74c-4299-99eb-48a1159c922b>.

<sup>4</sup> The Sydney Morning Herald, *Secret Service probes Hilton hack*, February 22, 2005. <http://www.smh.com.au/news/People/Secret-Service-probes-Hilton-hack/2005/02/22/1108834754446.html>. Accessed June 23, 2006.

<sup>5</sup> BBC News. *Paris Hilton Hacker sent to jail*. September 15, 2005. <http://news.bbc.co.uk/1/hi/technology/4249780.stm>. Accessed June 23, 2006.

<sup>6</sup> See chapter 3 of *The Computer Security Handbook 4<sup>th</sup> Edition.*, John Wiley & Sons, 2002.

The incident commonly thought of as the Paris Hilton T-Mobile hack may actually consist of at least 2 separate hacks, the earliest occurring in 2003, and at least one instance of social-engineering.<sup>7</sup> Given that the facts are spread between several sources, a correlated outline of events will serve to add clarity.

*October 2003:* T-Mobile discovers an intrusion on their network in which 400 customer records were accessed. The records of a Secret Service agent are counted among those compromised.<sup>8</sup> Hilton's information is also believed to have been accessed during this time.<sup>9</sup>

*February 14, 2005:* Nicolas Jacobsen pleads guilty to the October 2003 T-Mobile incident.<sup>10</sup>

*February 17, 2005:* Jack Koziol, an instructor for the InfoSec Institute posts technical details to his blog which were taken from a publicly available affidavit related to the Jacobsen case. These details were used to discuss the techniques (exploitation of an SQL injection vulnerability) possibly used by Jacobsen in the 2003 hack. The instructor posits that these vulnerabilities still exist and could be exploited. Koziol specifically mentions Hilton's account as an example target.<sup>11</sup>

*Early morning, February 19, 2005:* "Koziol received an e-mail from a reader complimenting him on his blog. The e-mail contained an exploit for a T-Mobile Web site hole that allowed anyone to gain access to a T-Mobile account from the T-mobile.com Web site, as long as they knew the account holder's T-Mobile phone number. In the e-mail message, the exploit was attributed to a hacking group called 'DFNCTSC Team.'<sup>12</sup> DFNCTSC is an acronym for the "Defonic Team Screen Name Club."<sup>13</sup> The sender identifies himself as not yet being of "legal age" and therefore able to attempt the attack without fear of jail.<sup>14</sup> It is reported that the

---

<sup>7</sup> There is actually so much information around this case and the T-Mobile security flaws that it is truly impossible to narrow the field down to one individual. There appear to be several flaws, and several individuals who have taken advantage of those flaws.

<sup>8</sup> PCWorld.com. January 14, 2005. *Secret Service Data Compromised in T-Mobile Hack.*

<http://www.pcworld.com/news/article/0,aid,119318,00.asp>. Accessed June 23, 2006.

<sup>9</sup> PCWorld.com. March 1, 2005 *Paris Hilton: Victim of T-Mobile's Web Flaws?*

<http://www.pcworld.com/news/article/0,aid,119851,00.asp>. Accessed June 23, 2006.

<sup>10</sup> Ibid.

<sup>11</sup> Ibid.

<sup>12</sup> Koziol reports that the hacker's email outlined a design flaw in T-Mobile's web-site that did not even rely on SQL injection. Instead "[a] flaw in the design of the reset feature allows Internet users who know the URL of the password reset page to bypass a user authentication page and change an account's password without having to provide information that proves they are the account's owner."

<sup>13</sup> WashingtonPost.com. September 13, 2005. *Teen Pleads Guilty to Hacking Paris Hilton's Phone.* <http://www.washingtonpost.com/wp-dyn/content/article/2005/09/13/AR2005091301423.html>. Accessed June 23, 2006.

<sup>14</sup> PCWorld.com. March 1, 2005 *Paris Hilton: Victim of T-Mobile's Web Flaws?* <http://www.pcworld.com/news/article/0,aid,119851,00.asp>. Accessed June 23, 2006.

sender may have already been exploiting this vulnerability in T-Mobile's web-site.<sup>15</sup>

*Afternoon, February 19, 2005:* A teen member of the DFNCTSC Team carries out a social engineering attack by telephoning a T-Mobile store and "posing as a supervisor from T-Mobile inquiring about reports of slowness on the company's internal networks."<sup>16</sup> The social engineer directed the victim to a fraudulent T-Mobile customer service web-site where the victim was prompted to enter his T-Mobile employee credentials. These credentials were then collected by the perpetrator, used to access internal T-Mobile systems, and harvest sensitive customer information – including Ms. Hilton's personal phone number and account data.<sup>17</sup>

After her phone number was known to the group, the attackers could then use a design flaw in T-Mobile's web-site to reset the password on Ms. Hilton's account, thereby allowing the group access to her online data-store which included email, contacts, and photos.<sup>18</sup>

*Early morning, February 20, 2005:* Hilton's address book and other materials associated with her T-Mobile account are posted to the internet. "Posts of the information were accompanied by a message that claimed credit for the hack for DFNCTSC."<sup>19</sup>

*September 8, 2005:* An unnamed juvenile pleads guilty for the Paris Hilton T-Mobile incident. The T-Mobile case was but one in a series of crimes for which the youth was charged. Other notable crimes for which he was indicted included the attack on LexisNexis which exposed approximately 310,000 customer records<sup>20</sup>, attacks on America Online,

---

<sup>15</sup> In the WashingtonPost.com report, *Teen Pleads Guilty to Hacking Paris Hilton's Phone*, the hacker is said to have been exploiting the design error since January of 2005, and only turned his sights to Ms. Hilton's account on Feb 19. See: <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711.html>. It should be noted that other reports suggest that Ms. Hilton's account had already been compromised in January of 2005 (see MSNBC Gossip: January 17, 2005. *Hacker reads Paris Hilton's e-mail*. <http://msnbc.msn.com/id/6836110>).

<sup>16</sup> WashingtonPost.com. May 19, 2005. *Paris Hilton Hack Started With Old-Fashioned Con*. <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711.html>. Accessed June 23, 2006.

<sup>17</sup> Ibid.

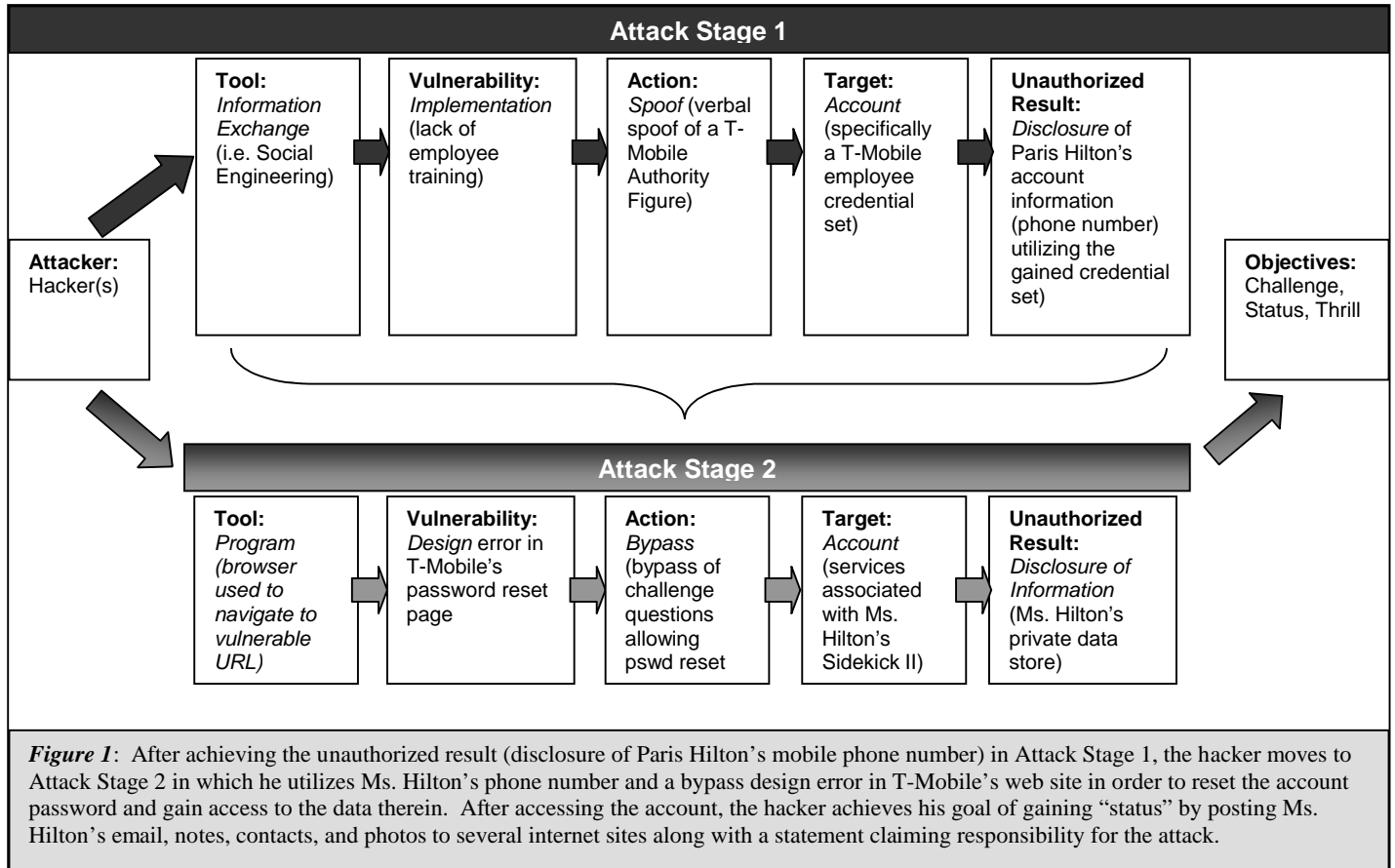
<sup>18</sup> WashingtonPost.com. September 13, 2005. *Teen Pleads Guilty to Hacking Paris Hilton's Phone*. <http://www.washingtonpost.com/wp-dyn/content/article/2005/09/13/AR2005091301423.html>. Accessed June 23, 2006.

<sup>19</sup> PCWorld.com. March 1, 2005 *Paris Hilton: Victim of T-Mobile's Web Flaws?* <http://www.pcworld.com/news/article/0,aid,119851,00.asp>. Accessed June 23, 2006.

<sup>20</sup> LexisNexis released data related to this breach in two waves. See *Hackers Hit Lexis Nexis Database: Personal Data Of As Many As 32,000 People May Have Been Stolen*. CBS News. March 10, 2005. <http://www.cbsnews.com/stories/2005/03/10/tech/main679237.shtml> and *LexisNexis acknowledges more ID theft: Personal info on 310,000 people possibly stolen, 10 times more than what was disclosed last*

bomb threats against schools in Massachusetts and Florida, as well as attacks on other telecommunications providers.<sup>21</sup>

Figure 1 is a visual representation of the attack events leading to the posting of Ms. Hilton's data.



**Conclusion:**

There are several factors leading the situation in which Ms. Hilton and T-Mobile find themselves. In this case, the two factors that stand at the forefront are 1) inadequate training of frontline employees, and 2) failure to secure the T-Mobile customer web-site.<sup>22</sup> A common theme in security failures of this magnitude is "the human factor." Whereas computers will only do what they are designed to do (albeit sometimes the design is flawed or can be taken advantage of), humans can be manipulated in myriad ways (such as implied authority, tone of voice,

month. CNN Money. June 2, 2005.

<http://money.cnn.com/2005/04/12/technology/personaltech/lexis/?cnn=yes>. Accessed June 23, 2006.

<sup>21</sup> PCWorld.com. September 15, 2005. *Paris Hilton Hacker Sentenced: Teen gets 11 months' detention for charming, hacking data out of T-Mobile.* <http://www.pcworld.com/news/article/0,aid,122559,00.asp>. Accessed June 23, 2006.

<sup>22</sup> A further factor for consideration is that Ms. Hilton may have exercised a lack of sound judgment by storing such volatile data in the 1<sup>st</sup> place; but that is beyond the scope of this paper.

gender differences, intimidation, and so on). The infamous hacker Kevin Mitnick accomplished most of his goals by manipulating people rather than technology. Company personnel must be trained to detect and resist social engineering techniques.

The second failure, not resolving security issues with the T-Mobile.com web-site, is simply inexcusable. T-Mobile had just lived through the investigation and prosecution of a hacker who had broken into their customer database by exploiting SQL injection vulnerabilities in their web-site in 2003. For the same, or similar, vulnerabilities to exist in 2005 demonstrates a lack of due diligence.<sup>23</sup>

With over 30 individual state breach notification laws on the books and the specter of Federal legislation looming, privacy and the protection of personal information is at the forefront of the American mind. It is our job, as Information Assurance professionals, to be proactive and ensure that failures, like those noted in the T-Mobile case, become a thing of the past.

---

<sup>23</sup> Other articles mention successful attacks on Ms. Hilton's account by simply utilizing the "forgot password" function of the site without any technical exploit. Hilton's "challenge question" is said to have been "What is your favorite pet's name?" Questions like this are known to be weak, especially for a celebrity for whom much can be learned via a simple Google search. See the O'Reilly Network article, *How Paris Got Hacked?* February 22, 2005. <http://www.macdevcenter.com/pub/a/mac/2005/01/01/paris.html>