In recent weeks, I’ve been looking at intrusion detection systems. Today, I’d like to draw on lessons from a disturbing theft of a celebrated piece of sculpture.

At about 0400 on Sunday the 11\textsuperscript{th} of May 2003, a thief climbed up some temporary scaffolding on the Vienna Art History Museum, entered the Museum through a second-story window, broke the unprotected glass display case and stole the famous gold and enamel salt cellar by Renaissance genius Benvenuto Cellini. This unique work of art is valued \textit{pro forma} at about US$65M (although it cannot possibly be sold on the open market because all dealers will know it has been stolen).

Now for the interesting parts from a network security standpoint. Ian Traynor, reporting in \textit{The Guardian}, wrote, “Entry to escape … can have taken no more than 54 seconds, according to a police reconstruction. Halfway through that brief period the museum's alarm system rang. The guard switched it off – before it could have alerted the police – assuming that it was yet another false alarm of the type that occurs in the museum once a week on average. It was left to a cleaning lady to discover the theft more than four hours after the event.”

False alarms can occur for several reasons:
* A sensor has been set to excessive sensitivity; e.g., a window vibration sensor is responding to wind gusts by reporting glass breakage.
* A fault in the control system is misinterpreting signals; e.g., a normal voltage or a normal pattern of system activity is erroneously configured as a trigger for an alarm.
* Someone or something is generating abnormal inputs but not completing the attack; e.g., a criminal hacker is deliberately sending patterns of packets associated with attacks (attack \textit{prodromes}) but not carrying out the actual attack.

Inappropriate responses to false alarm are a serious problem in all security systems. For example, I have personally seen people milling about discussing whether to respond to fire alarms. “Do you think it’s a false alarm?” they ask. Personally, I don’t care if it’s a false alarm or not: deciding that can come after the building is evacuated. The possible benefits from not responding to a false fire alarm are far outweighed by the possible losses if there really is a fire. I remember one incident where several hundred security experts were meeting in a hotel when the fire alarm went off; without a word, every single one of us collected his or her laptop computer, briefcase or purse and immediately filed outside without rushing. The hotel staff were astounded: they usually have to cajole their patrons to pay attention to the alarms and sometimes have to argue with people to leave their rooms.

Many untrained people respond to repeated false alarms by discounting all subsequent alarms (the “cry wolf” syndrome). A better response is to determine why the false alarms are occurring and to fix the problems. Similarly, some municipal police forces have taken to putting people or businesses on a blacklist when their burglar alarms produce more than a threshold number of false alarms. Burglars have exploited this absurd strategy by deliberately causing alarms (e.g., by rattling windows) until their targets are blacklisted, after which they can pillage at will. A
better response from police forces is to fine people for excessive false alarms. The penalties pressure people into fixing faulty alarm systems; those who will not or cannot do so have the option of withdrawing from coverage.

Another observation from the _Guardian_ story is that the museum director has been “shifting blame for the fiasco on to the security guards, three of whom were suspended from their jobs.” Although it is possible that the guards flagrantly disobeyed instructions, I am skeptical of that scenario. The story mentions that false alarms were a regular occurrence; in that case, I put responsibility for this fiasco squarely on the shoulders of management. No manager should tolerate repeated false alarms without escalating the problem with staff and vendors to fix the problem; in any such situation, all personnel should know that they are to _increase_ their responsiveness to all alarms, not make unfounded judgements about whether a particular incident is a false alarm. Incidentally, it is also possible that the guards (or, for that matter, the management) were colluding with the thief, but that’s pure speculation for the sake of completeness in this analysis.

I hope the applicability of these notes to network intrusion detection systems is clear. False alarms are a serious challenge to security; they are opportunities for exploitation by attackers. Instruct your staff to treat all alarms as if they are real; increase vigilance and responsiveness if false alarms have become common. Find out why false alarms are occurring, especially if they are frequent or increasing in frequency; fix the underlying problem.

* * *

For further reading:


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.
