

The IT Security Model – is history repeating itself?

Peter. D. Groom, *Member, IEEE*

Abstract—This paper considers the history of medieval castles and compares it to the evolution to-date of the IT Security Model. As a result of this comparison, various predictions can be made about the possible future of the IT Security Model.

I. INTRODUCTION

The first castles in medieval Europe appeared around the 9th century, as a result of Viking and Magyar raids. Nobles built castles to control and defend their land and assets. Initially these structures used natural defenses such as rivers or hills but soon, earthworks such as mounds, banks and ditches were added for greater defense [1].

In comparison, the first IT Security Model appeared in the early 1970s [2] when academic institutions and forward thinking corporations recognized the need to control and defend their information assets. These security measures started out as simple defenses, such as different passwords per user, and perhaps the odd access-list on a router. Soon, however, more advanced precautions were being implemented such as layered security, DMZs (De-Militarised Zones) and hardened hosts on the network.

II. COMPARISON OF A CASTLE WITH AN IT SECURITY MODEL

Figure 1(a) shows the typical components of a medieval castle, labeling the main functional areas, while Figure 1(b) shows the same areas but labeled from an IT Security Model standpoint.

In the same way as IT Security Models can be very expensive so the construction and maintenance of a medieval castle could cost a fortune. Furthermore, there are also similarities between medieval castles and IT Security Models when it comes to compromising them. For example, one method is to ‘lay siege’ to the castle by preventing all goods, people, food or water into or out of the castle, in much the same way as a ‘Denial of Service’ attack is carried out. Another method is to use ‘undermining’, whereby a tunnel is dug under a tower, propped up with wood which is then set alight, thus bringing down the tower. This is similar in nature to hacking. Other methods of compromising an IT Security model such as Trojans, Viruses and HTTP Tunneling have obvious counterparts in the

medieval castle environment

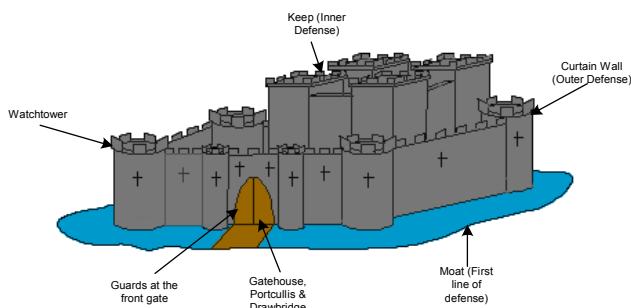


Figure 1(a)

Typical components of a medieval castle

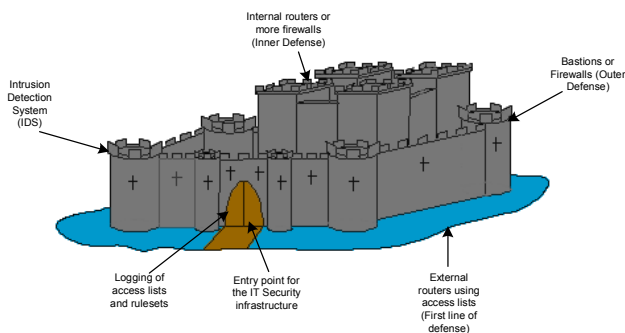


Figure 1(b)

Corresponding components of an IT Security Model

III. THE DEMISE OF MEDIEVAL CASTLES

Castles had their heyday in the Norman era of the 11th to 13th century and started to peter out during the early 15th century. One of the major reasons that castles became defunct was the changes in society. With the end of the feudal system, professional soldiers based in forts increasingly fought warfare while the nobles looked for comfortable homes. A further reason was that older castles could not withstand cannon fire, making them redundant, particularly given the cost of upgrading them would have been excessive.[3] Taking an IT Security perspective, the above reasons would translate into every organization, particularly on the Internet, agreeing to trust one another. The multiple layers of security

would be torn down, making the infrastructure, applications and data, much more accessible. There are clearly many problems with this scenario, the most important being:

- A single attacker cannot cause a considerable amount of damage to the assets of a noble in a castle, but most certainly can in the IT Security Model.
- Getting every organization to agree a set of behaviour standards is unrealistic, particularly given the opportunity for industrial espionage.

Older castles being unable to handle cannon fire can be compared to the IT infrastructure being unable to cope with a significant vulnerability. Clearly, the difference between the two, is the cost of applying a software patch throughout the infrastructure, as opposed to upgrading a castle, which is clearly significantly less. Although, that being said, given the number of critical vulnerabilities being produced, the proportional cumulative cost may be similar.

IV. COMPARISONS AND PREDICTIONS

It can be seen from records that castles were exceptionally expensive to build, with the mighty castle of Caernarvon costing £19,892 at 12th century prices. This compares well with the costs incurred today when building a secure e-commerce environment, for example, which can easily cost £1,000,000 to complete. [4]

Ongoing maintenance costs paint a similar picture and whilst there are no records of how much upkeep was required for a castle, they were clearly expensive to run. This was a further reason why the castle became defunct and more comfortable, and cheaper to run, properties became popular with the nobles of the day.

Likewise, in IT Security, a million pound gateway will cost 15% in hardware maintenance alone, without factoring costs for staff, business processes and technology updates.

The current level of cost of IT Security infrastructure cannot remain unchecked as the costs from carrying out upgrades or security patches are rapidly increasing. [5]. However, as mentioned earlier, the 'social changes' necessary to make IT Security Models defunct is also very unlikely to occur. Perhaps, more likely is the possibility of organizations grouping together to share common infrastructure and thus, share the costs. This could be mutually beneficial to all parties, since costs would be greatly reduced while the level of protection could remain unchanged. Let us assume that such a radical change as has just been discussed might happen, then when might it happen?

Currently, the world economy is in a slowdown, focusing a drive to reduce costs in every corporation. As a result, it is inevitable that should the current economic environment continue in the short to middle term, that corporations will start looking at solutions such as the one proposed by this paper.

Figure 2 shows the total number of security alerts and notes, as well as the number of reported vulnerabilities as a function of time [6]. As can be seen, it can only be a matter of time before a significant vulnerability is discovered and successfully exploited, thus rendering entire sections of infrastructure either redundant or unprotected. Such an action would have an effect that is very similar to the 'undermining' of a medieval castle.

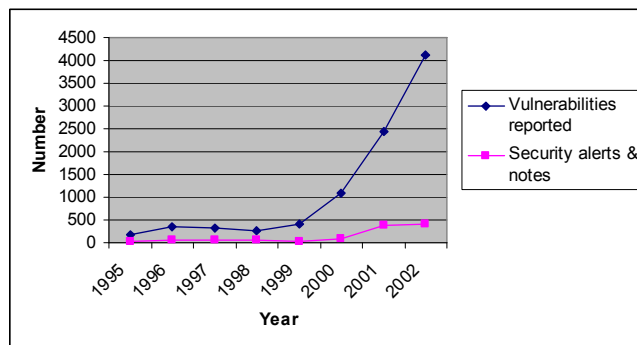


Figure 2
Number of vulnerabilities and security alerts/notes

V. CONCLUSIONS

This paper has discussed the relationships between medieval castles and IT Security Models, and highlighted the areas of commonality between the two. Based on the history of medieval castles and these common areas, a couple of predictions, regarding the future of IT Security Models, have been made.

It is believed that in the face of increasing costs of ownership, organizations will have to consider radical methods for limiting their financial exposure whilst reducing the infrastructure costs. This paper proposes that organization group together based on mutual advantage.

This paper also suggests that as the number of vulnerabilities continues to increase dramatically so the likelihood of a successfully exploited major vulnerability increases. This leaves the IT Security Model potentially redundant or unprotected.

REFERENCES

- [1] CastleXplorer – A short history of castles. Section 2 – Medieval Castles. Simon and Gina Robins, 2001, Available: [http://www.castlexplorer.co.uk/medieval-castles.php\(URL\)](http://www.castlexplorer.co.uk/medieval-castles.php(URL))
- [2] History of Computer Security. Available: <http://csrc.nist.gov/publications/history/>
- [3] CastleXplorer – A short history of castles. Section 3 – The Decline of Castles. Simon and Gina Robins, 2001, Available: [http://www.castlexplorer.co.uk/castle-decline.php\(URL\)](http://www.castlexplorer.co.uk/castle-decline.php(URL))
- [4] Castles of Britain, Lise Hall, 1995-2003. Available: <http://castles-of-britain.com/castle88.htm>
- [5] The Code Red Worm. Hal Berghel. Available: http://www.acm.org/~hlb/col-edit/digital_village/nov-01/dv_11-01.html

- [6] CERT/CC website, Statistics section, 1995-2003.
Available: <http://www.cert.com/stats>

Peter D Groom (M'91) currently works at Credit Suisse First Boston and is also a chartered engineer of the IEE and a member of ISSA. He graduated in Electronic Systems Engineering at the University of Essex, United Kingdom in 1992.

He has held technical positions at GEC, Thames Water Utilities and CSC Computer Sciences Corporation. He then consulted for CSC Computer Sciences Corporation, Logica, Level (3) Communications, Yava and Phoenix Datacom. He currently works at Credit Suisse First Boston, London, in the Global External Networks division.