Raytheon

Customer Success Is Our Mission

Castle Warrior: Redefining 21st Century Network Defense

IEEE ISI 2009, June 8-11

Dallas, TX, USA

Monty D. McDougal

Raytheon Information Security Solutions (ISS)

+1 (972) 205-8650

monty_d_mcdougal@raytheon.com

Castle Doctrine

- Historical
  - Build walls to keep the intruders out
  - Limit ingress points to the Castle
  - Deploy outward facing defenses to keep enemies outside the gates
  - Use guards to look for signs of malicious activity inside the Castle Walls
- Network
  - Deploy firewalls to keep the attackers out
  - Limit ingress points to the network
  - Deploy outward facing defenses to keep enemies outside the firewall
  - Use IDS to look for signs of malicious activity reaching internal networks

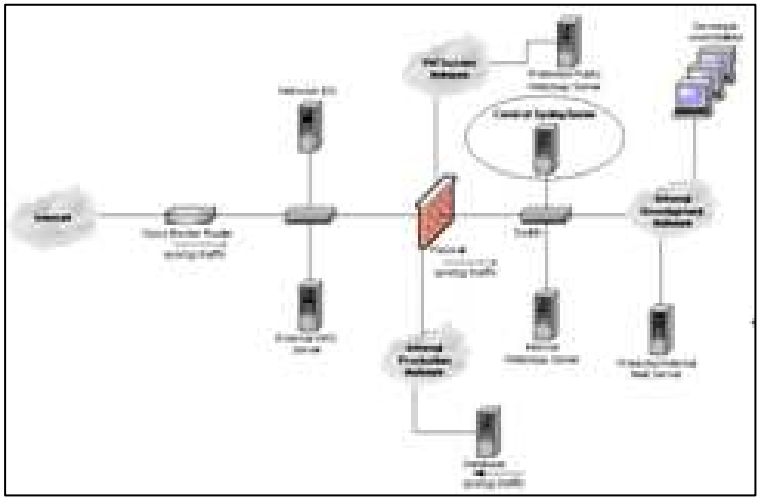
Storming Historical Castles

- Early Attacks
  - Battering Rams
  - Ladders
  - Siege
- Evolutionary Attacks
  - Bows and Arrows
  - Gun Powder

Traditional Castles Had Weaknesses…

Storming Network Castle

- Early Attacks
  - Port Scanning
  - DoS
  - Viruses / Worms
  - Buffer Overflows
  - Zero Day Flash / Warhol Worms
- Evolutionary Attacks
  - Spear Phishing and Targeted Attacks
  - One-Off and Polymorphic Threats



Is The Castle Doctrine Dead?

- Historical Castles – Yes
  - Force mobility
  - Force projection
  - "Shock and Awe"
- Network Castles – No
  - But… Traditional paradigms are completely broken!
  - Assume attackers will get inside
  - Defenders simply cannot keep them all out

Network Castle Still Have Some Benefits…

Why Build Network Castles Then?

- Early Threats Still Exist
  - Castle Walls keep out the roving hordes at fairly low cost
  - Acts as a “noise filter” to help you to see the real threats
- Unfortunately, Castle Walls will not defend against skilled attackers
  - Skilled attackers being defined as those who understand how to circumvent these barriers using a more sophisticated attack method
- For now, the Castle Walls keep out the horde
  - Don’t underestimate the horde’s ability to learn these new skills!
  - Advanced attacks today will become the norm over time

Asymmetric Economics (Defense)

- Building and defending Castles is expensive
- Defenders must mitigate all possible threats to the Castle
  - Asymmetric Cost challenge because a single flaw can mitigate the other defenses
  - Defenders “may” be able to exploit Asymmetric Resources of an attacker to make it too expensive or futile for a given attacker to attack the defender
- As the size / complexity of the Castle increases, so do the costs incurred to guard / maintain it effectively

Asymmetric Economics (Attack)

- Attackers have much lower costs
- Attackers need not defeat all defenses…
  - They simply need to circumvent the one(s) that impede their access to the Castle
- Attackers generally have less resources than the defenders but have an Asymmetric Cost advantage
  - Significant public / open source security research is available to the attacker with minimal costs or they can develop their own
  - Attacker's goal may be to "win" by making the defender spend more than they do (e.g. the Cold War model)
- Unlike with Traditional Castles, attackers face little risk of life or limb with high returns from their spoils of war

How Should We Evolve Our Castles? (1)

- Assume Attackers are going to get inside the Castle Walls
  - Software is inherently vulnerable to human coding error
  - Consider an Intruder Tolerance model (Risk Management vs. Risk Avoidance)
- It is impossible to keep threats out
  - Zero day, polymorphic and / or targeted threats cannot be conventionally defended against
    - Patch and pray is not sufficient protection
  - Attacks against endpoints perpetuate this problem
    - Mail clients, browsers, desktop applications, remote access, client devices, Web 2.0
  - Insider threats (how are users and administrators vetted?)
  - Supply chain threats (who provides your hardware/software/consulting?)

How Should We Evolve Our Castles? (2)

- You should still make it hard for attackers to get inside
  - Exploit your Asymmetric Resource advantages!
  - Look for defenses that increase the cost for the attacker
- Limit the window of time an attacker has inside the walls
  - Focus on real-time detection capabilities
  - Speed up the response times
- Modern Network Castles need controls that assume attackers are going to be inside the castle walls
  - They probably already are… even if you don't know it!

Turn Thy Castle Around (1)

- Traditionally, most Castle defense have been focused at the perimeter
  - Once breached, security is largely compromised
- Castle walls can be used offensively, too
  - Use Castle Walls to stop attackers from exiting
  - Channel the enemy into points that are closely watched and controlled
- Ingress vs. Egress rules
  - Traditional controls have been focused on what is entering the kingdom
  - It is time to start watching what is leaving because even if they get in we really want to make sure the crown jewels (data) don't go out the door

Turn Thy Castle Around (2)

- Slow data exfiltration and monitor data flows
  - Use the Castle Walls to create situational awareness
- Compartmentalization of the Castle
  - Change the paradigm to limit the damage that can be caused by a single breach
  - Try reversing the traditional model!
  - Use a model where the strongest defenses are closest to target (e.g. data) and get increasingly weaker as you reach the perimeter

Know Thy Castle (1)

- Defenders have one major advantage over the attacker… it is their Castle
- Assuming the defender has a proper baseline, they know what is the normal state of their Castle
  - Strong host-based lockdown and configuration control
  - Use whitelists as opposed to blacklists
  - Watch for and aggressively investigate anomalies

Know Thy Castle (2)

- Watch for secret tunnel as they can bypass your controls
  - Watch for things masquerading as legitimate traffic allowed to pass through the gates
    - HTTP / HTTPS, DNS, email, etc.
  - Watch for traffic that is going over / under the Castle Walls and bypassing the gate altogether
    - Rogue modems, rogue wireless, physical access, etc.
- Defenders can leverage their Castle Walls to choose the battlefield
  - Force attackers into vulnerable positions where their traffic can be monitored / observed in order to advance
  - Set traps and monitor them for intrusion

Raytheon

Customer Success Is Our Mission

Aggressively Defend Thy Castle

- Aggressively identify and defend the Crown Jewels of the kingdom
  - Apply the most aggressive defenses to the targets of highest value
  - A method of classifying and identifying the valuable assets of the kingdom must be employed
  - Moving these into protective compartments and enclaves facilitates providing a higher degree of protection based on higher scrutiny of access
- Increase the penalty for attackers
  - We may not be able to keep the attackers out of the Castle, but we should treat them with extreme prejudice for being there!
  - The specifics of this are up to you and your lawyer…
- Deception and misdirection of the enemy
  - May be a possible way of slowing their attacks or learning their tactics (e.g. honeynets)
- If only we could ride out and burn our attackers' Castle down…
  - At least for nation-states this is a viable option

The Future Of Castle Warfare

- We cannot abandon our defenses even though we must adapt how they are used and deployed
  - Techniques and strategies in this area are actively evolving
- Future (and/or current) technologies bring new challenges
  - Web Services
  - Wireless
  - VoIP
  - Cloud Computing
  - Mobile Computing / Mobile Devices
  - B2B and Partnering Relationships
  - Encryption?
- Technology should be introduced only when issues of complexity and security have been evaluated

Parting Words From A Sage…

- It is a lot easier to write the words on this scroll than to do them
  - A lot of the tools that are needed don't even exist
- That said, the existing defense paradigm is completely broken
  - It is getting worse every day so the problem cannot be ignored
- It is time to have a call to arms
  - Start aggressively defending the kingdom or there will be none to defend
- Pay attention to day-to-day Castle activities
  - Much of the insecurity of the Castle stems from the day-to-day activities of the people living / working there
- When building future defenses…
  - It is strongly encouraged that these activities be revisited in the light of the new threats and new technologies

Raytheon

Customer Success Is Our Mission

Questions?

Monty D. McDougal, CISSP-ISSEP-ISSAP
Principal Security Engineer
Raytheon Information Security Solutions (ISS)

+1 (972) 205-8650
monty_d_mcdougal@raytheon.com

Biography

- **Monty McDougal, Principal Security Engineer**, has been working for Raytheon IIS for the last 10+ years performing tasks ranging from programming to system administration. Monty has an extensive programming background spanning 15+ years in web development. His work has included development/integration/architecture/accreditation work on numerous security projects including multiple government programs, internal and external security assessments, wireless assessments, DCID 6/3 compliant web-based single sign-on solutions, PL-4 High-Speed Controlled Interfaces (guards), reliable human review processes, audit log reduction tools, mail bannering solutions, and advanced anti-malware IRADs.
- Monty holds the following major degrees and certifications: BBA in Computer Science / Management (double major) from Angelo State University, MS in Network Security from Capitol College, CISSP, ISSEP, ISSAP, GCFA, GCIH, GCUX, GCWN, GREM, GSEC, GAWN-C, and serves on the SANS Advisory Board.