SSM 6: Defence in Depth

i.g.batten@bham.ac.uk

Recap

- Logging tells us what happened, and might allow us to spot patterns early
- Patched systems have fewer security problems
- Services that aren’t running can’t be broken into
- Services which aren’t listening are hard to break into

Defence in Depth

- Idea is that multiple defences add (multiply?) together to improve security
- If one defence is breached, there are others still standing
- Model has a long history…

Castles

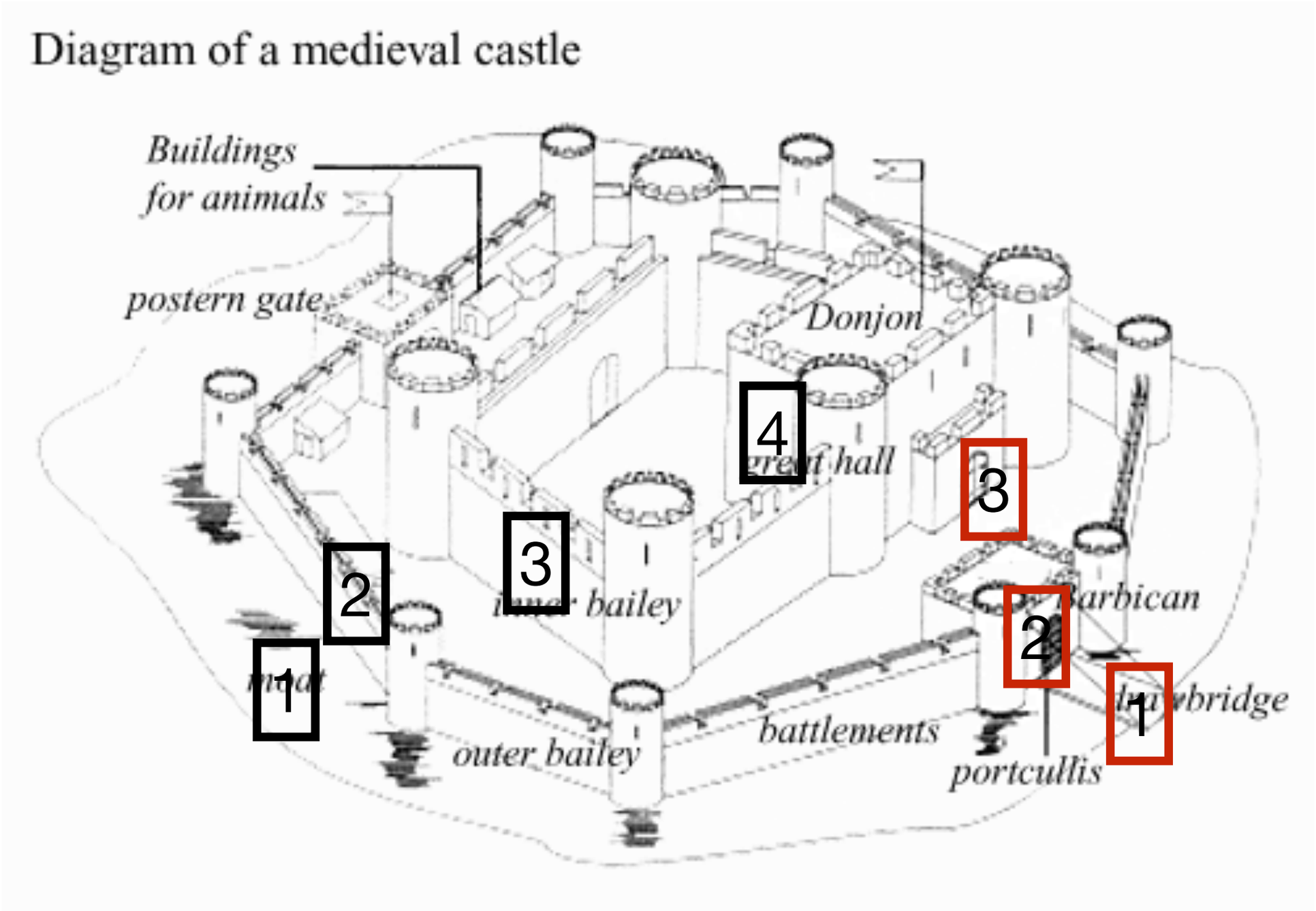


Diagram of a medieval castle
Buildings for animals
postern gate
Donjon
4
3
3
2
2
1
1
battlements
portcullis
outer bailey

Problems

- Assumption that defences are independent
  - Not just physically or logically, but in terms of tools needed to break them
  - Attacker who can knock down one wall can knock down others
  - Attacker who can brute-force one encryption key and brute-force orthers

And can be counter-intuitive: which is safer?

When do planes crash?

- Takeoff is the riskiest phase of flight
- An aircraft accelerates down the runway until it reaches speed V_1, at which point it cannot stop before the end of the runway.
- It needs to get to V_2 (usually greater than V_1, except on ten mile runways), which is minimum safe climb-out speed.
- At some point (usually between V_1 and V_2) it will reach V_R, at which point it “rotates” (starts to take off).
- Engine failure between V_1 and V_2 is very dangerous
- Certification rules are “must be able to get from V_1 to V_2 with one engine failed”. Twins therefore have 200% power installed, Fours 133%.

Twin v Four not obvious

- Twin will crash on takeoff or goaround if two engines fail
  - (0.01 + 0.01) * 0.01 = 0.0002
- Four will crash on takeoff or goaround if two engines fail
  - (0.01 + 0.01 + 0.01 + 0.01) * (0.01 + 0.01 + 0.01) = 0.0012
  - Six times greater risk!

Reality much more complex

- Reality is much more complex, and complicated by the certification regimes for twin-engined aircraft over water (ETOPS) being much stricter than for fours, while fours can fly on two engines and often land.

- But having 200% of minimum take off power is preferable to having 133%

Independence

- But if a plane runs out of fuel, or enters a cloud of volcanic dust, all the engines fail, whether there are one, two, three, four or eight engines

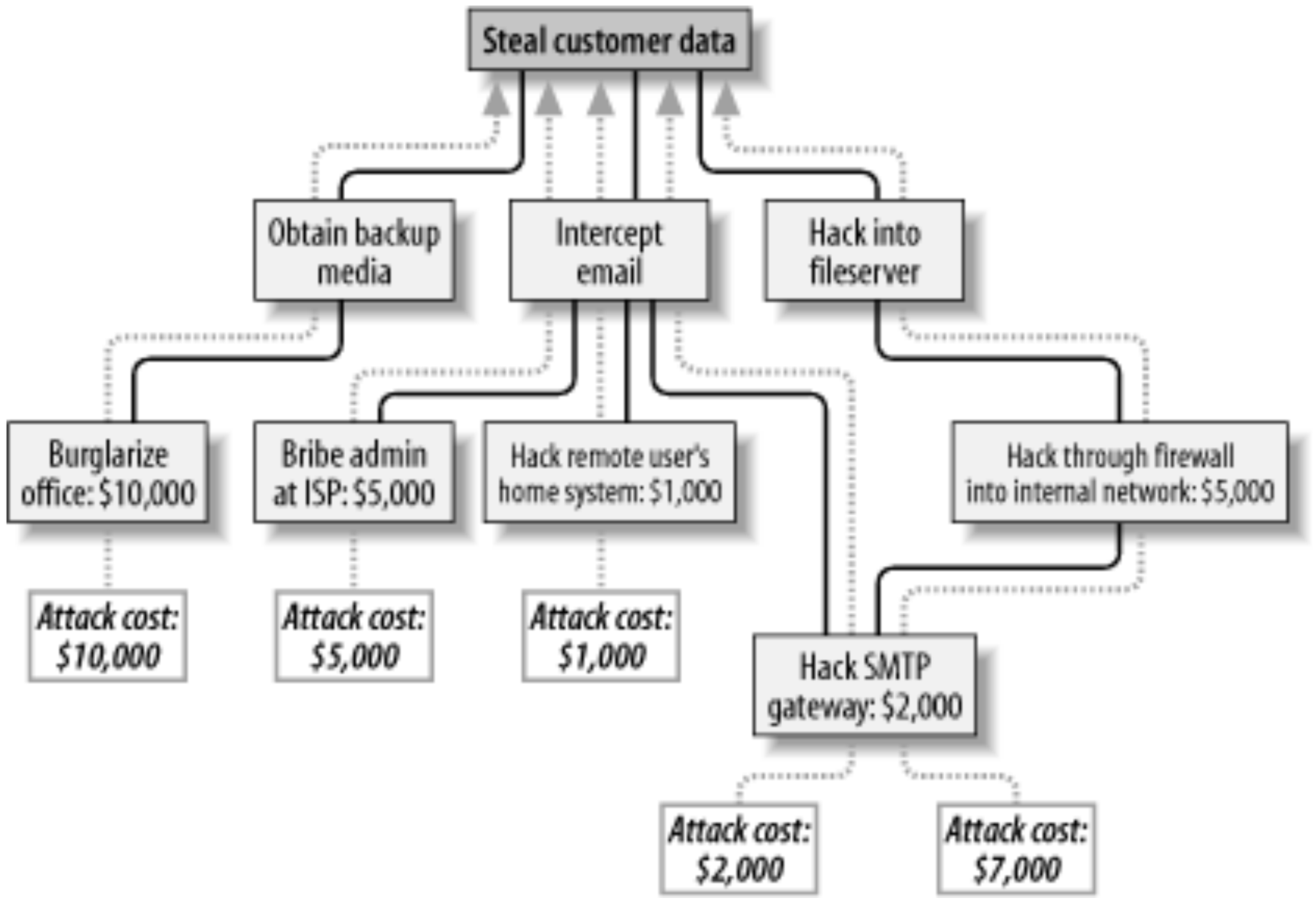
For Information Security

- It is very tempting to think that having lots of defences equates to having defence in depth.
- But one strong lock is preferable to ten weak locks, as an attacker who can break a weak lock can break ten.
  - And a door with ten locks is weakened by ten sets of holes drilled in it.
- We need to make sure we are getting increased protection.

Attack Trees

- Build a tree, with the attacker’s goal at the top, and the various ways he might achieve that descending from it.

Example


Steal customer data
Obtain backup media
Intercept email
Hack into fileserver
Burglarize office: $10,000
Bribe admin at ISP: $5,000
Hack remote user's home system: $1,000
Hack through firewall into internal network: $5,000
Attack cost: $10,000
Attack cost: $5,000
Attack cost: $1,000
Hack SMTP gateway: $2,000
Attack cost: $2,000
Attack cost: $7,000

For each risk, controls

- Backups can be encrypted
- Hackable systems can be made less hackable
- Bribeable staff can be vetted, their jobs divided in two, etc.

Building attack trees is hard

- There is research work both on building them and on analysing them (ripe field for PhD).

- Looking for independence is hard, too

Exercise

- Take five minutes, and build an attack tree for changing your end of year marks on a marks database.

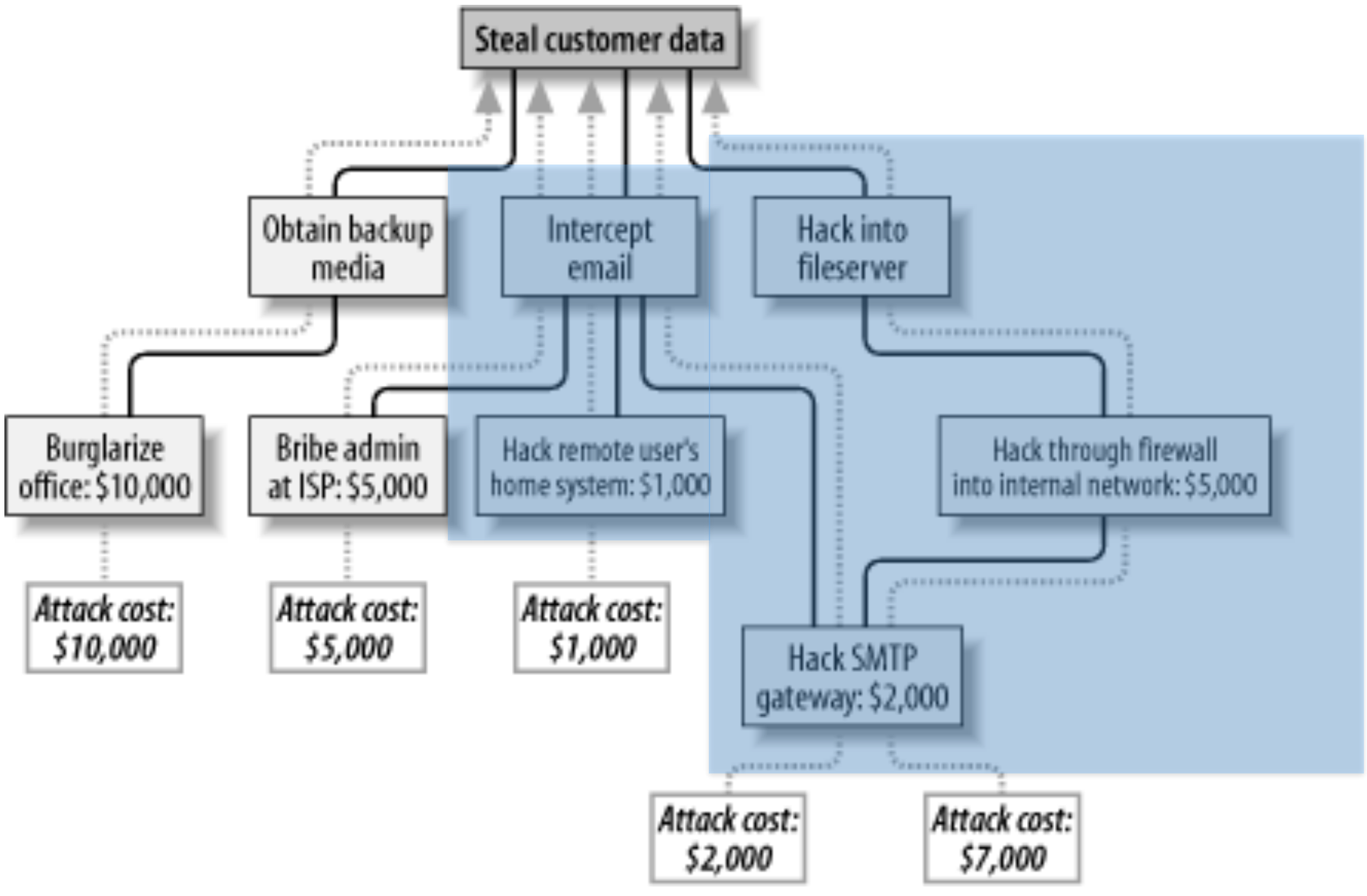
- Assume the database is on a computer, which is behind a firewall, which is administered by an administrator and used by lecturer

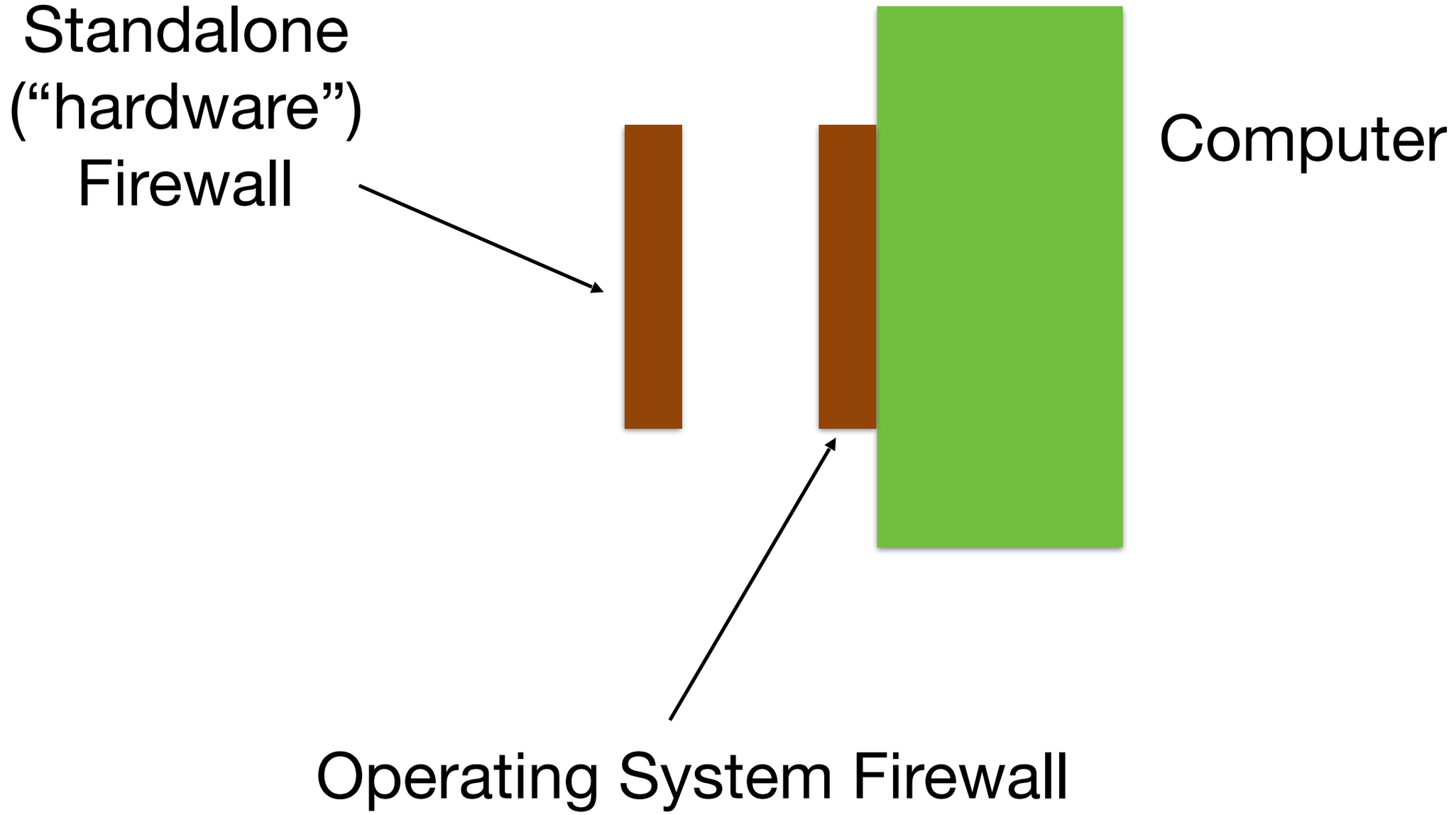
- Be imaginative

Depth?

- Tempting to think that a system protected by two firewalls (or whatever) both of which need to be hacked is more secure that a system protected by one.

Are these independent?




Standalone
(“hardware”)
Firewall
Computer
Operating System Firewall

Firewalls and Attack Surfaces

- You can filter packets using a firewall on a computer

- You can configure the services on that computer securely

- But an attacker who has a get-root privilege escalation attack can bypass both

Firewalls and Attack Surfaces

- You can filter packets using a firewall in a separate box, placed in front of a server
- However, if there is an authentication server which permits users to log in to the firewall and to the computer, an attacker who can attack the authentication server is admin on the firewall and the computer.

Complexity is hard

- In general, the more devices and elements are involved in a security solution, the less likely that it is accurately analysed

- Tradeoff between simplicity (and therefore ease of analysis) and defence in depth is not one that can be given a general answer.

Subsidiary Protocols

- Attack trees often miss attacks on “subsidiary protocols”.

- Classic example is DNS.

- Suppose I configure some access control mechanism (Apache .htaccess) to permit access to a sensitive document from secure.bigcorp.com.

DNS PTR records

- How do you find out the name of a machine from an IP number?
- For address 1.2.3.4, you form this name:
  - 4.3.2.1.in-addr.arpa
- And you look up the PTR record for that name.
- The 3.2.1.in-addr.arpa “zone” is controlled by the owner of 1.2.3.0/24.
- So they can add this record to the DNS.

Solution

- Attacker controls 3.2.1.in-addr.arpa, but does not control bigcorp.com.

- Solution is to follow up any query IP->name by looking up the name and checking that the IP number is one of the address records.

Example

```
ians-macbook-air:~ igb$ nsupdate -k update-key
> server offsite7.batten.eu.org
> update add 215.150.187.81.in-addr.arpa. 86400 in ptr gromit.cs.bham.ac.uk
>
> ians-macbook-air:~ igb$
```

```
ians-macbook-air:~ igb$ dig -x 81.187.150.215

; <<>> DiG 9.8.3-P1 <<>> -x 81.187.150.215
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4764
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;215.150.187.81.in-addr.arpa.  IN PTR

;; ANSWER SECTION:
215.150.187.81.in-addr.arpa. 86400 IN PTR    gromit.cs.bham.ac.uk.

;; Query time: 107 msec
;; SERVER: 147.188.244.250#53(147.188.244.250)
;; WHEN: Tue Jan 27 14:26:00 2015
;; MSG SIZE  rcvd: 79

ians-macbook-air:~ igb$
```

```
ians-macbook-air:~ igb$ dig gromit.cs.bham.ac.uk

; <<>> DiG 9.8.3-P1 <<>> gromit.cs.bham.ac.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32162
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;gromit.cs.bham.ac.uk.    IN A

;; ANSWER SECTION:
gromit.cs.bham.ac.uk.   85439 IN A
;; Query time: 6 msec
;; SERVER: 147.188.244.250#53(147.188.244.250)
;; WHEN: Tue Jan 27 14:27:02 2015
;; MSG SIZE  rcvd: 54

ians-macbook-air:~ igb$
```

Other Protocols

- NTP can be abused (but rarely is): if you really need accurate time and rely on it, then you need your own reference clock

- DHCP and other configuration protocols can be abused, but it is difficult to do remotely