

CLAIMS

1. A computer security protection module (22) arranged to provide cyber defence capabilities to a target computer resource (12), the target computer resource being a potential target of a cyber-attack from an attacker computer entity (14) and the target computer resource comprising a local network and a plurality of devices connected to the local network, the module comprising:
- a first communications interface (43) arranged to interface with a communications network, the attacker computer entity being remotely located from the computer resource via the communications network (18);
 - a second communications interface (45) arranged to interface with the target computer resource such that the protection module is located in a communications path between the communications network and the target computer resource;
 - a processor (47) arranged to inspect communications traffic between the communications network and the target computer resource;
- wherein, the processor is arranged to forward trusted communications traffic received at the first communications interface (43) to the target computer resource (12) via the second communications interface (45) and to forward communications traffic received at the first communications interface that is not trusted to a virtual target (24), the virtual target being arranged to be a substantial replica of the target computer resource
- wherein the processor is arranged to map the architecture of the target computer resource, the map of the architecture of the target computer resource (12) comprising configuration data relating to the target computer resource
- and wherein the processor is arranged to store the map of the architecture of the target computer resource, and the processor is arranged to periodically map the architecture of the target computer resource and compare to a previously stored map of the architecture of the target computer resource, the processor being arranged to output a notification message in the event of a change to the architecture of the target computer resource that does not conform to a stored security policy.
2. A computer security protection module as claimed in Claim 1, wherein the processor is arranged to forward communications traffic that is not trusted to the virtual target via the first communications interface (43).

3. A computer security protection module as claimed in Claim 1 or Claim 2, wherein the processor (47) is arranged to run penetration testing of the target computer resource (12).
- 5 4. A computer security protection module as claimed in any preceding claim, wherein the processor is arranged to output the map of the architecture of the target computer resource via the first communications interface (43) to a virtual resource module (24) in order that the virtual resource module can construct a substantial replica of the target computer resource.
- 10 5. A computer security protection module as claimed in any preceding claim, wherein the processor is arranged to output the map of the architecture of the target computer resource via the first communications interface to an emulation module (26), the emulation module being arranged to emulate the target computer resource on a
- 15 virtual machine.
6. A computer security protection module as claimed in any preceding claim, wherein the processor is arranged, in the event that a cyber-attack from an attacker computer entity is detected, to block the first communications interface (43).
- 20 7. A computer security protection module as claimed in any preceding claim, wherein the processor (47) is arranged, in the event that a cyber-attack from an attacker computer entity is detected, to block the second communications interface (45).
- 25 8. A computer security protection module as claimed in Claim 7, wherein the processor is arranged to continue forwarding communications traffic from the attacker computer entity to the virtual target while the second communications interface is blocked.
- 30 9. A computer security protection module as claimed in any preceding claim, wherein the module is arranged to receive computer resource updates for the target computer resource (12) and to apply updates to the computer resource.

10. A computer security system (20) comprising:

a protection module (22) according to any one of Claims 1 to 9;

a virtual resource module (24) for emulating a target computer resource (12) in the event of a cyber-attack, the virtual resource module comprising;

5 an input for receiving target computer resource configuration data from a computer security protection module (22) providing cyber defence capabilities to the computer resource (12);

a processor arranged to generate a virtual target to substantially mimic the target computer resource on the basis of the received configuration data;

10 an output arranged to output data to an attacker computer entity (14);

wherein the input is arranged to receive a redirected cyber-attack originating from the attacker computer entity, the attack being redirected from the computer security protection module (22); and the processor is arranged to generate responses to the cyber-attack, the responses being sent to the attacker computer entity from the output;

15 and

an emulation module (26) arranged to emulate a target computer resource (12) in order to run mock cyber-attacks against an emulated target computer resource, the emulation module comprising:

20 an input for receiving target computer resource configuration data from a computer security protection module (22) providing cyber defence capabilities to the target computer resource;

a processor arranged to emulate a representation of the target computer resource and to run mock cyber-attacks against the emulated target computer resource;

25 an output arranged to output target computer resource updates for the target computer resource in dependence on the outcome of the mock cyber-attacks against the emulated target computer resource.

11. A method of operating a computer security protection module (22) arranged to provide cyber defence capabilities to a target computer resource (12), the target

30 computer resource being a potential target of a cyber-attack from an attacker computer entity (14) and the target computer resource comprising a local network and a plurality of devices connected to the local network, the method comprising:

interfacing (120) via a first communications interface (43) with a communications network (18), the attacker computer entity (14) being remotely located from the computer

35 resource via the communications network;

interfacing (122) via a second communications interface (45) with the target computer resource such that the protection module is located in a communications path between the communications network and the target computer resource;

5 inspecting (124), using a processor (47), communications traffic between the communications network and the target computer resource;

forwarding (126) trusted communications traffic received at the first communications interface to the target computer resource (12) via the second communications interface and

10 forwarding (128) communications traffic received at the first communications interface that is not trusted to a virtual target, the virtual target being arranged to be a substantial replica of the target computer resource

mapping the architecture of the target computer resource, the map of the architecture of the target computer resource (12) comprising configuration data relating to the target computer resource

15 storing the map of the architecture of the target computer resource

periodically mapping the architecture of the target computer resource and comparing to a previously stored map of the architecture of the target computer resource

outputting a notification message in the event of a change to the architecture of the target computer resource that does not conform to a stored security policy.

20

12. A carrier medium for carrying a computer readable code for controlling a computing device to carry out the method of Claim 11.