Measuring Cyber Essentials Security Policies

Sándor Bartha [1], Russell Ballantine [2], David Aspinall [1]

[1]The University of Edinburgh

[2]TEK Systems Global Services

August 13, 2024

Cyber Essentials (CE)

UK

- scheme backed by the UK government
- recognized security certification for SMEs
- requirement for certain government contracts

US

- based on CE experience in UK, CISA created its own variant
- compatible with NIST Cybersecurity Framework

"Requirements for IT infrastructure"

A security policy is a high level description, prescribing some combination of *security controls*. The controls are grouped into control themes:

Technical control themes

- Firewalls
- Secure configuration
- Security update management (patch policy)
- User Access Control (UAC)
- Malware protection

We considered an additional control theme:

- Business resiliency

encompassing important controls used in practice by practitioners.

Goal of research

SME's requirement

Rely on expert opinion for designing and choosing policies, while also have a *repeatable process* which *can be re-evaluated and adjusted* later, when requirements change.

Our goal

Allow the integration of CE security policies into decision-making frameworks.

Basis of decision

Decision between security policies is a cost-benefit analysis.

- Estimating costs (direct and indirect) ✗
- **Score measuring potential benefits** ✓
- Process to determine optimum ✗

Our goal (refined): a numerical score representing the benefits of a high-level CE security policy.

Idea

Build on the Common Vulnerability Scoring System (CVSS, v3.1).

Base score

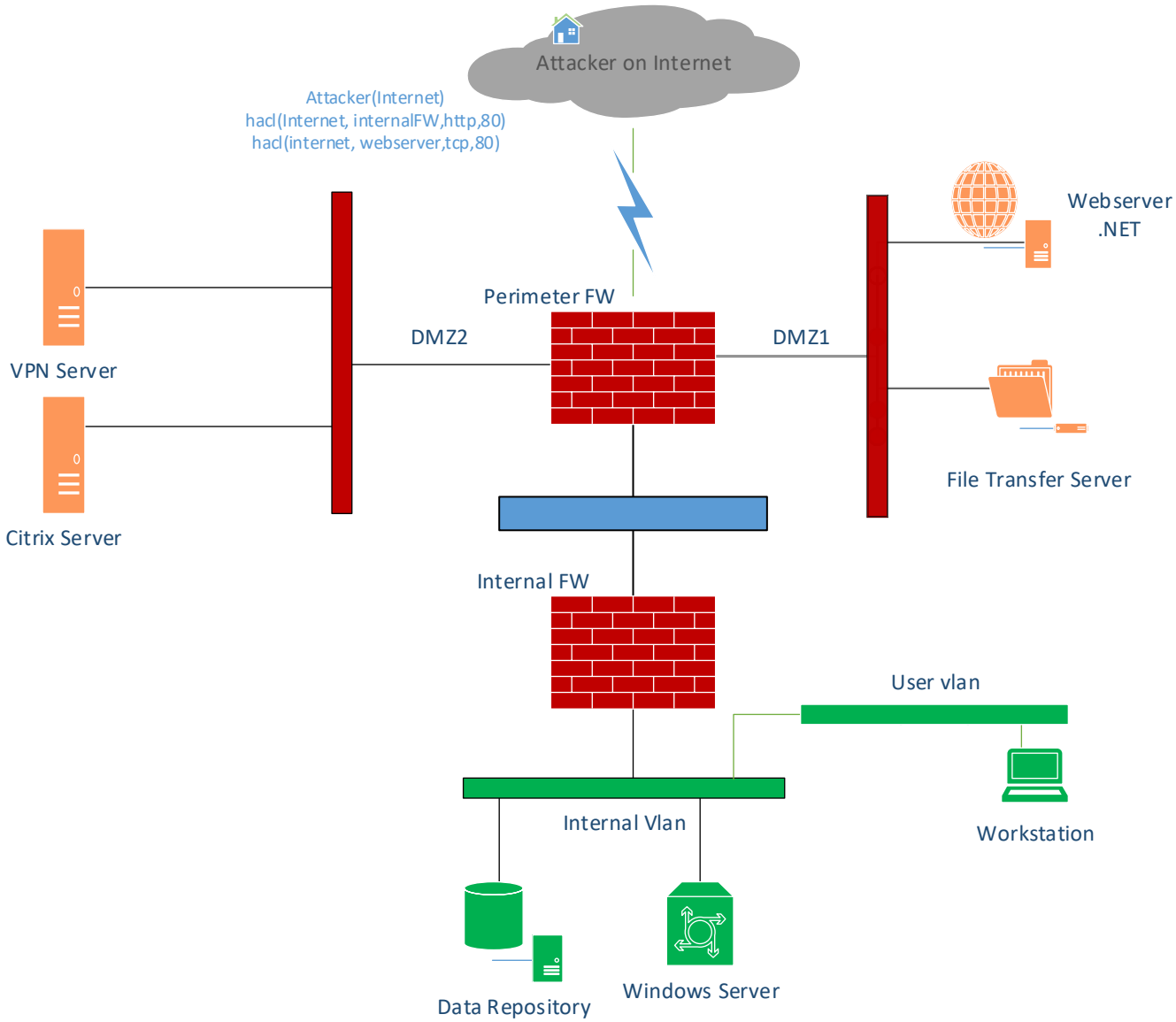
- Provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity
- The base CVSS score is based on 8 metrics, each which measures the vulnerability along a different aspect.
- Base metrics for common vulnerabilities are provided by the CVE database.

Environmental score

- Allows modifying the base metrics according to the environment

Idea: Use environmental CVSS not to order vulnerabilities, but to order environments.

Example scenario



Example policy

8 CE policies were given to 10 security practitioners to choose between based on the example scenario. Example policy:

Policy 1:

Firewall Network firewall present, but no host firewalls are used.

Secure configuration Device hardening is employed on all server instances.

Patch policy Patching strategy is not in use.

UAC RSA two factor authentication is used on the servers.

Malware protection – intrusion detection/prevention No intrusion detection system (IDS) or intrusion prevention system (IPS) is used on the network.

Malware protection – whitelisting or sandbox No application whitelisting or sandbox is used.

Business resiliency – disaster recovery A full disaster recovery strategy is in place.

Business resiliency – encryption VPN is used for external access to the servers.

Formalizing policies - I

Define 7 control groups, roughly corresponding to CE control themes.

CE control theme	CE Control group
Firewall	Firewall
Secure configuration	Secure configuration
Security update management	Security update management
User Access Control	User access control
Malware protection	Intrusion control
	Application control
Business resiliency	Disaster recovery
	Pipeline encryption

Formalizing policies - II

Each control group is the set of possible controls. Example:

CE control group: Firewall

- **Network firewall OOB**
- **Network firewall in-band MFA**
- **Network firewall in-band admin password**
- **Network+Host firewalls OOB**
- **Network+Host firewalls in-band MFA**
- **Network+Host firewalls in-band admin password**

A CE policy contains at most **one** control from each group.

Formalizing policies

Policy = At most 1 control from each group. Example:

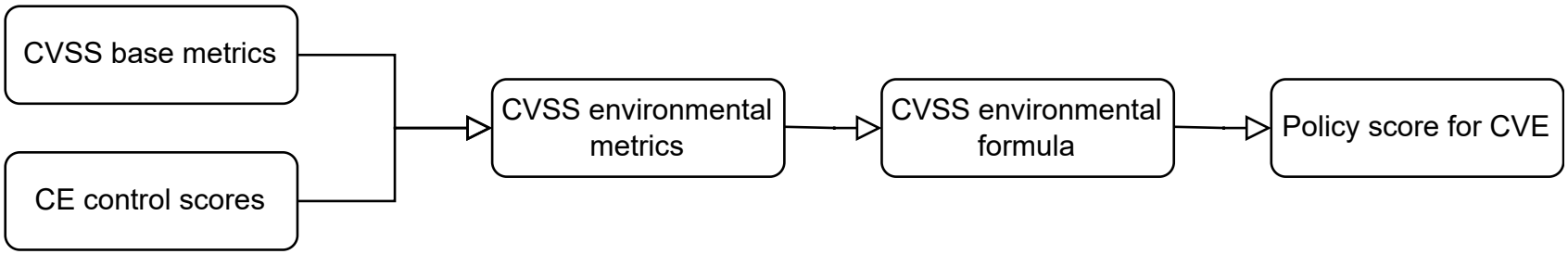
CE Control group	Policy 1 CE control
Firewall	**Network firewall OOB**
Secure configuration	**Device hardening, no audit**
Security upd. management	-
User access control	**MFA**
Intrusion control	-
Application control	-
Disaster recovery	**Full disaster recovery strategy**
Pipeline encryption	**End2End pipeline encryption**

CE control groups $\leftrightarrow$ CVSS metrics

Idea: policy determines the environment, so CE controls modify the environmental CVSS metrics

CE control group	CVSS metric
Firewall	Modified Attack Vector
Secure configuration	Modified Attack Complexity
Security update management	Remediation Level
User access control	Modified Privileges Required
Intrusion control	Modified Integrity
Application control	Modified User Interaction
Disaster recovery	Modified Availability
Pipeline encryption	Modified Confidentiality

Scheme to calculate CVSS score



1. Assign scores to CE controls
2. Set a function for CE control groups to combine the base metric and the CE control score

We estimate the defence policy's effect on the class of vulnerabilities characterised by the CVSS vector of the CVE.

We collect a representative set of CVEs for the system.

Example CE control scores

CE control group Firewall

Associated CVSS metric Modified Attack Vector

CE Control	CVSS value	min score
Network firewall, OOB or MFA	**adjacent**	0.646
Network firewall, inband admin password	**adjacent**	0.73
Network+Host firewall, OOB or MFA	**local**	0.395
Network+Host firewall, inband admin password	**local**	0.52

$$\text{Modified Attack Vector } score \triangleq max(\text{Attack Vector score}, \text{CE control score})$$

Example

CVSS metrics	base score	CE control	control score	operation	modified score
Attack Vector	0.85	**Network firewall OOB**	0.646	min	0.646
Attack Complexity	0.77	**Device hardening, On build, no audit**	0.48	max	0.77
Remediation Level	-	**No pathcing policy**	1	-	1
Privileges Required	0.62	**MFA**	0.27	max	0.62
User Interaction	0.85	**No application control**	1	$*$	0.85
Confidentiality	0.56	**Partial pipeline encryption**	0.275	min	0.275
Integrity	0.56	**IPS and DoS mitigation**	0.075	min	0.075
Availability	0.56	**Full disaster recovery strategy**	0.0	min	0.0

Environmental CVSS score: 6.6

Aggregating individual scores

Problem: CVSS is ordinal
(order is significant but magnitude is not)

Simple model: use weighted median

Caveats and discussion

- Our work suggests a possible methodology exploiting CVSS scores, but obviously this must be done carefully in practice
  - risk versus severity
  - CVSS scores are ordinal
- CVSS v4 was released after we completed the work, it has clarified terminology and added granularity
- The essential aspect we are interested in is an ordering on environmental improvements given by controls. We would be happy to discuss how this approach can be improved.

Thanks for your attention!