Overcoming Fear of the Threat Model

Scott Cadzow(✉)

Cadzow Communications Consulting Ltd., Sawbridgeworth, UK
scott@cadzow.com

Abstract. In recognising that it is the human factor that generally identifies risk and maps out the functionality of a system - its goal in other words - it is clear that this strength can be undermined by fallibility. The question we need to ask is how do we optimise the strengths of the human element and minimise the risk they present to the system? How do we do the security job effectively without leading to a climate of fear? Unfortunately undertaking a critical security analysis of a design will almost inevitably point out critical errors, or required design adjustments. When applied late in the design process the impact is high - often working against the analyst when presenting the results. This time around the fear starts with the analyst. The purpose of this paper is to mark those elements of the connected world and the publicised attacks on it, and to identify steps that security engineers should be taking to minimise the concerns raised. Addressing the fear of the threat model, promoting why good design works, relegating the "movie plot" threats to the fiction they belong in.

Keywords: Human factors · Standards · Risk modelling

1 Extended Introduction

The purpose of this short paper, and its accompanying presentation material, is to open a debate that marks out those elements of the connected world and the publicized attacks on it that give rise to fear. From a view of that world of risk and uncertainty we need to ask what should security engineers be doing that will minimize the concerns raised without escalating the level of fear. The worry is that in looking at all the issues of what could possibly go wrong and working out means to ensure they don't ever happen is that they find those things that could go wrong and end up in some endless loop of despair. So the paper is going to assert that we need to know what can go wrong, how we can be exploited, and use that knowledge to learn to recognize wrongness and the exploits, and then defend against them. This is something I'm terming "overcoming the fear of the threat model" by taking steps to address the fear of the threat model, promoting why good design works, and relegating the "movie plot" threats to the fiction they belong in.

The role of standards in this endeavor should not be understated. As engineers and scientists we need to respect issues such as scientific method, repeatability, ethical behavior and presentation of results, and we need to be as objective as possible - presenting facts and evidence that support any claim. This paper will assert that

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 14–24, 2017.
DOI: 10.1007/978-3-319-58460-7_2

standards, when used correctly, underpin scientific method and can be used to give greater assurance to users that a product will not be a liability with regards to security.

2 Human Fallibility

We start with a simple assertion: Humans design, operate and are the net beneficiaries of most systems. We can also assert as a consequence that humans are the net losers when systems go wrong. If that failure is in the security systems trust in the system can disappear.

Humans are fallible and make mistakes. One of the roles of security engineers is to recognize this fallibility and to be up front about what can and cannot be done with respect to countering threats that limits the damage of such fallibility. In doing this it is essential to also recognize that humans are adaptable and resourceful in both designing systems and correcting them when they go wrong. These characteristics mean that humans can be both the strongest and the weakest link in system security. It also means that there is an incentive to manage the human element in systems such that those systems work well (functionality matches the requirement), efficiently (don't overuse resources), safely and securely. Thus human centric design, even for mostly machine based systems, is essential.

The need to understand risk, attack vectors, mitigation strategies, attacker motivation, resilience, cryptography, protocols, data value and many other application specific topics in order to be effective in designing security into systems from day zero marks the rounded security engineer out as a maverick entity.

In recognizing that it is the human factor that generally identifies risk and maps out the functionality of a system - its goal in other words - it is clear that this strength can be undermined by fallibility. The question we need to ask is how do we optimize the strengths of the human element and minimize the risk they present to the system? How do we do the security job effectively without leading to a climate of fear?

Unfortunately undertaking a critical security analysis of a design will almost inevitably point out critical errors, or required design adjustments. When applied late in the design process the impact is high - often working against the analyst when presenting the results. This time around the fear starts with the analyst.

The purpose of this paper is to mark those elements of the connected world and the publicized attacks on it, and to identify steps that security engineers should be taking to minimize the concerns raised. Addressing the fear of the threat model, promoting why good design works, relegating the "movie plot" threats to the fiction they belong in.

3 Security Controls? Security Awareness?

The set of Critical Security Controls (CSC) published by the SANS [SANS] Institute (see list below) are proposed as key to understanding the provision of security to systems, however selling the benefits of such controls, and the threat modelling that underpins many security programmes, including Common Criteria [CC] and ETSI's Threat Vulnerability Risk Analysis (TVRA) [E-TVRA] method to the end user is

difficult and more often appears to induce fear rather than contentment that the experts understand their work.

Misapplication of the Critical Security Controls by human error, malicious or accidental, will lead to system vulnerabilities. The importance of such controls has been widely recognized and they can be found, either duplicated or adopted and adapted for sector specific spaces, in ETSI, ISO and in a number of industry best practice guides.

1. Inventory of Authorized and Unauthorized Devices
   (a) On the face of it this is relatively simple - identify the devices you want to authorize and, those you don't. However this introduces the Rumsfeld[1] conundrum "… there are known knowns … there are known unknowns … there are also unknown unknowns …", it is not possible to identify everything.
2. Inventory of Authorized and Unauthorized Software
   (a) As for devices the Rumsfeld conundrum applies.
3. Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewall Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

The more flexible a device is the more likely it is to be attacked by exploiting its flexibility. We can also assert that the less flexible a device is it is less able to react to a threat by allowing itself to be modified.

The use of the Johari Window [JOHARI] to identify issues is of interest here (using the phrasing of Rumsfeld).

[1] "Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones." Attributed to Donald Rumsfeld on 12-February-2002.

	Known to self	Not known to self
Known to others	Known knowns - BOX 1	Unknown knowns - BOX 2
Not known to others	Known unknowns - BOX 3	Unknown unknowns - BOX 4

The human problem is that the final window, the unknown unknowns, is the one that gives rise to most fear but it is the one that is not reasonable (see movie plot threats below). The target of security designers is to maximize the size of box 1 and to minimize the relative size of each of box 2 and box 3. In so doing the scope for box 4 to be of unrestrained size is hopefully minimized (it can never be of zero size).

We can consider the effect of each "box" on the spread of fear:

BOX 1: Knowledge of an attack is public knowledge and resources can be brought to bear to counter the fear by determining an effective countermeasure

BOX 2: The outside world is aware of a vulnerability in your system and will distrust any claim you make if you do not address this blind spot

BOX 3: The outside world is unaware of your knowledge and cannot make a reasonable assessment of the impact of any attack in this domain and the countermeasures applied to counter it

BOX 4: The stuff you can do nothing about as as far as you know nothing exists here.

The obvious challenge is thus to bring tools such as the 20 controls listed above to bear to maximize box 1 at the same time as using education and dissemination to minimize the size of boxes 2 and 3. Box 3 is characteristic of the old, mostly discredited, approach of security by secrecy, whereas Box 1 is characteristic of the open dissemination and collaborative approach of the world of open standards and open source development. Box 1 approaches are not guarantees of never having a security problem ever, problems migrate from box 4 to boxes 2 and 3 before reaching box 1 and, hopefully, mitigation.

In the security domain we can achieve our goals both technically and procedurally. This also has to be backed up by a series of non-system deterrents that may include the criminalisation under law of the attack and a sufficient judiciary penalty (e.g. interment, financial penalty) with adequate law enforcement resources to capture and prosecute the perpetrator. This also requires proper identification of the perpetrator as traditionally security is considered as attached by *threat agents,* entities that adversely act on the system. However in many cases there is a need distinguish between the threat source and the threat actor even if the end result in terms of technical countermeasures will be much the same, although some aspects of policy and access to non-system deterrents will differ. A *threat source* is a person or organisation that desires to breach security and ultimately will benefit from a compromise in some way (e.g. nation state, criminal organisation, activist) and who is in a position to recruit, influence or coerce a threat actor to mount an attack on their behalf. A *Threat Actor* is a person, or group of persons, who actually performs the attack (e.g. hackers, script kiddy, insider (e.g. employee), physical intruders). In using botnets of course the coerced actor is a machine and its recruiter may itself be machine. This requires a great deal of work to eliminate the innocent threat actor and to determine the threat source.

The technical domain of security is often described in terms of the CIA paradigm (Confidentiality Integrity Availability) wherein security capabilities are selected from the CIA paradigm to counter risk to the system from a number of forms of cyber attack. The common model is to consider security in broad terms as determination of the triplet {threat, security-dimension, countermeasure} leading to a triple such as {interception, confidentiality, encryption} being formed. The threat in this example being interception which risks the confidentiality of communication, and to which the recommended countermeasure (protection measure) is encryption.

The very broad view is thus that security functions are there to protect user content from eavesdropping (using encryption) and networks from fraud (authentication and key management services to prevent masquerade and manipulation attacks). What security standards cannot do is give a guarantee of safety, or give assurance of the more ephemeral definitions of security that dwell on human emotional responses to being free from harm. Technical security measures give hard and fast assurance that, for example, the contents of an encrypted file cannot, ever, be seen by somebody without the key to decrypt it. So just as you don't lock your house then hang the key next to the door in open view you have to take precautions to prevent the key getting into the wrong hands. The French mathematician Kerchoff has stated "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge". In very crude terms the mathematics of security, cryptography, provides us with a complicated set of locks and just as in choosing where to lock up a building or a car we need to apply locks to a technical system with the same degree of care. Quite simply we don't need to bother installing a lock on door if we have an open window next to it - the attacker will ignore the locked door and enter the house through the open window. Similarly for a cyber system if crypto locks are put in the wrong place the attacker will bypass them.

It may be argued that common sense has to apply in security planning but the problem is that often common sense is inhibited by unrealistic threats such as the movie plot scenarios discussed below.

4 Movie Plot Threats

Bruce Schneier has defined movie plot threats as "*... a scary-threat story that would make a great movie, but is much too specific to build security policies around*"[2] and rather unfortunately a lot of the real world security has been in response to exactly these kind of threats. Why? The un-researched and unproven answer is that movie plots are easy to grasp and they tend to be wrapped up for the good at the end.

The practical concerns regarding security and the threats they involve is that they are somewhat insidious, like dripping water they build up over time to radically change the landscape of our environment.

Taking Schneier's premise that our imaginations run wild with detailed and specific threats it is clear that if a story exists that anthrax is being spread from crop dusters over

[2] https://www.schneier.com/blog/archives/2014/04/seventh_movie-p.html.

a city, or that terrorists are contaminating the milk supply or any other part of the food chain, that action has to be taken to ground all crop dusters, or to destroy all the milk. As we can make psychological sense of such stories and extend them by a little application of imagination it is possible to see shoes as threats, or liquids as threats. So whilst Richard Reid[3] was not successful and there is no evidence to suggest that a group of terrorists were planning to mix a liquid explosive from "innocent" bottles of liquid, the impact is that due to the advertised concerns the policy response is to address the public fears. Thus we have shoe inspections and restrictions on carrying liquids onto planes. This form of movie theatre scenario and the response ultimately diverts funds and expertise from identifying the root of many of the issues.

Again taking Schneier's premise the problem with movie plot scenarios is that fashions change over time and if security policy is movie plot driven then it becomes a fashion item. The vast bulk of security protection requires a great deal of intelligence gathering, detail analysis of the data and the proposal of targeted counter measures. Very simply by reacting to movie plots the real societal threats are at risk of being ignored through misdirection.

Movie plot derived security policy only works when the movie plot becomes real. If we built out bus network on the assumptions behind Speed we'd need to build bus stops for ingress and egress that are essentially moving pavements that don't allow for the bus to ever slow down, and we'd need to be able to refuel and change drives also without slowing the bus. It'd be a massive waste of money and effort if the attackers did a Speed scenario on the tram or train network or didn't attack at all.

A real problem is that for those making security policy, and for those implementing the countermeasures, they will always be judged in hindsight. If the next attack targets the connected vehicle through the V2I network, we'll demand to know why more wasn't done to protect the connected vehicle. If it targets schoolchildren by attacking the exam results data, we'll demand to know why that threat was ignored. The answer "we didn't know … " or "we hadn't considered this …" is not acceptable.

The attractiveness of movie plot scenarios is probably hard to ignore - they give a focus to both the threat and the countermeasures. In addition we need to consider the role of Chinese Whispers[4] in extending a simple story over time.

We can imagine dangers of believing the end point of a Chinese Whispers game:

- Novocomstat has missile launch capability
- Novocomstat has launched a missile
- Novocomstat has launched a bio weapon
- Novocomstat has launched a bio weapon at Neighbourstat
- Neighbourstat is under attack
- Neighbourstat is an ally and we need to defend them
- We're at war with Novocomstat because they've attacked with the nuclear option

[3] https://en.wikipedia.org/wiki/Richard_Reid => The "shoe bomber".

[4] https://en.wikipedia.org/wiki/Chinese_whispers => A parlour game that passes a message round introducing subtle changes in meaning with each re-telling.

As security engineers the guideline is to never react without proof. Quite simply acting on the first of these Chinese Whispers is unwarranted, and acting on the 6th is unwarranted unless all the prior statements have been rigorously verified, quantified and assessed. The various risk management and analysis approaches that exist (there are many) all come together by quantifying the impact of an attack and its likelihood. In recent work in this field in ETSI the role of motivation as well as capability in assessing risk has been re-assessed and now added to the method [E-TVRA]. The aim in understanding where to apply countermeasures to perceived risk requires analysis. That analysis requires expertise and knowledge to perform. In the approach defined by ETSI in TS 102 165-1 this means being able to quantify many aspects of carrying out a technical threat including the time required, the knowledge of the system required, the access to the system, the nature of the attack tools and so forth.

5 The Role of Standards

Standards are peer reviewed and have a primary role in giving assurance of interoperability. Opening up the threat model and the threats you anticipate, moving everything you can into box 1, in a format that is readily exchangeable and understandable is key.

Standards are at the root of sharing a common syntactical and semantic understanding of our world. This is as true for security as it is for any other domain and has to be embraced.

The corollary of the above is that if we do not embrace a standards view we cannot share knowledge effectively and that means we grow our box 2, 3, 4 visions of the world and with lack of knowledge of what is going on the ability of fear to grow and unfounded movie plot threats to appear real gets ever larger.

Let us take health as a use case for the role of standards in achieving interoperability. When a patient presents with a problem the diagnostic tools and methods, the means to describe the outcome of the diagnosis, the resulting treatment and so on, have to be sharable with the wider health system. This core requirement arises from acceptance that more than one health professional will be involved. If this is true they need to discuss the patient, they need to do that in confidence, and they need to be accountable for their actions which need to be recorded. Some diseases are “notifiable” and, again, to meet the requirement records have to be kept and shared. When travelling a person may enter a country with an endemic health issue (malaria say) and require immunisation or medication before, during and following the visit. Sharing knowledge of the local environment and any endemic health issues requires that the reporting and receiving entities share understanding.

Shared understanding and the sharing of data necessary to achieve it is the essence of interoperability. A unified set of interoperability requirements addresses syntax, semantics, base language, and the fairly obvious areas of mechanical, electrical and radio interoperability.

Syntax derives from the Greek word meaning ordering and arrangement. The sentence structure of subject-verb-object is a simple example of syntax, and generally in formal language syntax is the set of rules that allows a well formed expression to be formed from a fundamental set of symbols. In computing science syntax refers to the

normative structure of data. In order to achieve syntactic interoperability there has to be a shared understanding of the symbol set and of the ordering of symbols. In any language the dictionary of symbols is restricted, thus in general a verb should not be misconstrued as a noun for example (although there are particularly glaring examples of misuse that have become normal use, e.g. the use of "medal" as a verb wherein the conventional text "He won a medal" has now been abused as "He medalled"). In the context of eHealth standardisation a formally defined message transfer syntax should be considered as the baseline for interoperability.

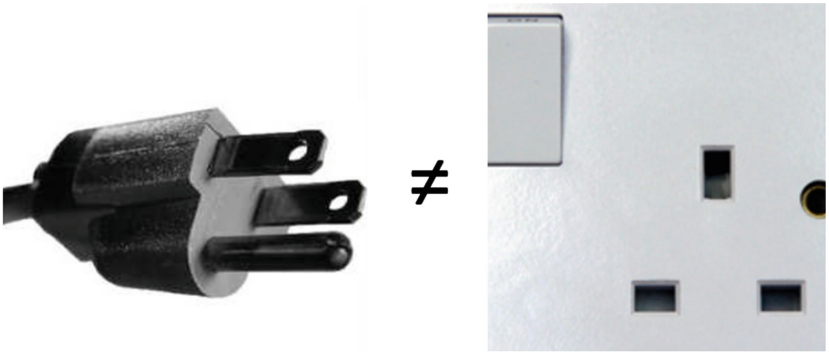
ASSERTION: All systems that need to share information require a formally defined message syntax.

Syntax cannot convey meaning and this is where semantics is introduced. Semantics derives meaning from syntactically correct statements. Semantic understanding itself is dependent on both pragmatics and context. Thus a statement such as "Patient-X has a heart-rate of 150 bpm" may be syntactically correct but has no practical role without understanding the context. Thus a heart-rate of 150 bpm for a 50-year old male riding a bike at 15 km/h up a 10% hill is probably not a health concern, but the same value when the same 50 year old male is at rest (and has been at rest for 60 min) is very likely a serious health concern. There are a number of ways of exchanging semantic information although the success is dependent on structuring data to optimise the availability of semantic content and the transfer of contextual knowledge (although the transfer of pragmatics is less clear).

ASSERTION: Semantic interoperability is essential to allow any machine based processing to be commonly understood across nodes in a network.

Underpinning the requirements for both syntactic and semantic interoperability is the further requirement of a common language. From the eHealth world it has become clear that in spite of a number of European agreements on implementation of a digital plan for Europe in which the early creation of 'e-health' was eagerly expected the uneven development of the digital infrastructure has in practice made for differing levels of initiative and success across the member states. These led to a confusing vocabulary of terms and definitions used by e-health actors and politicians alike. The meaning of the term e-health has been confused with 'tele-health' which in turn is confused with 'm-health;' 'Telemedicine,' a term widely used in the USA has been rejected in Europe in favour of 'tele-health.' There is general agreement that for these terms to be effective we need to redefine them in their practical context. Without an agreed glossary of terms, it will be hard to improve semantic interoperability - a corner stone for the effective building of e-health systems. The vocabulary is not extensive but at present it fails to address the need for clarity in exchange of information in the provision of medical services.

Finally we have to consider basic mechanical, electrical and radio interoperability. Quite simply a device with a power connector using, for example, a Type- IEC 60906-2 connection cannot accept power from anything other than a IEC 60906-2 connector. Similarly, for example, a serial port complying to USB-Type-A will not be able to directly interconnect with a USB-Type-C lead.



In addition to simple mechanical compatibility there is a requirement to ensure electrical interoperability covering amongst others the voltage level, amperage level, DC or AC, frequency if AC, variation levels and so forth. In the eHealth environment devices have to be able to interconnect and if wireless communication is deployed then it is obvious that the communicating end-points use the same means to communicate. In the radio sense this means sharing knowledge of frequency band, modulation technique, symbol rate, power, and so forth. The current Industrial Scientific Medical (ISM) band allocations are in this respect not strongly protected and many non-ISM devices use the ISM bands ("A" bands are allocated to ISM applications, "B" bands may be used by ISM and non-ISM applications). A consequence of the current management of the ISM bands is that knowledge of the frequency does not determine modulation waveform and vice versa.

Standards therefore enable and assert interoperability on the understanding that:

$$\text{Interoperability} = \textit{Semantics} \cup \textit{Syntax} \cup \textit{Language} \cup \textit{Mechanics}$$

Quite simply if any of the elements is missing then interoperability cannot be guaranteed. However we do tend to layer standards on top of one another, and alongside each other, and wind them through each other. The end result unfortunately can confuse almost as much as enlighten and unfortunately the solution of developing another standard to declutter the mess often ends up with just another standard in the mess.

However we can reasonably state that interoperability is the key to a solution where more than one stakeholder is involved and moreover that achieving interoperability requires standards. The nature of the standard is unimportant - it simply has to be accepted by the stakeholders. If the stakeholders are global and largely unknown then an internationally accepted standard is most likely to be the way forward. If, however, the stakeholders are members of a small local team the standard could be as simple as a set of guidance notes maintained on a shared file.

In the security domain understanding that we need interoperability is considered the default but simply achieving interoperability is a necessary but insufficient metric for making any claim for security. As has been noted above the technical domain of security is often described in terms of the CIA paradigm (Confidentiality Integrity Availability) wherein security capabilities are selected from the CIA paradigm to

counter risk to the system from a number of forms of cyber attack. The common model is to consider security in broad terms as determination of the triplet {threat, security-dimension, countermeasure} leading to a triple such as {interception, confidentiality, encryption} being formed. The threat in this example being interception which risks the confidentiality of communication, and to which the recommended countermeasure (protection measure) is encryption.

The very broad view is thus that security functions are there to protect user content from eavesdropping (using encryption) and networks from fraud (authentication and key management services to prevent masquerade and manipulation attacks). Technical security, particularly cryptographic security has on occasion climbed the ivory tower away from its core business of making everyday things simply secure.

6 Where to Go?

How do you get rid of fear and get acceptance of the threat model? Shared knowledge, shared understanding and willingness to educate each other about what we know and what we may not know. This is the only real way forward. This result is close to zero in boxes 2 and 3 and a bounteous box 1.

7 Conclusions

As stated in Sect. 6 of this paper the approach to getting rid of fear and get acceptance of the threat model is in the wider acceptance of shared knowledge, shared understanding and willingness to educate each other about what we know and what we may not know. The role of standards in giving assurance of interoperability as the key to a solution where more than one stakeholder is involved is difficult to argue against. The nature of the standard is unimportant - it simply has to be accepted by the stakeholders. If the stakeholders are global and largely unknown then an internationally accepted standard is most likely to be the way forward. If, however, the stakeholders are members of a small local team the standard could be as simple as a set of guidance notes maintained on a shared file.

Spreading of fear through a combination of movie plot threats and Chinese Whispers is an inevitable consequence of human curiosity and imagination.

Standards are at the root of sharing a common syntactical and semantic understanding of our world. This is as true for security as it is for any other domain and has to be embraced.

Acknowledgements. Contributions made by the author in development of this paper have in part been supported by EU projects i-locate (grant number 621040), SUNSHINE (grant number 325161) and UNCAP (grant number 643555).

References

[SANS] CIS Critical Security Controls, version 6.1. http://www.cisecurity.org/critical-controls/

[E-TVRA] ETSI TS 102 165-1. https://portal.etsi.org/webapp/WorkProgram/SimpleSearch/QueryForm.asp by searching

[CC] The Common Criteria. www.commoncriteriaportal.org

[JOHARI] Luft, J., Ingham, H.: The Johari window, a graphic model of interpersonal awareness. In: Proceedings of the Western Training Laboratory in Group Development, Los Angeles (1955)