Secure Connected Places Playbook
Cyber security resources for local authorities

Department for
Science, Innovation,
& Technology

Conducting a STRIDE-based threat analysis

Advisory

The Secure Connected Places Playbook is designed to meet the general cyber security needs of local authorities across the UK's four nations when integrating smart cities technologies. Whilst this guidance is appropriate to all local authorities there may be separate nation specific guidance and processes that should be considered.

Similarly, the resources within the playbook generally assume the local authority has control over technology policies and their implementation. Additional consideration may be required where this is not the case such as the interactions between combined and unitary authorities where one must collaborate and co-ordinate with other parties.

Executive summary

What is this resource?

This resource provides local authorities with a structured framework to better understand the risks that they are taking on with a proposed connected places technology.

How should I use it?

This guidance sets out how to conduct a STRIDE-based threat analysis workshop with your connected place technology suppliers. This STRIDE workshop format will help guide your local authority staff to ask probing questions of your suppliers and the solutions they provide. Doing so will help you understand the threats that might affect their systems and your connected places.

Who does this resource apply to?

The resource is targeted at connected places project managers and their supporting IT and cyber security staff. It can be used by project managers during project design and at regular points throughout the connected places project lifetime.

What will I get out of using this resource?

When designing and procuring connected places technologies, it is important to understand how they will behave at a systems level, i.e. beyond any individual deployed device. Systems often span internal organisations or partners. Therefore, understanding where data is likely to cross these trust boundaries, and what protections are in place, is necessary to know if a solution meets your authority's requirements.

For example, a frequently overlooked area is remotely supported supplier equipment. Performing a review of the proposed connected places solution may identify threats, like the possibility of trusted third parties' remote access being abused.

This STRIDE-based workshop format will help guide your staff to ask suppliers probing questions about their solutions to better understand the threats that might affect their systems. In connected places that operate under a shared responsibility model, these skills will help you to understand where the responsibility for controls should be retained by your authority.

THE ROYAL BOROUGH OF KENSINGTON AND CHELSEA

Case study: Royal Borough of Kensington and Chelsea (RBKC)

RBKC wanted to develop a consistent approach to understanding and communicating issues when designing and commissioning connected places projects. They already had established Information Security Information Governance and Risk Management functions, but they wanted to develop a process that would focus on the security posture of their connected devices at a granular level and engage all relevant stakeholders – business and technical alike. The STRIDE threat analysis resource has enabled RBKC to create a baseline set of resources to support their connected places initiatives. RBKC have now started to think about how they could create a dynamic view of connected places risks which would update regularly based on firmware updates or to showcase how the risk would be impacted by certain threat vectors.

Case study: South London Partnership (SLP)

South London Partnership
'Representing and connecting'

The South London Partnership used this STRIDE methodology to assess one of the connected technology devices they were deploying in the context of adult social care. They found that the STRIDE methodology enabled them to interrogate certain aspects of the data flow more effectively, and better understand the device's potential threats and impacts. Following the STRIDE analysis with the connected technology supplier, the South London Partnership were able to suggest improved procedures that would further bolster the system in their adult social care context.

See Appendix for more on these case studies and how this resource draws on the content of the NCSC's Connected Places Cyber Security Principles.

Contents

Introduction and definitions

What is a threat analysis?

A threat analysis is a structured and systematic process for reviewing how a system, service or process could be attacked, be that intentionally by malicious actors or unintentionally due to misconfiguration. The output of a threat analysis is the identification of a system's vulnerabilities and how they might be exploited.

Within connected places it is important to take a "systems approach" when conducting a threat analysis, which considers the interactions and relationships between a system's components across its lifetime. 'System' in this context is not just the product (such as a sensor being integrated) but the backend infrastructure, people and processes that it depends on, and vice versa.

Connected places may integrate many third-party services. Therefore, it is important to consider what trust and risk exposure is placed upon these.

Understanding the wider system is especially important in connected places due to the level of interconnectedness

What is STRIDE?

A structured, iterative methodology for identifying and assessing threats to a system.

STRIDE provides the mechanism to assess cyber threats within technology projects and gives teams an informed view of what technical risks they are managing.

STRIDE originated in industry to better understand the threats that arise when systems span trust boundaries.

Trust boundaries are the gaps created between entities that operate under different security policies. For example: between organisations (internal or external), suppliers and hosting providers.

STRIDE is advocated by the National Cyber Security Centre (NCSC) in their Connected Places Cyber Security Principles to assess and design systems architecture.

What does STRIDE stand for?

S	T	R	I	D	E
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege

Explanations and examples of these terms are presented later in this resource.

Why use STRIDE?

Whilst suppliers should (and do) care about security, this should not be relied upon when designing your local authority's security model.

Similarly, though a procured device may be secure, this does not mean that the system it is integrated into is also secure.

Procurement frameworks provided by Crown Commercial Services assess suppliers using the Cyber Essentials Plus accreditation. However, they do not review every individual product offered by suppliers. Therefore, it is important to conduct your own threat analysis.

A project team (in this case a local authority) asks questions of the supplier to understand how the system may be susceptible to threats from each aspect of STRIDE.

Our initial research discovered that many local authority staff assume that frameworks provide device security assurance.

How is STRIDE performed?

Rather than being a set workshop format with a strict agenda, the STRIDE methodology describes a process where the system designer (in this case a supplier of connected places technology or system provider) describes their design and a reviewer (in this case a local authority) holds a Q&A-led discussion structured around STRIDE's six aspects to try to model threats to it.

Asking yourself these questions will help to determine how your organisation should approach your STRIDE-based threat analysis activity:

1. Think about what connected places technologies or systems you want to perform a threat analysis on. STRIDE can be performed at a component or system level. You might want to review a small part of your connected place solution or the wholesale system.

2. Consider how much time your teams and suppliers have to engage with this process. Performing STRIDE on your wholesale connected places system will take longer than addressing small component technology parts.

3. Identify who will need to participate in the process. Typically no single person has all the knowledge or expertise to speak to a whole connected places system. Therefore, planning which team members will be available for each session will allow you to make the best use of each review.

After answering these questions, you should have a better idea of the scope of the STRIDE activity you wish to undertake and the resource it will require.

- If you're reviewing a wholesale solution, it can be useful to use a sprint-based approach to segment the analysis. Using this approach, you can break the solution into smaller component technology parts and review these in turn. This will allow for multiple sessions that are shorter in length (for instance 1 hour) and only involve people at relevant parts of the process.

- Or, if you have a simpler connected places solution with a small and consistent set of stakeholders, it might be quicker to use a traditional waterfall approach and review the whole system in one longer sitting (for instance a half full-day session).

Definitions and example questions to use in the STRIDE process are provided later in this resource.

Terms of reference

Due to differences in system scope and project budgets, terms of reference will be unique to each project. However, some general terms of reference for operating a STRIDE-based threat analysis assessment include:

Defining scope – what is the extent of the system, service or process under analysis?

Identifying stakeholders – who has valid inputs into the systems' design and needs to be involved in the STRIDE analysis? It is important to remember the supply chain aspect, for instance, your suppliers' suppliers and their interactions with the system.

Gathering relevant information - what systems architecture, deployment diagrams, processes and policies will you need to collect and who from?

Identification of threats – use the STRIDE methodology to analyse a given system, project or service.

Risk management – assess the probability and impact of a threat being exploited. If unacceptable, devise a treatment plan that brings the risk to an acceptable level.

Maintenance – connected places and their systems are living environments. Threat analyses and risk assessments should be reviewed regularly and also when a substantial change is made to the system.

Resourcing a STRIDE analysis

To conduct a STRIDE analysis, it is important that the person leading the review has the following skills:

1 **Communication skills** – the inputs of the review can be quite technical. These will need to be translated and communicated into findings and recommendations.

2 **Basic understanding of security terms and concepts** – understanding how confidentiality, integrity and availability relate to a system's security and the threats to it. Technology teams can assist project managers on this.

The person who leads the review is not expected to be an expert in cyber security or the solution being reviewed. Having the right people attend and knowing who to call on for answers is crucial.

3 **Analytical skills** – based on provided documentation and discussion with the systems' designers, they will need to apply their knowledge of security concepts and how they might be exploited within the given system.

4 **Collaboration skills** – STRIDE analyses require working with many stakeholders across internal and external teams; understanding how to work within a team and get the best out of others is essential. Having the skills to interpret accidental or purposeful misdirection, assumptions in lieu of facts, or technical expertise is highly recommended.

Additional resourcing needs

In addition to the project manager who is leading the STRIDE analysis, depending on the nature of the project, the following (non-exhaustive) list of roles will need to be consulted.

Depending on the operating model of the project, these roles may be either authority or supplier staff:

Network Administrator – if the solution makes use of local authority networks, they may have specific requirements and considerations for the analysis.

Security Officer – who can advise whether the proposed design meets your authority's standards.

Cloud/DevOps staff – where the solution requires some hosting by your authority they can advise if it meets their architectural requirements.

Software Developer – someone that can advise on how the software operates and how the API calls are made and secured.

Hardware Developer – someone that can advise on how the hardware operates and any protections it may have to safeguard sensitive credentials.

STRIDE Responsibility Assignment Matrix (RACI)

	Responsible	Accountable	Consulted	Informed
Cabinet / Elected Members		✕		
Governance Board (CPSSG)		✕		
Risk Management and Audit				✕
Project Manager	✕			
Network Administrator			✕	
Security Officer			✕	
Cloud/DevOps staff			✕	
Software Developer			✕	
Hardware Developer			✕	

The above assumes that such reviews are convened by the project management for a given deployment, however the review could equally be the responsibility of the security organisation where they are appropriate resourced to do so.

Vulnerability disclosure and management

Before conducting a threat analysis of a connected place system, your local authority and your suppliers should:

1

Understand that a vulnerability being discovered is not a formal security incident/project management issue. Instead, it should be considered a project management risk. If there is evidence the vulnerability has been exploited, then it should be considered a security incident and a project management issue.

Please review the Procurement and Supply Chain Management resource for further support on supplier relationship management.

2

Operate a vulnerability disclosure process allowing the public to "responsibly" report vulnerabilities, mitigating the reputational damage of "full disclosure".

3

Have a vulnerability management policy and process to discover and respond to vulnerabilities.

4

Have a legal framework within which vulnerabilities can be disclosed and responses co-ordinated.

The National Cyber Security Centre provides a vulnerability disclosure toolkit. It includes materials for the public and security community to securely disclose details relating to a vulnerability.

Providing a public means for disclosure

Connected Places by their very nature operate in an exposed environment, where members of the public and other well-intentioned individuals may investigate what these devices are and how they operate. It is therefore likely that individuals may find systems that are vulnerable and seek to inform the local authority of their discovery.

An approach to solving this problem of vulnerability disclosure and identifying whom to contact is being advocated across UK government. This approach is known as "security.txt" or RFC9116.

It involves defining a security policy, publishing it and providing a point of contact to report vulnerabilities. This is achieved by creating a text file and placing it on the authority's web site under a fixed location.

The following website provides details on how to implement the process: securitytxt.org

By providing a means for individuals to report vulnerabilities it can enable each authority to continue to provide secure services to the public. In contrast, by not providing a means to contact the authority, in the best case vulnerabilities remain unknown and in the worst case the authority risks reputational damage by an individual publishing details of their discovery.

Systems modelling

Systems modelling

STRIDE concentrates on modelling threats to systems. Therefore, systems modelling is essential to communicating and understanding the design of a system and is a key step before the STRIDE analysis can begin.

STRIDE assessments are best served with good systems documentation and diagramming that provide detail on what components make up the solution and how they integrate together.

Unified Modelling Language (UML) and data flow diagrams provide a standardised language to communicate. However try not to be too rigid. An ad-hoc box and line diagram will still provide better clarity than nothing.

A common language between the designer and assessor, such as UML, reduces ambiguity and allows assumptions about the security of the system to be identified, challenged and corrected.

System modelling aids in the identification of trust boundaries (the gaps created between entities that operate under different security policies) and what controls may, or may not be, present to protect these data flows.

More mature authorities may wish to more formally model their systems using frameworks such as TOGAF (The Open Group Architecture Framework) in order to integrate the design within their wider Enterprise Architecture practice.

STRIDE

The following section explains what the six aspects of STRIDE are and provides example questions that could be asked of a supplier to identify whether threats exist within the connected places solution.

The section finishes with definitions of mitigations for each class of threat.

S

Spoofing

How do we know who is sending us data?

- Do we authenticate users / devices?
- What data can users / devices submit?

Can someone pretend to be someone else?

- Do we authenticate, if so, is it only at the system boundary?
- How well do we protect sensitive credentials on systems?

In the case of a smart parking solution, can a user spoof a sensor, falsely providing their entry/exit times resulting in lost revenue?

T

Tampering

Can someone modify what they submit?
For example:

- Is the integrity of data validated using hashes, message authentication codes, or digital signatures?
- Is it understood what unique properties each of the three above controls offer?

Can someone break a trust boundary and cause changes?
For example:

- Are inputs validated before being processed? If not, then an attacker may be able to exploit vulnerabilities in the processing and tamper with the system.

It is essential to know your local authority’s desired business outcomes and how these can be affected.

R
Repudiation

Can an action be associated to a unique identity? For instance, can someone or something perform an action and deny that it was them who performed it? For example:

- If a sensor reading is authenticated using symmetric cryptography, it would not prove whether the sender or receiver sent the reading. Compare this to a digital signature of the reading, which would prove which end of the communication was the source.

In the case of smart lighting, can a criminal request cause lighting to be switched off in an area of town to provide cover for their actions and deny they were the requestor?

I

Information disclosure

Can others access information they should not have access to? For example:

- Is data communicated in an unencrypted form?
- Does it utilise weak encryption or is the handling of cryptographic material, such as keys or the data from which keys are derived, poor?
- When someone changes role or leaves an organisation is their access removed?

With an in-home health monitoring system, can someone within range see the unencrypted data and know who the data relates to?

D

Denial of service

Can someone affect a system to degrade the ability of others to use it? For example:

- How well protected is the system from an internet-based denial of service?
- How resilient is the IoT network to radio frequency jamming?
- Are system inputs validated to ensure that a maliciously crafted input cannot cause the application layer to become unresponsive?

In a smart transport system that provides e-scooters, can a user make many reservation requests and deny other users access to their means of transport?

E

Elevation of privilege

Can an unprivileged user/process gain access beyond their established permissions? For example:

- Can they gain access to shared memory/storage where administrator credentials may be stored or hashed?

In an environmental monitoring scenario where the authority allows its citizens to connect their own sensors to its IoT network - can a citizen impersonate an administrator through the user interface and remove other users?

Mitigations

When threats are identified in the system they should be risk assessed and managed. If your local authority determines that a risk should be mitigated, then each of the threats in STRIDE can be addressed with the following high-level mitigation categories. As risk assessment is a regular process, these mitigations may be applied to reduce residual risk during procurement or operation. Mitigations during operation should be discussed and agreed upon with your supplier.

	S	T	R	I	D	E
Threat:	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Mitigation:	Authenticity	Integrity	Non-repudiation	Confidentiality	Availability	Authorisation

Risk assessment

Risk assessment

The initial outputs of a threat assessment will be abstract - they will not have an assigned probability or impact, and therefore will exist as an unknown risk.

Some threats may only be exploitable by well-funded state actors, while others will not be relevant due to existing mitigations that sit outside of the threat analysis. However, some threats may be easily exploited for instance, they could be hosted on a weakly protected internet-facing system where there is limited vulnerability management, and therefore easily subjected to a ransomware attack.

The next step of conducting a risk assessment process is necessary to understand the probability and impact of identified threats. Doing so allows you and your authority to make informed risk management decisions.

Please review the Governance in a Box resource for further support on risk management.

Summary and next steps

Conducting a STRIDE-based threat analysis: summary and next steps

1

Key take aways

Completing this resource should help you to understand why threat analyses are important when delivering connected places projects.

It should also equip you with a framework to assess threats that arise from connected places technologies.

2

Questions to ask

Do we have an appropriate understanding of what threats our connected places face?

Do we understand where our data flows in connected places projects, who owns those other systems and what trust relationships we want with those parties?

3

Next steps

Utilising this resource will provide you with the methods to assess how your connected places solutions are designed and whether their risks are appropriately managed.

This process should be performed regularly to ensure that risks arising from changes in threats are identified.

Consult the Procurement & Supply Chain Management and Governance in a box resources for more information on risk management.

Appendix

Example implementation

Case study: South London Partnership (SLP)

South London Partnership
'Representing and connecting'

Need:

Adult social care at the South London Partnership is transforming with the analogue to digital switch - telecare devices are being recommissioned and there is an influx of novel Internet of Things (IoT) devices and solutions. With more adult social care services utilising novel connected places technologies, both sensors and cloud-based services, it is important to understand the potential cyber threats and risks to residents and councils. There is a need for security triage to be done by more officers. Using a resource such as STRIDE makes it easier to understand threats and where they can come from.

Solution:

The South London Partnership used this STRIDE methodology to assess an IoT device which is being trialled in the context of adult social care. These devices are currently being used in vulnerable residents' homes around Sutton as a secondary, passive way to monitor the well-being of residents. These devices are being considered for inclusion in business as usual, therefore advanced threat and risk analysis was required.

Outcome:

The STRIDE methodology enabled the South London Partnership to interrogate certain aspects of the IoT device's data flow more effectively and better understand the potential threats and impacts. They found that STRIDE was a useful tool to approach threat analysis, especially for staff members who are not accustomed to these types of investigations. It also helped them to target questions and root out potential problems with their IoT supplier.

Following the STRIDE analysis with the IoT supplier, the South London Partnership were able to suggest improved procedures that would further bolster the system in their context if it moved into business as usual.

Example implementation

Case study: Case study: Royal Borough of Kensington and Chelsea (RBKC)

THE ROYAL BOROUGH OF
KENSINGTON
AND CHELSEA

Use case(s):

Community safety, environmental management, smart lighting, air quality, traffic monitoring, footfall monitoring, social care, transport management

Need:

Sheffield City Council are enhancing their Adult Social Care Technology Enabled Care Service to RBKC wanted to develop a consistent approach to understanding and communicating issues when designing and commissioning connected places projects. They already had established Information Security Information Governance and Risk Management functions, but they wanted to develop a process that would focus on the security posture of their connected devices at a granular level and engage all relevant stakeholders – business and technical alike.

Solution:

RBKC used the STRIDE-based threat analysis and Cyber Security Principles 101 resources to create a business level playbook that mapped the technical detail needed so that business stakeholders were able to participate fully in the design and commissioning of secure connected places technologies. They have also used the STRIDE based threat analysis resource to improve the assessment and modelling of their security threats in their extended supply chain.

Outcome:

The STRIDE threat analysis resource has enabled RBKC to add value and efficiency to their connected places projects by providing a baseline set of resources to support their connected places initiatives. It helped them to engage a wider range of relevant stakeholders for projects so decisions can be made quicker, and risks can be fully quantified with the appropriate expertise. RBKC have now started to think about how they could create a dynamic view of connected places risks which would update regularly based on firmware updates or to showcase how the risk would be impacted by certain threat vectors.

Example implementation

Case study: Sefton Council

Use case(s):

Air Quality Monitoring

Need:

Sefton Council was developing its connected places networks across various work streams including Environmental Health and Highways. They used Air Quality sensors and cloud-based services to provide information on air pollution levels and traffic flows. Sefton Council wanted to enhance the understanding of connected places projects across business and technical stakeholders to ensure there was an awareness of the threat landscape. Without this understanding, a joined-up approach to these projects would not have been possible and it could have led to an over-reliance on suppliers.

Solution:

The STRIDE resource was used to create an ICT security questionnaire for use in the procurement process for Air Quality sensors. Specific cyber security questions were included to ensure a sufficient threat assessment and enable the project lead to understand the potential threats and controls that could be applied to a connected places network.

Outcome:

The questionnaire will form the basis of Sefton Council's procurement procedure rules and will apply to all procurement of connected places systems and sensors in the future. This will enable a sufficient STRIDE-based threat assessment to be undertaken and provide guidance to all key stakeholders – technical and business to ensure a robust cyber security assessment process for their connected places projects.

Example implementation

Case study: Coventry City Council

Use case(s):

Very Light Railway (VLR) System, Traffic Management

Need:

Coventry City Council are implementing a Very Light Railway (VLR) transport system. The project will involve multiple control and safety systems to create an innovative track design and vehicle which will deliver an affordable light rail system for Coventry and beyond. Coventry City Council did not have an equivalent STRIDE analysis process although they did have security principles embedded in their digital procurements.

Solution:

As Coventry City Council worked through the STRIDE analysis resource, they identified areas within digital services which could be improved with greater control and security. Combining this with the Cyber Security Principles 101 resource enabled them to embed secure principles and guidance into their VLR project.

Outcome:

The STRIDE analysis will now also be added to their procurement process as part of their wider project management activities. The Council was able to identify areas of concern that would not have been picked up were it not for going through the STRIDE resource. Furthermore, as a result of sharing the Cyber Security Principles 101 resource with their connected places teams, the awareness of the need for the security of connected places products has increased with 90% of attendees now understanding the need for secure connected places with the remaining 10% keen to learn more to enhance their learning. Ultimately, the Council have been able to use the resources to help them ask the right questions when purchasing, implementing and the ongoing management of connected assets to enable the better management of cyber risk and financial resources in public spaces and cities.

Glossary of terms

Term / acronym	**Definition**
Asymmetric cryptography	A subset of cryptography where sender and receiver can communicate securely through using different keys unknown to each other
Authentication	The proof of information having integrity
Authorisation	The specification of access rights to an object by a subject
Availability	The property that information can be used when and where needed
Confidentiality	The property that information is not disclosed to an unauthorised party
Digital Signature	A keyed hash which provides guarantees of the author
Encryption	The use of cryptography to protect the confidentiality of information
Hash	The output of a cryptographic function which provides integrity of the input it is generated from
HMAC	A keyed hash which provides guarantees that the author must have had access to a shared key
Identity	An identifier that uniquely represents a user, machine or process
Integrity	The property that information cannot be tampered with
IoT	The Internet of Things describes physical objects with sensors, processing ability and software that connect and exchange data with other devices and systems over the Internet or other communications networks'
Repudiation	The ability for a claim's author to deny its validity

Glossary of terms

Term / acronym	Definition
Resiliency	The property of a system remaining operational
Symmetric cryptography	A subset of cryptography where sender and receiver can communicate securely using the same shared key
Trust boundaries	The gaps created between entities who operate under different security policies. For example: between organisations (internal or external), suppliers and hosting providers.

NCSC Principles coverage

This key depicts where this resource draws content from the following principles of the NCSC's Connected Places Cyber Security Principles

Focus: The guidance provided in this resource will help you to understand your suppliers' role and manage your supply chain throughout your connected place's lifecycle.

Gaps: There are some gaps in the principles around understanding and designing the connected place, but there is broad coverage given the end-to-end lifecycle nature of this tool.

■ Fully aligns with the Principle

□ Does not align with the Principle

Understanding your connected place

#1 Understanding your connected place and the potential impacts	□
#2 Understanding the risks to your connected place	■
#3 Understanding cyber security governance and skills	□
#4 Understanding your suppliers' role within your connected place	■
#5 Understanding legal and regulatory requirements	□

Designing your connected place

#6 Designing your connected place architecture	■
#7 Designing your connected place to reduce exposure	■
#8 Designing your connected place to protect its data	■
#9 Designing your connected place to be resilient and scalable	■
#10 Designing your connected place monitoring	■

Managing your connected place

#11 Managing your connected place's privileges	■
#12 Managing your connected place's supply chain	■
#13 Managing your connected place throughout its life cycle	■
#14 Managing incidents and planning your response and recovery	□

Secure Connected Places Playbook
Cyber security resources for local authorities

Department for
Science, Innovation,
& Technology

Please contact secureconnectedplaces@dcms.gov.uk with any questions or feedback on these resources.

This Playbook was produced in collaboration with:

plexal DAINTTA Configured THINGS