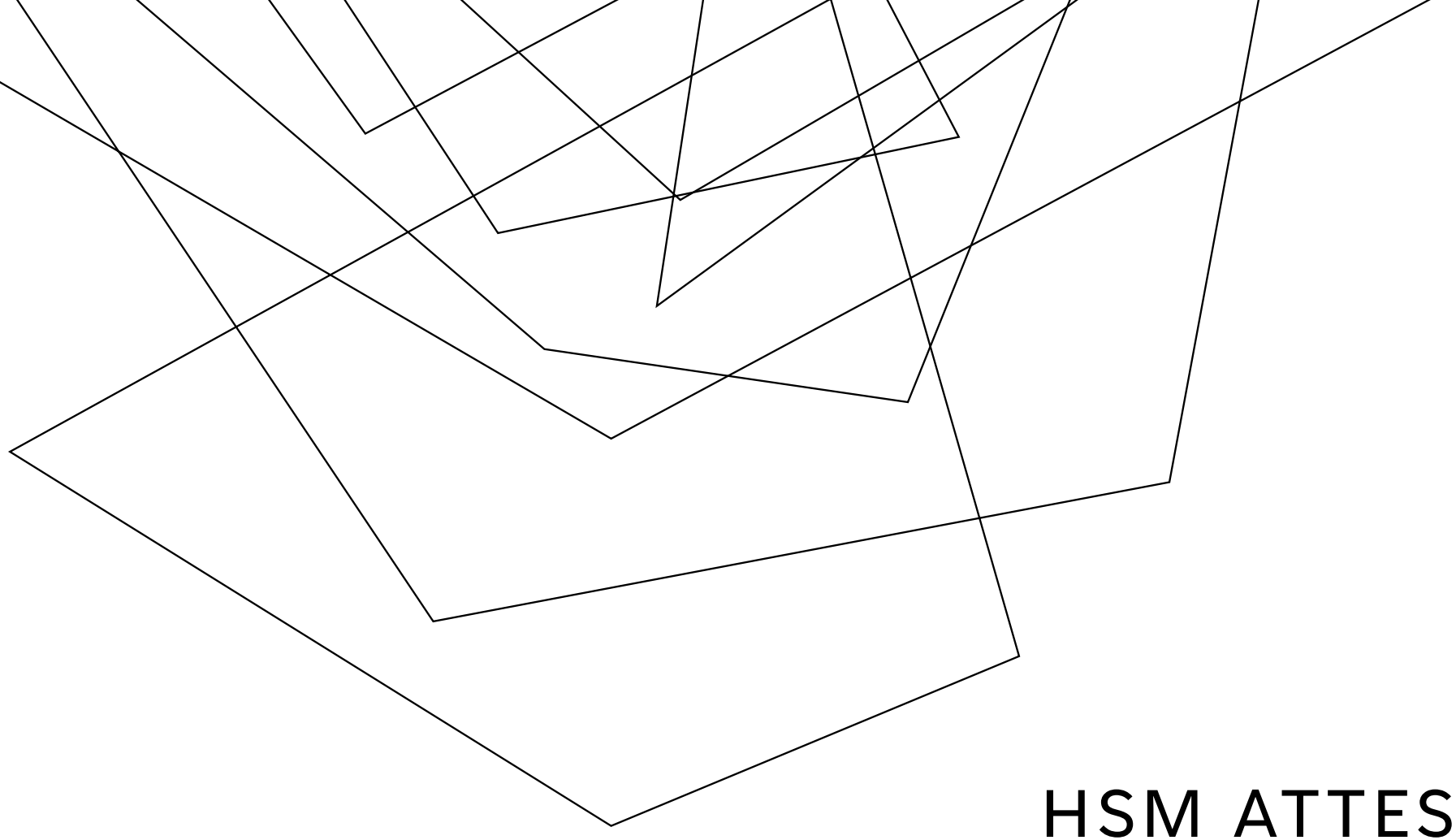


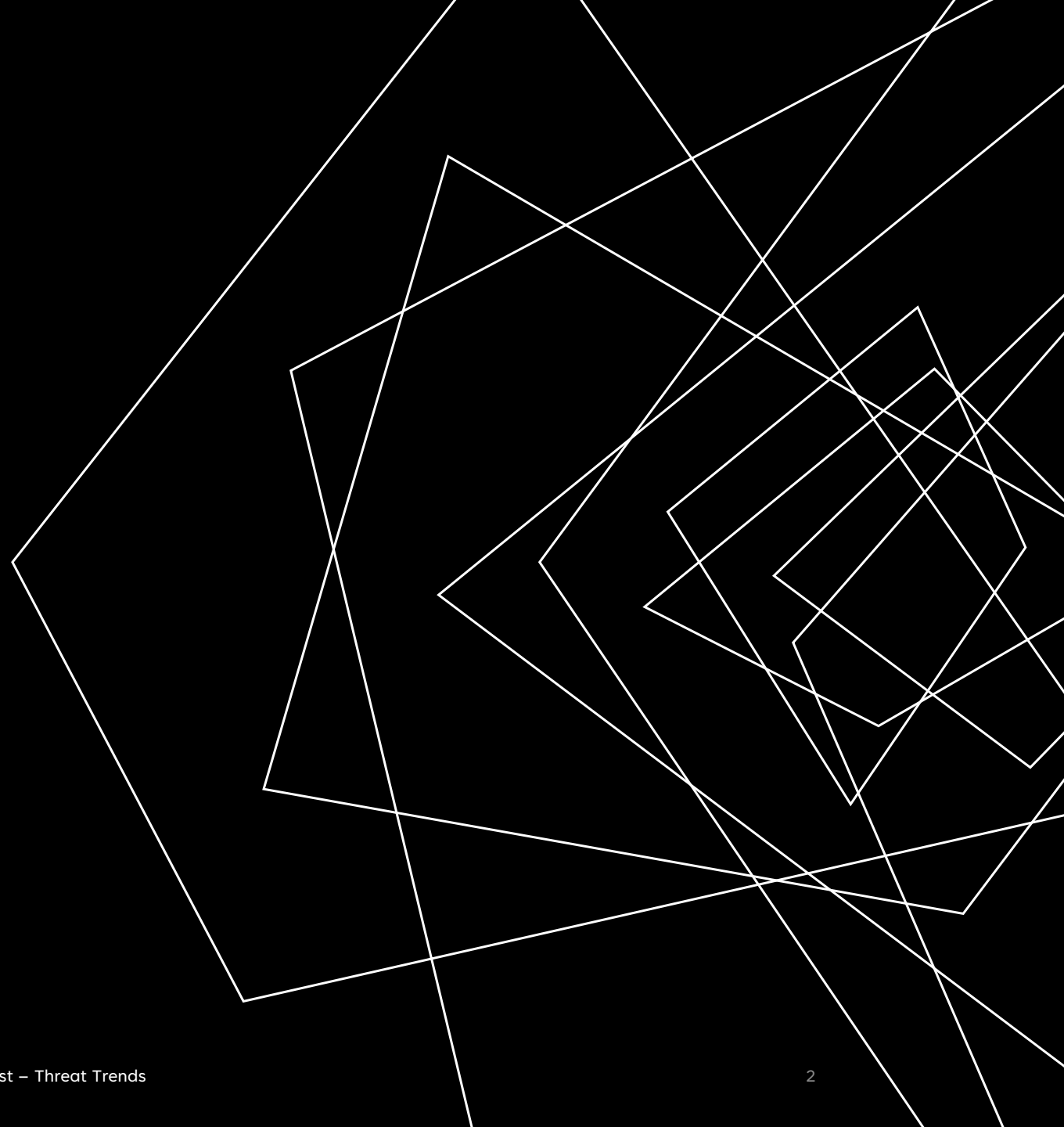
HSM ATTEST: TRENDS IN THREATS

Chris Cracknell

ABOUT HSM ATTEST

This presentation describes the current Trends in Threats to modern systems and is part of a series of presentations introducing HSM Attest.

HSM Attest is a security solution focussed on Transparent, Granular and Enforceable Governance to protect the most critical security artefacts in a system.



PROBLEMS, PROBLEMS...

HISTORICAL

Security focussed on perimeter measures; Once through the perimeter (VPN, Connector HW, secure access portals...) onto the internal environment then all actors were assumed to be trustworthy (Implicit Trust). With this in mind threats and associated mitigation focussed on endpoint security.

SOURCES

The OWASP Top 10 Threat list and its' historical development is an excellent initial source for information about what is actually happening in the field. The most recent is 2021.

Experience and news reports of individual cases are also taken into account.

TRENDS

The perimeter security model is increasingly being compromised through internal attack vectors such as insecure design, failed governance and insecure development and operations. Increasingly the threat is not to steal general access but to steal the results of having access, e.g. the money...

IMPACT

The consequences of a Perimeter breach for a system relying on a hardened perimeter are potentially huge, impacting the entire system through a single failure.

Relying on Perimeter Security makes migration to cloud hosting untenable.

TYPES OF BREACH

Secret Exfiltration

Secrets are exposed to attackers. These could be used to stage further attacks, embarrass the system owner or exploited directly (see Data Theft)

System Manipulation

The internal state and behaviour of the system can be manipulated to provide advantage to an attacker. E.g. issue a false access token, revoke a legitimate user, attack personal data or customers, change system date to allow use of expired artefacts...

Data Theft

Working Data from the system is exfiltrated. This is usually a mass exfiltration and the data is either directly exploitable (e.g. Credit card info) or can be harvested for Metadata exploits.

Third Party target

The direct ill effect of a breach is not targeted at the system itself but at some other goal, e.g. Metadata attacks used to deanonymize a health record or data that can be used to exploit some other system (e.g. password to email address, social engineering background info).

RISING THREATS

Failed Governance

Operations being allowed that should not be. Broken access control, failed Authentication or Authorisation operations. Some actor being able to do something not intended by the design.

Failed System Integrity

Compromised software images or configuration used in the productive system. The system is not running the software and configuration that is intended in the design.

Insecure Design

Fundamental weaknesses in the design allowing behaviour inconsistent with the System goals.

Failed Security Reactions

A breach or potential breach is allowed to escalate due to not noticing it early and/or reacting appropriately.

SPECIFIC THREATS

The OWASP Top Ten list includes some specific technical threats that are well understood, but very prevalent in the marketplace. These are part of what would normally be considered known vulnerabilities but are common enough in the field that they merit special attention. Do not include these in new development, eliminate them from old development and do not pull dependencies known to include them.

Injection

Both SQL, XML and all other variations on this theme. These are addressed by cleaning all inputs to a system (not just web form data entry fields...) before using them. Tattacks based on these are reducing compared to previous OWASP lists where they long held position #1.

Server Side Request Forgery

New to the OWASP List in 2024, this affects server-side systems that invoke URLs on other servers. Attacks manipulate the target URL or the results of that URL to affect system behaviour. This becomes increasingly relevant as system interdependence grows.

FAILED GOVERNANCE

OWASP 2021 #1, #7

Operations being allowed that should not be.

- Broken access control. The implementation does not properly enforce the designed access controls.
- Failed Authentication. The system fails to reliably identify an actor.
- Failed Authorisation. The system inappropriately assigns access rights to an actor. This can be by technical error, by process or by design.
- The above applies to the Governors themselves, who can act falsely – either by malice, error, blackmail or identity theft.

FAILED SYSTEM INTEGRITY

OWASP 2021 #5, #6, #8

The system is not running the software and config that is intended in the design. Compromised Software Images or Configuration are run in the final Environment.

- The products of the build and deployment pipeline are manipulated on their way to the productive environment.
- Vulnerable and outdated components are included in the deployed images (software supply chain “SSSC”). Note that this was the cause of the largest and costliest security breaches ever (epsilon, Equifax, Log4j).
- Security Misconfiguration. Components are not configured according to the principle of least privilege. Often this takes the form of unchanged default configurations being used productively.

INSECURE DESIGN

OWASP 2021 #2, #4

Fundamental weaknesses in the design allowing behaviour inconsistent with the System goals. Usually derived from:

- Failure to place Security at the centre of the software development lifecycle, (“Secure SDLC” – “SSDLC”)
- Inadequate training of architects, engineers and operators.
- Failure to consider Security from the start and at all other stages of the design and development process.
- Failure to include security quality gateways in the SSDLC. i.e. Review, TEST, Test, test...
- Inappropriate or poorly communicated security design decision - a failure to properly understand the Security requirements, especially for Governance, and then failure to cover them in the design.

FAILED SECURITY REACTIONS

A breach or potential breach is allowed to escalate due to not noticing it early and/or reacting appropriately . This is known as “SIEM”.

- Security Logging (recording data) and Monitoring (checking the data that has been recorded) must be suited to spotting attacks and threats in a timely manner. Logging may or may not be linked to system requirements for Auditing.
- Inappropriate Reactions to a threat. This could be:
  - Ad-hoc reactions, i.e. no reaction has been planned for this event
  - Denial – attempts to cover up and pretend that the breach did not happen. This may be combined with:
  - Failure to act to close the breach or prevent further exploitation.
  - Failure to investigate and address root cause of event.
  - Failure to communicate with affected parties, especially third parties. (This is usually a statutory as well as a moral duty.)
- Failure to prevent manipulation of the SIEM system itself as part of an attack.

SUMMARY
Then and Now:

OLD WORLD

Security and threats focus on the perimeter of systems, usually endpoints and logon mechanisms.

A breach of the perimeter, e.g. access to the internal network, means a complete breach of the whole system.

There is an implicit assumption that insiders can be trusted.

NEW WORLD

Threats come from inside the system perimeter. Either by classical endpoint compromise as above or, increasingly, through insider attack vectors:

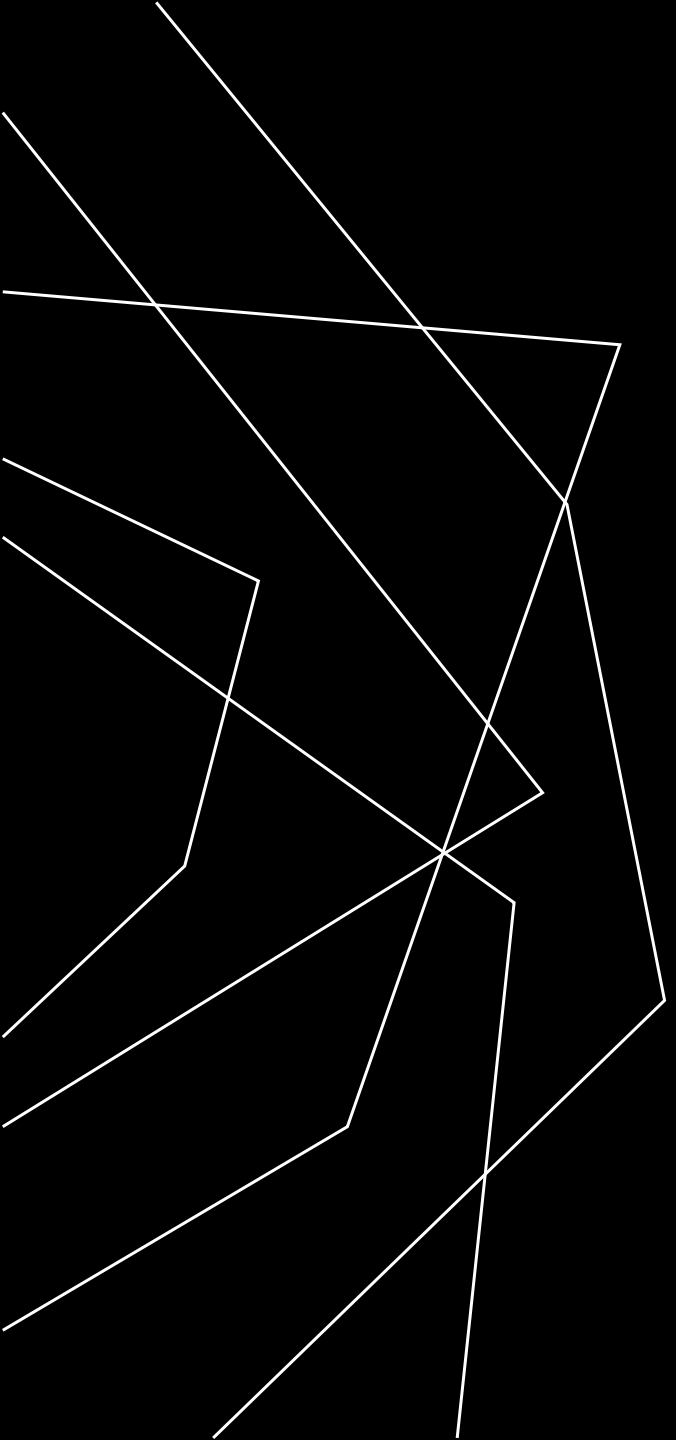
- Failure of System Design meaning that the system is not suited to fulfil the requirements.
- Failure of system delivery meaning that the running system is not what it should be. Here one component may be the attacker of another.
- Failure of Governance allowing failures of authentication, authorisation and access control enforcement.
- Failure of Logging and Monitoring allowing breaches to be extensively and damagingly exploited.

WHAT TO DO?

The follow up presentation :

- HSM Attest – Trends in Security Measures

describes how the IT Ecosystem is reacting to these changing threats.



THANK YOU

Chris Cracknell

+49 176 7087 7764

chris@cracknell.de