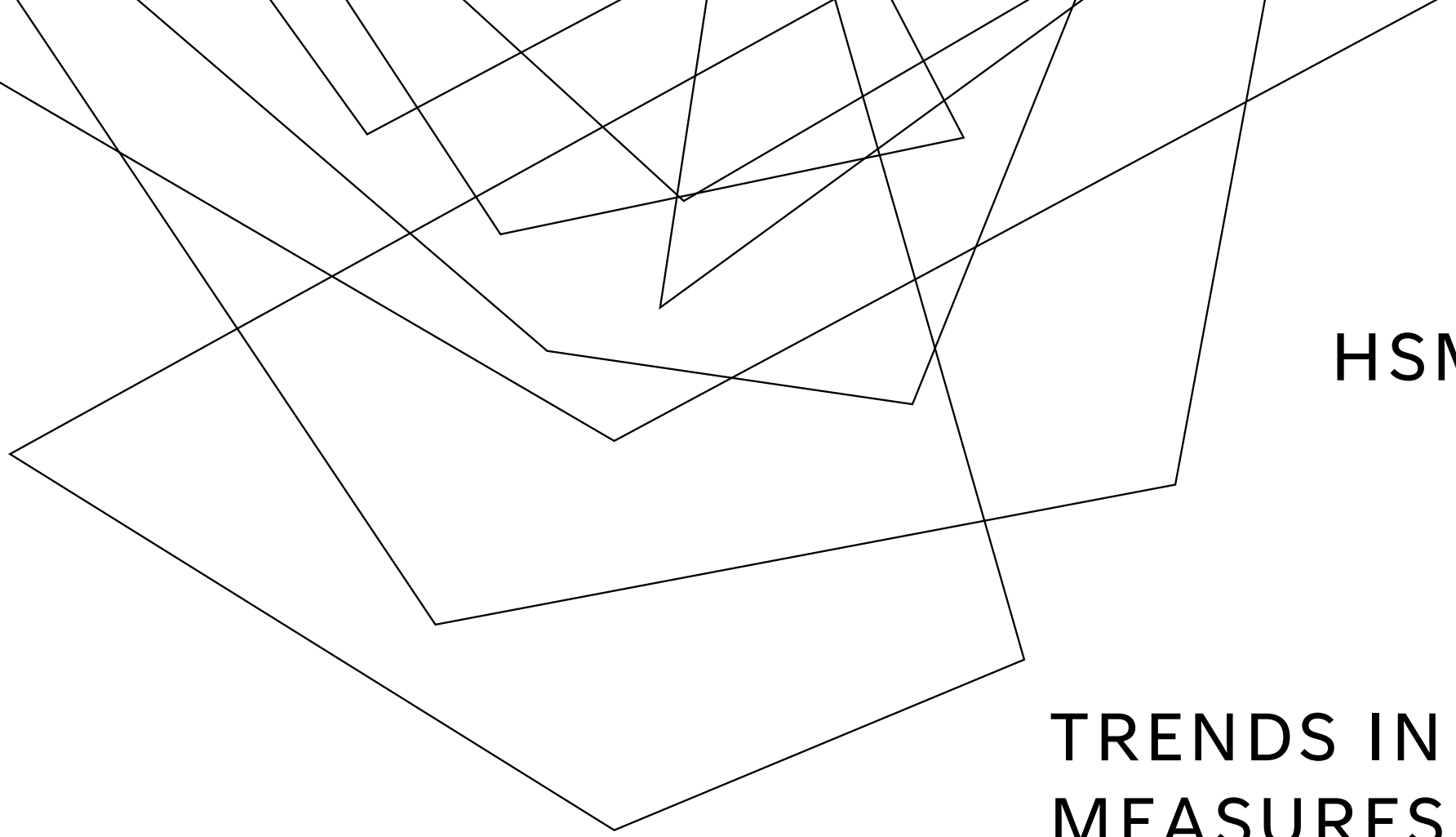


HSM ATTEST

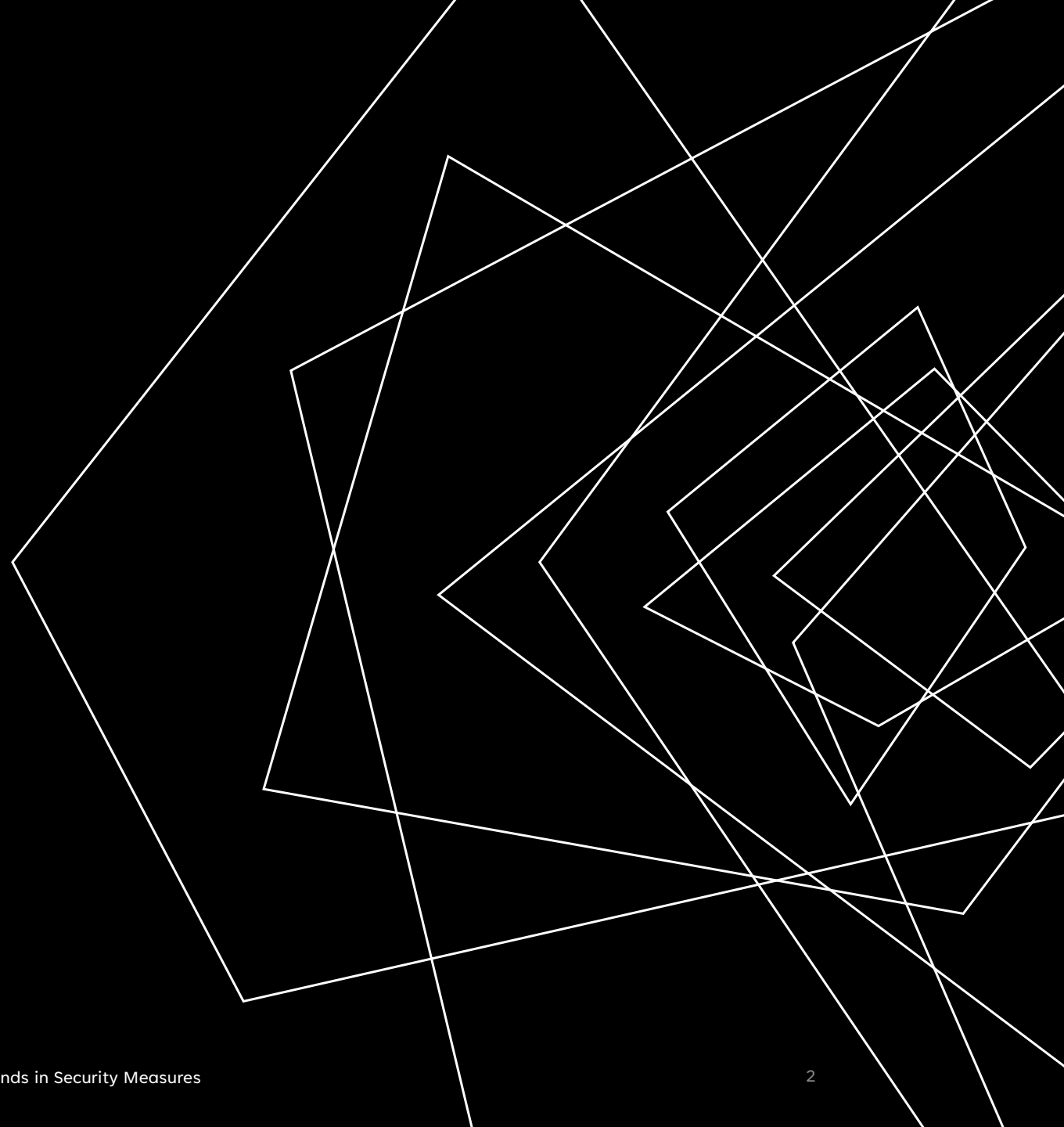
TRENDS IN SECURITY MEASURES

Chris Cracknell

ABOUT HSM ATTEST

This presentation describes the current Trends in Security Measures used in 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.



© Chris Cracknell 2024

HISTORICAL

Security was 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, threat awareness and associated mitigation were focussed on endpoint and perimeter security.

TRENDS

- The hardened perimeter security model is being replaced with hardened structure – internal system components do not trust each other without cause. ("zero Trust", "zero Implicit Trust")
- Security Planning is taking a much more up-front role in system delivery. There is a recognition that security must be holistic – i.e. covering all aspects of system delivery from requirements to analysis to design to implementation to deployment to operations to update cycle to end of life...
- Security is being integrated into the software delivery chain to prevent questionable workloads from being deployed and trusted.
- There is an increased focus on transparent and specific Governance.
- Secure Operations are being emphasised with formalised SIEM processes.
- Confidential Computing is growing as a means of achieving the above.

SOLUTIONS...

© Chris Cracknell 2024

TYPES OF MEASURES

Conceptual

- Identifying what in the system needs to be protected, how strongly and how we are to protect it.
- Specifying how we will construct the system to achieve this.
- Specifying how we will prove that the measures are implemented, active and working.

Technical

- Select and use appropriate system stacks. (HW & SW)
- Select and use appropriate tooling, e.g. dependency scanners, Confidential Computing, SIEM.
- Relate technical measures to the security goals they are meant to achieve.

Organisational

- Construct, implement and maintain processes to create the initial and manage the ongoing security of the system.
- Acquire, train and retain appropriate personnel
- Implement controls to assure compliance with Processes.

Governance

- Specify and use comprehensive, transparent and enforceable Governance for every element of the system that is part of the final productive system.
- Every security decision must be auditable back to a specific event where that decision was taken by an identifiable group of people entitled to make it.

© Chris Cracknell 2024

HARDENED STRUCTURE VS PERIMETER – "ZERO TRUST"

Better called: "Zero Implicit Trust".

Internal components do not trust each other without a reason to do so. This means components must:

- Identify other components with which they interact both inside the system as well as outside.
- Decide whether to trust other identified components according to a set of rules...
- ...created by Governance Decisions...
- ...and applying to specific operations

There are a variety of mechanisms that can be used to identify other components; from passwords through shared secrets such as mTLS, up to attestation and measurement methods supported by hardware (TPM, SGX, AMD/SEV...)

Trust can also be defined at different levels of detail, for example, the right to open a session for a limited period of time and use it to access an API on the client. Or the right to carry out a specific operation a single time, such as a cryptographic signing. Or even, a general access to a whole application front end.

© Chris Cracknell 2024

SECURITY PLANNING

Security is NOT an after-market bolt-on...

It is recognised that modern security can only be achieved by:

- Including security in every step of the software delivery process. And by ...
- Covering the whole system (“holistic” security)

Some, but by no means all, areas to be included in planning:

- Top level security concept – what is to be protected, how much and how.
- Security in the software supply chain; dependencies, skillsets of developers, process quality gates for security.
- Deployment management; repositories, secret provisioning, change control boards.
- Operational monitoring, reporting and reactions. (SIEM)
- Governance processes
- Auditing

© Chris Cracknell 2024

SECURE SUPPLY CHAIN

Often described as SSSC “Secure Software Supply Chain” though it should actually be extended to platforms and hosting as well.

At its’ simplest, this means knowing and having control of all inputs to your productive system, including toolsets, external dependencies (open source?), internal developments (See next slide on SSDLC) Infrastructure (IaaS?). Areas include:

- External software dependencies. Software stack, third party libraries and tools. Do not just blindly pull the latest from the web.
- Internal software. Strong processes mandating security at all stages of design, development and devops. See SSDLC on next slide.
- Partner organisations. They need to be organisationally aligned with your security goals and methods.
- Quality gates including production-near test deployments.
- Integrated Governance. Progression of build artefacts through to deployment with authorisation at appropriate steps.
- Software integrity. Ensure that system artefacts cannot be manipulated on their way to the final system. Use SBOMs, signatures...

© Chris Cracknell 2024

GOVERNANCE

Governance is the process by which decisions affecting the (security of the) system are made, enforced and checked, including the revocation of previous decision. Organisations are becoming increasingly aware of the importance of getting this right.

- Transparency. It must be clear at all times, where, when and by whom a security relevant decision was made.
- Appropriate. Governance processes must support the goals of the security plan but no more.
- Usable. It must be easy for Governors to make informed and correct Governance decisions.
- Rigorous. Governance must cover all aspects of the system, including the management of the governance processes and plan themselves. Note, this makes it unlikely that a single mechanism of governance will cover everything.
- Enforceable. Technical and organisational means to ensure that Governance decision are active.
- Verifiable. Monitoring and Auditing processes must be in place and used to verify that Governance has been applied according to the plan.

© Chris Cracknell 2024

SECURE OPERATIONS

The operation of a system from Day 2+, i.e. after the initial project setup, must planned, staffed and enforced to cover at least:

- Physical and technical access controls for the hardware, software and other infrastructure hosting the system, including the update and maintenance cycles.
- Security Logging (recording data) and Monitoring (checking the data that has been recorded) in order to detect and react to threats as early as possible.
- Planned-for security reactions to foreseen events, with play books and service level commitments, including at least:
    - Closing the breach to prevent further exploitation.
    - Investigating and addressing the root cause of the event.
    - Communicating with affected parties, especially third parties. (This is usually a statutory as well as a moral duty.)
- Support Auditing. This may or may not be piggybacked off the Logging system. It is critical that the Audit log is protected from manipulation.

© Chris Cracknell 2024

CONFIDENTIAL COMPUTING

This is a technical measure that supports internal hardening of a system as well as widespread distribution (e.g. for Scaling, High Availability). From IEEE.org:

> *Confidential computing uses hardware-based techniques to isolate data, specific functions, or an entire application from the operating system, hypervisor or virtual machine manager, and other privileged processes. Data is stored in the trusted execution environment (TEE), where it's impossible to view the data or operations performed on it from outside, even with a debugger. The TEE ensures that only authorized code can access the data. If the code is altered or tampered with, the TEE denies the operation.*

- Additionally CC supports identifying system components through hardware-supported measurement of the TEE. Think of this as Hashes over the running software, OS, HW etc. which can be requested and checked by other components at runtime. These checks are called Attestation and can be used by one component to decide whether to trust another.
- Confidential Computing CANNOT tell you if the software is secure – it can only verify whether it is the software that you think it is and whether it is free from outside observation or interference.

SUMMARY
Then and Now:

OLD WORLD

- Focus on preventing attacks originating at the perimeter of the system. Invest in vulnerability tracking and Penetration Testing. Still VITAL!
- Internal actors, including Staff and other system components are assumed to be trusted – a bad actor inside the perimeter has full access to the system.

NEW WORLD

- Harden the internal structure of the system, so that the consequences of a breach are limited by safeguards between system components – "Zero (implicit) trust". Apply specific technical measures to do so, e.g. internal mTLS, Confidential Computing.
- Plan for and implement security at the heart of the project delivery process. Know what you are protecting, how you plan to do so and how you will know if you have done so. Make Governance effective and workable. Train everyone involved.
- Protect the project delivery processes, i.e. Software Supply Chain, Devops, Day 2+ Operations, SIEM, Staffing levels and Skillsets. Auditing, both internal and external.

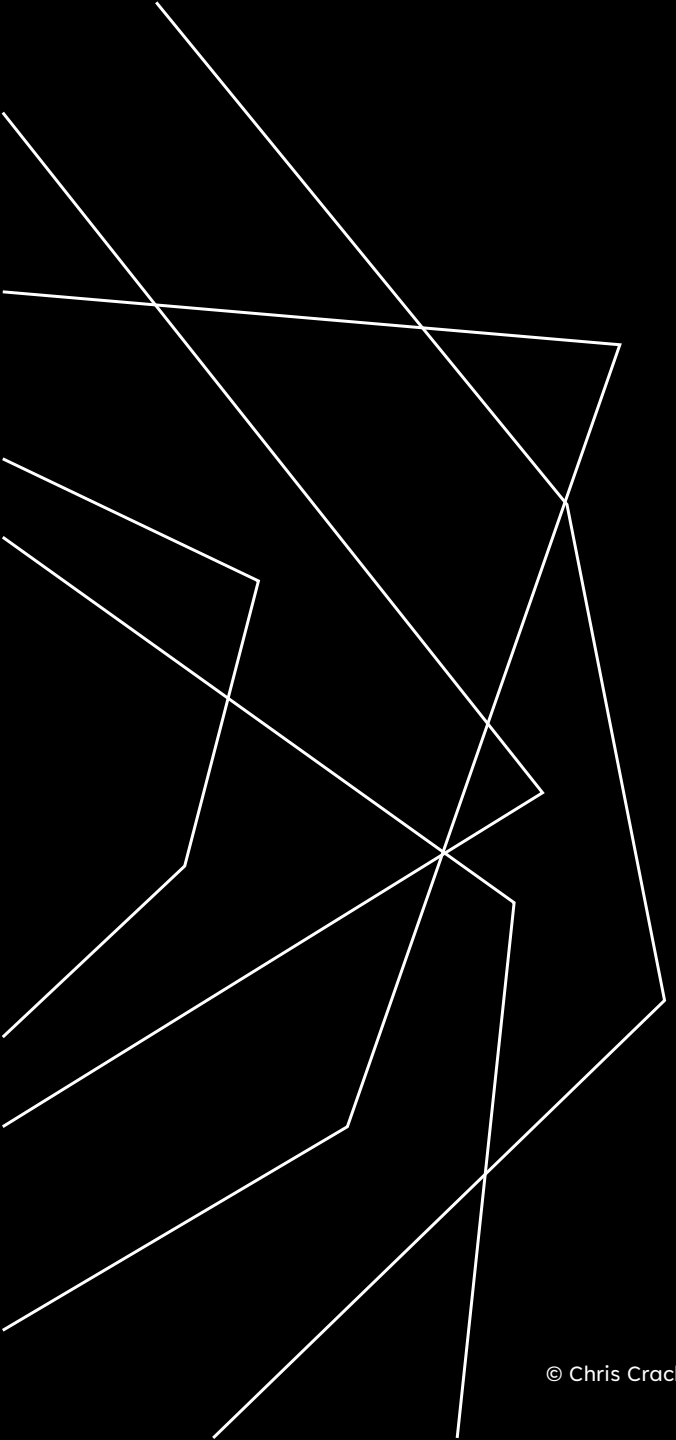
WHAT TO DO?

The follow up presentation :

- HSM Attest – Ecosystem Niche

describes how HSM Attest can support secure system delivery and how it relates to other tools and techniques in the ecosystem.

© Chris Cracknell 2024



THANK YOU

Chris Cracknell

+49 176 7087 7764

chris@cracknell.de

© Chris Cracknell 2024