

SECURING NEXT APPLICATION THROUGH SECURITY ARCHITECTURE

Htaik Htaik Thone

Assistant Vice President - Network Security Expert

04 Sep 2025

Thank You to Our Sponsors and Hosts!



OWASP
**NEW
ZEALAND**
owasp.org.nz



Waipapa
Taumata Rau
**University
of Auckland**



BASTION

SECURITY GROUP



**SECURE
CODE
WARRIOR**



plexure



Without them, this conference couldn't happen.

INTRODUCTION

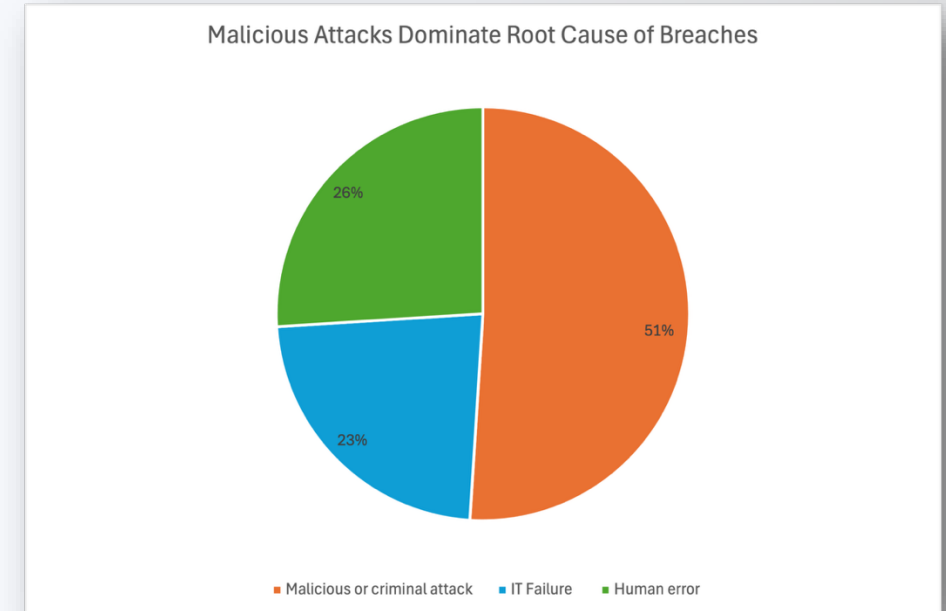
- IT Security professional with more than a decade of experience across different industries
- Network Security Expert at **Natixis Corporate & Investment Banking, Singapore Branch**
- Oversee **Network Security Perimeter for APAC region**
- Responsible for security review and network security architecture
- MBA | B.C.Sc (Hons:) | Specialist Dip. in Network Security
- CISSP | CCSP | CISM | CRISC | CEH

AGENDA

- WHY SECURITY ARCHITECTURE MATTERS?
- WHAT IS SECURITY ARCHITECTURE?
- DESIGNING THE NEXT APP
- APPLYING CORE PRINCIPLES
- THE GOOD, THE NOT-SO-GOOD
- CHALLENGES
- SECURITY AND BUSINESS BENEFITS
- REAL-WORLD INSIGHTS
- BEST PRACTICES
- KEY TAKEAWAYS

WHY SECURITY ARCHITECTURE MATTERS?

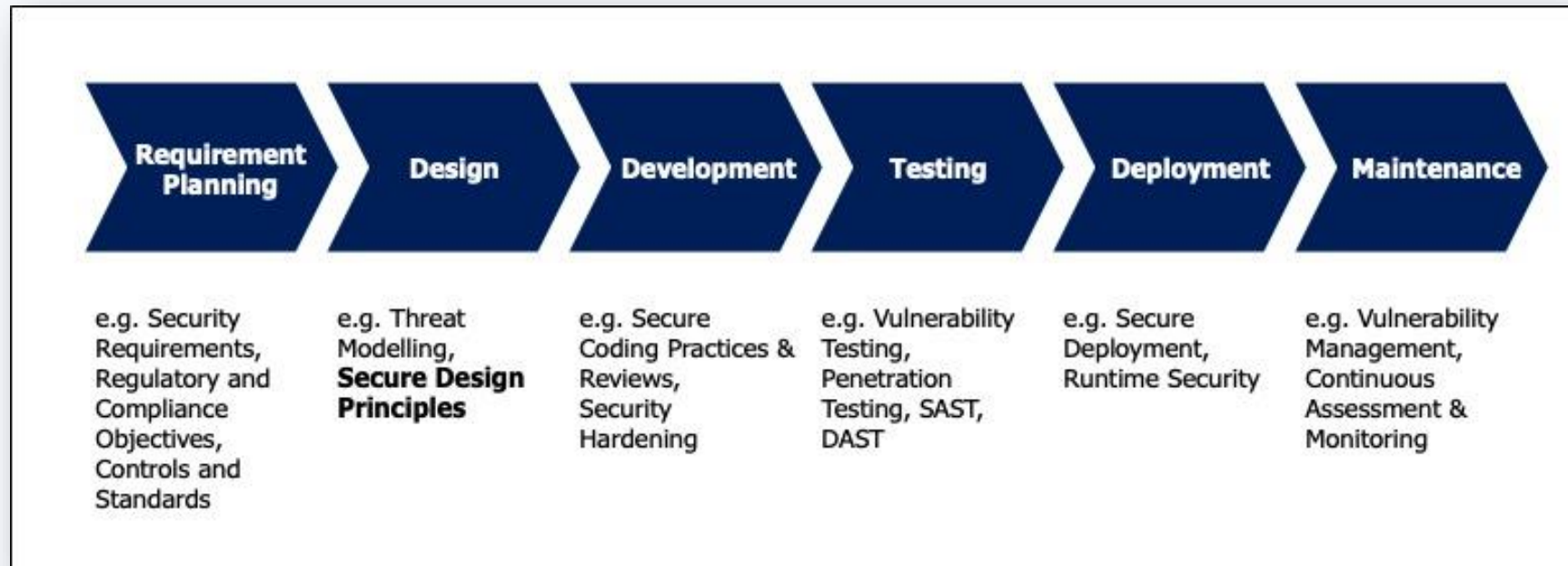
- Breaches cost millions and more (both \$\$\$ and reputation) due to weak designs.
- Fast-moving innovations in technology outpaces the security resources and capabilities i.e. AI, IoT, Cloud Computing.
- OWASP Top 10 issues continue to highlight fundamental architecture problems i.e. Broken access control, Injection, **Insure design**, Security Misconfiguration.



Source: Cost of a Data Breach Report 2025 by IBM:

<https://www.ibm.com/reports/data-breach>

WHAT IS SECURITY ARCHITECTURE?



Secure Software Development Lifecycle (SSDLC)

Security embedded into system structure



Goals:

- Reduce attack surface
- Enable compliance
- Build resiliency

DESIGNING THE NEXT APP

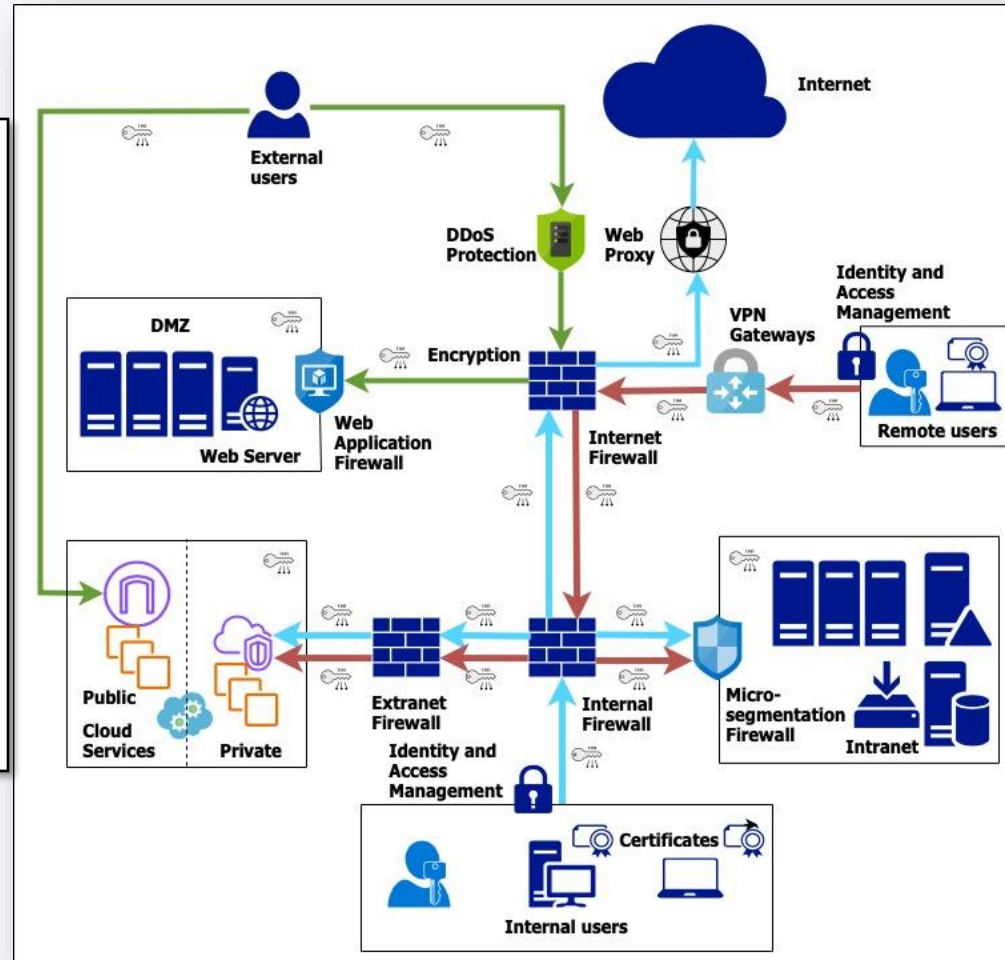
Core Principles:

- *Network Segmentation*
- *Zero Trust Architecture*
- Encryption
- Identity and Access (Least privilege, MFA)
- Microservices and API Security
- Cloud-Native Security
- DevSecOps (Automated CI/CD security testing (SAST, DAST, SCA))

APPLYING CORE PRINCIPLES (1/3)

Secure Architectural Principles

- Least privilege → restrict access.
- Defense in depth → multiple security layers.
- Fail-safe defaults → remain secure on failure.
- Separation of duties and segmentation.



Data Protection Design

- Data encryption (in transit, at rest).
- Secure storage and retention policies.
- Integrity checks and audit trails.

Authentication and Authorization

- Role/attribute-based access control (RBAC/ABAC).
- Strong MFA and secure sessions.
- Prevent authorization bypasses.

APPLYING CORE PRINCIPLES (2/3) *Cont.*

Zero Trust is a philosophy for designing network security architecture in a way that withholds access until a user, device or even an individual packet has been thoroughly inspected and authenticated and authorized.

Source: Cloud Security Alliance

- Authentication before access
- Capability to limit network connectivity and exposure
- Granular trust authentication mechanism
- Monitoring suspicious activity

APPLYING CORE PRINCIPLES (3/3) *Cont.*

SECURE DESIGN PATTERNS

VS

ANTI-PATTERNS

SECURE DESIGN PATTERNS



Input validation



Output encoding

ANTI-PATTERNS



Hardcoded secrets



Excessive trust in inputs





COMPLIANCE & REGULATORY



Meet GDPR,
PCI DSS

Design for
privacy, consent
and auditability

THE GOOD, THE NOT-SO-GOOD

	The good	The not-so-good
What we've got	<p>Proactive Risk Mitigation Reduced Attack Surface Enhanced Compliance Stronger Data Protection Robust Access Controls A Culture of Security</p>  <p>Strengths</p>	<p>Balancing Security with Usability Increased Development Costs and Time Legacy System Integration Resistance to Change Complex Compliance Overhead</p>  <p>Weakness</p>
What's out there	<p>Scalable and Maintainable Security Faster Incident Detection Greater System Resilience Market Differentiation Automation and AI in Security</p>  <p>Opportunities</p>	<p>Rapidly Evolving Threat Landscape Credential Theft and Insider Threats Regulatory Penalties Cloud and Supply Chain Risks Zero Trust Implementation Gaps</p>  <p>Threats</p>

CHALLENGES

Challenge	Description	Mitigation Approach
Balancing Security with Usability	Strong security can frustrate users and hurt productivity	<ul style="list-style-type: none">- Design security with users in mind- Use adaptive MFA only for high-risk cases- Test usability alongside security
Increased Development Costs and Time	Secure design adds complexity and slows delivery	<ul style="list-style-type: none">- Integrate DevSecOps with automation- Leverage existing security frameworks and libraries- Focus on highest risks first
Complexity of Regulatory Compliance	Overlapping, evolving standards (GDPR, PCI DSS, ISO, NIST)	<ul style="list-style-type: none">- Create clear compliance mapping- Automate logging, monitoring, reporting- Assign dedicated compliance roles
Legacy Systems and Integration Issues	Outdated systems lack modern security, complicating integrations	<ul style="list-style-type: none">- Segment and isolate legacy systems- Plan gradual modernization
Resistance to Cultural Change	Teams may push back on security-first approaches	<ul style="list-style-type: none">- Cultivate security culture through training- Appoint security champions within development teams- Highlight business value like brand protection and cost savings
Rapidly Evolving Threat Landscape	New threats constantly emerge, outpacing static security designs	<ul style="list-style-type: none">- Apply continuous threat intelligence and monitoring- Use agile security to adapt defenses quickly- Keep threat models and requirements up to date

SECURITY AND BUSINESS BENEFITS

Security Benefits	Business Benefits	Example
Proactive Risk Mitigation	Stops threats before they become crises	Catching vulnerabilities early prevents costly breaches
Reduced Attack Surface	Keeps operations running smoothly without surprises	Limiting access to what's essential protects critical systems
Enhanced Compliance	Avoids fines and builds customer trust	Designing for GDPR compliance keeps regulators and clients happy
Stronger Data Protection	Safeguards your reputation and competitive edge	Encrypting customer data protects your brand and customer loyalty
Greater System Resilience	Ensures your business stays up and running, no matter what	Layered defenses help avoid costly downtime
Lower Remediation Costs	Saves money by fixing issues before they explode	Automated testing cuts down expensive emergency patches
Robust Access Controls	Shields valuable assets and boosts stakeholder confidence	Multi-factor authentication reduces risks of account hacks
Faster Incident Detection	Limits damage with quick response times	Real-time alerts help nip breaches in the bud
Scalable & Maintainable Security	Supports growth with flexible, secure systems	Modular security lets you expand without adding risk
A Culture of Security	Turns security into everyone's responsibility, fueling innovation	DevSecOps builds proactive teams who own security

REAL-WORLD INSGIHTS

- Compliance challenges
- Network zoning for sensitive apps
- Lessons: Early design review saves millions (Scalability and Maintainability)

BEST PRACTICES

- Start with architecture reviews
- Exercise reviews when there are changes occur
- Document all the updates
- Record risk treatment and action items

KEY TAKEAWAYS

- Security by design is non-negotiable
- Every design choice = Security aware decision



Image Source: Cursor



Jewel World's Tallest Indoor Waterfall, *Image Source: Changi Airport Singapore*

LET'S CONNECT!



Htaik Htaik Thone

MBA, B.C.Sc (Hons:), CISSP, CCSP, CISM,
CRISC, CEH



